

# HP Switch Software

## Advanced Traffic Management Guide YA/YB.15.16

### Abstract

This switch software guide is intended for network administrators and support personnel and applies to the switch models listed on this page. This guide does not provide information about upgrading or replacing switch hardware.

### Applicable Products

HP Switch 2530 Series

(J9772A, J9773A, J9774A, J9775A, J9776A, J9777A, J9778A, J9779A, J9780A, J9781A, J9782A, J9783A, )



© Copyright 2014 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

#### **Acknowledgments**

Microsoft, Windows, Windows XP, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

Java and Oracle are registered trademarks of Oracle and/or its affiliates. UNIX is a registered trademark of The Open Group.

#### **Warranty**

For the software end user license agreement and the hardware limited warranty information for HP Networking products, visit [www.hp.com/networking/support](http://www.hp.com/networking/support).

---

# Contents

1 Static Virtual LANs (VLANs).....	10
Using VLANs.....	11
Static VLAN operation.....	11
VLAN environments.....	12
VLAN operation.....	13
General VLAN operation.....	13
Types of static VLANs available in the switch.....	13
Port-based VLANs.....	13
Protocol-based VLANs.....	13
Designated VLANs.....	13
The default VLAN.....	14
Multiple port-based VLANs.....	14
Protocol VLAN environment.....	15
Routing options for VLANs.....	15
Overlapping (Tagged) VLANs.....	15
Configuring VLANs.....	16
Port VLAN tagged status.....	17
Per-port static VLAN configuration options example.....	17
Configuring port-based and protocol-based VLAN parameters (CLI).....	17
Displaying a switch's VLAN configuration (CLI).....	18
Viewing the VLAN membership of one or more ports (CLI).....	19
Viewing the configuration for a particular VLAN (CLI).....	20
Customizing the show VLANs output (CLI).....	22
Creating an alias for show VLAN commands (CLI).....	24
Using pattern matching with the show VLANs custom command.....	24
Changing the number of VLANs allowed on the switch (CLI).....	24
Assigning the Primary VLAN (CLI).....	25
Adding or editing VLAN names (Menu).....	25
Changing VLAN support settings (Menu).....	27
Creating a new static VLAN (port-based or protocol-based) (CLI) .....	28
Deleting a static VLAN (CLI).....	29
Converting a dynamic VLAN to a static VLAN (CLI).....	30
Configuring static VLAN per-port settings (CLI).....	30
Using IP enable/disable for all VLANs.....	31
Interaction with other features.....	32
Interactions with DHCP.....	33
Adding or changing a VLAN port assignment (Menu).....	33
Deleting multiple VLANs.....	35
Correcting an unsupported configuration.....	35
The problem.....	35
The solution.....	36
Connecting an HP Switch to another with a multiple forwarding database (Example).....	37
Configuring a secure Management VLAN (CLI).....	37
Preparation.....	37
Configuring an existing VLAN as the Management VLAN (CLI).....	38
Obtaining an IP address using DHCP (CLI).....	39
Disabling the Management feature (CLI).....	42
Prioritizing voice VLAN QoS (CLI) (Optional).....	42
Configuring a VLAN MAC address with heartbeat interval (CLI).....	43
Displaying a VLAN MAC address configuration (CLI).....	43
Introducing tagged VLAN technology into networks running untagged VLANs.....	43

VLAN Operating Rules.....	44
Multiple VLAN considerations.....	48
Single forwarding database operation.....	49
802.1Q VLAN tagging.....	49
VLAN tagging considerations:.....	51
Special VLAN types.....	53
VLAN support and the default VLAN.....	53
The primary VLAN.....	53
The secure Management VLAN.....	54
Operating notes for Management VLANs.....	55
Voice VLANs.....	56
Operating rules for voice VLANs.....	56
Components of voice VLAN operation.....	57
Voice VLAN access security.....	57
Effects of VLANs on other switch features.....	57
Spanning Tree operation with VLANs.....	57
Spanning Tree operates differently in different devices.....	57
IP interfaces.....	57
VLAN MAC address.....	57
Port trunks.....	58
Port monitoring.....	58
Jumbo packet support.....	58
VLAN restrictions.....	58
Migrating Layer 3 VLANs using VLAN MAC configuration.....	58
VLAN MAC address reconfiguration.....	59
Handling incoming and outgoing VLAN Traffic.....	59
Incoming VLAN data packets and ARP requests.....	59
Outgoing VLAN traffic .....	59
Sending heartbeat packets with a configured MAC Address.....	59
<b>2 GVRP.....</b>	<b>61</b>
Using GVRP.....	61
Planning for GVRP operation.....	62
Displaying switch current GVRP configuration (CLI).....	62
Displaying switch current GVRP configuration (CLI).....	63
Viewing and configuring GVRP (Menu).....	64
Enabling and disabling GVRP on the switch (CLI).....	65
Controlling how individual ports handle advertisements for new VLANs (CLI).....	65
Listing static and dynamic VLANs on a GVRP-enabled switch (CLI).....	66
Converting a Dynamic VLAN to a Static VLAN (CLI).....	67
About GVRP.....	67
GVRP operational rules.....	68
Example of GVRP operation.....	68
Options for a GVRP-aware port receiving advertisements.....	69
Options for a port belonging to a Tagged or Untagged static VLAN.....	69
IP addressing.....	69
Per-port options for handling GVRP "unknown VLANs".....	69
Per-port options for dynamic VLAN advertising and joining.....	70
Initiating advertisements.....	70
Enabling a port for dynamic joins.....	70
Parameters for controlling VLAN propagation behavior.....	70
GVRP and VLAN access control.....	72
Advertisements and dynamic joins.....	72
Port-Leave from a dynamic VLAN.....	72

<b>3 Multimedia traffic control with IP multicast (IGMP).....</b>	<b>73</b>
Operation and features.....	73
IGMP devices .....	73
IGMP operating features.....	73
CLI: Configuring and displaying IGMP.....	74
Web: Enabling and disabling IGMP.....	77
How IGMP operates.....	77
Message types.....	77
IGMP multicasting.....	77
Displaying IGMP data.....	78
Supported standards and RFCs.....	78
Operation with or without IP addressing .....	78
Automatic Fast-Leave IGMP.....	79
Using delayed group flush .....	81
Forced Fast-Leave IGMP.....	81
Setting Fast-Leave and Forced Fast-Leave from the CLI.....	82
Setting Forced Fast-Leave using the MIB.....	82
Listing the MIB-Enabled Forced Fast-Leave configuration.....	82
Configuring per-port Forced Fast-Leave IGMP.....	83
Using the switch as querier.....	84
Querier operation.....	84
Excluding multicast addresses from IP multicast filtering .....	84
<b>4 Multiple instance spanning tree operation.....</b>	<b>86</b>
Planning an MSTP application.....	91
Configuring MSTP at a glance.....	91
Configuring MSTP operation mode and global settings.....	93
Selecting MSTP as the spanning tree mode.....	93
Clearing spanning tree debug counters.....	93
Resetting the configuration name of the MST region in which a switch resides.....	93
Designating the revision number of the MST region for a switch.....	93
Setting the spanning tree compatibility mode.....	94
Setting the time interval between listening, learning and forwarding states.....	94
Setting spanning tree to operate in 802. ID legacy mode.....	95
Setting spanning tree to operate with 802. ID legacy path cost values.....	95
Specifying the time interval between BPDU transmissions.....	95
Setting the hop limit for BPDUs.....	95
Setting the maximum age of received STP information.....	96
Manipulating the pending MSTP configuration.....	96
Setting the bridge priority for a region and determining the root switch.....	96
Enabling SNMP traps.....	97
Configuring MSTP per-port parameters.....	97
Enabling immediate transition to forwarding on end nodes.....	97
Identifying edge ports automatically.....	98
Specifying the interval between BPDU transmissions.....	98
Forcing a port to send RST/MST BPDUs.....	98
Determining which ports are forwarding ports by assigning port cost.....	98
Informing the switch of the device type to which a port connects .....	99
Determining which port to use for forwarding.....	99
Denying a port the role of root port.....	99
Denying a port propagation change information.....	100
Configuring BPDU filtering.....	100
Viewing BPDU filtering.....	101
Enabling and disabling BPDU protection.....	101
Viewing BPDU protection status.....	102

Configuring PVST.....	103
Enabling and disabling PVST protection on ports.....	103
Enabling and disabling PVST filters on ports.....	103
Re-enabling a port manually.....	103
Displaying ports configured with PVST protection and filtering.....	104
Listing ports to see which have PVST protection or filtering enabled.....	104
Configuring MST instances.....	104
Configuring MST instance parameters.....	104
Setting the bridge priority for an instance.....	105
Configuring MST instance per-port parameters.....	105
Assigning a port cost for an MST instance.....	105
Setting the priority for a port in a specified MST instance.....	106
Setting the priority for specified ports for the IST.....	106
Enabling or disabling spanning tree operation.....	107
Enabling an entire MST region at once or exchanging one region configuration for another...	107
Creating a pending MSTP configuration.....	108
MSTP topologies.....	109
Preconfiguring an MSTP regional topology.....	109
Preconfiguring VLANs in an MST instance.....	109
Configuring MSTP instances with the VLAN range option (Example).....	111
Saving the current configuration before a software upgrade.....	111
Displaying MSTP statistics.....	112
Displaying global MSTP status.....	112
Displaying detailed port information.....	113
Displaying status for a specific MST instance.....	114
Displaying the MSTP configuration.....	115
Displaying the global MSTP configuration.....	115
Displaying per-instance MSTP configurations.....	116
Displaying the region-level configuration.....	117
Displaying the pending MSTP configuration.....	118
Configuring loop protection.....	118
Enabling loop protection in port mode.....	119
Enabling loop protection in VLAN mode.....	120
Changing modes for loop protection.....	120
Displaying loop protection status .....	120
Displaying loop protection status in VLAN mode.....	120
STP loop guard.....	121
Troubleshooting an MSTP configuration.....	124
Displaying the change history of root bridges.....	125
Displaying debug counters for all MST instances.....	127
Displaying debug counters for one MST instance .....	128
Displaying debug counters for ports in an MST instance.....	129
Field descriptions in MSTP debug command output.....	131
Troubleshooting MSTP operation.....	133
About MSTP.....	133
Overview.....	133
MSTP structure.....	135
How MSTP operates.....	136
802.1s Multiple Spanning Tree Protocol (MSTP).....	136
MST regions.....	137
How separate instances affect MSTP.....	137
Regions, legacy STP and RSTP switches and the Common Spanning Tree (CST).....	139
MSTP operation with 802.1Q VLANs.....	139
Types of Multiple Spanning Tree Instances.....	139
Operating rules.....	140

Operating notes for the VLAN configuration enhancement.....	141
MSTP compatibility with RSTP or STP.....	142
PVST protection and filtering.....	142
PVST protection.....	143
PVST filtering.....	143
Loop protection.....	143
Operating notes.....	144
<b>5 Quality of Service: Managing bandwidth effectively.....</b>	<b>145</b>
Overview.....	147
Using QoS to classify and prioritize network traffic.....	147
Applying QoS to inbound traffic at the network edge.....	148
Preserving QoS in outbound traffic in a VLAN.....	148
Using QoS to optimize existing network resources.....	148
Using classifier-based QoS to provide additional policy actions and aid migration in networks with legacy and OEM devices.....	148
Configuring QoS globally.....	149
Viewing a global QoS configuration.....	150
Assigning an 802.1p priority for a global TCP/UDP classifier.....	150
Displaying a list of all TCP and UDP QoS classifiers.....	151
Assigning a DSCP policy for a global TCP/UDP classifier.....	151
Creating a DSCP policy based on TCP/UDP port number classifiers.....	151
Assigning DSCP policies to packets matching specified TCP and UDP port applications (Example).....	154
Displaying resource usage for QoS policies.....	155
Assigning a priority for a global IP-device classifier.....	156
Assigning a DSCP policy for a global IP-device classifier.....	158
Creating a policy based on IP address.....	158
Assigning DSCP policies to packets matching specified global classifiers.....	161
Assigning an 802.1p priority for a global IP-precedence classifier.....	162
Using a global IP-Diffserv classifier to mark matching packets with an 802.1p priority.....	163
Assigning a DSCP policy for a global IP-Diffserv classifier.....	164
Assigning a priority for a global layer 3 protocol classifier.....	167
Assigning a priority for a global VLAN-ID classifier.....	168
Assigning a DSCP policy for a global VLAN-ID classifier.....	169
Creating a policy based on the VLAN-ID classifier.....	170
Assigning a priority for a global source-port classifier.....	172
Assigning a DSCP policy for a global source-port classifier.....	173
Creating a policy based on source-port classifiers.....	173
Configuring classifier-based QoS.....	177
Configuring QoS actions in a policy.....	180
Reconfiguring the 802.1p priority value currently assigned to a DSCP codepoint.....	183
Viewing a classifier-based QoS configuration.....	184
Configuring a QoS policy for Voice over IP and Data traffic (Example).....	187
Configuring a QoS policy for layer 4 TCP/UDP traffic (Example).....	188
Configuring a QoS policy for subnet traffic (Example).....	188
Using Differentiated Services Codepoint (DSCP) mapping.....	188
Displaying non-default codepoint settings (Example).....	190
Default priority settings for selected codepoints.....	190
Changing the priority setting on a policy when classifiers are currently using the policy (Example)....	190
Configuring QoS queues.....	190
Viewing the QoS queue configuration.....	191
Using the outbound queue monitor.....	191
Displaying per-queue counts.....	192
About QoS.....	192

QoS operation.....	192
Globally-configured QoS.....	192
Classifier-based QoS.....	193
QoS packet classification.....	194
Using multiple global criteria.....	194
Classifier-based match criteria.....	194
QoS traffic marking.....	195
Globally-configured traffic marking.....	195
Layer 2 802.1p prioritization.....	195
Layer 3 DSCP marking.....	196
VLAN and untagged VLAN environments.....	197
Classifier-based traffic marking.....	197
No override.....	198
Global QoS restrictions.....	198
All switches.....	199
For devices that do not support 802.1Q VLAN-tagged ports.....	199
Port tagging rules.....	199
Maximum global QoS remarking entries.....	199
Not supported.....	199
Fragmented packets and TCP/UDP.....	200
Monitoring shared resources.....	200
Global QoS classifiers.....	200
Global TCP/UDP classifier.....	200
Global QoS classifier precedence: 1.....	200
Options for assigning priority.....	200
TCP/UDP port number ranges.....	200
Operating notes on using TCP/UDP port ranges.....	201
About global IP-device classifier.....	201
Global QoS classifier precedence: 2.....	201
Options for assigning priority.....	202
Global IP type-of-service classifier.....	202
Global QoS classifier precedence: 3.....	202
Global Layer-3 protocol classifier.....	203
Global QoS Classifier Precedence: 4.....	203
Global VLAN-ID classifier.....	203
Global QoS Classifier Precedence: 5.....	203
Options for assigning priority.....	203
Global source-port classifier.....	203
Global QoS Classifier Precedence: 6.....	203
Options for assigning priority on the switch.....	204
Options for assigning priority from a RADIUS server.....	204
Radius override field.....	204
IPv4 ToS/IPv6 traffic class byte.....	204
Comparing global IP type-of-service classifiers.....	206
Advanced classifier-based QoS.....	207
Classifier-based QoS model.....	207
Override of global QoS settings.....	208
Effect of No-override.....	209
Classifier-based QoS restrictions.....	209
Interaction with other software features.....	209
Notes on changing priority settings.....	210
Error messages for DSCP policy changes.....	210
QoS queue configuration.....	211
Mapping of outbound port queues.....	211
Impact of QoS queue configuration on guaranteed minimum bandwidth (GMB).....	212



Setting minimum guaranteed bandwidth with 8 queues.....	212
Assigning an 802.1p priority for a global IP-diffserv classifier.....	213
Assigning an 802.1p priority for a global IP-diffserv classifier.....	213
Viewing logging output.....	214
<b>6 BYOD-redirect.....</b>	<b>216</b>
Introduction.....	216
Features.....	216
SNMP Interactions.....	218
Interoperability with other switch features.....	218
Interoperability with other vendors.....	219
Restrictions.....	219
Configuring.....	219
Creating a BYOD server.....	219
Associating a BYOD server.....	219
Creating a BYOD ACL rule.....	220
Implementing BYOD-redirect configuration.....	221
Implementing BYOD-redirect configuration examples.....	221
Show commands.....	224
Show portal server.....	224
Show portal redirect statistics.....	225
Show portal free rule .....	225
Associating with the BYOD server on a specified VLAN.....	226
<b>7 Support and other resources.....</b>	<b>227</b>
Intended audience.....	227
Related documentation.....	227
Contacting HP.....	227
HP technical support.....	227
Subscription service.....	227
Related information.....	228
HP websites.....	228
Typographical conventions.....	228
HP customer support services.....	228
Before calling support.....	229
<b>Index.....</b>	<b>230</b>

# 1 Static Virtual LANs (VLANs)

Command Syntax	Description	Default	CLI reference page	Menu reference page
show vlans	Displays VLAN configuration		18	
show vlans <vid>				
show vlans ports <port-list>				
show vlan ports <port-list> [detail]	Displays VLAN memberships		19	
show vlans custom[port <port-list>] column-list	Customizes show vlan output		22	
max-vlans <1-2048>	Changes the number of VLANs allowed on a switch		24	
primary-vlan [ <vid>   <ascii-name-string> ]	Assigns the primary VLAN		25	
vlan [ <vid>   <ascii-name-string> ]	Creates a new static VLAN		28	
no vlan <vid>	Deletes a static VLAN		29	
static-vlan <vlan-id>	Converts a dynamic to a static VLAN		30	
[no] vlan <vid>	Configures static VLAN per-port settings		30	27
[no] management-vlan [ <vlan-id>   <vlan-name> ]	Makes an existing VLAN the management VLAN	Disabled	38	
vlan <vid> qos priority <0- 7>	Prioritizes Voice VLAN QoS	1 (normal)	42	
[no] ip-recv-mac-address <mac-address> [interval <seconds>]	Configures a VLAN MAC address with heartbeat interval	60 seconds	43	
show ip-recv-mac-address	Displays the VLAN MAC address configuration		43	

## Using VLANs

VLANs enable grouping users by logical function instead of physical location. They make managing bandwidth usage within networks possible by:

- Allowing grouping of high-bandwidth users on low-traffic segments
- Organizing users from different LAN segments according to their need for common resources and individual protocols
- Improving traffic control at the edge of networks by separating traffic of different protocol types.
- Enhancing network security by creating subnets to control in-band access to specific network resources.

This chapter describes static VLANs configured for port-based or protocol-based operation.

Static VLANs are configured with a name, VLAN ID number (VID) and port members. For dynamic VLANs, see [“GVRP” \(page 61\)](#). 802.1Q compatibility enables you to assign each switch port to multiple VLANs.

Some recommended steps to take for using VLANs:

1. Plan your VLAN strategy and create a map of the logical topology. Include consideration for the interaction between VLANs and other features such as Spanning Tree Protocol, port trunking and IGMP. See [“Effects of VLANs on other switch features” \(page 57\)](#). If you plan on using dynamic VLANs, include the port configuration planning necessary to support this feature, see [“GVRP” \(page 61\)](#).

By default, the switches covered in this guide are 802.1Q VLAN-enabled, allow for up to 256 static VLANs and 2048 total static and dynamic VLANs.

2. Configure at least one VLAN in addition to the default VLAN.
3. Assign the desired switch ports to the new VLANs.
4. If you are managing VLANs with SNMP in an IP network, the VLAN through which you are managing the switch must have an IP address. For information on the procedure and restrictions when you configure an IP address on a VLAN interface, see [Table 1 \(page 11\)](#).

## Static VLAN operation

A group of networked ports assigned to a VLAN form a broadcast domain configured on the switch. On a given switch, packets are bridged between source and destination ports that belong to the same VLAN. Thus, all ports passing traffic for a particular subnet address should be configured to the same VLAN. Cross-domain broadcast traffic in the switch is eliminated and bandwidth is saved by not allowing packets to flood out all ports.

**Table 1 Comparative operation of port based and protocol based VLANs**

Function	Port-Based VLANs	Protocol-Based VLANs
IP Addressing	<p>Usually configured with at least one unique IP address.</p> <p>A port-based VLAN can have no IP address. However, this limits the switch features available to ports on that VLAN, see "How IP Addressing Affects Switch Operation" in the chapter "Configuring IP Addressing" in the <i>Basic Operation Guide</i> for the switch.</p> <p>Multiple IP addresses allow multiple subnets within the same VLAN, see the chapter on "Configuring IP Addressing" in the <i>Basic Operation Guide</i> for the switch.</p>	<p>You can configure IP addresses on all protocol VLANs. However, IP addressing is used only on IPv4 and IPv6 VLANs.</p> <p><b>Restrictions:</b></p> <p>Loopback interfaces share the same IP address space with VLAN configurations.</p> <p>The maximum number of IP addresses supported on a switch is 2048, which includes all IP addresses configured for both VLANs and loopback interfaces (except for the default loopback IP address 127.0.0.1).</p> <p>Each IP address configured on a VLAN interface must be unique in the switch it cannot be used</p>

**Table 1 Comparative operation of port based and protocol based VLANs (continued)**

Function	Port-Based VLANs	Protocol-Based VLANs
		<p>by a VLAN interface or another loopback interface.</p> <p>For more information, see the chapter on "Configuring IP Addressing" in the <i>Basic Operation Guide</i>.</p>
Untagged VLAN Membership	A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged.	<p>A port can be an untagged member of one protocol VLAN of a specific protocol type, such as IPX or IPv6. If the same protocol type is configured in multiple protocol VLANs, then a port can be an untagged member of only one of those. For example, if you have two protocol VLANs, 100 and 200 and both include IPX, then a port can be an untagged member of either VLAN 100 or VLAN 200, but not both</p> <p>A port's untagged VLAN memberships can include up to four different protocol types. It can be an untagged member of one of the following:</p> <ul style="list-style-type: none"> <li>• Four single-protocol VLANs</li> <li>• Two protocol VLANs where one VLAN includes a single protocol and the other includes up to three protocols</li> <li>• One protocol VLAN where the VLAN includes four protocols</li> </ul>
Tagged VLAN Membership	A port can be a tagged member of any port-based VLAN (see above).	A port can be a tagged member of any protocol-based VLAN (see above).
Routing	<p>The switch can internally route IP (IPv4) traffic between port-based VLANs and between port-based and IPv4 protocol-based VLANs if the switch configuration enables IP routing.</p> <p>If the switch is not configured to route traffic internally between port-based VLANs, then an external router must be used to move traffic between VLANs.</p>	<p>If the switch configuration enables IP routing, the switch can internally route IPv4 traffic as follows:</p> <ul style="list-style-type: none"> <li>• Between multiple IPv4 protocol-based VLANs</li> <li>• Between IPv4 protocol-based VLANs and port-based VLANs.</li> </ul> <p>Other protocol-based VLANs require an external router for moving traffic between VLANs.</p> <p><b>NOTE:</b> NETbeui and SNA are non-routable protocols. End stations intended to receive traffic in these protocols must be attached to the same physical network.</p>
Commands for Configuring Static VLANs	<code>vlan &lt;vid&gt; [ tagged   untagged [ e   &lt;port-list&gt; ] ]</code>	<code>vlan &lt;vid&gt; protocol [ ipx   ipv4   ipv6   arp   appletalk   sna   netbeui ]</code> <code>vlan &lt;vid&gt; [ tagged   untagged [ e   &lt;port-list&gt; ] ]</code>

## VLAN environments

You can configure different VLAN types in any combination. The default VLAN will always be present. For more on the default VLAN, see ["VLAN support and the default VLAN" \(page 53\)](#).

VLAN environment	Elements
The default VLAN (port-based; VID of 1) only	In the default VLAN configuration, all ports belong to VLAN 1 as untagged members.

VLAN environment	Elements
	VLAN 1 is a port-based VLAN, for IPv4 traffic.
Multiple VLAN environment	<p>In addition to the default VLAN, the configuration can include one or more other port-based VLANs and one or more protocol VLANs.</p> <p>The switches covered in this guide allow up to 2048 (vids up to 4094) VLANs of all types.</p> <p>Using VLAN tagging, ports can belong to multiple VLANs of all types.</p> <p>Enabling routing on the switch enables it route IPv4 traffic between port-based VLANs and between port-based VLANs and IPv4 protocol VLANs. Routing other types of traffic between VLANs requires an external router capable of processing the appropriate protocols.</p>

## VLAN operation

### General VLAN operation

- A VLAN is composed of multiple ports operating as members of the same subnet or broadcast domain.
- Ports on multiple devices can belong to the same VLAN.
- Traffic moving between ports in the same VLAN is bridged (or switched).
- Traffic moving between different VLANs must be routed.
- A static VLAN is an 802.1Q-compliant VLAN, configured with one or more ports that remain members regardless of traffic usage.
- A dynamic VLAN is an 802.1Q-compliant VLAN membership that the switch temporarily creates on a port to provide a link to another port either in the same VLAN on another device.

### Types of static VLANs available in the switch

#### Port-based VLANs

This type of static VLAN creates a specific layer-2 broadcast domain comprised of member ports that bridge IPv4 traffic among themselves. Port-Based VLAN traffic is routable on the switches covered in this guide.

#### Protocol-based VLANs

This type of static VLAN creates a layer-3 broadcast domain for traffic of a particular protocol and is composed of member ports that bridge traffic of the specified protocol type among themselves. Some protocol types are routable on the switches covered in this guide; see [Table 1 \(page 11\)](#).

#### Designated VLANs

The switch uses these static, port-based VLAN types to separate switch management traffic from other network traffic. While these VLANs are not limited to management traffic, they provide improved security and availability.

##### Default VLAN

This port-based VLAN is always present in the switch and, in the default configuration, includes all ports as members. See [“VLAN support and the default VLAN” \(page 53\)](#).

##### Primary VLAN

The switch uses this port-based VLAN to run certain features and management functions, including DHCP/Bootp responses for switch management. In the default configuration, the Default VLAN is also the Primary VLAN. However, any port-based, non-default VLAN can be designated the Primary VLAN. See [“The primary VLAN” \(page 53\)](#).

## Secure Management VLAN

This optional, port-based VLAN establishes an isolated network for managing HP switches that support this feature. Access to this VLAN and to the switch's management functions are available only through ports configured as members. See [“The primary VLAN” \(page 53\)](#).

## Voice VLANs

This optional, port-based VLAN type enables separating, prioritizing and authenticating voice traffic moving through your network, avoiding the possibility of broadcast storms affecting VoIP (Voice-over-IP) operation. See [“Voice VLANs” \(page 56\)](#).

---

**NOTE:** In a multiple-VLAN environment that includes older switch models there may be problems related to the same MAC address appearing on different ports and VLANs on the same switch. In such cases the solution is to impose cabling and VLAN restrictions. For more on this topic, see [“Multiple VLAN considerations” \(page 48\)](#).

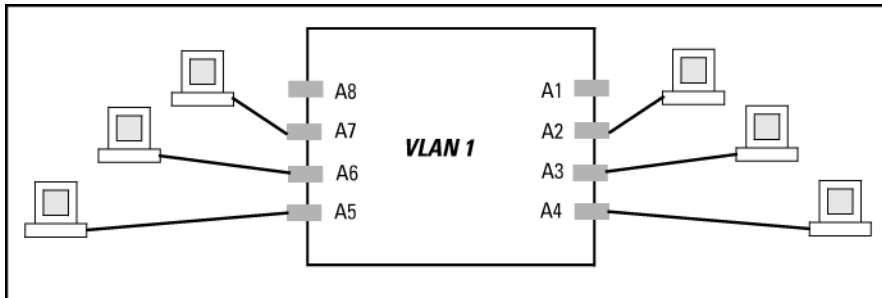
---

## The default VLAN

Except for an IP address and subnet, no configuration steps are needed.

### Example 1 A switch in the default VLAN configuration

In this example, devices connected to these ports are in the same broadcast domain.

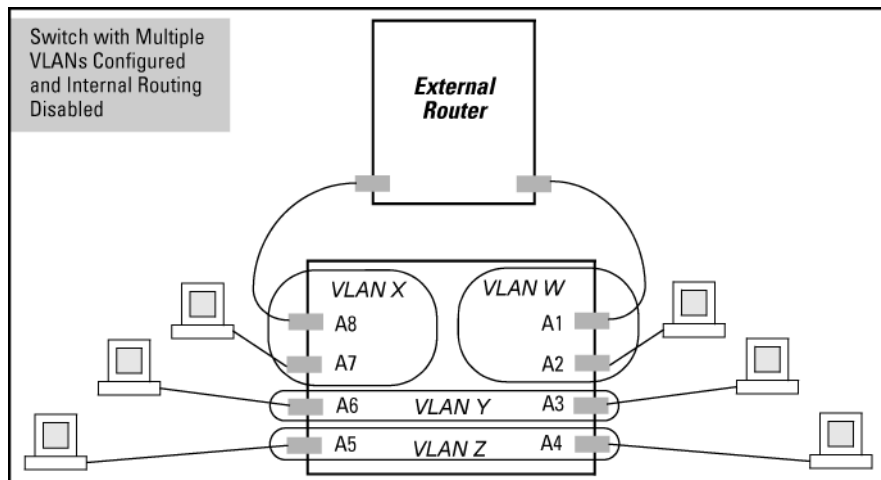


## Multiple port-based VLANs

In [Example 2 \(page 15\)](#), routing within the switch is disabled (the default). Thus communication between any routable VLANs on the switch must go through the external router. In this case, VLANs W and X can exchange traffic through the external router, but traffic in VLANs Y and Z is restricted to the respective VLANs.

Note that VLAN 1 (the default) is present but not shown. The default VLAN cannot be deleted from the switch, but ports assigned to other VLANs can be removed from the default VLAN. If internal (IP) routing is enabled on the switch, then the external router is not needed for traffic to move between port-based VLANs.

## Example 2 A switch with multiple VLANs configured and internal routing disabled



### Protocol VLAN environment

Example 2 (page 15) illustrates a protocol VLAN environment also. In this case, VLANs W and X represent routable protocol VLANs. VLANs Y and Z can be any protocol VLAN.

As noted for the discussion of multiple port-based VLANs, VLAN 1 is not shown. Enabling internal (IP) routing on the switch allows IP traffic to move between VLANs on the switch, but routable, non-IP traffic always requires an external router.

### Routing options for VLANs

Table 2 Options for routing between VLAN types in the switch

	Port-Based	IPX	IPv4	IPv6	ARP	AppleTalk	SNA <sup>1</sup>	NETbeui <sup>1</sup>
Port-Based	Yes	—	Yes	—	—	—	—	—
Protocol	IPX	—	Yes <sup>2</sup>	—	—	—	—	—
	IPX4	Yes	—	Yes	—	—	—	—
	IPV6	—	—	—	Yes <sup>2</sup>	—	—	—
	ARP	—	—	—	—	Yes <sup>2</sup>	—	—
	AppleTalk	—	—	—	—	—	Yes <sup>2</sup>	—
	SNA	—	—	—	—	—	—	—
	NETbeui	—	—	—	—	—	—	—

<sup>1</sup> Not a routable protocol type. End stations intended to receive traffic in these protocols must be attached to the same physical network.

<sup>2</sup> Requires an external router to route between VLANs.

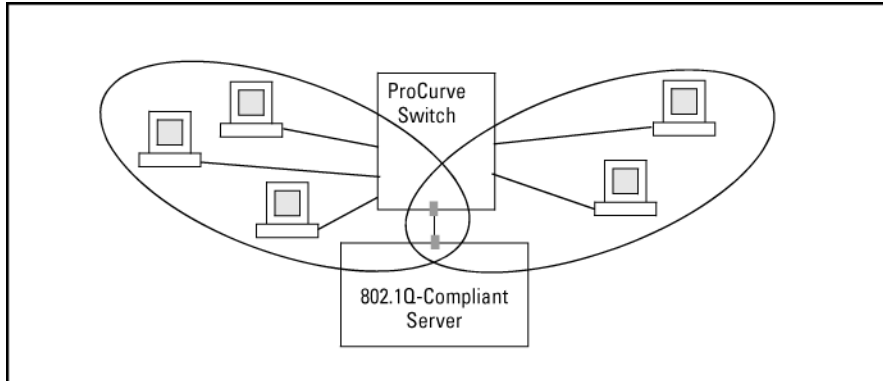
### Overlapping (Tagged) VLANs

A port can be a member of more than one VLAN of the same type if the device to which the port connects complies with the 802.1Q VLAN standard.

For example, a port connected to a central server using a network interface card (NIC) that complies with the 802.1Q standard can be a member of multiple VLANs, allowing members of multiple VLANs to use the server.

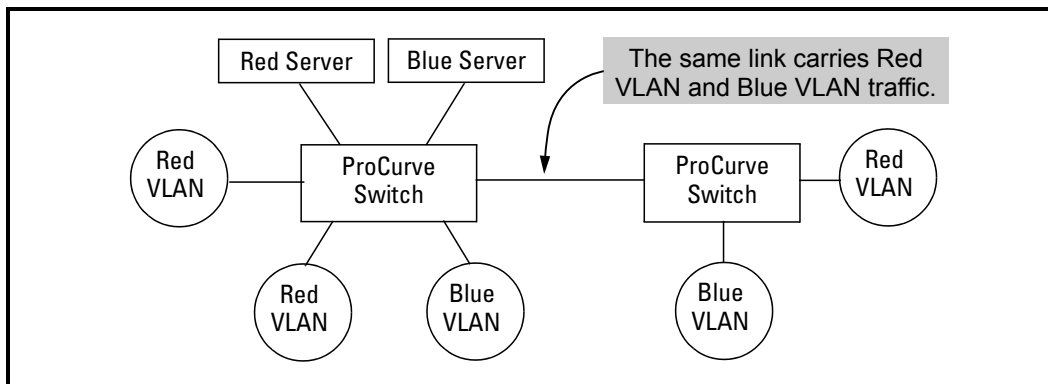
- Although these VLANs cannot communicate with each other through the server, they can all access the server over the same connection from the switch.
- Where VLANs overlap in this way, VLAN "tags" are used in the individual packets to distinguish between traffic from different VLANs.
- A VLAN tag includes the particular VLAN I.D. (VID) of the VLAN on which the packet was generated.

### Example 3 Overlapping VLANs using the same server



Similarly, using 802.1Q-compliant switches, you can connect multiple VLANs through a single switch-to-switch link.

### Example 4 Connecting multiple VLANs through the same link



## Configuring VLANs

The **Menu** interface enables configuration and display of port-based VLANs only. The CLI configures and displays port-based and protocol-based VLANs.

In the factory default state, the switch is enabled for up to 16 VLANs, all ports belong to the default primary VLAN and are in the same broadcast/multicast domain. You can reconfigure the switch to support up to 512 VLANs.



## Port VLAN tagged status

Port VLAN tagged status enables identification of ports as access, trunk, or voice. Use `show interfaces status` to display tagged and untagged VLAN information for a port.

## Per-port static VLAN configuration options example

This example shows the options available to assign individual ports to a static VLAN. Note that GVRP, if configured, affects these options and the VLAN behavior on the switch.

**Figure 1 Comparing per-port VLAN options with and without GVRP**

Example of Per-Port VLAN Configuration with GVRP Disabled (the default)			Example of Per-Port VLAN Configuration with GVRP Enabled		
Port	DEFAULT_VLAN	VLAN-22	Port	DEFAULT_VLAN	VLAN-22
A1	Untagged	Forbid	A1	Untagged	Forbid
A2	No	Tagged	A2	Auto	Tagged
A3	No	Tagged	A3	Auto	Tagged
A4	Forbid	Tagged	A4	Forbid	Tagged
A5	Untagged	No	A5	Untagged	Auto

Enabling GVRP causes "No" to display as "Auto".

**Table 3 Per-port VLAN configuration options**

Parameter	Effect on port participation in designated VLAN
Tagged	Allows the port to join multiple VLANs.
Untagged	<ul style="list-style-type: none"> <li>Allows VLAN connection to a device that is configured for an untagged VLAN instead of a tagged VLAN.</li> <li>A port can be an untagged member of only one port-based VLAN.</li> <li>A port can be an untagged member of only one protocol-based VLAN for any given protocol type.</li> </ul> <p>For example, if the switch is configured with the default VLAN plus three protocol-based VLANs that include IPX, then port 1 can be an untagged member of the default VLAN and one of the protocol-based VLANs.</p>
No or Auto	<p>No:</p> <p>When the switch is not GVRP-enabled; prevents the port from joining that VLAN.</p> <p>Auto: When GVRP is enabled on the switch; allows the port to dynamically join any advertised VLAN that has the same VID.</p>
Forbid	Prevents the port from joining the VLAN, even if GVRP is enabled on the switch.

## Configuring port-based and protocol-based VLAN parameters (CLI)

In the factory default state, all ports on the switch belong to the port-based default VLAN (DEFAULT\_VLAN; VID=1) and are in the same broadcast/multicast domain.

The default VLAN is also the Primary VLAN. You can configure up to 255 additional static VLANs by adding new VLAN names and then assigning one or more ports to each VLAN.

The switch accepts a maximum of 2048 VLANs with VIDs numbered up to 4094. This must include the default VLAN and any dynamic VLANs the switch creates if you enable GVRP.

**NOTE:** Each port can be assigned to multiple VLANs by using VLAN tagging. See "802.1Q VLAN tagging" (page 49).

## Displaying a switch's VLAN configuration (CLI)

The `show vlans` command lists the VLANs currently running in the switch, with VID, VLAN name and VLAN status. Dynamic VLANs appear only if the switch is running with GVRP enabled and one or more ports has dynamically joined an advertised VLAN. In the default configuration, GVRP is disabled.

### Syntax:

`show vlans`

Primary VLAN	See <a href="#">“The primary VLAN” (page 53)</a> .
Management VLAN	See <a href="#">“The secure Management VLAN” (page 54)</a> .
802.1Q VLAN ID	The VLAN identification number, or VID.
Name	The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of <code>VLAN-x</code> where <code>x</code> matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of <code>GVRP_x</code> where <code>x</code> matches the applicable VID.
Status	Port-Based      Port-Based, static VLAN Protocol        Protocol-Based, static VLAN Dynamic         Port-Based, temporary VLAN learned through GVRP Voice            Indicates whether a port-based VLAN is configured as a voice VLAN. See <a href="#">“Voice VLANs” (page 56)</a> . Jumbo            Indicates whether a VLAN is configured for Jumbo packets. For more on jumbos, see "Port Traffic Controls" in the <i>Management and Configuration Guide</i> for your switch.

## Example 5 Displaying VLAN listing with GVRP enabled

This example shows the listing from the `show vlans` command. When GVRP is disabled (the default), Dynamic VLANs do not exist on the switch and do not appear in this listing. For more information, see [“GVRP” \(page 61\)](#).

```
HP Switch#: show vlans
```

```
Status and Counters - VLAN Information
```

```
Maximum VLANs to support : 256  
Primary VLAN : DEFAULT_VLAN  
Management VLAN :
```

VLAN ID	Name	Status	Voice	Jumbo
1	DEFAULT_VLAN	Port-based	No	No
10	VLAN_10	Port-based	Yes	Yes
15	VLAN_15	Port-based	No	No
20	VLAN_20	Protocol	No	No
33	VLAN_33	Dynamic	No	No

## Viewing the VLAN membership of one or more ports (CLI)

### Syntax:

```
show vlan ports <port-list> [detail]
```

Displays VLAN information for an individual port or a group of ports, either cumulatively or on a detailed per-port basis.

`port-list` Specifies a single port number or a range of ports (for example, `a1-a16`), or `all` for which to display information.

`detail` Displays detailed VLAN membership information on a per-port basis.

Descriptions of items displayed by the command are:

**Port name** The user-specified port name, if one has been assigned.

**VLAN ID** The VLAN identification number, or VID.

**Name** The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of `VLAN-x` where `x` matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of `GVRP_x` where `x` matches the applicable VID.

**Status**

Port-Based	Port-Based, static VLAN.
Protocol	Protocol-Based, static VLAN.
Dynamic	Port-Based, temporary VLAN learned through GVRP.

**Voice** Indicates whether a port-based VLAN is configured as a voice VLAN.

**Jumbo** Indicates whether a VLAN is configured for jumbo packets. For more on jumbos, see "Port Traffic Controls" in the *Management and Configuration Guide* for your switch.

**Mode** Indicates whether a VLAN is tagged or untagged.

## Example 6 Displaying VLAN ports (cumulative listing)

```
HP Switch(config)#:show vlan ports a1-a24
```

```
Status and Counters - VLAN Information - for ports A1-A24
```

VLAN ID	Name	Status	Voice	Jumbo
1	DEFAULT_VLAN	Port-based	No	No
10	VLAN_10	Port-based	Yes	No
15	VLAN_15	Protocol	No	No

## Example 7 Displaying VLAN ports (detailed listing)

```
HP Switch(config)#:show vlan ports a1-a3 detail
```

```
Status and Counters - VLAN Information - for ports A1
```

VLAN ID	Name	Status	Voice	Jumbo	Mode
1	DEFAULT_VLAN	Port-based	No	No	Untagged
10	VLAN_10	Port-based	Yes	No	Tagged

```
Status and Counters - VLAN Information - for ports A2
```

VLAN ID	Name	Status	Voice	Jumbo	Mode
1	DEFAULT_VLAN	Port-based	No	No	Untagged
20	VLAN_20	Protocol	No	No	Untagged

```
Status and Counters - VLAN Information - for ports A3
```

VLAN ID	Name	Status	Voice	Jumbo	Mode
1	DEFAULT_VLAN	Port-based	No	No	Untagged
33	VLAN_33	Port-based	No	No	Tagged

## Viewing the configuration for a particular VLAN (CLI)

### Syntax:

```
show vlans <vlan-id>
```

Uses the VID to identify and display the data for a specific static or dynamic VLAN.

**802.1Q VLAN ID** The VLAN identification number, or VID.

**Name** The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of `VLAN-x` where `x` matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of `GVRP_x` where `x` matches the applicable VID.

**Status**

Port-Based	Port-Based, static VLAN.
Protocol	Protocol-Based, static VLAN
Dynamic	Port-Based, temporary VLAN learned through GVRP. See <a href="#">"GVRP" (page 61)</a> .

**Voice** Indicates whether a port-based VLAN is configured as a voice VLAN. See ["Voice VLANs" \(page 56\)](#).

Jumbo	Indicates whether a VLAN is configured for Jumbo packets. For more on jumbos, see "Port Traffic Controls" in the <i>Management and Configuration Guide</i> for your switch.
Port Information	Lists the ports configured as members of the VLAN.
DEFAULT	Shows whether a port is a tagged or untagged member of the listed VLAN.
Unknown VLAN	Shows whether the port can become a dynamic member of an unknown VLAN for which it receives an advertisement. GVRP must be enabled to allow dynamic joining to occur.
Status	Shows whether the port is participating in an active link.

## Example 8 Displaying information for a specific static VLAN

---

```
HP Switch(config)#:show vlans 22

Status and Counters - VLAN Information - VLAN 22

VLAN ID : 22
Name : VLAN22
Status : Port-based
Voice : Yes
Jumbo : No

Port Information Mode      Unknown VLAN Status
-----
12          Untagged Learn      Up
13          Untagged Learn      Up
14          Untagged Learn      Up
15          Untagged Learn      Down
16          Untagged Learn      Up
17          Untagged Learn      Up
18          Untagged Learn      Up
```

---

## Example 9 Displaying information for a specific dynamic VLAN

---

The following example shows the information displayed for a specific dynamic VLAN. The `show vlans` command lists this data when GVRP is enabled and at least one port on the switch has dynamically joined the designated VLAN.

```
HP Switch(config)#: show vlans 22

Status and Counters - VLAN Information - VLAN 22

VLAN ID : 33
Name : GVRP_33
Status : Dynamic
Voice : No
Jumbo : No

Port Information Mode      Unknown VLAN Status
-----
6          Auto      Learn      Up
```

---

## Customizing the show VLANs output (CLI)

### Syntax

```
show vlans custom [port <port-list>] <column-list>
```

Specifies the order you want information to display for the `show vlans` command.  
Displays information for one port or a range of ports. If `<port-list>` is not specified, all ports display.

Fields that can be included in the customized display:

Field	Display	Example	Default width
id	VLAN id	5	6
name	VLAN name	Vlan55	32
status	Status	Port-based	10
voice	Voice enabled	No	5
jumbo	Jumbos enabled	No	5
ipconfig	How the IP address was configured	Manual Disabled DHCP/BootP	10
ipaddr (IPv4) ipaddr (IPv6)	The IP addresses	10.10.10.3 fe80::212:79ff:fe8d:8000	15 for IPv4 46 for IPv6
ipmask	The subnet masks	255.255.255.6 /64 (prefix for IPv6 is in format "/XX")	15
proxyarp	Whether proxy ARP is configured	No	5
localproxyarp	Whether local proxy ARP is configured	No	9
state	"Up" if at least one port is up	Up	5

### Example 10 Customizing the VLAN display

The following example displays `id` at its default width and `name:20` allows up to 20 characters of the VLAN `name` to be displayed. The columns selected for display are separated by spaces. If the width of the column requested is smaller than the header name of the column, the display of the header name is truncated.

```
HP Switch(config)#: show vlan custom A1-A3 id name:20 ipaddr state
```

```
Status and Counters - VLAN Information - Custom view
```

```
VLANID  VLAN name                IP Addr                                State
-----  -
1        DEFAULT_VLAN                  15.255.134.74                          Up
33       Vlan33                        10.10.10.01                             Up
44       Vlan44                        15.255.164.13                          Up
55       Vlan55                        15.255.178.2                            Down
                               15.255.178.3
                               15.255.178.4
60       Vlan60                        fe80::212:79ff:fe8d:8000%vlan60       Up
```

---

## Example 11 Wrapping column headers

---

The total output wraps if it is longer than the terminal width; it is not truncated.

```
HP Switch(config)#: show vlan custom id
Status and Counters - VLAN Information - Custom view
```

```
VLANID
-----
1
33
44
```

```
HP Switch(config)#: show vlan custom id:2
Status and Counters - VLAN Information - Custom view
```

```
VL
--
1
33
44
```

---

## Creating an alias for show VLAN commands (CLI)

Create an alias for a frequently used `show vlans custom` command to avoid entering the selected columns each time you use the command.

### Example 12 Using a VLAN alias

---

```
HP Switch(config)#: alias showvlanstatus = "show vlan custom A1-A3 id name:20 status"
```

```
HP Switch(config)#: show vlan status
Status and Counters - VLAN Information - Custom view
```

VLANID	VLAN name	Status
1	DEFAULT_VLAN	Port-based
33	Vlan33	Port-based

---

## Using pattern matching with the show VLANs custom command

If a pattern matching command is in a search for a field in the output of the `show vlan custom` command and it produces an error, the error message may not be visible. For example, if you enter a command with the pattern matching `include` option that contains an error (such as 'vlan' is misspelled) as in the following example, the output may be empty:

```
HP Switch(config)#: show vlans custom 1-3 name vlun include vlan1
```

HP recommends that you try the `show vlans custom` command first to ensure there is output and then enter the command again with the pattern matching option.

## Changing the number of VLANs allowed on the switch (CLI)

### Syntax:

The default VLAN number is 1.

```
max-vlans<1-512>
```

Default number of VLANs: 16



If GVRP is enabled, this setting includes any dynamic VLANs on the switch. As part of implementing a new setting, you must execute a `write memory` command to save the new value to the startup-config file and then reboot the switch.

---

**NOTE:** If multiple VLANs exist on the switch, you cannot reset the maximum number of VLANs to a value smaller than the current number of VLANs.

---

### Example 13 Changing the number of allowed VLANs

---

The following example shows the command sequence for changing the number of VLANs allowed to 10. Note that you can execute the commands to `write memory` and `boot` at another time.

```
HP Switch(config)#: max-vlans 10
This command will take effect after saving the configuration
and rebooting the system.
HP Switch(config)#: write memory
HP Switch(config)#: boot
Device will be rebooted, do you want to continue [y/n]? Y
```

---

## Assigning the Primary VLAN (CLI)

### Syntax:

```
primary-vlan vid | <ascii-name-string>
```

In the default VLAN configuration, the port-based default VLAN (DEFAULT\_VLAN) is the Primary VLAN. This command allows reassignment of the Primary VLAN function to an existing, port-based, static VLAN.

The switch will not reassign the Primary VLAN function to a protocol VLAN.

---

**NOTE:** If you reassign the Primary VLAN to a non-default VLAN, you cannot later delete that VLAN from the switch until you assign the Primary VLAN to another port-based, static VLAN.

---

To identify the current Primary VLAN and list the available VLANs and their respective VIDs, use `show vlans`.

### Example 14 Re-assigning, renaming and displaying the VLAN command sequence

---

The following example shows how to re-assign the Primary VLAN to VLAN 22 (first command line), rename the VLAN **22-Primary** (second command line) and then display the result (third command line):

```
HP Switch(config)#: primary-vlan 22
HP Switch(config)#: vlan 22 name 22-Primary
HP Switch(config)#: show vlans
```

```
Status and Counters - VLAN Information
Maximum VLANs to support : 8
Primary VLAN : 22-Primary
Management VLAN :
```

VLAN ID	Name	Status	Voice	Jumbo
1	DEFAULT_VLAN	Static	No	No
22	22-Primary	Static	No	No

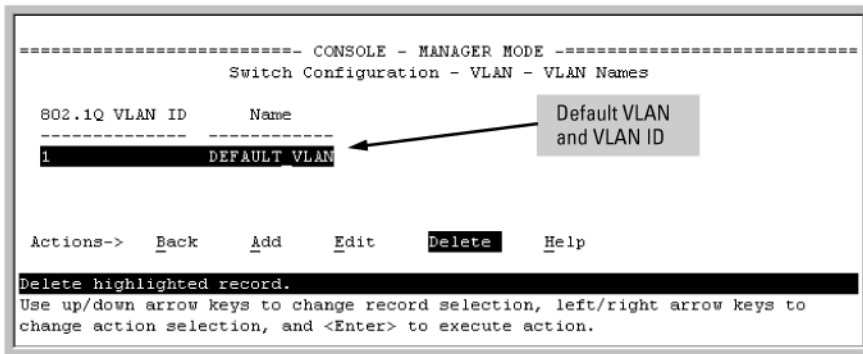
---

## Adding or editing VLAN names (Menu)

Use this procedure to add a new VLAN or to edit the name of an existing VLAN.

1. From the Main Menu select **2. Switch Configuration** —> **8. VLAN Menu ...** —> **2. VLAN Names**. If multiple VLANs are not yet configured, you will see a screen similar to [Figure 2 \(page 26\)](#).

**Figure 2 The default VLAN names screen**



2. Press **A** (for Add).

You will be prompted for a new VLAN name and VLAN ID:

**802.1Q VLAN ID :**  
**1 Name : \_**

3. Type a VID (VLAN ID number). This can be any number from 2 to 4094 that is not already being used by another VLAN (the switch reserves 1 for the default VLAN).

---

**NOTE:** A VLAN must have the same VID in every switch in which you configure that same VLAN. GVRP dynamically extends VLANs with correct VID numbering to other switches; see “GVRP” (page 61) .

---

4. Press **↓** key to move the cursor to the **Name** line and enter the VLAN name, using up to 12 characters with no spaces. Press **Enter**.

---

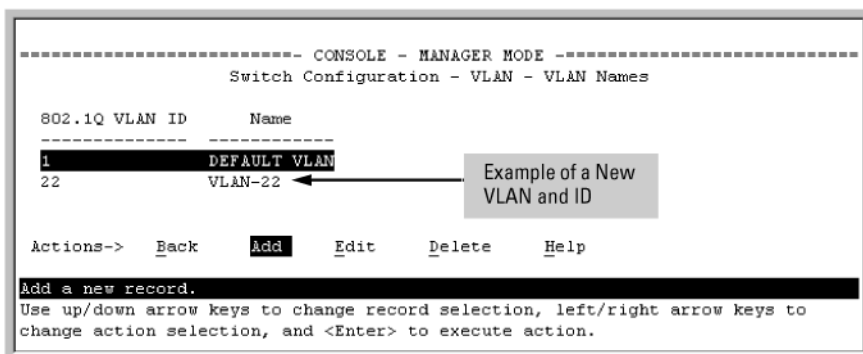
**NOTE:** Do not use the following characters in VLAN names: @, #, \$, ^, &, \*, ( and ).

---

5. Press **S** (for Save).

The VLAN Names screen appears with the new VLAN listed.

**Figure 3 VLAN Names screen with a new VLAN added**



6. Repeat steps 2 through 5 to add more VLANs.

You can add VLANs until you reach the number specified in the **Maximum VLANs to support** field on the VLAN Support screen. This includes any VLANs added dynamically due to GVRP operation.

Return to the VLAN Menu to assign ports to the new VLAN, as described in “[Adding or changing a VLAN port assignment \(Menu\)](#)” (page 33).

## Changing VLAN support settings (Menu)

The following procedure provides instructions for changing the maximum number of VLANs to support, changing the primary VLAN selection and enabling or disabling dynamic VLANs.

1. From the Main Menu select: **2. Switch Configuration** → **8. VLAN Menu ...** → **1. VLAN Support**

You see the following screen:

**Figure 4 The default VLAN support screen**

```
----- CONSOLE - MANAGER MODE -----
                Switch Configuration - VLAN - VLAN Support

Maximum VLANs to support [8] : 8
Primary VLAN : DEFAULT_VLAN
GVRP Enabled [No] : No

Actions->  Cancel   Edit   Save   Help

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

2. Press **E** (for Edit) and then do one or more of the following:
  - To designate a different VLAN as the Primary VLAN, select the **Primary VLAN** field and use the space bar to select from the existing options. The Primary VLAN must be a static, port-based VLAN.
  - To enable or disable dynamic VLANs, select the **GVRP Enabled** field and use the Space bar to toggle between options. For GVRP information, see “GVRP” (page 61).

**NOTE:** For optimal switch memory utilization, set the number of VLANs at the number you will likely be using or a few more. If you need more VLANs later, you can increase this number, but a switch reboot will be required at that time.

3. Press **Enter** and then **S** to save the VLAN support configuration and return to the VLAN Menu screen.

If you changed the value for Maximum **VLANs to support**, an asterisk appears next to the **VLAN Support** option; see [Figure 5 \(page 27\)](#).

**Figure 5 VLAN menu screen indicating the need to reboot the switch**

```
----- CONSOLE - MANAGER MODE -----
                Switch Configuration - VLAN Menu

*1. VLAN Support
  2. VLAN Names
  3. VLAN Port Assignment
  4. Return to Previous Menu...
  0. Return to Main Menu...

Displays the menu to activate and configure, or deactivate VLAN support.
To select menu item, press item number, or highlight item and press <Enter>.
(*Needs reboot to activate changes.)
```

An asterisk indicates you must reboot the switch to implement the new Maximum VLANs setting.

- If you changed the VLAN Support option, you must reboot the switch before the maximum VLANs change takes effect. You can go on to configure other VLAN parameters first, but you must reboot the switch when you finish.
- If you did not change the VLAN Support option, a reboot is not necessary.

4. Press **0** to return to the Main Menu.

## Creating a new static VLAN (port-based or protocol-based) (CLI)

The `vlan <vid>` command operates in the global configuration context to configure a static VLAN and/or take the CLI to a specified VLAN's context.

### Syntax:

```
vlan vid | <ascii-name-string>
```

```
[no] vlan <vid>
```

If `<vid>` does not exist in the switch, this command creates a port-based VLAN with the specified `<vid>`

If the command does not include options, the CLI, moves to the newly created VLAN context.

If an optional name is not specified, the switch assigns a name in the default format `VLAN n`, where `n` is the `<vid>` assigned to the VLAN.

If the VLAN already exists and you enter either the `<vid>` or the `<ascii-name-string>`, the CLI moves to the specified VLAN's context.

The `no` form of the command deletes the VLAN as follows:

If one or more ports belong only to the VLAN to be deleted, the CLI notifies you that these ports will be moved to the default VLAN and prompts you to continue the deletion. For member ports that also belong to another VLAN, there is no **move** prompt.

```
protocol [ ipx|ipv4|ipv6|arp|appletalk|sna|netbeui ]
```

Configures a static, protocol VLAN of the specified type.

If multiple protocols are configured in the VLAN, the `no` form removes the specified protocol

If a protocol VLAN is configured with only one protocol type and you use the `no` form of this command to remove that protocol, the switch changes the protocol VLAN to a port-based VLAN (if the VLAN does not have an untagged member port).

If an untagged member port exists on the protocol VLAN, you must either convert the port to a tagged member or remove the port from the VLAN before removing the last protocol type from the VLAN.

---

**NOTE:** If you create an IPv4 protocol VLAN, you must assign the ARP protocol option to it to provide IP address resolution. Otherwise, IP packets are not deliverable. A Caution message appears in the CLI if you configure IPv4 in a protocol VLAN that does not already include the ARP protocol option. The same message appears if you add or delete another protocol in the same VLAN.

---

```
name <ascii-name-string>
```

When included in a `vlan` command to create a new static VLAN, this command specifies a non-default VLAN name. Also used to change the current name of an existing VLAN.

---

**NOTE:** Avoid spaces and the following characters in the `<ascii-name-string>` entry: @, #, \$, ^, &, \*, ( and ). To include a blank space in a VLAN name, enclose the name in single or double quotes.

---

```
voice
```

Designates a VLAN for VoIP use. For more on this topic, see [“Voice VLANs” \(page 56\)](#).

**NOTE:** You can use these options from the configuration level by beginning the command with `vlan <vid>`, or from the context level of the specific VLAN by just entering the command option.

---

### Example 15 Creating a new port-based static VLAN

---

The following example shows how to create a new port-based, static VLAN with a VID of 100 using the following steps:

1. To create the new VLAN, type the `vlan 100` command.
2. To show the VLANs currently configured in the switch, type the `show vlans` command.

If the Management VLAN field (Primary VLAN : DEFAULT\_VLAN Management VLAN shown in the display information below) is empty, a Secure Management VLAN is not configured in the switch. For more information on configuring a secure management VLAN, see [“The secure Management VLAN” \(page 54\)](#).

```
HP Switch(config)#: vlan 100
HP Switch(config)#: show vlans
```

```
Status and Counters - VLAN Information
Maximum VLANs to support : 8
Primary VLAN : DEFAULT_VLAN
Management VLAN :
```

VLAN ID	Name	Status	Voice	Jumbo
1	DEFAULT_VLAN	Port-based	No	No
100	VLAN100	Port-based	No	No

---

### Example 16 Changing the VLAN context level

---

To go to a different VLAN context level, such as to the default VLAN:

```
HP Switch (vlan-100)#: vlan default_vlan HP Switch(vlan-1) _
```

## Deleting a static VLAN (CLI)

**Syntax:**

```
no vlan <vid>
```

---

**⚠ CAUTION:** Before deleting a static VLAN, re-assign all ports in the VLAN to another VLAN.

---

## Example 17 Deleting a static VLAN

---

Following [Figure 3 \(page 26\)](#), if ports B1-B5 belong to both VLAN 2 and VLAN 3 and ports B6-B10 belong to VLAN 3, deleting VLAN 3 causes the CLI to prompt you to approve moving ports B6 - B10 to VLAN 1 (the default VLAN). (Ports B1-B5 are not moved because they still belong to another VLAN.)

```
HP Switch(config)#: no vlan 3
The following ports will be moved to the default VLAN:
B6-B10
Do you want to continue?
[y/n] Y
HP Switch(config)#: :
```

---

## Converting a dynamic VLAN to a static VLAN (CLI)

### Syntax:

```
static-vlan <vlan-id>
```

Converts a dynamic, port-based VLAN membership to static, port-based VLAN membership (allows port-based VLANs only).

For this command, <vlan-id> refers to the VID of the dynamic VLAN membership. Use `show vlan` to help identify the VID.

This command requires that GVRP is running on the switch and a port is currently a dynamic member of the selected VLAN.

After you convert a dynamic VLAN to static, you must configure the switch's per-port participation in the VLAN in the same way that you would for any static VLAN. For GVRP and dynamic VLAN operation, see ["GVRP" \(page 61\)](#).

## Example 18 Converting a dynamic VLAN to a port-based static VLAN

---

Suppose a dynamic VLAN with a VID of 125 exists on the switch. The following command converts the VLAN to a port-based, static VLAN:

```
HP(config)#: static-vlan 125
```

---

## Configuring static VLAN per-port settings (CLI)

### Syntax:

```
[no] vlan <vid>
```

This command, used with the options listed below, changes the name of an existing static VLAN and the per-port VLAN membership settings.

---

**NOTE:** You can use these options from the configuration level by beginning the command with `vlan <vid>`, or from the context level of the specific VLAN by just entering the command option.

---

```
tagged <port-list>
```

Configures the indicated port as Tagged for the specified VLAN. The `no` version sets the port to either **No** or (if GVRP is enabled) to **Auto**.

```
untagged <port-list>
```

Configures the indicated port as Untagged for the specified VLAN. The `no` version sets the port to either **No** or (if GVRP is enabled) to **Auto**.

```
forbid <port-list>
```

Used in port-based VLANs, configures `<port-list>` as forbidden, to become a member of the specified VLAN, as well as other actions. Does not operate with option not allowed protocol VLANs. The `no` version sets the port to either `No` or (if GVRP is enabled) to `Auto`. See “GVRP” (page 61).

`auto <port-list>`

Available if GVRP is enabled on the switch. Returns the per-port settings for the specified VLAN to `Auto` operation. `Auto` is the default per-port setting for a static VLAN if GVRP is running on the switch. For information on dynamic VLAN and GVRP operation, see “GVRP” (page 61).

---

### Example 19 Changing the VLAN name and set ports to tagged

---

Suppose there is a VLAN named VLAN100 with a VID of 100 and all ports are set to **No** for this VLAN. To change the VLAN name to `Blue_Team` and set ports A1 - A5 to `Tagged`, use the following commands:

```
HP Switch(config)#: vlan 100 name Blue_Team
HP Switch(config)#: vlan 100 tagged a1-a5
```

---

---

### Example 20 Moving the context level

---

To move to the `vlan 100` context level and execute the same commands:

```
HP Switch(config)#: vlan 100
HP Switch(vlan-100)#: name Blue_Team
HP Switch(vlan-100)#: tagged a1-a5
```

---

---

### Example 21 Changing tagged ports

---

Similarly, to change the tagged ports in the above examples to `No` (or `Auto`, if GVRP is enabled), use either of the following commands.

At the global config level, use:

```
HP Switch(config)#: no vlan 100 tagged a1-a5
```

- or -

At the VLAN 100 context level, use:

```
HP Switch(vlan-100)#: no tagged a1-a5
```

---

**NOTE:** You cannot use these commands with dynamic VLANs. Attempting to do so displays the message `VLAN already exists with no change`.

---

## Using IP enable/disable for all VLANs

You can administratively disable the IP address on specified VLANs with static IP addresses without removing the Layer 3 configuration. The switch can be pre-configured as a backup router, then quickly transition from backup to active by re-enabling Layer 3 routing on one or more VLANs. While the switch is in “backup” mode, it will still performing Layer 2 switching.

A MIB object will be toggled to make Layer 3 routing active or inactive on a VLAN.

## Interaction with other features

This feature affects management access to the switch as follows:

- IP—SNMP, Telnet, SSH, HTTP, TFTP, SCP, SFTP
- Routing—RIP, OSPF, PIM, VRRP

When the `disable layer3` command is configured on a VLAN, the behavior is as if no IP address were configured for that VLAN. There is no other change in behavior.

### Syntax:

```
[no] disable layer3 vlan [ <vid> <vid range>]
```

In config context, turns off Layer 3 routing for the specified VLAN or VLANs. When executed in vlan context, turns off Layer 3 routing for that VLAN.

The `no` form turns on Layer 3 routing for the specified VLAN or VLANs.

The `show ip` command displays `disabled` in the IP Config column if Layer 3 has been disabled, or if the VLAN has no IP configuration. You can tell which is the case by viewing the remaining columns; if there is no IP configuration, the remaining columns are blank.

### Example 22 Displaying a VLAN disabled for Layer 3

---

```
HP Switch(config)#: show ip
```

```
Internet (IP) Service
```

```
IP Routing : Disabled
```

```
Default Gateway : 172.22.16.1
```

```
Default TTL      : 64
```

```
Arp Age         : 20
```

```
Domain Suffix   :
```

```
DNS server      :
```

VLAN	IP Config	IP Address	Subnet Mask	Proxy ARP
-----+-----				
DEFAULT_VLAN	DHCP/Bootp	172.22.18.100	255.255.248.0	No No
VLAN3	Disabled	172.17.17.17	255.255.255.0	No No
VLAN6	Disabled			
VLAN7	Manual	10.7.7.1	255.255.255.0	No No

---

For IPv6, the `Layer 3 Status` field displays the status of Layer 3 on that VLAN.



## Example 23 Displaying IPv6 Layer 3 status for a VLAN

---

```
HP Switch(config)#: show ipv6
```

```
Internet (IPv6) Service
```

```
IPv6 Routing      : Disabled
Default Gateway  :
ND DAD           : Enabled
DAD Attempts     : 3
```

```
Vlan Name        : DEFAULT_VLAN
IPv6 Status      : Disabled
Layer 3 Status   : Enabled
```

```
Vlan Name        : layer3_off_vlan
IPv6 Status      : Disabled
Layer 3 Status   : Disabled
```

Address Origin	IPv6 Address/Prefix Length	Address Status
manual	abcd::1234/32	tentative
autoconfig	fe80::218:71ff:febd:ee00/64	tentative

---

### Interactions with DHCP

Disabling Layer 3 functionality and DHCP are mutually exclusive, with DHCP taking precedence over `disable layer3` on a VLAN. The following interactions occur:

- If the `disable layer3` command is executed when DHCP is already configured, no disabling of the VLAN occurs. This error message displays: “Layer 3 cannot be disabled on a VLAN that has DHCP enabled.”
- From the CLI: If `disable layer3` is configured already and an attempt is made to configure DHCP, DHCP takes precedence and will be set. The warning message displays: “Layer 3 has also been enabled on this VLAN since it is required for DHCP.”
- From the CLI: When disabling a range of VLAN IDs, this warning message displays: “Layer 3 will not be disabled for any LANs that have DHCP enabled.”
- From SNMP: If the `disable layer3` command is executed when DHCP is already configured, no disabling of the VLAN occurs. An `INCONSISTENT_VALUE` error is returned.
- From SNMP: If `disable layer3` is configured already and an attempt is made to configure DHCP, DHCP takes precedence and will be set.

## Adding or changing a VLAN port assignment (Menu)

Ports not specifically assigned to a VLAN are automatically in the default VLAN.

- From the Main Menu select: **2. Switch Configuration** —> **8. VLAN Menu ...** —> **3. VLAN Port Assignment**

You will see a screen similar to the following:

**Figure 6** Port-based VLAN port assignment screen in the menu interface

**Default:** In this example, the "VLAN-22" has been defined, but no ports have yet been assigned to it. ("No" means the port is not assigned to that VLAN.)

**Using GVRP?** If you plan on using GVRP, any ports you don't want to join should be changed to "Forbid".

A port can be assigned to several VLANs, but only one of those assignments can be "Untagged".

```

----- CONSOLE - MANAGER MODE -----
Switch Configuration - VLAN - VLAN Port Assignment

Port  DEFAULT_VLAN  VLAN-22  |  Port  DEFAULT_VLAN  VLAN-22
----+-----+-----+-----+-----+-----+
A1   | Untagged   No      |  A8   | Untagged   No
A2   | Tagged     No      |  A9   | Untagged   No
A3   | Untagged   No      |  A10  | Untagged   No
A4   | Untagged   No      |  A11  | Untagged   No
A5   | Untagged   No      |  A12  | Untagged   No
A6   | Untagged   No      |  A13  | Untagged   No
A7   | Untagged   No      |  A14  | Untagged   No

Actions->  C a n c e l   E d i t   S a v e   H e l p
Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.

```

**NOTE:** The "VLAN Port Assignment" screen displays up to 32 static, port-based VLANs in ascending order, by VID. If the switch configuration includes more than 32 such VLANs, use the following CLI command to list data on VLANs having VIDs numbered sequentially higher than the first 32.

```
show vlans [ <vid> | ports [ <port-list> ] ]
```

- To change a port's VLAN assignment:
  - Press **E** (for Edit).
  - Use the arrow keys to select a VLAN assignment you want to change.
  - Press the Space bar to make your assignment selection (**No**, **Tagged**, **Untagged**, or **Forbid**). For information on VLAN tags, see ["802.1Q VLAN tagging"](#) (page 49).
  - If you are finished assigning ports to VLANs, press **Enter** and then **S** (for Save) to activate the changes and return to the Configuration menu. (The console then returns to the VLAN menu.)
- Return to the Main menu.

**NOTE:** For GVRP Operation: If you enable GVRP on the switch, **No** converts to **Auto**, which allows the VLAN to dynamically join an advertised VLAN that has the same VID.

**Untagged VLANs** Only one untagged VLAN is allowed per port. Also, there must be at least one VLAN assigned to each port. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT\_VLAN).

For ports A4 and A5 to belong to both DEFAULT\_VLAN and VLAN-22 and ports A6 and A7 to belong only to VLAN-22, use the settings in ["The default VLAN names screen"](#) (page 26). This example assumes that the default GVRP setting is disabled and that you do not plan to enable GVRP later.

## Example 24 Displaying port-based VLAN assignments for specific ports

Ports A4 and A5 are assigned to both VLANs.

Ports A6 and A7 are assigned only to VLAN-22.

All other ports are assigned only to the Default VLAN.

```
----- CONSOLE - MANAGER MODE -----
Switch Configuration - VLAN - VLAN Port Assignment

Port  DEFAULT_VLAN  VLAN-22  |  Port  DEFAULT_VLAN  VLAN-22
-----+-----+-----+-----+-----+-----+
A1 | Untagged  No      |  A8 | Untagged  No
A2 | Untagged  No      |  A9 | Untagged  No
A3 | Untagged  No      |  A10| Untagged  No
A4 | Untagged  Tagged  |  A11| Untagged  No
A5 | Untagged  Tagged  |  A12| Untagged  No
A6 | No        Untagged|  A13| Untagged  No
A7 | No        Untagged|  A14| Untagged  No

Actions->  _Cancel  _Edit  _Save  _Help

Select the tagging mode for the port/VLAN combination.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

## Deleting multiple VLANs

Enables the user to add or delete interfaces from multiple tagged or untagged VLANs or SVLANs using a single command. Interfaces can be added or deleted up to 256 VLANs at a time. If more than 256 VLANs are specified, an error displays. The `forbid` command option prevents specified ports from becoming members of specified VLANs or SVLANs when used with GVRP. The command is executed in the interface context.

### Syntax

```
[no]interface <port-list> <tagged | untagged | forbid> <vlan
| svlan <vlan-id-list>>
```

- The specified interfaces are added to existing VLANs or SVLANs. If a VLAN or SVLAN does not exist, an error message displays.
- The **[no]** option removes the specified interfaces from the specified VLANs or SVLANs.
- The **forbid** option prevents an interface from becoming a member of the specified VLANs or SVLANs. It is executed in interface context.

### Example 25 Removing an interface from several VLANs

The `vlan-id-list` includes a comma-separated list of VLAN IDs and/or VLAN ID ranges.

### Example 26 To remove interface 1 from VLANs 1, 3, 5, 6, 7, 8, 9, 10

```
HP Switch(config)#: no interface 1,6,7-10 tagged vlan 1,3,5-10
```

### Example 27 To specify that an interface cannot become a member of VLANs 4 and 5

```
HP Switch(config)#: interface 2 forbid vlan 4-5
```

## Correcting an unsupported configuration

The following example provides a method to identify and correct an unsupported configuration.

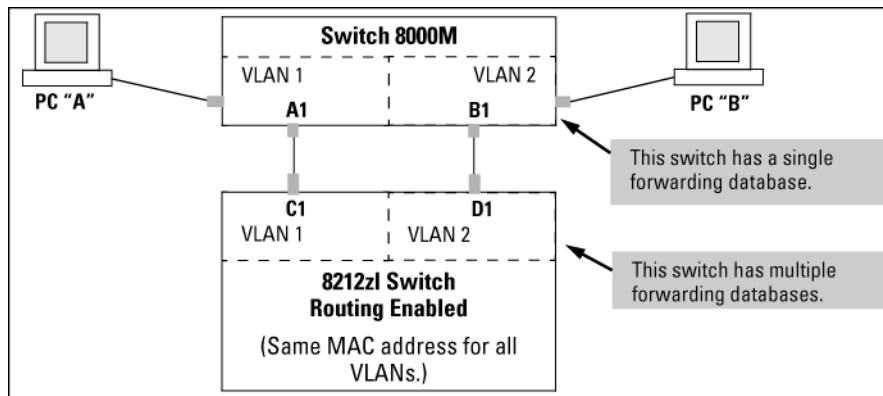
### The problem

In [Figure 7 \(page 36\)](#), the MAC address table for Switch 8000M will sometimes record the switch as accessed on port A1 (VLAN 1) and other times as accessed on port B1 (VLAN 2):

PC A sends an IP packet to PC B.

1. The packet enters VLAN 1 in the Switch 8000 with the 8212zl switch's MAC address in the destination field. Because the 8000M has not yet learned this MAC address, it does not find the address in its address table and floods the packet out all ports, including the VLAN 1 link (port "A1") to the 8212zl switch. The 8212zl switch then routes the packet through the VLAN 2 link to the 8000M, which forwards the packet on to PC "B". Because the 8000M received the packet from the 8212zl switch on VLAN 2 (port "B1"), the 8000M's single forwarding database records the 8212zl switch as being on port "B1" (VLAN 2).
2. PC "A" now sends a second packet to PC "B". The packet again enters VLAN 1 in the Switch 8000 with the 8212zl switch's MAC address in the destination field. However, this time the Switch 8000M's single forwarding database indicates that the 8212zl is on port B1 (VLAN 2) and the 8000M drops the packet instead of forwarding it.
3. Later, the 8212zl switch transmits a packet to the 8000M through the VLAN 1 link and the 8000M updates its address table to indicate that the 8212zl switch is on port A1 (VLAN 1) instead of port B1 (VLAN 2). Thus, the 8000M's information on the location of the 8212zl switch changes over time. For this reason, the 8000M discards some packets directed through it for the 8212zl switch, causing poor performance and the appearance of an intermittent or broken link.

**Figure 7 Invalid forwarding**

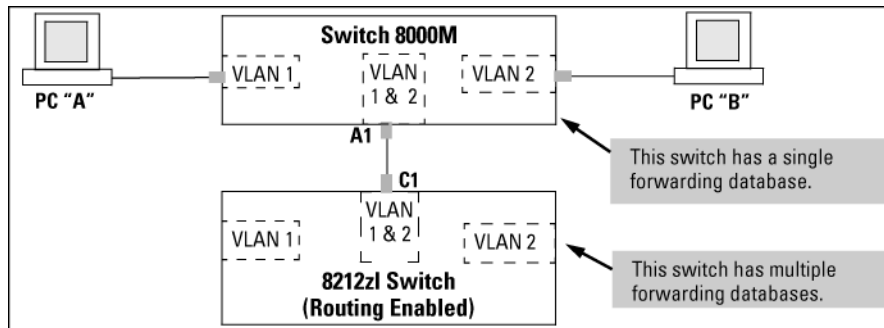


## The solution

1. Use only one cable or port trunk between the single-forwarding and multiple-forwarding database devices
2. Configure the link with multiple, tagged VLANs.
3. To increase the network bandwidth of the connection between devices, use a trunk of multiple physical links.

Now, the 8000M forwarding database always lists the 8212zl MAC address on port A1 and the 8000M will send traffic to either VLAN on the 8212zl.

**Figure 8 A solution for single-forwarding to multiple-forwarding database devices in a multiple VLAN environment**



## Connecting an HP Switch to another with a multiple forwarding database (Example)

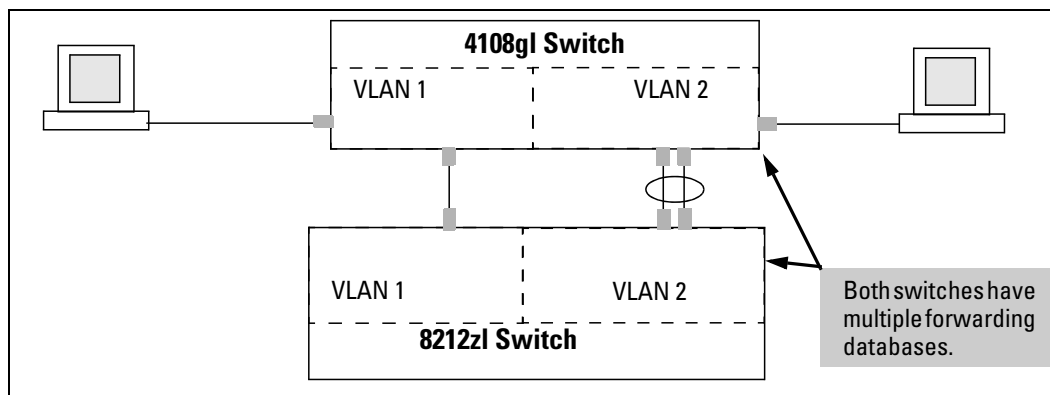
### Example 28 Example

Use one or both of the following connection options:

- A separate port or port trunk interface for each VLAN. This results in a forwarding database having multiple instances of the same MAC address with different VLAN IDs and port numbers. See [Table 4 \(page 48\)](#). The fact that the switches covered by this guide use the same MAC address on all VLAN interfaces causes no problems.
- The same port or port trunk interface for multiple (tagged) VLANs. This results in a forwarding database having multiple instances of the same MAC address with different VLAN IDs, but the same port number.

Allowing multiple entries of the same MAC address on different VLANs enables topologies such as the following:

### Example 29 Topology for devices with multiple forwarding databases in a multiple VLAN environment



## Configuring a secure Management VLAN (CLI)

### Preparation

1. Determine a VID and VLAN name suitable for your Management VLAN.
2. Plan your topology to use HP switches that support Management VLANs. See [“The secure Management VLAN” \(page 54\)](#).

3. Include only the following ports:
  - Ports to which you will connect authorized management stations, such as Port A7 in [Example 45 \(page 54\)](#).
  - Ports on one switch that you will use to extend the Management VLAN to ports on other HP switches, such as ports A1 and [Example 45 \(page 54\)](#).
4. Half-duplex repeaters dedicated to connecting management stations to the Management VLAN can also be included in this topology. Note that any device connected to a half-duplex repeater in the Management VLAN will also have Management VLAN access.
5. Configure the Management VLAN on the selected switch ports.
6. Test the Management VLAN from all of the management stations authorized to use it, including any SNMP-based network management stations. Also test any Management VLAN links between switches.

---

**NOTE:** If you configure a Management VLAN on a switch using a Telnet connection through a port not in the Management VLAN, you will lose management contact with the switch if you log off your Telnet connection or execute `write memory` and `reboot` the switch.

---

## Configuring an existing VLAN as the Management VLAN (CLI)

### Syntax:

```
[no] management-vlan [ <vlan-id> | <vlan-name> ]
```

Configures an existing VLAN as the Management VLAN.

The `no` form disables the Management VLAN and returns the switch to its default management operation.

Default: Disabled. In this case, the VLAN returns to standard VLAN operation.

### Example 30 Switch configuration

---

You have configured a VLAN named `My_VLAN` with a VID of 100 and want to configure the switch to do the following:

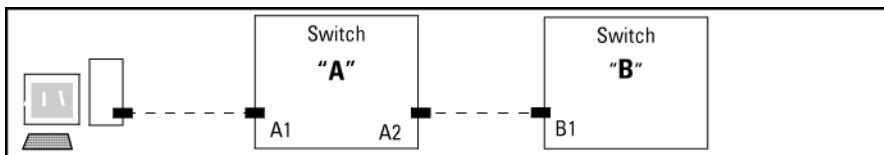
- Use `My_VLAN` as a Management VLAN (tagged, in this case) to connect port A1 on switch "A" to a management station. The management station includes a network interface card with 802.1Q tagged VLAN capability.
- Use port A2 to extend the Management VLAN to port B1 which is already configured as a tagged member of `My_VLAN`, on an adjacent HP switch that supports the Management VLAN feature.

```
HP Switch (config)#: management-vlan 100
HP Switch (config)#: vlan 100 tagged a1
HP Switch (config)#: vlan 100 tagged a2
```

---

### Example 31 Configuration Example

---

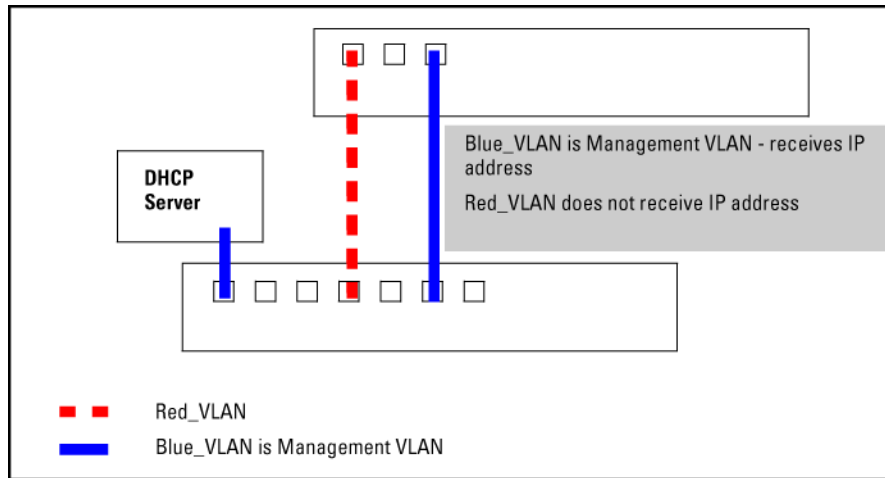


### Obtaining an IP address using DHCP (CLI)

Use DHCP to obtain an IPv4 address for your Management VLAN or a client on that VLAN. The following examples illustrate when an IP address will be received from the DHCP server.

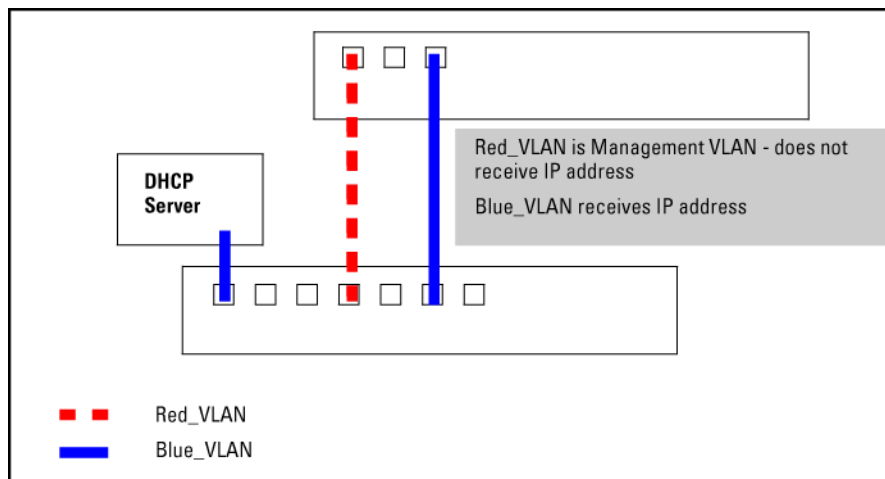
### Example 32 DHCP server on a Management VLAN

If Blue\_VLAN is configured as the Management VLAN and the DHCP server is also on Blue\_VLAN, Blue\_VLAN receives an IP address. Because DHCP Relay does not forward onto or off of the Management VLAN, devices on Red\_VLAN cannot get an IP address from the DHCP server on Blue\_VLAN (Management VLAN) and Red\_VLAN does not receive an IP address.



### Example 33 DHCP server on a different VLAN from the Management VLAN

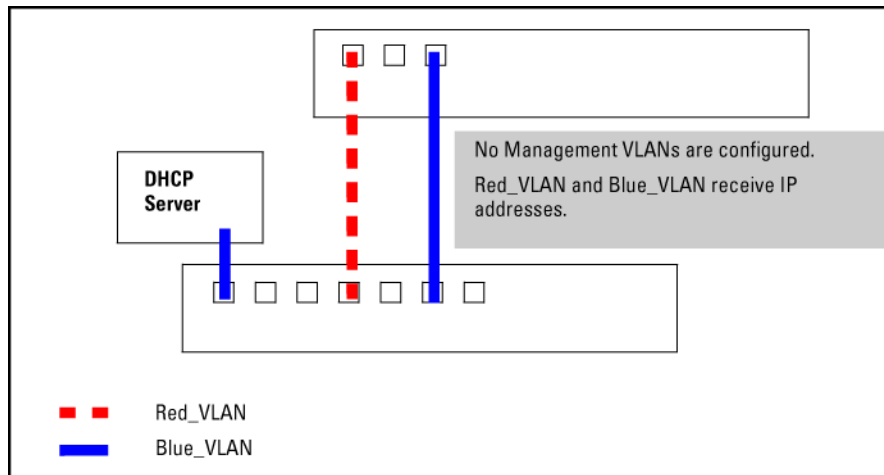
If Red\_VLAN is configured as the Management VLAN and the DHCP server is on Blue\_VLAN, Blue\_VLAN receives an IP address but Red\_VLAN does not.





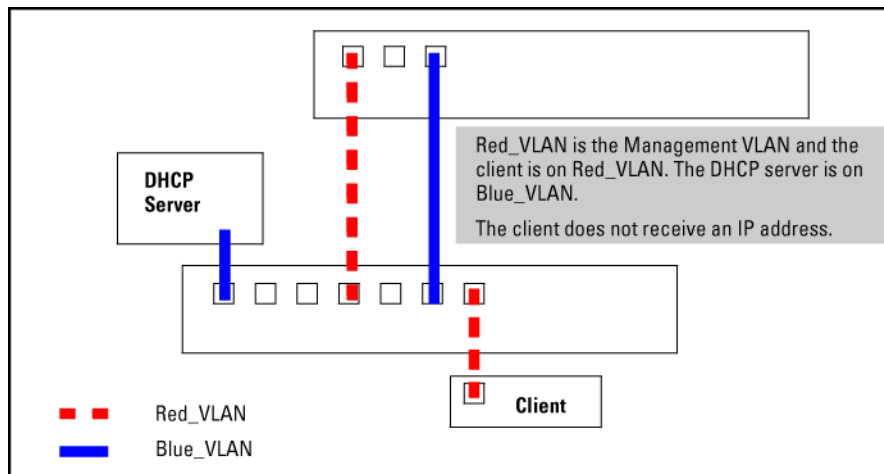
### Example 34 No Management VLANs configured

If no Management VLAN is configured, both Blue\_VLAN and Red\_VLAN receive IP addresses.



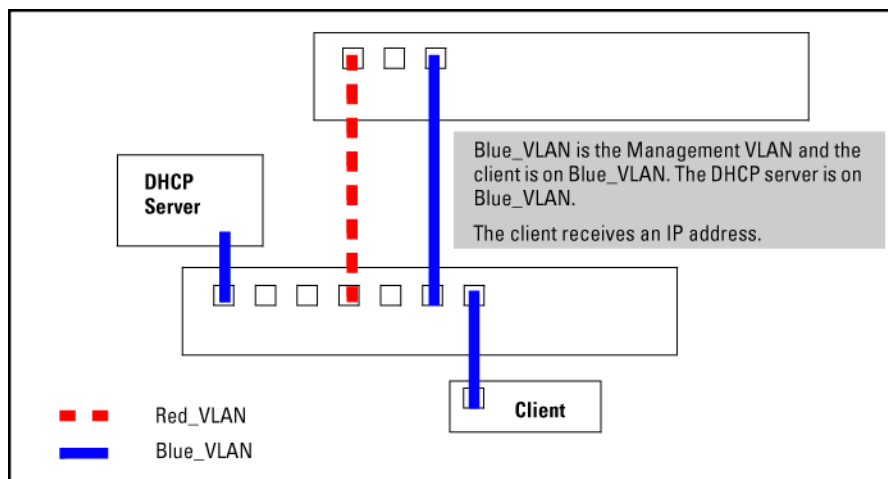
### Example 35 A client on a different Management VLAN from the DHCP server

If Red\_VLAN is configured as the Management VLAN and the client is on Red\_VLAN, but the DHCP server is on Blue\_VLAN, the client will not receive an IP address.



## Example 36 A DHCP server and client on the Management VLAN

If Blue\_VLAN is configured as the Management VLAN, the client is on Blue\_VLAN and the DHCP server is on Blue\_VLAN, the client receives an IP address.



## Disabling the Management feature (CLI)

You can disable the Secure Management feature without deleting the VLAN.

### Example 37 Disabling the secure management feature

The following commands disable the Secure Management feature in the above example:

```
HP Switch (config)#: no management-vlan 100
HP Switch (config)#: no management-vlan my_vlan
```

For more information, see [“The secure Management VLAN” \(page 54\)](#).

## Prioritizing voice VLAN QoS (CLI) (Optional)

Without configuring the switch to prioritize voice VLAN traffic, one of the following conditions applies:

- If the ports in a voice VLAN are not tagged members, the switch forwards all traffic on that VLAN at "normal" priority.
- If the ports in a voice VLAN are tagged members, then the switch forwards all traffic on that VLAN at whatever priority the traffic has when received inbound on the switch.

Using the switch's QoS VLAN-ID (VID) priority option, you can change the priority of voice VLAN traffic moving through the switch. If all port memberships on the voice VLAN are tagged, the priority level you set for voice VLAN traffic is carried to the next device. With all ports on the voice VLAN configured as tagged members, you can enforce a QoS priority policy moving through the switch and through your network.

### Syntax:

```
vlan <vid> qos priority <0 - 7>
```

The qos priority default setting is 0 (normal), with 1 as the lowest priority and 7 as the highest priority.

If you configure a voice VLAN with a VID of 10 and want the highest priority for all traffic on this VLAN, execute the following commands:

```
HP Switch(config) #: vlan 10 qos priority 7
HP Switch (config) #: write memory
```

You also have the option of resetting the DSCP (DiffServe Codepoint) on tagged voice VLAN traffic moving through the switch. For more information, see [“Quality of Service: Managing bandwidth effectively”](#) (page 145).

If all port memberships on the voice VLAN are tagged:

- The priority level set for voice VLAN traffic is carried to the next device.
- You can enforce a QoS priority policy moving through the switch and network.

For more information, see [“Voice VLANs”](#) (page 56).

## Configuring a VLAN MAC address with heartbeat interval (CLI)

When installing HP routing switches in the place of existing routers in a network configuration, you can achieve Layer 3 VLAN migration by using the `ip-recv-mac-address` command at the VLAN configuration level to:

- Configure the MAC address of the previously installed router on each VLAN interface of an HP routing switch.
- Optionally configure the time interval to use for sending heartbeat packets with the configured MAC address.

### Syntax:

```
[no] ip-recv-mac-address <mac-address> [ interval <seconds> ]
```

Configures a VLAN interface with the specified MAC address. Enter the `no` version of the command to remove the configured MAC address and return to the original MAC address of the HP switch.

`interval <seconds>` (Optional) Configures the time interval in seconds used between transmissions of heartbeat packets to all network devices configured on the VLAN. Valid values are from one to 255 seconds.

Default: 60 seconds.

## Displaying a VLAN MAC address configuration (CLI)

### Syntax:

```
show ip-recv-mac-address
```

### Example 38 Displaying a VLAN MAC address

```
HP Switch#: show ip-recv-mac-address
```

```
VLAN L3-Mac-Address Table
```

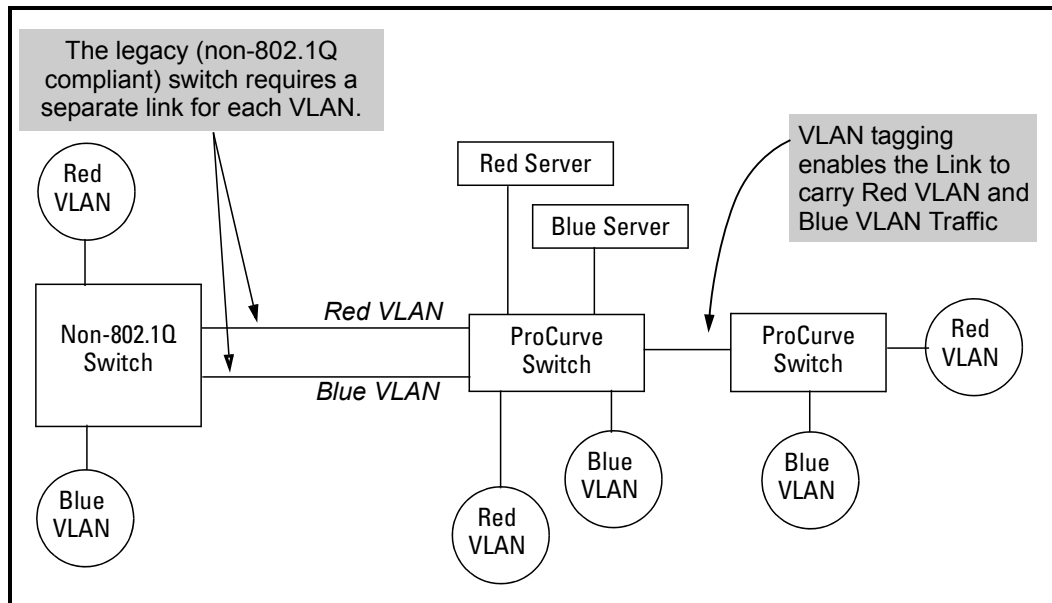
VLAN	L3-Mac-Address	Timeout
-----	-----	-----
DEFAULT_VLAN	001635-024467	60
VLAN2	001635-437529	100

## Introducing tagged VLAN technology into networks running untagged VLANs

You can introduce 802.1Q-compliant devices into networks that have built untagged VLANs based on earlier VLAN technology. The fundamental rule is that legacy/untagged VLANs require a

separate link for each VLAN, while 802.1Q, or tagged VLANs can combine several VLANs in one link. Thus on the 802.1Q-compliant device, separate ports (configured as untagged) must be used to connect separate VLANs to non-802.1Q devices.

### Example 39 Tagged and untagged VLAN technology in the same network



## VLAN Operating Rules

Disabled overlapping subnet configuration

Previous software versions allowed configuration of VLAN IP addresses in overlapping subnets, which can cause incorrect routing of packets and result in IP communication failure. As of software version K.15.09, overlapping subnet configurations are no longer allowed. An overlapping subnet is determined by the configuration order. The subnet that is configured first is valid, but any subsequent IP addresses that overlap are not allowed.

When the switch is booted into software version K.15.09 or later and the configuration file includes overlapping subnets, the following occurs:

- The event log provides an error message in the format:  
`ip: VLANx : IP initialization failed for vlan x.`

For a multinetted VLAN (multiple IP addresses assigned to the VLAN), only the IP addresses that are overlapping subnets are removed. The other IP addresses on the VLAN are retained and function correctly. The error message can be somewhat misleading; the IP addresses on the VLAN that are not overlapping are initialized correctly.

- The output of the `show ip` command correctly indicates that the overlapping IP address does not exist on the VLANs that have error messages in the event log.
- The output of the `show running-config` command incorrectly indicates that the overlapping IP address is

configured. For example, in the following output, the IP address shown in VLAN6 is not actually configured on the VLAN; it has been removed.

#### Example 40 An IP address that is not actually configured on the VLAN

---

```
HP Switch(config)#: show running-config
.
.
.
vlan 5
  name "VLAN5"
  ip address 11.22.33.1 255.0.0.0
  exit
vlan 6
  name "VLAN6"
  ip address 11.23.34.1 255.255.255.0
  exit
```

---

The information is retained in the config file to allow you to boot up the switch and have it function as it did when it was configured with earlier software that allows overlapping subnets. This occurs because the overlapping IP address has been removed and is not visible to the switch. To resolve this:

If you attempt to remove the overlapping subnet from the VLAN, the switch displays an error message similar to:

The IP address *<ip address>* is not configured on this VLAN

This occurs because the overlapping IP address has been removed and is not visible to the switch. To resolve this:

- Enter the `show ip` command to determine which addresses are visible to the switch.
- Remove the erroneous IP addresses from the config file by entering the `no ip address` command to remove all the IP addresses from the specific VLAN. Be sure to document the other valid IP addresses on that VLAN so they can be restored after removing the erroneous IP addresses from the config file.

If you go back to a software version prior to K.15.09 before removing the overlapping IP address, the prior software version enables the overlapping IP subnet.

#### DHCP/Bootp

If you are using DHCP/Bootp to acquire the switch's configuration, packet time-to-live and TimeP information, designates the VLAN on which DHCP is configured as the Primary VLAN.

---

**NOTE:** In the factory-default configuration, the DEFAULT\_VLAN is the Primary VLAN.

---

#### Per-VLAN features

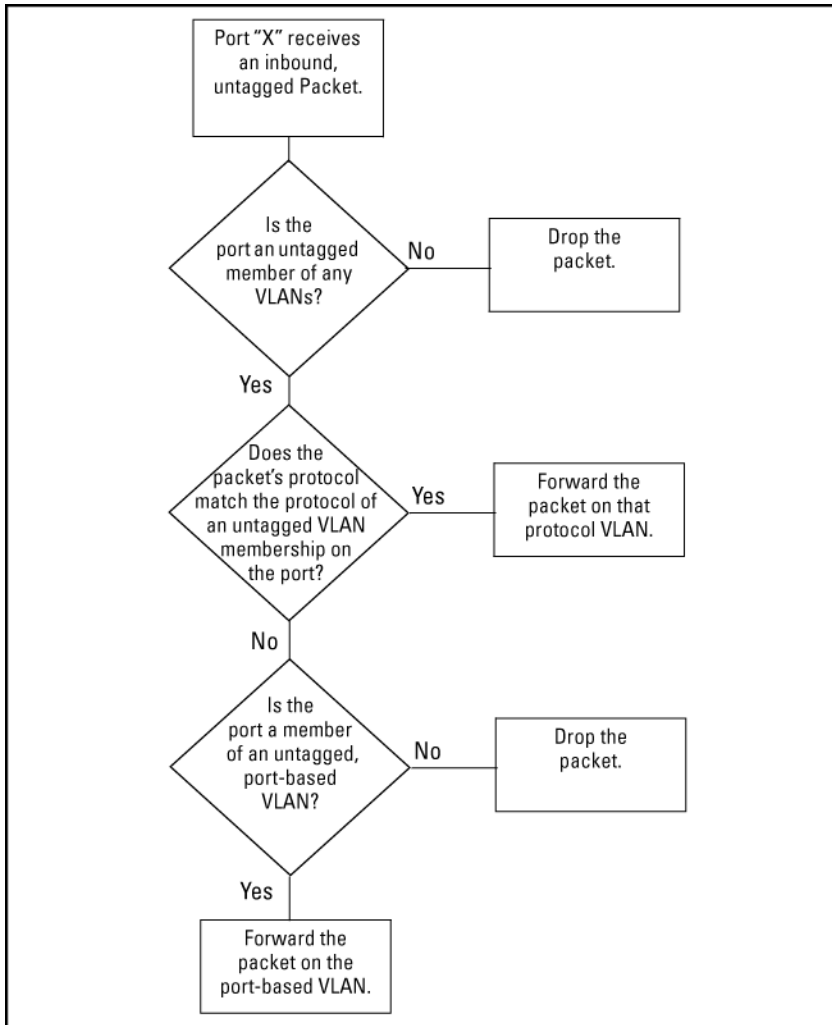
IGMP and some other features operate on a per VLAN basis. This means you must configure such features separately for each VLAN in which you want them to operate.

Default VLAN	You can rename the default VLAN, but you cannot change its VID (1) or delete it from the switch.
VLAN port assignments	Any ports not specifically removed from the default VLAN remain in the DEFAULT_VLAN, regardless of other port assignments. Also, a port must always be a tagged or untagged member of at least one port-based VLAN.
Voice-Over-IP (VoIP)	VoIP operates only over static, port-based VLANs.
Multiple VLAN types configured on the same port	A port can simultaneously belong to both port-based and protocol-based VLANs.
Protocol Capacity	<p>A protocol-based VLAN can include up to four protocol types. In protocol VLANs using the IPv4 protocol, to support normal IP network operation ARP must be one of these protocol types (to support normal IP network operation). Otherwise, IP traffic on the VLAN is disabled.</p> <p>If you configure an IPv4 protocol VLAN that does not include the ARP VLAN protocol, the switch displays the following message which indicates a protocol VLAN configured with IPv4 but not ARP:</p> <pre>HP Switch(config)#: vlan 97 protocol ipv4  IPv4 assigned without ARP, this may result in undeliverable IP packets.</pre>
Deleting Static VLANs	A VLAN can be deleted even if there are currently ports belonging to it. The ports are moved to the default VLAN.
Adding or Deleting VLANs	To Change the number of VLANs supported on the switch requires a reboot.
	<hr/> <p><b>NOTE:</b> From the CLI, you must perform a <code>write memory</code> command before rebooting. Other VLAN configuration changes are dynamic.</p> <hr/>
Inbound Tagged Packets	<p>If a tagged packet arrives on a port that is not a tagged member of the VLAN indicated by the packet's VID, the switch drops the packet.</p> <p>Similarly, the switch will drop an inbound, tagged packet if the receiving port is an untagged member of the VLAN indicated by the packet's VID.</p>
Untagged Packet Forwarding	<p>To enable an inbound port to forward an untagged packet, the port must be an untagged member of either a protocol VLAN matching the packet's protocol, or an untagged member of a port-based VLAN.</p> <p>That is, when a port receives an incoming, untagged packet, it processes the packet according to the following ordered criteria:</p> <ol style="list-style-type: none"> <li>1. If the port has no untagged VLAN memberships, the switch drops the packet.</li> <li>2. If the port has an untagged VLAN membership in a protocol VLAN that matches the protocol type of the</li> </ol>

incoming packet, then the switch forwards the packet on that VLAN.

3. If the port is a member of an untagged, port-based VLAN, the switch forwards the packet to that VLAN. Otherwise, the switch drops the packet.

Figure 9 Untagged VLAN operation

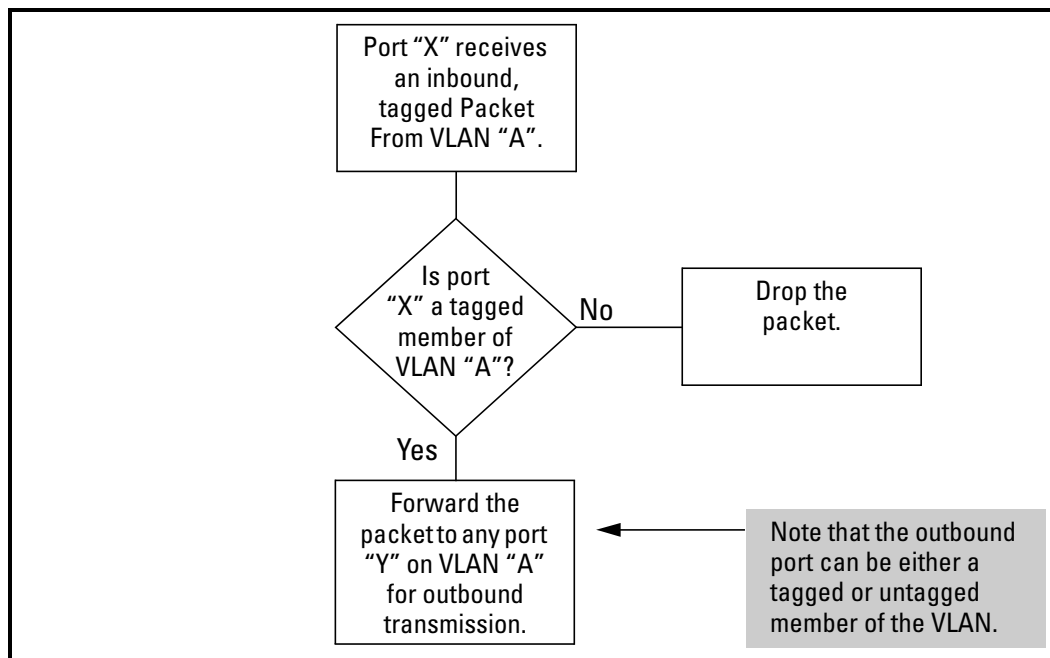


### Tagged packet forwarding

If a port is a tagged member of the same VLAN as an inbound, tagged packet received on that port, then the switch forwards the packet to an outbound port on that VLAN.

To enable the forwarding of tagged packets, any VLAN to which the port belongs as a tagged member must have the same VID as that carried by the inbound, tagged packets generated on that VLAN.

Figure 10 Tagged VLAN operation



See also “Multiple VLAN considerations” (page 48).

## Multiple VLAN considerations

Switches use a forwarding database to maintain awareness of which external devices are located on which VLANs. Some switches, such as the switches covered in this guide, have a multiple forwarding database, which means the switch allows multiple database entries of the same MAC address, with each entry showing the (different) source VLAN and source port. Other switch models have a single forwarding database, which allows only one database entry of a unique MAC address, along with the source VLAN and source port on which it is found. All VLANs on a switch use the same MAC address. Thus, connecting a multiple forwarding database switch to a single forwarding database switch where multiple VLANs exist imposes some cabling and port VLAN assignment restrictions. The following table illustrates the functional difference between the two database types.

Table 4 Forwarding database content

Multiple forwarding database			Single forwarding database		
MAC address	Destination VLAN ID	Destination port	MAC address	Destination VLAN ID	Destination port
0004ea-84d9f4	1	A5	0004ea-84d9f4	100	A9
0004ea-84d9f4	22	A12	0060b0-880af9	105	A10
0004ea-84d9f4	44	A20	0060b0-880a81	107	A17
0060b0-880a81	33	A20			
This database allows multiple destinations for the same MAC address. If the switch detects a new destination for an existing MAC entry, it just adds a new instance of that MAC to the table.			This database allows only one destination for a MAC address. If the switch detects a new destination for an existing MAC entry, it replaces the existing MAC instance with a new instance showing the new destination.		



## Single forwarding database operation

When a packet arrives with a destination MAC address that matches a MAC address in the switch's forwarding table, the switch tries to send the packet to the port listed for that MAC address. But if the destination port is in a different VLAN than the VLAN on which the packet was received, the switch drops the packet. This is not a problem for a switch with a multiple forwarding database because the switch allows multiple instances of a given MAC address, one for each valid destination. However, a switch with a single forwarding database allows only one instance of a given MAC address.



---

**TIP:** If you (1) connect both switch types through multiple ports or trunks belonging to different VLANs and (2) enable routing on the switch with the multiple-forwarding database, then the port and VLAN record maintained on the switch with the single-forwarding database for the multiple-forwarding database can change frequently. This may cause poor performance and the appearance of an intermittent or broken connection.

---

## 802.1Q VLAN tagging

- The switch requires VLAN tagging on a given port if more than one VLAN of the same type uses the port. When a port belongs to two or more VLANs of the same type, they remain as separate broadcast domains and cannot receive traffic from each other without routing.

---

**NOTE:** If multiple, non-routable VLANs exist in the switch—such as NETbeui protocol VLANs—they cannot receive traffic from each other.

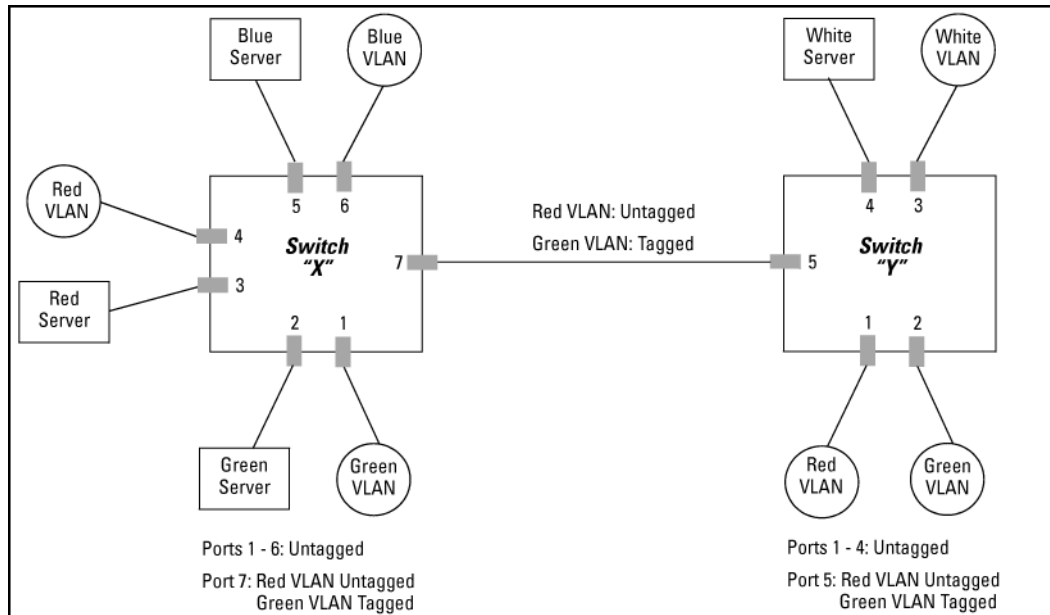
---

- The switch requires VLAN tagging on a given port if the port will be receiving inbound, tagged VLAN traffic that should be forwarded. Even if the port belongs to only one VLAN, it forwards inbound tagged traffic only if it is a tagged member of that VLAN.
- If the only authorized, inbound VLAN traffic on a port arrives untagged, then the port must be an untagged member of that VLAN. This is the case where the port is connected to a non 802.1Q-compliant device or is assigned to only one VLAN.

## Example 41 Tagged and untagged VLAN port assignments

If port 7 on an 802.1Q-compliant switch is assigned to only the Red VLAN, the assignment can remain "untagged" because the port will forward traffic only for the Red VLAN. However, if both the Red and Green VLANs are assigned to port 7, then at least one of those VLAN assignments must be "tagged" so that Red VLAN traffic can be distinguished from Green VLAN traffic.

Figure 11 Tagged and untagged VLAN port assignments



In switch X:

- VLANs assigned to ports X1 - X6 can be untagged because there is only one VLAN assignment per port. Red VLAN traffic will go out only the Red ports, Green VLAN traffic will go out only the Green ports and so on. Devices connected to these ports do not have to be 802.1Q-compliant.
- However, because both the Red VLAN and the Green VLAN are assigned to port X7, at least one of the VLANs must be tagged for this port.

In switch Y:

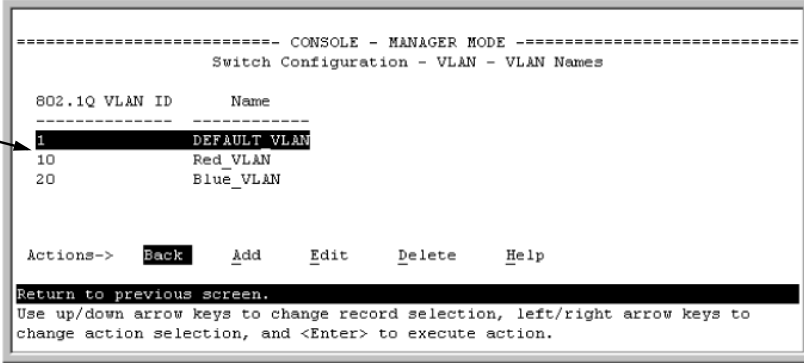
- VLANs assigned to ports Y1 - Y4 can be untagged because there is only one VLAN assignment per port. Devices connected to these ports do not have to be 802.1Q-compliant.
- Because both the Red VLAN and the Green VLAN are assigned to port Y5, at least one of the VLANs must be tagged for this port.

In both switches:

- The ports on the link between the two switches must be configured the same. As shown in [Example 42 "VLAN ID numbers assigned in the VLAN names screen"](#), the Red VLAN must be untagged on port X7 and Y5 and the Green VLAN must be tagged on port X7 and Y5, or vice-versa.

**NOTE:** Each 802.1Q-compliant VLAN must have its own unique VID number and that VLAN must be given the same VID in every device where configured. That is, if the Red VLAN has a VID of 10 in switch X, then 10 must also be the Red VID in switch Y.

## Example 42 VLAN ID numbers assigned in the VLAN names screen



```

----- CONSOLE - MANAGER MODE -----
Switch Configuration - VLAN - VLAN Names

802.1Q VLAN ID      Name
-----
1                   DEFAULT_VLAN
10                  Red_VLAN
20                  Blue_VLAN

Actions->  Back   Add   Edit   Delete   Help

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

### VLAN tagging considerations:

- Since the purpose of VLAN tagging is to allow multiple VLANs on the same port, any port that has only one VLAN assigned to it can be configured as "Untagged" (the default) if the authorized inbound traffic for that port arrives untagged.
- Any port with two or more VLANs of the same type can have one such VLAN assigned as "Untagged." All other VLANs of the same type must be configured as "Tagged," that is:

Port-Based VLANs	Protocol VLANs
A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged.	A port can be an untagged member of one protocol-based VLAN of each protocol type. When assigning a port to multiple, protocol-based VLANs sharing the same type, the port can be an untagged member of only one such VLAN.
A port can be a tagged member of any port-based VLAN.	A port can be a tagged member of any protocol-based VLAN. See above.
<p><b>NOTE:</b> A given VLAN must have the same VID on all 802.1Q-compliant devices in which the VLAN occurs. Also, the ports connecting two 802.1Q devices should have identical VLAN configurations.</p>	

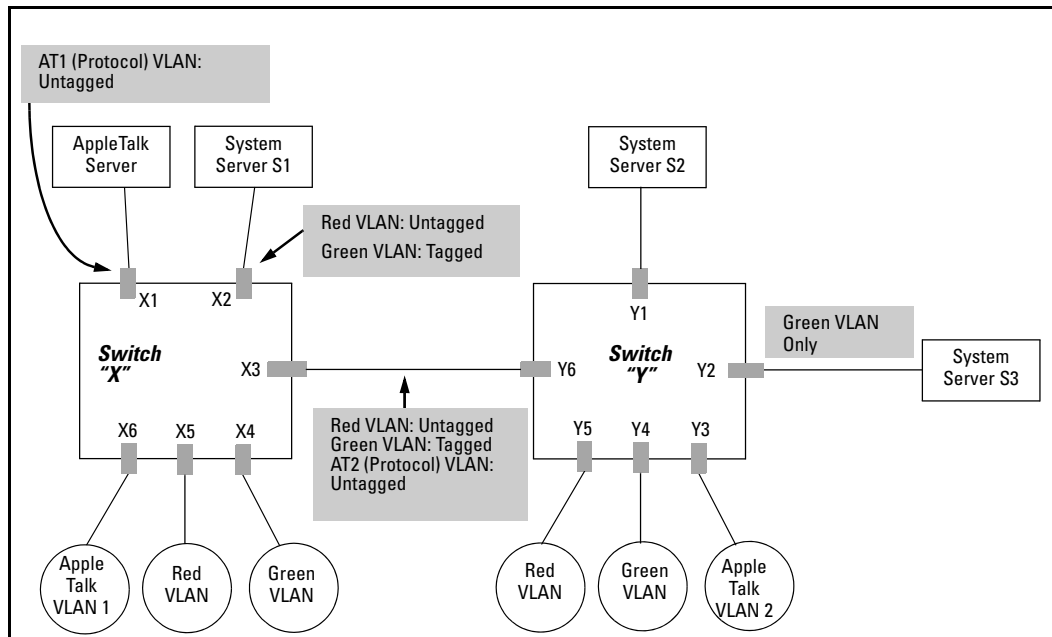
- If all end nodes on a port comply with the 802.1Q standard and are configured to use the correct VID, you can configure all VLAN assignments on a port as "Tagged" if doing so either makes it easier to manage your VLAN assignments, or if the authorized, inbound traffic for all VLANs on the port will be tagged.

For a summary and flowcharts of untagged and tagged VLAN operation on inbound traffic, see the following under "VLAN Operating Rules" (page 44):

- "Inbound Tagged Packets"
- "Untagged Packet Forwarding" and [Figure 9 \(page 47\)](#)
- "Tagged Packet Forwarding" and [Figure 10 \(page 48\)](#)

### Example 43 Networked 802.1Q-compliant devices with multiple VLANs on some ports

In the following network, switches X and Y and servers S1, S2 and the AppleTalk server are 802.1Q-compliant. (Server S3 could also be 802.1Q-compliant, but it makes no difference for this example.) This network includes both protocol-based (AppleTalk) VLANs and port-based VLANs.



- The VLANs assigned to ports X4 - X6 and Y2 - Y5 can all be untagged because there is only one VLAN assigned per port.
- Port X1 has two AppleTalk VLANs assigned, which means that one VLAN assigned to this port can be untagged and the other must be tagged.
- Ports X2 and Y1 have two port-based VLANs assigned, so one can be untagged and the other must be tagged on both ports.
- Ports X3 and Y6 have two port-based VLANs and one protocol-based VLAN assigned. Thus, one port-based VLAN assigned to this port can be untagged and the other must be tagged. Also, since these two ports share the same link, their VLAN configurations must match.

Switch X					Switch Y				
Port	AT-1 VLAN	AT-2 VLAN	Red VLAN	Green VLAN	Port	AT-1 VLAN	AT-2 VLAN	Red VLAN	Green VLAN
X1	Untagged	Tagged	No <sup>1</sup>	No <sup>1</sup>	Y1	No <sup>1</sup>	No <sup>1</sup>	Untagged	Tagged
X2	No <sup>1</sup>	No <sup>1</sup>	Untagged	Tagged	Y2	No <sup>1</sup>	No <sup>1</sup>	No <sup>1</sup>	Untagged
X3	No <sup>1</sup>	Untagged	Untagged	Tagged	Y3	No <sup>1</sup>	Untagged	No <sup>1</sup>	No <sup>1</sup>
X4	No <sup>1</sup>	No <sup>1</sup>	No <sup>1</sup>	Untagged	Y4	No <sup>1</sup>	No <sup>1</sup>	No <sup>1</sup>	Untagged
X5	No <sup>1</sup>	No <sup>1</sup>	Untagged	No <sup>1</sup>	Y5	No <sup>1</sup>	No <sup>1</sup>	Untagged	No <sup>1</sup>
X6	Untagged	No <sup>1</sup>	No <sup>1</sup>	No <sup>1</sup>	Y6	No	Untagged	Untagged	Tagged

<sup>1</sup> No means the port is not a member of that VLAN. For example, port X3 is not a member of the Red VLAN and does not carry Red VLAN traffic. Also, if GVRP were enabled (port-based only), Auto would appear instead of No.

**NOTE:** VLAN configurations on ports connected by the same link must match. Because ports X2 and Y5 are opposite ends of the same point-to-point connection, both ports must have the same VLAN configuration, configuring the Red VLAN as "Untagged" and the Green VLAN as "Tagged."

## Special VLAN types

### VLAN support and the default VLAN

In the factory default configuration, VLAN support is enabled and all ports on the switch belong to the port-based, default VLAN (named `DEFAULT_VLAN`). This places all ports in the switch into one physical broadcast domain. In the factory-default state, the default VLAN is also the Primary VLAN.

- You can partition the switch into multiple virtual broadcast domains by configuring one or more additional VLANs and moving ports from the default VLAN to the new VLANs.
- The switch supports up to 2048 static and dynamic VLANs, with VIDs numbered up to 4094. You can change the name of the default VLAN, but not its VID, which is always 1.
- You can remove all ports from the default VLAN by placing them in another port-based VLAN, but this VLAN remains and cannot be deleted from the switch.

For details on port VLAN settings, see [“Configuring static VLAN per-port settings \(CLI\)”](#) (page 30).

### The primary VLAN

As certain features and management functions run on only one VLAN in the switch and because DHCP and Bootp can run per-VLAN, there is a need for a dedicated VLAN to manage these features and ensure that multiple instances of DHCP or Bootp on different VLANs do not result in conflicting configuration values for the switch.

The Primary VLAN is the VLAN the switch uses to run and manage these features and data. In the factory-default configuration, the switch designates the default VLAN (`DEFAULT_VLAN`; VID=1) as the Primary VLAN. However you can designate another static, port-based VLAN as primary.

To summarize, designating a non-default VLAN as primary means that:

- The switch reads DHCP responses on the Primary VLAN instead of on the default VLAN. This includes such DHCP-resolved parameters as the TimeP server address, Default TTL and IP addressing—including the Gateway IP address—when the switch configuration specifies DHCP as the source for these values.
- The default VLAN continues to operate as a standard VLAN you cannot delete it or change its VID.
- Any ports not specifically assigned to another VLAN will remain assigned to the Default VLAN, even if it is the Primary VLAN.

Candidates for Primary VLAN include any static, port-based VLAN currently configured on the switch.

Protocol-Based VLANs and dynamic (GVRP-learned) VLANs that have not been converted to a static VLAN cannot be the Primary VLAN. To display the current Primary VLAN, use the CLI `show vlan` command.

---

**NOTE:** If you configure a non-default VLAN as the Primary VLAN, you cannot delete that VLAN unless you first select a different VLAN to serve as primary.

If you manually configure a gateway on the switch, it ignores any gateway address received via DHCP or Bootp.

To change the Primary VLAN configuration, see [“Changing VLAN support settings \(Menu\)”](#) (page 27).

---

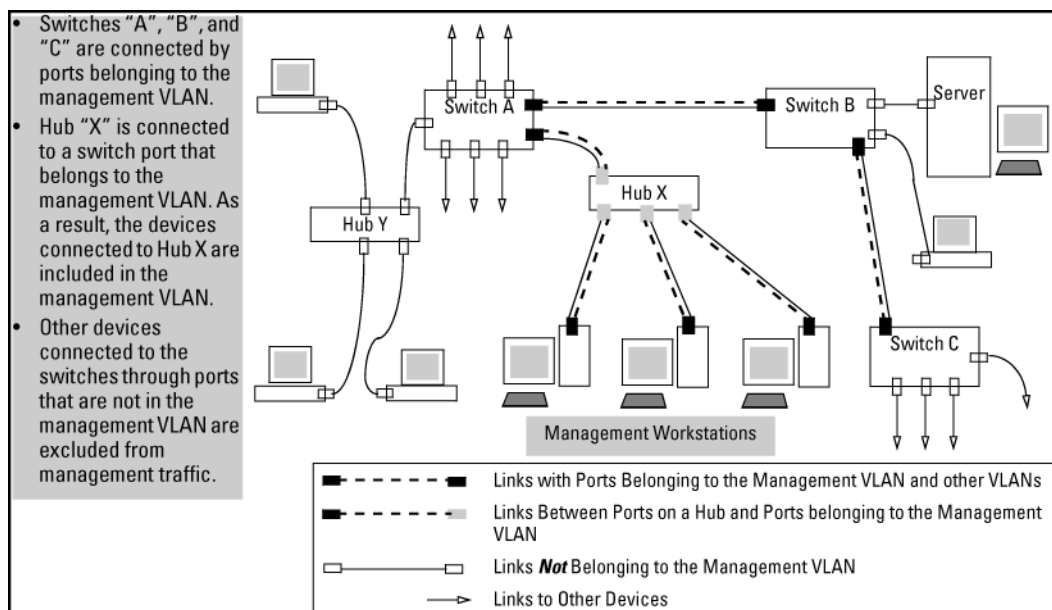
## The secure Management VLAN

Configuring a secure Management VLAN creates an isolated network for managing the HP switches that support this feature. Access to a secure Management VLAN and the switch's management functions (Menu and CLI), is available only through ports configured as members.

- Multiple ports on the switch can belong to the Management VLAN. This allows connections for multiple management stations to the Management VLAN, while allowing Management VLAN links between switches configured for the same Management VLAN.
- Only traffic from the Management VLAN can manage the switch, which means that only the workstations and PCs connected to ports belonging to the Management VLAN can manage and reconfigure the switch.

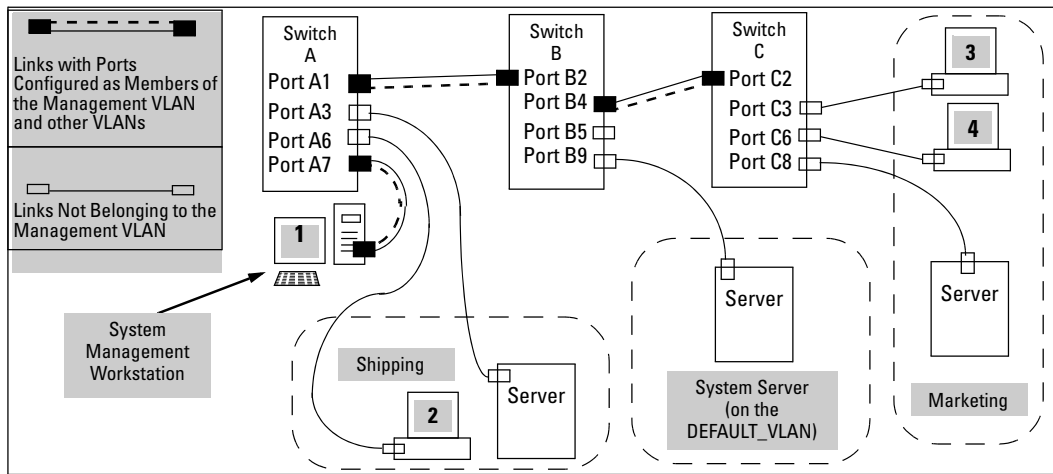
### Example 44 Potential security breaches in a network

This illustrates use of the Management VLAN feature to support management access by a group of management workstations.



### Example 45 Management VLAN control in a LAN

In this example, Workstation 1 has management access to all three switches through the Management VLAN, while the PCs do not. This is because configuring a switch to recognize a Management VLAN automatically excludes attempts to send management traffic from any other VLAN.



**Table 5 VLAN membership in Example 45 “Management VLAN control in a LAN”**

Switch	A1	A3	A6	A7	B2	B4	B5	B9	C2	C3	C6	C8
Management VLAN (VID = 7)	Y	N	N	Y	Y	Y	N	N	Y	N	N	N
Marketing VLAN (VID = 12)	N	N	N	N	N	N	N	N	N	Y	Y	Y
Shipping Dept. VLAN (VID = 20)	N	Y	Y	N	N	N	N	N	N	N	N	N
DEFAULT-VLAN (VID = 1)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

See “Configuring a secure Management VLAN (CLI)” (page 37) for configuration details.

### Operating notes for Management VLANs

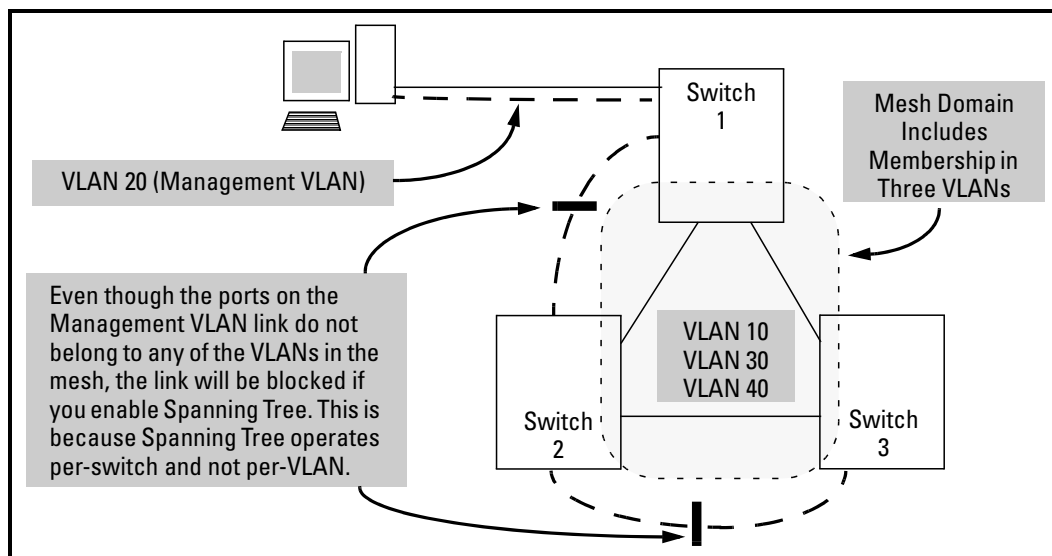
- Use only a static, port-based VLAN for the Management VLAN.
- The Management VLAN feature applies to both IPv4 and IPv6 traffic.
- The Management VLAN does not support IGMP operation.
- Routing between the Management VLAN and other VLANs is not allowed.
- If there are more than 25 VLANs configured on the switch, reboot the switch after configuring the Management VLAN.
- If you implement a Management VLAN in a switch mesh environment, all meshed ports on the switch will be members of the Management VLAN.
- Only one Management VLAN can be active in the switch. If one Management VLAN VID is saved in the startup-config file and you configure a different VID in the running-config file, the switch uses the running-config version until you either use the `write-memory` command or reboot the switch.
- During a Telnet session to the switch, if you configure the Management VLAN to a VID that excludes the port through which you are connected to the switch, you will continue to have access only until you terminate the session by logging out or rebooting the switch.

**NOTE:** The Management VLAN feature does not control management access through a direct connection to the switch's serial port.

- During a WebAgent session, if you configure the Management VLAN to a VID that excludes the port through which you are connected to the switch, you will continue to have access only until you close the browser session or reboot the switch.

- Enabling Spanning Tree between a pair of switches where there are multiple links using separate VLANs, including the Management VLAN, will force the blocking of one or more links. This may include the link carrying the Management VLAN, which will cause loss of management access to some devices. This can also occur where meshing is configured and the Management VLAN is configured on a separate link.
- Monitoring Shared Resources: The Management VLAN feature shares internal switch resources with several other features. The switch provides ample resources for all features. However, if the internal resources become fully subscribed, the Management VLAN feature cannot be configured until the necessary resources are released from other uses. For information on determining the current resource availability and usage, see the appendix titled "Monitoring Resources" in the *Management and Configuration Guide* for your switch.

### Example 46 Inadvertently blocking a Management VLAN link by implementing spanning tree



## Voice VLANs

Configuring voice VLANs separates voice traffic from data traffic and shields your voice traffic from broadcast storms.

### Operating rules for voice VLANs

- You must statically configure voice VLANs. GVRP and dynamic VLANs do not support voice VLAN operation.
- Configure all ports in a voice VLAN as tagged members of the VLAN. This ensures retention of the QoS (Quality of Service) priority included in voice VLAN traffic moving through your network.
- If a telephone connected to a voice VLAN includes a data port used for connecting other networked devices (such as PCs) to the network, then you must configure the port as a tagged member of the voice VLAN and a tagged or untagged member of the data VLAN you want the other networked device to use.



## Components of voice VLAN operation

- Voice VLAN: Configure one or more voice VLANs on the switch. Some reasons for having multiple voice VLANs include:
  - Employing telephones with different VLAN requirements
  - Better control of bandwidth usage
  - Segregating telephone groups used for different, exclusive purposes

Where multiple voice VLANs exist on the switch, you can use routing to communicate between telephones on different voice VLANs.

- Tagged/Untagged VLAN Membership: If the appliances using a voice VLAN transmit tagged VLAN packets, then configure the member ports as tagged members of the VLAN. Otherwise, configure the ports as untagged members.

## Voice VLAN access security

You can use port security configured on an individual port or group of ports in a voice VLAN. That is, you can allow or deny access to a phone having a particular MAC address. See chapter titled "Configuring and Monitoring Port Security" in the *Access Security Guide* for your switch.

---

**NOTE:** MAC authentication is not recommended in voice VLAN applications.

---

## Effects of VLANs on other switch features

### Spanning Tree operation with VLANs

Depending on the spanning tree option configured on the switch, the spanning tree feature may operate as:

- A single instance across all ports on the switch regardless of VLAN assignments
- Multiple instances per-VLAN

For single-instance operation, if redundant physical links exist between the switch and another 802.1Q device, all but one link will be blocked, even if the redundant links are in separate VLANs. In this case you can use port trunking to prevent Spanning Tree from unnecessarily blocking ports (and to improve overall network performance). For multiple-instance operation, physically redundant links belonging to different VLANs can remain open. For more information, see "[Multiple instance spanning tree operation](#)" (page 86).

---

**NOTE:** Spanning Tree operates differently in different devices. For example, in the (obsolete, non-802.1Q) HP Switch 2000 and the HP Switch 800T, Spanning Tree operates per-VLAN, allowing redundant physical links as long as they are in separate VLANs.

---

## Spanning Tree operates differently in different devices

### IP interfaces

There is a one-to-one relationship between a VLAN and an IP network interface. Since the VLAN is defined by a group of ports, the state (up/down) of those ports determines the state of the IP network interface associated with that VLAN. When a port-based VLAN or an IPv4 or IPv6 protocol-based VLAN comes up because one or more of its ports is up, the IP interface for that VLAN is also activated. Likewise, when a VLAN is deactivated because all of its ports are down, the corresponding IP interface is also deactivated.

### VLAN MAC address

The switches have one unique MAC address for all of their VLAN interfaces. You can send an 802.2 test packet to this MAC address to verify connectivity to the switch and you can assign an

IP address to the VLAN interface. When you Ping that address, ARP will resolve the IP address to this single MAC address.

In a topology where a switch has multiple VLANs and must be connected to a device having a single forwarding database, such as the Switch 4000M, some cabling restrictions apply. For more on this topic, see [“Multiple VLAN considerations” \(page 48\)](#).

## Port trunks

When assigning a port trunk to a VLAN, all ports in the trunk are automatically assigned to the same VLAN. Do not split trunk members across multiple VLANs. A port trunk is tagged, untagged, or excluded from a VLAN the same way as individual, untrunked ports.

## Port monitoring

If you designate a port on the switch for network monitoring, the port will appear in the PortVLAN Assignment screen and can be configured as a member of any VLAN. For information on how broadcast, multicast and unicast packets are tagged inside and outside of the VLAN to which the monitor port is assigned, see the section titled "VLAN-Related Problems" in the "Troubleshooting" appendix of the *Management and Configuration Guide* for your switch.

## Jumbo packet support

Jumbo packet support is enabled per-VLAN and applies to all ports belonging to the VLAN. For more information, see the chapter titled "Port Traffic Controls" in the *Management and Configuration Guide* for your switch.

## VLAN restrictions

- A port must be a member of at least one VLAN. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT\_VLAN; VID=1).
- A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged. The "Untagged" designation enables VLAN operation with non 802.1Q-compliant devices.
- A port can be an untagged member of one protocol-based VLAN of each protocol type. When assigning a port to multiple, protocol-based VLANs sharing of the same type, note that the port can be an untagged member of only one such VLAN.
- With routing enabled on the switch, the switch can route traffic between:
  - Multiple, port-based VLANs
  - A port-based VLAN and an IPv4 protocol-based VLAN
  - A port-based VLAN and an IPv6 protocol-based VLAN
  - An IPv4 protocol-based VLAN and an IPv6 protocol VLAN

Other, routable, protocol-based VLANs must use an external router to move traffic between VLANs. With routing disabled, all routing between VLANs must be through an external router.

- Before deleting a static VLAN, first re-assign all ports in the VLAN to another VLAN. You can use the `no vlan <vid>` command to delete a static VLAN. For more information, see [“Creating a new static VLAN \(port-based or protocol-based\) \(CLI\)” \(page 28\)](#).
- Protocol-based VLANs, port-based VLANs and LLDP radio port VLANs cannot run concurrently with RPVST+.

## Migrating Layer 3 VLANs using VLAN MAC configuration

HP switches provide for maintaining Layer 3 VLAN configurations when migrating distribution routers in networks not centrally managed, by configuring the MAC address of the previous router on the VLAN interfaces of the HP routing switch.

## VLAN MAC address reconfiguration

HP switches use one unique MAC address for all VLAN interfaces. If you assign an IP address to a VLAN interface, ARP resolves the IP address to the MAC address of the routing switch for all incoming packets.

The Layer 3 VLAN MAC Configuration feature lets you reconfigure the MAC address used for VLAN interfaces, using the CLI. Packets addressed to the reconfigured Layer 3 MAC address, such as ARP and IP data packets, are received and processed by the HP routing switch.

Packets transmitted from the routing switch (packets originating from the router and forwarded packets) use the original HP Switch MAC address as the source MAC address in Ethernet headers.

ARP reply packets use the reconfigured MAC address in both the:

- ARP Sender MAC address field
- Source MAC address field in the Ethernet frame header

When reconfiguring the MAC address, you may specify a keepalive timeout to transmit heartbeat packets that advertise the new MAC address

By configuring the MAC address of the previously installed router as the MAC address of each VLAN interface on an HP Switch, you can swap the physical port of a router to the HP Switch after the switch has been properly configured in the network.

## Handling incoming and outgoing VLAN Traffic

### Incoming VLAN data packets and ARP requests

These are received and processed on the routing switch according to the MAC address of the previously installed router configured for each VLAN interface.

### Outgoing VLAN traffic

This uses the MAC address of the HP Sswitch as the source MAC address in packet headers. The MAC address configured on VLAN interfaces is not used on outbound VLAN traffic.

When the routing switch receives an ARP request for the IP address configured on a VLAN interface, the ARP reply uses the reconfigured MAC address in both the:

- ARP Sender MAC address field
- Source MAC address field in the Ethernet frame header

When proxy ARP is enabled on a VLAN interface, the "gracious" ARP reply sent for an ARP request received from VLAN devices located outside the directly connected IP subnets also contains the reconfigured MAC address in both the:

- ARP Sender MAC address field
- Source MAC address field in the Ethernet frame header

To hosts in the network, VLAN traffic continues to be routed (using the reconfigured MAC address as destination address), but outbound VLAN traffic appears to be sent from another router attached to the same subnet (using the HP Switch MAC address as source address) attached to the same subnet. Although it appears as an asymmetric path to network hosts, the MAC address configuration feature enables Layer 3 VLAN migration. (A successful VLAN migration is achieved because the hosts do not verify that the source MAC address and the destination MAC address are the same when communicating with the routing switch.)

## Sending heartbeat packets with a configured MAC Address

On the VLAN interfaces of a routing switch, the user-defined MAC address only applies to inbound traffic. As a result, any connected switches need to learn the new address that is included in the Ethernet frames of outbound VLAN traffic transmitted from the routing switch.

If a connected switch does not have the newly configured MAC address of the routing switch as a destination in its MAC address table, it floods packets to all of its ports until a return stream allows the switch to learn the correct destination address. As a result, the performance of the switch is degraded as it tries to send Ethernet packets to an unknown destination address.

To allow connected switches to learn the user-configured MAC address of a VLAN interface, the HP routing switch can send periodic heartbeat-like Ethernet packets. The Ethernet packets contain the configured MAC address as the source address in the packet header. IP multicast packets or Ethernet service frames are preferred because they do not interrupt the normal operation of client devices connected on the segment.

Because the aging time of destination addresses in MAC address tables varies on network devices, you must also configure a time interval to use for sending heartbeat packets.

Heartbeat packets are sent at periodic intervals with a specific HP Switch unicast MAC address in the destination field. This MAC address is assigned to the HP Switch and is not used by other non-HP routers. Because the heartbeat packet contains a unicast MAC address, it does not interrupt host operation. Even if you have multiple 1-65 Static Virtual LANs (VLANs) Introducing tagged VLAN technology into networks running untagged VLANs HP switches connected to the network, there is no impact on network performance because each switch sends heartbeat packets with its configured MAC address as the destination address.

The format of a heartbeat packet is an extended Ethernet OUI frame with an extended OUI Ethertype (88B7) and a new protocol identifier in the 5-octet protocol identifier field.

## 2 GVRP

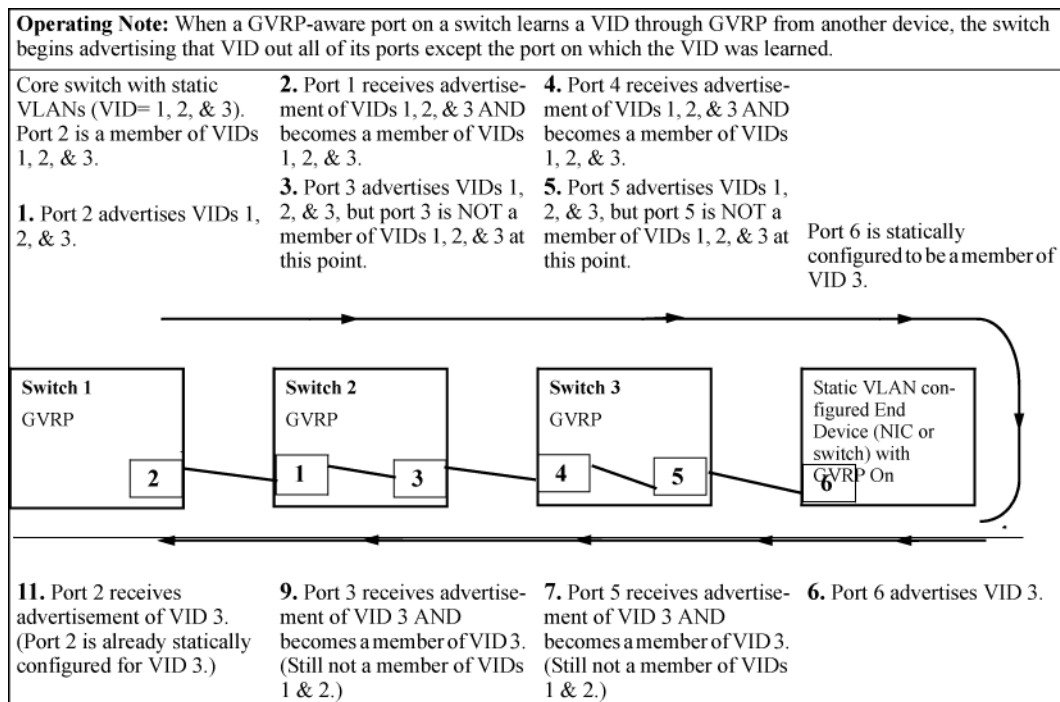
Command syntax	Description	Default	CLI reference page	Menu reference page
<code>show gvrp</code>	Shows whether GVRP is disabled and the current settings for the maximum number of VLANs and the current Primary VLAN.		<a href="#">62</a>	<a href="#">64</a>
<code>show vlans</code>	Lists static and dynamic VLANs on a GVRP-enabled switch.		<a href="#">66</a>	
<code>gvrp</code> <code>no gvrp</code>	Enables or disables GVRP on the switch	Disabled	<a href="#">65</a>	<a href="#">64</a>
<code>interface &lt;port-list&gt; unknown-vlans [ &lt;learn&gt;   &lt;block&gt;   &lt;disable&gt; ]</code>	Controls how individual ports handle advertisements for new VLANs	Learn	<a href="#">65</a>	<a href="#">64</a>
<code>static &lt;dynamic-vlan-id&gt;</code>	Converts a dynamic VLAN to a static VLAN		<a href="#">67</a>	

### Using GVRP

When GVRP is enabled on a switch, the VID for any static VLAN configured on the switch is advertised, using BPDUs (Bridge Protocol Data Units), out all ports regardless of whether a port is up or assigned to any particular VLAN. A GVRP-aware port on another device that receives the advertisements over a link can dynamically join the advertised VLAN.

A dynamic VLAN (that is, a VLAN learned through GVRP) is tagged on the port on which it was learned. Also, a GVRP-enabled port can forward an advertisement for a VLAN it learned about from other ports on the same switch (internal source), but the forwarding port will not itself join that VLAN until an advertisement for that VLAN is received through a link from another device (external source) on that specific port.

**Figure 12 Forwarding advertisements and dynamic joining**



If a static VLAN is configured on at least one switch port and that port has established a link with another device, then all other ports of that switch will send advertisements for that VLAN.

**NOTE:** A port can learn of a dynamic VLAN through devices that are not aware of GVRP. VLANs must be disabled in GVRP-unaware devices to allow tagged packets to pass through.

## Planning for GVRP operation

To set up dynamic VLANs for a segment:

1. Determine the VLAN topology required for each segment (broadcast domain) on the network.
2. Determine which VLANs must be static and which can be dynamically propagated.
3. Determine the devices on which static VLANs must be manually created to propagate VLANs throughout the segment.
4. Determine security boundaries and how individual ports in the segment are to handle dynamic VLAN advertisements (see [Table 6 \(page 66\)](#) and [Table 7 \(page 71\)](#)).
5. Enable GVRP on all devices to be used with dynamic VLANs and configure the appropriate "Unknown VLAN" parameter (Learn, Block, or Disable) for each port.
6. Configure static VLANs on the switches, where needed, with their per-VLAN parameters (Tagged, Untagged, Auto and Forbid—see [Table 7 \(page 71\)](#)) on each port.
7. Dynamic VLANs will then appear automatically, according to the chosen configuration options.
8. Convert dynamic VLANs to static VLANs, where dynamic VLANs are to become permanent.

## Displaying switch current GVRP configuration (CLI)

### Syntax:

```
show gvrp
```

Shows GVRP status (enabled or disabled), current maximum number of VLANs supported and the current Primary VLAN.

## Example 47 Displaying GVRP status with GVRP disabled

---

```
HP Switch(config)#: show gvrp

GVRP support

Maximum VLANs to support [256] : 256
Primary VLAN : DEFAULT_VLAN
GVRP Enabled [No] : No
```

---

## Example 48 Displaying GVRP status with GVRP enabled

---

This example shows the output for the `show gvrp` command with GVRP enabled. It includes non-default settings for the Unknown VLAN field for some ports (see Port number 3, 4, 5 below).

```
HP Switch(config)#: show gvrp

GVRP support

Maximum VLANs to support [256] : 256
Primary VLAN : DEFAULT_VLAN
GVRP Enabled [No] : Yes
```

Port	Type	Unknown VLAN	Join	Leave	Leaveall
1	10/100TX	Learn	20	300	1000
2	10/100TX	Learn	20	300	1000
3	10/100TX	Block	20	300	1000
4	10/100TX	Disable	20	300	1000
5	10/100TX	Disable	20	300	1000
6	10/100TX	Learn	20	300	1000
7	10/100TX	Learn	20	300	1000

---

## Displaying switch current GVRP configuration (CLI)

### Syntax:

```
show gvrp
```

Shows GVRP status (enabled or disabled), current maximum number of VLANs supported and the current Primary VLAN.

## Example 49 Displaying GVRP status with GVRP disabled

```
HP Switch(config)#: show gvrp

GVRP support

Maximum VLANs to support [256] : 256
Primary VLAN : DEFAULT_VLAN
GVRP Enabled [No] : No
```

## Example 50 Displaying GVRP status with GVRP enabled

This example shows the output for the `show gvrp` command with GVRP enabled. It includes non-default settings for the Unknown VLAN field for some ports (see Port number 3, 4, 5 below).

```
HP Switch(config)#: show gvrp

GVRP support

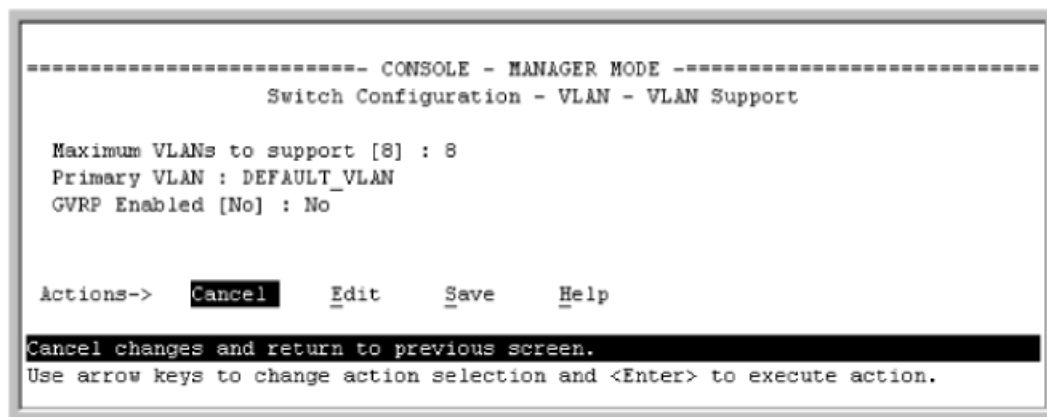
Maximum VLANs to support [256] : 256
Primary VLAN : DEFAULT_VLAN
GVRP Enabled [No] : Yes
```

Port	Type	Unknown VLAN	Join	Leave	Leaveall
1	10/100TX	Learn	20	300	1000
2	10/100TX	Learn	20	300	1000
3	10/100TX	Block	20	300	1000
4	10/100TX	Disable	20	300	1000
5	10/100TX	Disable	20	300	1000
6	10/100TX	Learn	20	300	1000
7	10/100TX	Learn	20	300	1000

## Viewing and configuring GVRP (Menu)

1. From the Main Menu, select: **2. Switch Configuration** ⇒ **8. VLAN Menu** ⇒ **1. VLAN Support**

Figure 13 The VLAN Support screen (default configuration)



2. Do the following to enable GVRP and display the Unknown VLAN fields:
  - a. Press **E** (for Edit).
  - b. Use **↓** to move the cursor to the **GVRP Enabled** field.
  - c. Press the Space bar to select **Yes**.
  - d. Press **↓** again to display the **Unknown VLAN** fields.



## Example 51 Default settings for handling advertisements

The Unknown VLAN fields enable you to configure each port to:

- **Learn** - Dynamically join any advertised VLAN and advertise all VLANs learned through other ports.
- **Block** - Do not dynamically join any VLAN, but still advertise all VLANs learned through other ports.
- **Disable** - Ignore and drop all incoming advertisements and do not transmit any advertisements.

```
----- CONSOLE - MANAGER MODE -----
Switch Configuration - VLAN - VLAN Support
Maximum VLANs to support [8] : 8
Primary VLAN : DEFAULT_VLAN
GVRP Enabled [No] : Yes

Port      Type      Unknown VLAN | Port      Type      Unknown VLAN
-----+-----+-----+-----+-----+-----
A1      10/100TX | Learn     | A8      10/100TX | Learn
A2      10/100TX | Learn     | A9      10/100TX | Learn
A3      10/100TX | Learn     | A10     10/100TX | Learn
A4      10/100TX | Learn     | A11     10/100TX | Learn
A5      10/100TX | Learn     | A12     10/100TX | Learn
A6      10/100TX | Learn     | A13     10/100TX | Learn
A7      10/100TX | Learn     | A14     10/100TX | Learn

Actions->  Cancell  Edit    Save    Help
-----+-----+-----+-----+-----+-----
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

3. Use the arrow keys to select the port you want and the Space bar to select the Unknown VLAN option for any ports you want to change.
4. When you finish making configuration changes, press **Enter**, then **S** (for Save) to save your changes to the Startup-Config file.

To view or configure static VLANs for GVRP operation, see “VLAN Operating Rules” (page 44)

## Enabling and disabling GVRP on the switch (CLI)

### Syntax:

```
gvrp
```

Enables GVRP on the switch.

```
no gvrp
```

Disables GVRP on the switch.

**NOTE:** GVRP can be enabled only if `max-vlans` is set to no more than 256 VLANs. While GVRP is enabled on the switch, you cannot apply any ACLs to VLANs configured on the same switch. A GVRP link can include intermediate devices that are not GVRP-aware. To understand and use GVRP, you need a working knowledge of 802.1Q VLAN tagging. See “802.1Q VLAN tagging” (page 49).

GVRP assigns dynamic VLANs as Tagged VLANs. To configure the VLAN as Untagged, you must first convert it to a static VLAN.

A VLAN enabled for jumbo traffic cannot be used to create a dynamic VLAN. A port belonging to a statically configured, jumbo-enabled VLAN cannot join a dynamic VLAN.

## Controlling how individual ports handle advertisements for new VLANs (CLI)

When GVRP is enabled on the switch, use the `unknown-vlans` command to change the Unknown VLAN field for one or more ports.

### Syntax:

```
interface <port-list> unknown-vlans [ <learn | <block> | <disable> ]
```

Changes the Unknown VLAN field in order to control how one or more ports handle advertisements. Use at either the Manager or interface context level for a port.

## Example 52 Changing the Unknown VLANs field

In the following example, the first command changes the configuration to Block, the second command displays the new configuration:

```
HP Switch(config)#: interface 1-2 unknown-vlans block
```

```
Switch(config)#: show gvrp
GVRP support
Maximum VLANs to support [256] : 256
Primary VLAN : DEFAULT_VLAN
GVRP Enabled [No] : Yes

Port Type          | Unknown VLAN Join  Leave  Leaveall
-----+-----
1   10/100TX       | Block             20    300    1000
2   10/100TX       | Block             20    300    1000
3   10/100TX       | Learn             20    300    1000
4   10/100TX       | Learn             20    300    1000
```

When you enable GVRP on a switch, you have the per-port join-request options listed in the following table:

**Table 6 Options for handling unknown VLAN advertisements**

Unknown VLAN Mode	Operation
Learn (the Default)	Enables the port to become a member of any unknown VLAN for which it receives an advertisement. Allows the port to advertise other VLANs that have at least one other port on the same switch as a member.
Block	Prevents the port from joining any new dynamic VLANs for which it receives an advertisement. Allows the port to advertise other VLANs that have at least one other port as a member.
Disable	Causes the port to ignore and drop all GVRP advertisements it receives and prevents the port from sending any GVRP advertisements.

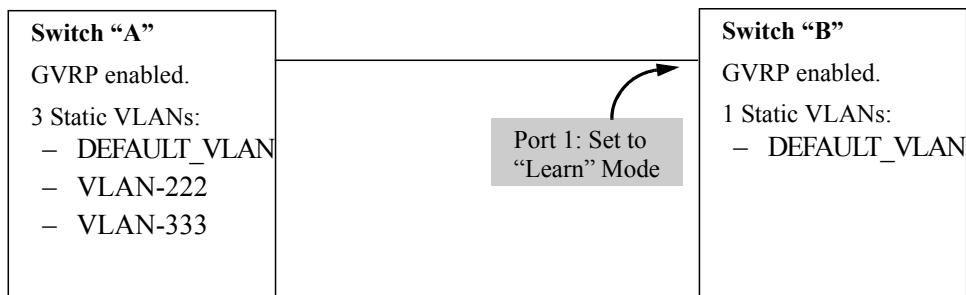
## Listing static and dynamic VLANs on a GVRP-enabled switch (CLI)

### Syntax:

```
show vlans
    Lists all VLANs present in the switch.
```

### Example 53 Using the `show vlans` command

In the following illustration, switch B has one static VLAN (the default VLAN), with GVRP enabled and port 1 configured to Learn for Unknown VLANs. Switch A has GVRP enabled and has three static VLANs: the default VLAN, VLAN-222 and VLAN-333. In this scenario, switch B will dynamically join VLAN-222 and VLAN-333:



The `show vlans` command lists the dynamic (and static) VLANs in switch B after it has learned and joined VLAN-222 and VLAN-333.

```
Switch-B> show vlans
```

```
Status and Counters - VLAN Information
```

```
VLAN support : Yes
Maximum VLANs to support : 8
Primary VLAN : DEFAULT_VLAN
```

802.1Q	VLAN ID	NAME	Status
1		DEFAULT_VLAN	Static
222		GVRP_222	Dynamic
333		GVRP_333	Dynamic

## Converting a Dynamic VLAN to a Static VLAN (CLI)

If a port on the switch has joined a dynamic VLAN, you can use the following command to convert that dynamic VLAN to a static VLAN:

```
static <dynamic-vlan-id>
```

### Example 54 Converting a dynamic VLAN 333 to a static VLAN

When converting a dynamic VLAN to a static VLAN as shown here, all ports on the switch are assigned to the VLAN in Auto mode.

```
HP Switch(config)#: static 333
```

## About GVRP

GVRP (GARP VLAN Registration Protocol) is an application of GARP (Generic Attribute Registration Protocol.) It enables a switch to dynamically create 802.1Q-compliant VLANs on links with other devices running GVRP and automatically create VLAN links between GVRP-aware devices. (A GVRP link can include intermediate devices that are not GVRP-aware.) This operation reduces the chance for errors in VLAN configurations by automatically providing VID (VLAN ID) consistency across the network. After the switch creates a dynamic VLAN, the CLI `static <vlan-id>` command can be used to convert it to a static VLAN. GVRP can also be used to dynamically enable port membership in static VLANs configured on a switch.

GVRP uses GVRP BPDUs (GVRP Bridge Protocol Data Units) to advertise static VLANs; this a GVRP BPDU is called an *advertisement*. On a switch, advertisements are sent outbound from ports to the devices directly connected to those ports.

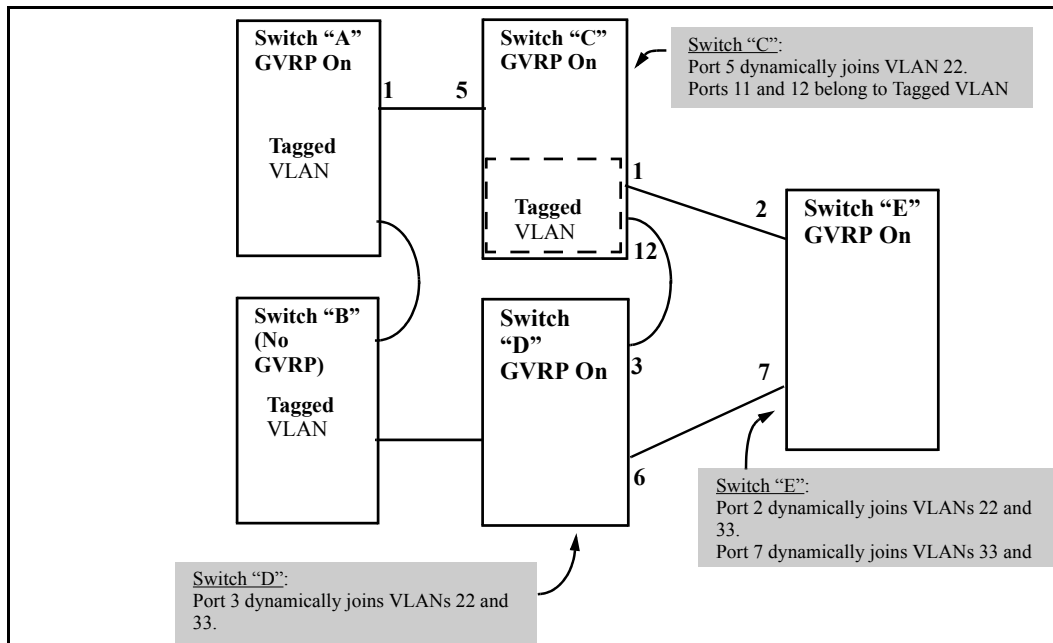
## GVRP operational rules

- A dynamic VLAN must be converted to a static VLAN before it can have an IP address.
- The total number of VLANs on the switch (static and dynamic combined) cannot exceed the current Maximum VLANs setting. For example, in the factory default state, the switch supports up to eight VLANs. Thus, where four static VLANs are configured on the switch, the switch can accept up to four additional VLANs in any static and dynamic combination. Any additional VLANs advertised to the switch will not be added unless you first increase the Maximum VLANs setting. In the Menu interface, click on **2. Switch Configuration ... | 8. VLAN Menu | 1. VLAN Support**. In the global config level of the CLI, use **max-vlans**.
- Converting a dynamic VLAN to a static VLAN and then executing the `write memory` command saves the VLAN in the startup-config file and makes it a permanent part of the switch's VLAN configuration.
- Within the same broadcast domain, a dynamic VLAN can pass through a device that is not GVRP-aware. This is because a half-duplex repeater, a hub or a switch that is not GVRP-aware will flood the GVRP (multicast) advertisement packets out all ports.
- GVRP assigns dynamic VLANs as Tagged VLANs. To configure the VLAN as Untagged, first convert it to a static VLAN.
- Rebooting a switch on which a dynamic VLAN exists deletes that VLAN. However, the dynamic VLAN reappears after the reboot if GVRP is enabled and the switch again receives advertisements for that VLAN through a port configured to add dynamic VLANs.
- By receiving advertisements from other devices running GVRP, the switch learns of static VLANs on those other devices and dynamically (automatically) creates tagged VLANs on the links to the advertising devices. Similarly, the switch advertises its static VLANs to other GVRP-aware devices, as well as the dynamic VLANs the switch has learned.
- A GVRP-enabled switch does not advertise any GVRP-learned VLANs out of the ports on which it originally learned of those VLANs.

## Example of GVRP operation

In the following example, Tagged VLAN ports on switch A and switch C advertise VLANs 22 and 33 to ports on other GVRP-enabled switches that can dynamically join the VLANs.

## Example 55 GVRP operation



## Options for a GVRP-aware port receiving advertisements

- If there is not already a static VLAN with the advertised VID on the receiving port, such a port can dynamically create the VLAN and become a member.
- If the switch already has a static VLAN assignment with the same VID as in the advertisement and the port is configured to `Auto` for that VLAN, then the port will dynamically join the VLAN and begin moving that VLAN's traffic. For more detail on `Auto`, see ["Per-port options for dynamic VLAN advertising and joining"](#) (page 70).
- Ignore the advertisement for that VID.
- Not participate in that VLAN.

## Options for a port belonging to a Tagged or Untagged static VLAN

- Send VLAN advertisements
- Receive advertisements for VLANs on other ports and dynamically join those VLANs.
- Send VLAN advertisements but ignore advertisements received from other ports.
- Avoid GVRP participation by not sending advertisements and dropping any advertisements received from other devices.

## IP addressing

A dynamic VLAN does not have an IP address and moves traffic on the basis of port membership in VLANs. However, after GVRP creates a dynamic VLAN, you can convert it to a static VLAN. Note that it is then necessary to assign ports to the VLAN in the same way that you would for a static VLAN created manually. In the static state you can configure IP addressing on the VLAN and access it in the same way that you would any other static VLAN.

## Per-port options for handling GVRP "unknown VLANs"

An "unknown VLAN" is a VLAN that the switch learns of by receiving an advertisement for that VLAN on a port that is not already a member of that VLAN. If the port is configured to learn

unknown VLANs, then the VLAN is dynamically created and the port becomes a tagged member of the VLAN.

### Example 56 GVRP unknown VLAN settings

Suppose that in [Example 55 \(page 69\)](#), port 1 on switch A is connected to port 5 on switch C. Because switch A has VLAN 22 statically configured, while switch C does not have this VLAN statically configured (and does not "Forbid" VLAN 22 on port 5), VLAN 22 is handled as an "Unknown VLAN" on port 5 in switch C. Conversely, if VLAN 22 was statically configured on switch C, but port 5 was not a member, port 5 would become a member when advertisements for VLAN 22 were received from switch A.

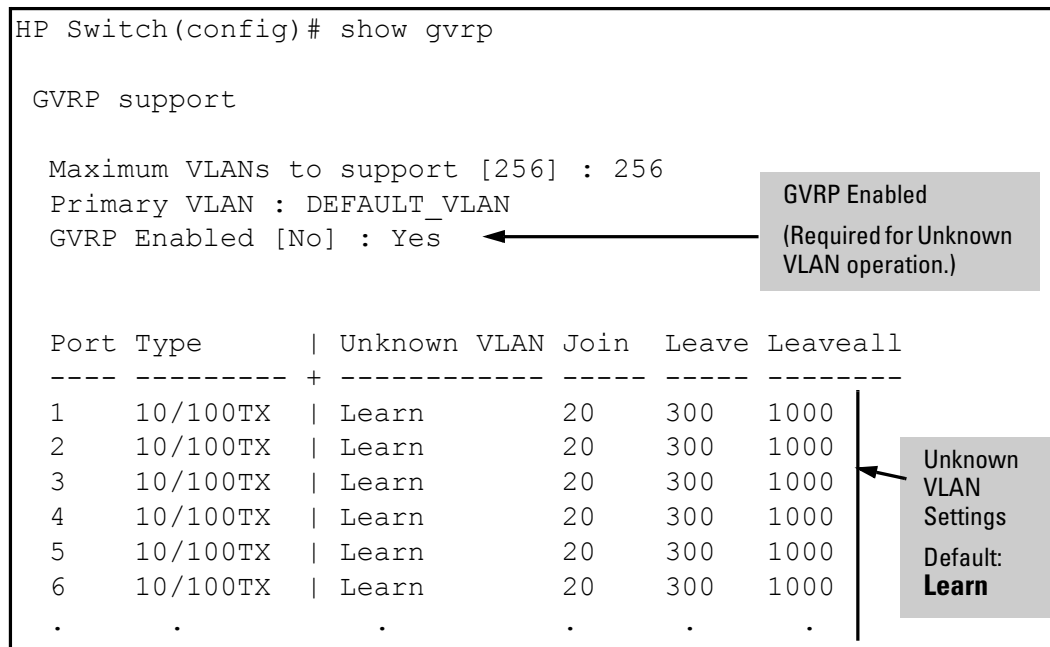
The CLI `show gvrp` command and the menu interface VLAN Support screen show a switch's current GVRP configuration, including the Unknown VLAN settings.

```
HP Switch(config)# show gvrp

GVRP support

Maximum VLANs to support [256] : 256
Primary VLAN : DEFAULT_VLAN
GVRP Enabled [No] : Yes

Port Type      | Unknown VLAN Join  Leave  Leaveall
-----+-----
1  10/100TX    | Learn           20    300    1000
2  10/100TX    | Learn           20    300    1000
3  10/100TX    | Learn           20    300    1000
4  10/100TX    | Learn           20    300    1000
5  10/100TX    | Learn           20    300    1000
6  10/100TX    | Learn           20    300    1000
.      .      | .              .    .    .
```



## Per-port options for dynamic VLAN advertising and joining

### Initiating advertisements

As described in the preceding section, to enable dynamic joins, GVRP must be enabled and a port must be configured to Learn (the default). However, to send advertisements in your network, one or more static (Tagged, Untagged, or Auto) VLANs must be configured on one or more switches (with GVRP enabled), depending on your topology.

### Enabling a port for dynamic joins

You can configure a port to dynamically join a static VLAN. The join will occur if that port subsequently receives an advertisement for the static VLAN. This is done by using the Auto and Learn options described in [Table 7 \(page 71\)](#).

### Parameters for controlling VLAN propagation behavior

You can configure an individual port to actively or passively participate in dynamic VLAN propagation or to ignore dynamic VLAN (GVRP) operation. These options are controlled by the GVRP "Unknown VLAN" and the static VLAN configuration parameters, as described in [Table 7 \(page 71\)](#).

**Table 7 Controlling VLAN behavior on ports with static VLANs**

Per-Port "Unknown VLAN" (GVRP) configuration	Static VLAN Options—Per VLAN Specified on Each Port <sup>1</sup>		
	Port Activity: Tagged or Untagged (Per VLAN) <sup>2</sup>	Port Activity: Auto <sup>2</sup> (Per VLAN)	Port Activity: Forbid (Per VLAN) <sup>2</sup>
Learn (the Default)	<p>The port:</p> <ul style="list-style-type: none"> <li>• Belongs to specified VLAN.</li> <li>• Advertises specified VLAN.</li> <li>• Can become a member of dynamic VLANs for which it receives advertisements.</li> <li>• Advertises dynamic VLANs that have at least one other port (on the same switch) as a member.</li> </ul>	<p>The port:</p> <ul style="list-style-type: none"> <li>• Will become a member of specified VLAN if it receives advertisements for specified VLAN from another device.</li> <li>• Will advertise specified VLAN.</li> <li>• Can become a member of other, dynamic VLANs for which it receives advertisements.</li> <li>• Will advertise a dynamic VLAN that has at least one other port (on the same switch) as a member.</li> </ul>	<p>The port:</p> <ul style="list-style-type: none"> <li>• Will not become a member of the specified VLAN.</li> <li>• Will not advertise specified VLAN.</li> <li>• Can become a member of other dynamic VLANs for which it receives advertisements.</li> <li>• Will advertise a dynamic VLAN that has at least one other port on the same switch as a member.</li> </ul>
Block	<p>The port:</p> <ul style="list-style-type: none"> <li>• Belongs to the specified VLAN.</li> <li>• Advertises this VLAN.</li> <li>• Will not become a member of new dynamic VLANs for which it receives advertisements.</li> <li>• Will advertise dynamic VLANs that have at least one other port as a member.</li> </ul>	<p>The port:</p> <ul style="list-style-type: none"> <li>• Will become a member of specified VLAN if it receives advertisements for this VLAN.</li> <li>• Will advertise this VLAN.</li> <li>• Will not become a member of new dynamic VLANs for which it receives advertisements.</li> <li>• Will advertise dynamic VLANs that have at least one other port (on the same switch) as a member.</li> </ul>	<p>The port:</p> <ul style="list-style-type: none"> <li>• Will not become a member of this VLAN.</li> <li>• Will ignore GVRP PDUs.</li> <li>• Will not join any dynamic VLANs.</li> <li>• Will not advertise VLANs.</li> </ul>
Disable	<p>The port:</p> <ul style="list-style-type: none"> <li>• Is a member of the specified VLAN.</li> <li>• Will ignore GVRP PDUs.</li> <li>• Will not join any advertised VLANs.</li> <li>• Will not advertise VLANs.</li> </ul>	<p>The port:</p> <ul style="list-style-type: none"> <li>• Will not become a member of the specified VLAN.</li> <li>• Will ignore GVRP PDUs.</li> <li>• Will not join any dynamic VLANs.</li> <li>• Will not advertise VLANs.</li> </ul>	<p>The port:</p> <ul style="list-style-type: none"> <li>• Will not become a member of this VLAN.</li> <li>• Will ignore GVRP PDUs.</li> <li>• Will not join any dynamic VLANs.</li> <li>• Will not advertise VLANs.</li> </ul>

<sup>1</sup> Each port of the switch must be a Tagged or Untagged member of at least one VLAN. Thus, any port configured for GVRP to Learn or Block will generate and forward advertisements for static VLAN(s) configured on the switch and also for dynamic VLANs the switch learns on other ports.

<sup>2</sup> To configure tagging, Auto, or Forbid, see [“Configuring static VLAN per-port settings \(CLI\)”](#) (page 30) (for the CLI) or [“Adding or changing a VLAN port assignment \(Menu\)”](#) (page 33) (for the menu).

As the preceding table indicates, when you enable GVRP, a port that has a Tagged or Untagged static VLAN has the option for both generating advertisements and dynamically joining other VLANs.

---

**NOTE:** In [Table 7 \(page 71\)](#), the Unknown VLAN parameters are configured on a per-port basis using the CLI. The Tagged, Untagged, Auto and Forbid options are configured per static VLAN on every port, using either the menu interface or the CLI.

Because dynamic VLANs operate as Tagged VLANs and because a tagged port on one device cannot communicate with an untagged port on another device, HP recommends that you use Tagged VLANs for the static VLANs you will use to generate advertisements.

---

## GVRP and VLAN access control

### Advertisements and dynamic joins

When you enable GVRP on a switch, the default GVRP parameter settings allow all of the switch's ports to transmit and receive dynamic VLAN advertisements (GVRP advertisements) and to dynamically join VLANs.

Enabling GVRP:

- Allows a port to both advertise and join dynamic VLANs (Learn mode—the default).
- Allows a port to send VLAN advertisements, but not receive them from other devices; that is, the port cannot dynamically join a VLAN but other devices can dynamically join the VLANs it advertises (Block mode).
- Prevents a port from participating in GVRP operation (Disable mode).

### Port-Leave from a dynamic VLAN

A dynamic VLAN continues to exist on a port for as long as the port receives its advertisements from another device connected to that port, or until:

- Converting the VLAN to a static VLAN
- Reconfiguring the port to `Block` or `Disable`
- Disabling GVRP
- Rebooting the switch.

The time-to-live for dynamic VLANs is 10 seconds, if a port has not received an advertisement for an existing dynamic VLAN during that time, the port removes itself from that dynamic VLAN.



---

## 3 Multimedia traffic control with IP multicast (IGMP)

### Operation and features

---

**NOTE:** Multicast filtering is not supported on HP switches J9779A, J9780A, J9782A and J9783A.

In a network where IP multicast traffic is transmitted for multimedia applications, you can use a switch to reduce unnecessary per-port bandwidth usage by configuring IGMP (Internet Group Management Protocol) controls. In the factory default state (IGMP disabled), the switch floods all IP multicast traffic it receives on a given VLAN through all ports on that VLAN, except the port on which it received the traffic. This can cause significant and unnecessary bandwidth use in networks employing IP multicast traffic. With IGMP, ports can detect IGMP queries, report packets and manage IP switch multicast traffic.

IGMP is useful in multimedia applications such as LAN TV, desktop conferencing and collaborative computing that have multipoint communication (communication from one-to-many or many-to-many hosts). In such multipoint applications, IGMP is configured on the hosts and multicast traffic is generated by one or more servers (inside or outside the local network). Switches in the network that support IGMP can then be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP by VLAN.

Enabling IGMP allows detection of IGMP queries and report packets to manage IP multicast traffic through the switch. If no other querier is detected, the switch then also functions as the querier. To disable the querier feature, use the IGMP configuration MIB (see [“Configuring the querier function”](#)).

**NOTE:** IGMP configuration on the switch operates at the VLAN context level. If you are not using VLANs, then configure IGMP in VLAN 1 (the default VLAN) context.

---

### IGMP devices

- **IGMP device:** A switch or router running IGMP traffic control features.
- **IGMP host:** An end-node device running an IGMP (multipoint or multicast communication) application.
- **Querier:** A required IGMP device that facilitates IGMP protocol and traffic flow on a given LAN. This device tracks which ports are connected to devices (IGMP clients) that belong to specific multicast groups and triggers updates of this information.

A querier uses data received from the queries to determine whether to forward or block multicast traffic on specific ports. When the switch has an IP address on a given VLAN, the switch automatically operates as a querier for that VLAN if it does not detect a multicast router or another switch functioning as a querier.

When enabled (the default state), the switch’s querier function eliminates the need for a multicast router. In most cases, HP recommends that you leave this parameter in the default enabled state even if you have a multicast router performing the querier function in your multicast group. For more information, see [“How IGMP operates”](#) (page 77).

### IGMP operating features

In the factory default configuration, IGMP is disabled. If multiple VLANs are not configured, configure IGMP on the default VLAN (DEFAULT\_VLAN; VID = 1); if multiple VLANs are configured, configure IGMP on a per-VLAN basis for every VLAN where this feature is needed.

With the CLI, you can also configure the following options:

- **Forward with high priority.** Disabling this parameter (the default) causes the switch or VLAN to process IP multicast traffic and other traffic, in the order received (usually normal priority).

Enabling this parameter causes the switch or VLAN to give higher priority to IP multicast traffic than to other traffic.

- **Auto/blocked/forward:** You can configure individual ports to any of the following states:
  - **Auto (the default):** Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for ports belonging to a multicast group. Thus IGMP traffic is forwarded on a specific port only if an IGMP host or multicast router is connected to the port.
  - **Blocked:** Causes the switch to block IGMP joins arriving on the blocked port. A multicast stream will still flood out a blocked port if no active joins have been received.
  - **Forward:** Causes the switch to forward all IGMP and IP multicast transmissions through the port.
- **Operation with or without IP addressing:** Helps conserve IP addresses by enabling IGMP to run on VLANs that do not have an IP address. See [“Operation with or without IP addressing” \(page 78\)](#).
- **Querier capability:** The switch performs this function for IGMP on VLANs having an IP address when no other device in the VLAN is acting as querier. See [“Using the switch as querier” \(page 84\)](#).

---

**NOTE:** Whenever IGMP is enabled, the switch generates an Event Log message indicating whether querier functionality is enabled.

IP multicast traffic groups are identified by IP addresses in the range of 224.0.0.0 to 239.255.255.255 and incoming IGMP packets intended for reserved, or “well-known” multicast addresses automatically flood through all ports (except the port on which the packets entered the switch). For more on this topic, see [“Excluding multicast addresses from IP multicast filtering” \(page 84\)](#).

---

## CLI: Configuring and displaying IGMP

**Viewing the Current IGMP Configuration.** The `show ip igmp config` command lists the IGMP configuration for all VLANs configured on the switch or for a specific VLAN.

**Syntax:** `show ip igmp config`

IGMP configuration for all VLANs on the switch.

`show ip igmp < vid > config`

IGMP configuration for a specific VLAN on the switch, including per-port data.

(For IGMP operating status, see the appendix on monitoring and analyzing switch operation in the *Management and Configuration Guide*.)

For example, given the following VLAN and IGMP configurations on the switch:

VLAN ID	VLAN Name	IGMP Enabled	Forward with High Priority	Querier
1	DEFAULT_VLAN	Yes	No	No
22	VLAN-2	Yes	Yes	Yes
33	VLAN-3	No	No	No

The following examples display the data for `show ip igmp config`, `statistics`, and `group` commands:

## Example 57 IGMP configuration for all VLANs on a switch

```
Switch> show ip igmp config
IGMP Service
VLAN ID      VLAN NAME      IGMP Enabled Forward with High Priority Querier
-----
1            DEFAULT_VLAN   Yes           No           No
22           VLAN-2         Yes           Yes          Yes
33           VLAN-3         No            No           No
```

## Example 58 Displaying igmp high level statistics for all VLANs on a switch

**Syntax:** show ip igmp statistics

```
HP Switch(config)# show ip igmp statistics
IGMP Service Statistic
Total VLAN's with IGMP enabled:    33
Current count of multicast groups joined: 21
IGMP Service Statistics
VLAN ID  VLAN Name      Total  Filtered Standard Static
-----
1        DEFAULT_VLAN   52     50      0         2
300      Office Client  80     75      5         0
300      Data Center    1100   1000    99        1
```

## Example 59 Displaying igmp group address information

**Syntax:** show ip igmp groups

```
HP Switch(config)# show ip igmp groups
IGMP Group Address Information
VLAN ID Group Address Expires      UpTime      Last Reporter | Type
-----
2       226.0.6.7    0h 2m 58s  1h 13m 4s   192.168.0.2 | Filter
2       226.0.6.8    0h 2m 58s  1h 13m 4s   192.168.0.2 | Standard
2       226.0.6.9    0h 2m 58s  1h 13m 4s   192.168.0.2 | Static
```

## Example 60 Displaying the IGMP configuration for a specific VLAN

The following **show ip igmp** command example shows the VLAN ID (*vid*) designation and the IGMP per-port configuration:

**Figure 14** Displaying the IGMP configuration for a specific VLAN

```
HP Switch(config)# show ip igmp 1 config
IGMP Service
VLAN ID : 1
VLAN NAME : DEFAULT_VLAN
IGMP Enabled : Yes
Forward with High Priority : No
Querier Allowed : Yes

Port Type      | IP Mcast
-----
1  100/1000TX   | Auto
2  100/1000TX   | Auto
3  100/1000TX   | Forward
4  100/1000TX   | Forward
5  100/1000TX   | Blocked
6  100/1000TX   | Blocked
```

**Enabling or disabling IGMP on a VLAN.** You can enable IGMP on a VLAN with the last-saved or default IGMP configuration (whichever was most recently set) or you can disable IGMP on a selected VLAN.

**NOTE:** The `ip igmp` command must be executed in a VLAN context.

**Syntax:** `[no] ip igmp`

Examples of enabling and disabling IGMP on the default VLAN (VID = 1):

Command syntax	Task
<code>Switch(config)# vlan 1 ip igmp</code>	Enables IGMP on VLAN 1.
<code>Switch(vlan-1)# ip igmp</code>	Disables IGMP on VLAN 1.
<code>Switch(config)# no vlan 1 ip igmp</code>	Disables IGMP on VLAN 1.

**NOTE:** If you disable IGMP on a VLAN and then later re-enable IGMP on that VLAN, the switch restores the last-saved IGMP configuration for that VLAN. For more information on switch memory operation, see the chapter on switch memory and configuration in the *Basic Operation Guide*.

You can also combine the `ip igmp` command with other IGMP-related commands, as described in the following sections.

### Configuring Per-Port IGMP Packet Control.

Command syntax	Task
<code>vlan &lt; vid &gt; ip igmp [ auto &lt;port-list&gt;   blocked &lt;port-list&gt;   forward &lt;port-list&gt; ]</code>	Use this command in the VLAN context to specify how each port should handle IGMP traffic.
<code>vlan &lt; vid &gt; ip igmp</code>	Enables IGMP on the specified VLAN. In a VLAN context, use only <code>ip igmp</code> without the VLAN specifier.
<code>vlan &lt; vid &gt; ip igmp auto &lt;port-list&gt;(default)</code>	Filter multicast traffic on the specified ports. Forward IGMP traffic to hosts on the ports that belong to the multicast group for which the traffic is intended. (Also forward any multicast traffic through any of these ports that is connected to a multicast router.) This is the default IGMP port configuration.
<code>vlan &lt; vid &gt; ip igmp blocked &lt;port-list&gt;</code>	Drop all multicast traffic received from devices on the specified ports and prevent any outgoing multicast traffic from moving through these ports.
<code>vlan &lt; vid &gt; ip igmp forward &lt;port-list &gt;</code>	Forward all multicast traffic through the specified port.

For example, to configure IGMP as follows for VLAN 1 on ports 1 - 6:

- Ports 1 - 2: Auto
- Ports 3 - 4: Forward
- Ports 5 - 6: Block

Depending on privilege level, use the following commands to configure IGMP on VLAN 1:

```
Switch(config)# vlan 1
HP Switch(vlan-1)# ip igmp auto 1,2
HP Switch(vlan-1)# ip igmp forward 3,4
HP Switch(vlan-1)# ip igmp blocked 5,6
```

After executing the above commands, use the following command to display the VLAN and per-port configuration .

## Configuring the querier function

The `ip igmp querier` command lets you disable or re-enable the ability for the switch to become querier on the specified VLAN. The default querier capability is “enabled”.

**Syntax:** `[no] vlan <vid> ip igmp querier`

For example, the following `no vlan 1` command disables the querier function on VLAN 1.

```
Switch(config)# no vlan 1 ip igmp querier
```

The following `show` command displays results of the previous querier command.

```
Switch> show ip igmp config
```

## Web: Enabling and disabling IGMP

In the web browser, you can enable or disable IGMP per-VLAN. To configure other IGMP features, use the CLI on the switch console.

### To enable or disable IGMP:

1. Click the **Configuration** tab.
2. Click the **Device Features** button.
3. If more than one VLAN is configured, use the VLAN pull-down menu to select the VLAN on which to enable or disable IGMP.
4. Use the Multicast Filtering (IGMP) menu to enable or disable IGMP.
5. Click the **Apply Changes** button to implement the configuration change.

For web-based help on how to use the web browser interface screen, click the **?** button on the web browser screen.

## How IGMP operates

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, multicast routers and hosts that support IGMP. (In HP’s implementation of IGMP, a multicast router is not necessary as long as a switch is configured to support IGMP with the querier feature enabled.) A set of hosts, routers or switches that send or receive multicast data streams to or from the same sources is called a multicast group and all devices in the group use the same multicast group address.

## Message types

The multicast group running IGMP uses three message types to communicate:

- **Query:** A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If no multicast router supporting IGMP is present, then the switch assumes this function to elicit group membership information from the hosts on the network. (To disable the querier, use the CLI IGMP configuration MIB. See [“Configuring the querier function”](#))
- **Report (join):** A message sent by a host to the querier indicating that the host wants to be or is a member of a given group in the report message.
- **Leave group:** A message sent by a host to the querier indicating that the host has ceased to be a member of a specific multicast group.

## IGMP multicasting

IGMP identifies members of a multicast group within a subnet and lets IGMP-configured hosts and routers join or leave multicast groups based on the following:

- An IP multicast packet includes the multicast group address to which the packet belongs.
- When an IGMP client connected to a switch port needs to receive multicast traffic from a specific group, it joins the group by sending an IGMP report (join request) to the network. The

multicast group specified in the join request is determined by the requesting application running on the IGMP client.

- When a networking device with IGMP enabled receives the join request for a specific group, it forwards any IP multicast traffic it receives for that group through the port on which the join request was received.
- When the client is ready to leave the multicast group, it sends a Leave Group message to the network and ceases to be a group member.
- When the leave request is detected, the appropriate IGMP device ceases to transmit traffic for the designated multicast group through the port on which the leave request was received, as long as there are no other current members of that group on the affected port.

## Displaying IGMP data.

To display data showing active group addresses, reports, queries, querier access port and active group address data (port, type and access), see the appendix on monitoring and analyzing switch operation in the *Management and Configuration Guide*.

## Supported standards and RFCs

The HP implementation of IGMP supports the following standards and operating capabilities:

- RFC2236 (IGMP V.2 with backwards support for IGMP V.1).
- IETF draft for IGMP and MLD snooping switches (for IGMP V1, V2 V3).
- Full IGMPv2 support and full support for IGMPv1 Joins.
- Ability to operate in IGMPv2 querier mode on VLANs with an IP address.

The HP implementation is subject to the following restrictions:

- Interoperability with RFC3376 (IGMPv3).
- Interoperability with IGMPv3 Joins. When the switch receives an IGMPv3 Join, it accepts the host request and begins forwarding the IGMP traffic. Thus ports that have not joined the group and are not connected to routers or the IGMP querier will not receive the group's multicast traffic.
- No support for the IGMPv3 "Exclude Source" or "Include Source" options in Join Reports; the group is simply joined from all sources.
- No support for becoming a version 3 querier. The switch becomes a version 2 querier in the absence of any other querier on the network.

---

**NOTE:** IGMP is supported in the HP MIB, not in standard IGMP MIBs, as the latter reduce Group Membership detail in switched environments.

---

## Operation with or without IP addressing

You can configure IGMP on VLANs that do not have IP addressing. Using IGMP without IP addressing reduces the number of IP addresses you use and configure, significant in a network with many VLANs. The limitation on IGMP without IP addressing is that the switch cannot become querier on any VLANs for which it has no IP address; thus the network administrator must ensure that another IGMP device act as querier. HP also advises that an additional IGMP device be available as backup querier.

**Table 8 Comparison of IGMP operation with and without IP addressing**

IGMP Function available with IP Addressing configured on the VLAN	Available without IP Addressing?	Operating Differences without an IP Address
Forward multicast group traffic to any port on the VLAN that has received a join request for that multicast group.	Yes	None
Forward join requests (reports) to the querier.	Yes	None
Configure individual ports in the VLAN to <b>Auto</b> (the default) <b>Blocked</b> , or <b>Forward</b> .	Yes	None
Configure IGMP traffic forwarding to normal or high-priority forwarding.	Yes	None
Age-Out IGMP group addresses when the last IGMP client on a port in the VLAN leaves the group.	Yes	Requires that another IGMP device in the VLAN have an IP address and can operate as querier. This can be a multicast router or another switch configured for IGMP operation. HP recommends that the VLAN also include a device operating as a backup querier in case the device operating as the primary querier fails.
Support Fast-Leave IGMP (below) and Forced Fast-Leave IGMP.	Yes	
Support automatic querier election.	No	Querier operation not available.
Operate as the querier.	No	Querier operation not available.
Available as a backup querier.	No	Querier operation not available.

## Automatic Fast-Leave IGMP

**IGMP Operation Presents a “Delayed Leave” Problem.** Where multiple IGMP clients are connected to the same port on an IGMP device (switch or router), if only one IGMP client joins a given multicast group, then later sends a Leave Group message and ceases to belong to that group, the IGMP device retains that IGMP client in its IGMP table and continues forwarding IGMP traffic to the IGMP client until the querier triggers confirmation that no other group members exist on the same port. Thus the switch continues to transmit unnecessary multicast traffic through the port until the querier renews its multicast group status.

**Fast-Leave IGMP.** Depending on the switch model, Fast-Leave is enabled or disabled in the default configuration (see [Table 9 \(page 80\)](#)).

**Table 9 IGMP: data-driven and non-data driven behavior**

Switch Model or Series	Data-Driven IGMP Included?	IGMP Fast-Leave Setting	Default IGMP Behavior
Switch 2500	Yes	Always enabled	Drops unjoined multicast traffic except for always-forwarded traffic toward the querier or multicast routers and out IGMP-forward ports. Selectively forwards joined multicast traffic.
Switch 2510-48			
Switch 2520			
Switch 2800			
Switch 2810			
Switch 3400cl			
Switch 3500			
Switch 3500yl			
Switch 4200vl			
Switch 5300xl			
Switch 5400zl			
Switch 6200yl			
Switch 6400cl			
Switch 8200zl			
Switch 2510-24	No	Disabled in the default configuration.	IGMP Fast-Leave disabled in the default configuration. Floods unjoined multicast traffic to all ports. Selectively forwards joined multicast traffic.
Switch 2600			
Switch 2600-PWR			
Switch 4100gl			
Switch 6108			

When unregistered multicasts are received on HP switches that support Data-Driven IGMP (“Smart” IGMP), the switch automatically drops them. Thus the sooner the IGMP Leave is processed, the sooner this multicast traffic stops flowing.

On switches that do not support Data-Driven IGMP, unregistered multicast groups are flooded to the VLAN rather than pruned. In this scenario, Fast-Leave IGMP can actually increase the problem of multicast flooding by removing the IGMP group filter before the querier has recognized the IGMP Leave. The querier continues to transmit the multicast group during this short time and because the group is no longer registered the switch then floods the multicast group to all ports. Because of such multicast flooding, the IGMP Fast-Leave feature is disabled by default on all HP switches that do not support Data-Driven IGMP (see [Table 9 \(page 80\)](#)). The feature can be enabled on these switches using an SNMP set of the following object:

```
hpSwitchIgmpportForceLeaveState.< vid >.< port number >
```

However, this is not recommended as this will increase the amount of multicast flooding during the period between the client's IGMP Leave and the querier's processing of that Leave. For more on this topic, see [“Forced Fast-Leave IGMP” \(page 81\)](#).

**Automatic Fast-Leave Operation** The Fast-Leave operation applies if a switch port has the following characteristics:

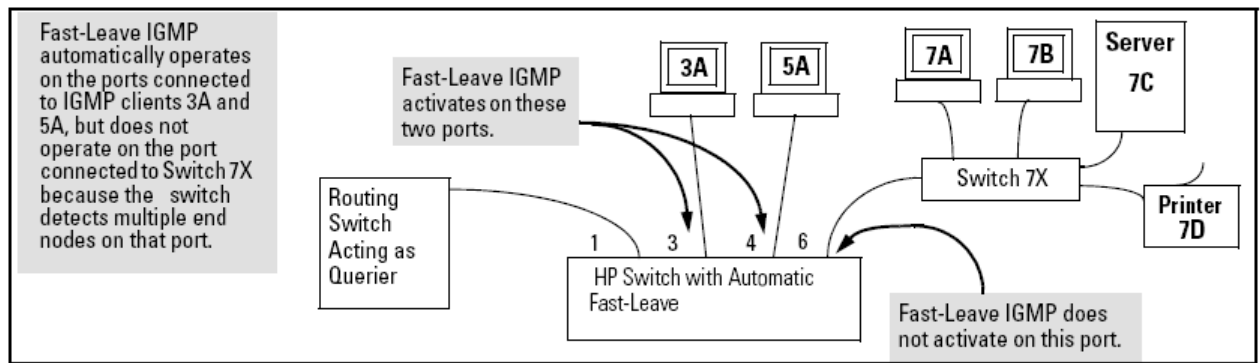
- Is connected to only one end node.
- Is an IGMP client (the end node currently belongs to a multicast group).
- The end node subsequently leaves the multicast group.



The switch need not wait for the querier status update interval but instead immediately removes the IGMP client from its IGMP table and ceases transmitting IGMP traffic to the client. (If the switch detects multiple end nodes on the port, automatic Fast-Leave does not activate – regardless of whether one or more of these end nodes are IGMP clients.)

In [Figure 15 \(page 81\)](#), automatic Fast-Leave operates on the switch ports for IGMP clients “3A” and “5A”, but not on the switch port for IGMP clients “7A” and 7B, Server “7C” and printer “7D”.

**Figure 15 Automatic Fast-Leave IGMP Criteria**



When client “3A” running IGMP is ready to leave the multicast group, it transmits a Leave Group message. Because the switch knows that there is only one end node on port 3, it removes the client from its IGMP table and halts multicast traffic (for that group) to port 3. If the switch is not the querier, it does not wait for the actual querier to verify that there are no other group members on port 3. If the switch itself is the querier, it does not query port 3 for the presence of other group members.

**NOTE:** Fast-Leave operation does not distinguish between end nodes on the same port that belong to different VLANs. Thus even if all devices on port 6 in [Figure 15 \(page 81\)](#) belong to different VLANs, Fast-Leave does not operate on port 6.

### Using delayed group flush

This feature continues to filter IGMP-Left groups for a specified additional time. Delay in flushing the group filter prevents stale traffic from being forwarded by the server. Delayed group flush is enabled or disabled for the entire switch.

**Syntax:** `igmp delayed-flush <time period>`

Enables the switch to continue to flush IGMP-Left groups for a specified period of time (0 - 255 seconds). The default setting is **Disabled**. To disable, reset the time period to zero.

**Syntax:** `show igmp delayed-flush`

Displays the current setting for the switch.

### Forced Fast-Leave IGMP

Forced Fast-Leave IGMP speeds up the process of blocking unnecessary IGMP traffic to a switch port that is connected to multiple end nodes. (This feature does not activate on ports where the switch detects only one end node.) For example, in [Figure 15 \(page 81\)](#), even if you configured Forced Fast-Leave on all ports in the switch, the feature would activate only on port 6 (which has multiple end nodes) when a Leave Group request arrived on that port.

When a port having multiple end nodes receives a Leave Group request from one end node for a given multicast group “X”, Forced Fast-Leave activates and waits a short time to receive a join request from any other group “X” member on that port. If the port does not receive a join request for that group within the forced-leave interval, the switch then blocks any further group “X” traffic to the port.

## Setting Fast-Leave and Forced Fast-Leave from the CLI

Previously, Fast-Leave and Forced Fast-Leave options for a port were set exclusively through the MIB. The following commands now allow a port to be configured for Fast-Leave or Forced Fast-leave operation from the CLI. These commands must be executed in a VLAN context.

**Syntax:** [no] ip igmp fastleave <port-list>

Enables IGMP Fast-Leaves on the specified ports in the VLAN (the default setting). In the Config context, use the VLAN specifier <vid>, for example, `vlan < vid > ip igmp fastleave <port-list>`. The “no” form disables Fast-Leave on the specified ports.

**Syntax:** [[no]] ip igmp forcedfastleave <port-list>

Forces IGMP Fast-Leaves on the specified ports in the VLAN, even if they are cascaded.

To view the IGMP Fast-Leave status of a port use the **show running-config** or **show config** command.

## Setting Forced Fast-Leave using the MIB

Fast-Leave and Forced Fast-Leave options for a port can also be set through the switch MIB (Management Information Base).

**Table 10 Forced Fast-Leave States**

Feature	Default	Settings	Function
Forced Fast-Leave state	2 (disabled)	1 (enabled)	Uses the <b>setmib</b> command to enable or disable Forced Fast-Leave on individual ports. When enabled on a port, Forced Fast-Leave operates only if the switch detects multiple end nodes (and at least one IGMP client) on that port
		2 (disabled)	

### **NOTE: VLAN Numbers**

In the HP switches covered in this manual, the **walkmib** and **setmib** commands use an internal VLAN number, not the VLAN ID or VID, to display or change many per-vlan features, such as the Forced Fast-Leave state. Because the internal VLAN number for the default VLAN is always 1, whether or not VLANs are enabled on the switch, examples herein use the default VLAN.

## Listing the MIB-Enabled Forced Fast-Leave configuration

Forced Fast-Leave configuration data available in the switch MIB includes the state (enabled or disabled) for each port and the Forced-Leave Interval for all ports on the switch.

**To List the Forced Fast-Leave State for all Ports in the Switch.** In the CLI, use the **walkmib** command, as shown below.

Enter either of the following **walkmib** commands (generic or explicit):

```
walkmib hpSwitchIcmpPortForcedLeaveState (generic command)
```

OR

```
walkmib 1.3.6.1.4.1.11.2.14.11.5.1.7.1.15.3.1.5 (explicit command)
```

The result shows the Forced Fast-Leave state for all ports in the switch, by VLAN. (A port belonging to more than one VLAN is shown once for each VLAN; if multiple VLANs are not configured, all ports are shown as members of the default VLAN.) For example, [Figure 16 \(page 83\)](#) shows output of the **walkmib** command.

**Figure 16 Forced Fast-Leave output where all ports are members of the default VLAN**

```
Switch(config)# walkmib hpswitchigmpportforcedleavestate.1
hpSwitchIgmpPortForcedLeaveState.1.1 = 2
hpSwitchIgmpPortForcedLeaveState.1.2 = 2
hpSwitchIgmpPortForcedLeaveState.1.3 = 2
hpSwitchIgmpPortForcedLeaveState.1.4 = 2
hpSwitchIgmpPortForcedLeaveState.1.5 = 1
hpSwitchIgmpPortForcedLeaveState.1.6 = 2
```

Internal VLAN Number for the Default VLAN  
**Note:** Internal VLAN numbers reflect the sequence in which VLANs are created, and are not related to the unique VID assigned to each VLAN.

Sequential Port Numbers

Ports 1-6: 6- Port 109/100T

The 2 at the end of a port listing shows that Forced Fast-Leave is **disabled** on the corresponding port.

The 1 at the end of a port listing shows that Forced Fast-Leave is **enabled** on the corresponding port.

**To show the Forced Fast-Leave state for a single port** (See “NOTE”.)

Use the following getmib command (see Figure 17 (page 83)).

**Syntax:**

```
getmib hpSwitchIgmpPortForcedLeaveState.<vlan number><.port number>
OR
```

```
getmib 1.3.6.1.4.1.11.2.14.11.5.1.7.1.15.3.1.5.<vlan number><.port number>
```

For example, the following getmib command shows the state for port 6 on the default VLAN.

**Figure 17 Forced Fast-Leave state for a single port on the default VLAN**

```
HP Switch(config) # getmib hpswitchigmpportforcedleavestate.1.6
hpSwitchIgmpPortForcedLeaveState.1.6 = 2
```

The 2 shows that Fast Forced-Leave is disabled on the selected port.

The 6 specifies port 6.

The 1 indicates the default VLAN.

### Configuring per-port Forced Fast-Leave IGMP

In the factory-default configuration, Forced Fast-Leave is disabled for all ports on the switch. To enable (or disable) this feature on individual ports, use the switch **setmib** command.

**Configuring Per-Port Forced Fast-Leave IGMP on Ports.** This procedure enables or disables Forced Fast-Leave on ports in a given VLAN.

```
HP Switch(config)# setmib hpswitchigmpportforcedleavestate.1.6 -i 1
hpSwitchIgmpPortForcedLeaveState.1.6 = 2
```

where **1** in .1.6 is the default VLAN, **6** in .1.6 indicates port 6 and = **2** verifies Forced Fast-Leave disabled.

**NOTE:** TO REVIEWERS: there is an inconsistency here in the source manual: -i 1 is missing from the screen capture above. Which is correct?

**Syntax:**

```
setmib hpSwitchIgmpPortForcedLeaveState.< vlan number >< .port number >
-i < 1 / 2 >
```

OR

```
setmib 1.3.6.1.4.1.11.2.14.11.5.1.7.1.15.3.1.5.< vlan number >< .port
number > -i < 1 | 2 >
```

where:

**Table 11 Forced Fast-Leave values**

1	Enabled
2	Disabled

For example, suppose that your switch has six ports as members of the default VLAN. To enable Forced Fast-Leave on port 6, you would execute the following command to obtain the result.

### Example 61 Changing the Forced Fast-Leave Configuration on Port 6.

```
HP Switch(config)# setmib hpswitchigmpportforcedleavestate.1.6 -i 1
hpSwitchIgmpPortForcedLeaveState.1.6 = 1
```

where **1** in .1.6 is the default VLAN, **6** in .1.6 indicates port 6 and **= 1** verifies Forced Fast-Leave enabled.

## Using the switch as querier

### Querier operation

The function of the IGMP querier is to poll other IGMP-enabled devices in an IGMP-enabled VLAN to elicit group membership information. The switch performs this function if there is no other device in the VLAN, such as a multicast router, to act as querier. Although the switch automatically ceases querier operation in an IGMP-enabled VLAN if it detects another querier on the VLAN, you can also use the CLI to disable the querier capability for that VLAN.

**NOTE:** A querier is required for proper IGMP operation. Thus, if you disable the querier function on a switch, ensure that there is an IGMP querier (and, preferably, a backup querier) available on the same VLAN.

If the switch becomes the querier for a particular VLAN (for example, the DEFAULT\_VLAN), then subsequently detects queries transmitted from another device on the same VLAN, the switch ceases to operate as the querier for that VLAN. If this occurs, the switch Event Log lists a pair of messages such as:

```
I 01/15/01 09:01:13 igmp: DEFAULT_VLAN: Other Querier detected
I 01/15/01 09:01:13 igmp: DEFAULT_VLAN: This switch is no longer Querier
```

In the above scenario, if the other device ceases to operate as a querier on the default VLAN, then the switch detects this change and can become the querier as long as it is not pre-empted by some other IGMP querier on the VLAN. In this case, the switch Event Log lists messages such as the following to indicate that the switch has become the querier on the VLAN:

```
I 01/15/01 09:21:55 igmp: DEFAULT_VLAN: Querier Election in process
I 01/15/01 09:22:00 igmp: DEFAULT_VLAN: This switch has been elected
as Querier
```

## Excluding multicast addresses from IP multicast filtering

Each multicast host group is identified by a single IP address in the range 224.0.0.0 through 239.255.255.255. Specific groups of consecutive addresses in this range are “well-known” addresses and are reserved for predefined host groups. IGMP does not filter these addresses, so any packets the switch receives for such addresses are flooded out all ports assigned to the VLAN on which they were received (except the port on which the packets entered the VLAN).

The following table lists the 32 well-known address groups (8192 total addresses) that IGMP does not filter on the switches covered in this manual and on 1600M, 2400M, 2424M, 2650M, 4000M, 6108M, 8000M and switch 2500 series devices.

**Table 12 IP multicast address groups excluded from IGMP filtering**

Groups of consecutive addresses in the range of 224.0.0.x to 239.0.0.x <sup>1</sup>		Groups of consecutive addresses in the range of 224.128.0.x to 239.128.0.x <sup>1</sup>	
224.0.0.x	232.0.0.x	224.128.0.x	232.128.0.x
225.0.0.x	233.0.0.x	225.128.0.x	233.128.0.x
226.0.0.x	234.0.0.x	226.128.0.x	234.128.0.x
227.0.0.x	235.0.0.x	227.128.0.x	235.128.0.x
228.0.0.x	236.0.0.x	228.128.0.x	236.128.0.x
229.0.0.x	237.0.0.x	229.128.0.x	237.128.0.x
230.0.0.x	238.0.0.x	230.128.0.x	238.128.0.x
231.0.0.x	239.0.0.x	231.128.0.x	239.128.0.x

<sup>1</sup> x is any value from 0 to 255.

**NOTE: IP multicast filters.** This operation applies to HP Switches 1600M, 2400M, 2424M, 4000M and 8000M, but not to HP Switches 2500, 2600, 2600PWR, 2800, 2810, 2510, 4100 and 5300 Series devices or Switch 6108, which do not have static multicast traffic/security filters).

IP multicast addresses occur in the range 224.0.0.0 through 239.255.255.255 (corresponding to the Ethernet multicast address range 01005e-000000 through 01005e-7fffff). Where a switch has a static Traffic/Security filter configured with a “Multicast” filter type and a “Multicast Address” in this range, the switch uses the static filter unless IGMP learns of a multicast group destination in this range. In this case, IGMP dynamically takes over the filtering function for the multicast destination addresses) for as long as the IGMP group is active. If the IGMP group subsequently deactivates, the switch returns filtering control to the static filter.

**Reserved addresses excluded from IP multicast (IGMP) filtering.**

Traffic to IP multicast groups in the IP address range 224.0.0.0 to 224.0.0.255 are always flooded because addresses in this range are well known or reserved addresses. Thus, if IP multicast is enabled and there is an IP multicast group within the reserved address range, traffic to that group is flooded, not filtered, by the switch.

**Number of IP multicast addresses allowed.** Multicast filters and IGMP filters (addresses) together can total up to 255 in the switch. If multiple VLANs are configured, then each filter is counted once per VLAN in which it is used.

## 4 Multiple instance spanning tree operation

Command syntax	Description	Default value	CLI reference page
<code>spanning-tree mode mstp</code> <code>spanning-tree clear-debug-counters</code>	Specifies that spanning tree will run in MSTP mode		<a href="#">93</a>
<code>[no] spanning-tree config-name &lt;ascii-string&gt;</code>	Resets the configuration name of the MST region in which the switch resides	A text string using the switch's MAC address	<a href="#">93</a>
<code>spanning-tree config-revision &lt;revision-number&gt;</code>	Sets the revision number designated for the MST region in which you want the switch to reside	0	<a href="#">93</a>
<code>spanning-tree force-version [ &lt;stp-compatible&gt;   &lt;rstp-operation&gt;   &lt;mstp-operation&gt; ]</code>	Sets the spanning tree compatibility mode		<a href="#">94</a>
<code>spanning-tree forward-delay</code>	Sets the time in seconds the switch waits between transitioning from listening to learning and from learning to forwarding states	15	<a href="#">94</a>
<code>[no]spanning-tree legacy-mode</code>	Forces spanning tree to operate in legacy (802.1D) mode	Native mode: MSTP	<a href="#">95</a>
<code>spanning-tree legacy-path-cost</code>	Forces spanning tree to operate with legacy (802.1D) path cost values	802.1t	<a href="#">95</a>
<code>spanning-tree hello-time &lt;1..10&gt;</code>	Sets the time in seconds between transmissions of BPDUs for all ports on the switch configured with the Global option. (the default)	2	<a href="#">95</a>

Command syntax	Description	Default value	CLI reference page
<code>spanning-tree max-hops &lt;hop-count&gt;</code>	Resets the number of hops allowed for BPDUs in an MST region	20	<a href="#">95</a>
<code>spanning-tree maximum age</code>	Sets the maximum age (in seconds) for received STP information before it is discarded	20	<a href="#">96</a>
<code>spanning-tree pending [ apply   &lt;config-name&gt;   &lt;config-revision&gt;   &lt;instance&gt;   reset ]</code>	Manipulates the pending MSTP configuration		<a href="#">96</a>
<code>spanning-tree priority &lt;priority-multiplier&gt;</code>	Sets the switch (bridge) priority for a region, which determines its priority as the spanning tree root switch		<a href="#">96</a>
<code>[no] spanning-tree trap { errant-bpdu   loop-guard   new-root   root-guard }</code>	Enables or disables SNMP traps for errant-BPDU, loop guard, new root and root guard event notifications	Disabled	<a href="#">97</a>
<code>[no] spanning-tree&lt;port-list&gt; admin-edge-port</code>	Allows specified port(s) to transition immediately to a forwarding state	Disabled	<a href="#">97</a>
<code>[no] spanning-tree &lt;port-list&gt; auto-edge-port</code>	Supports the automatic identification of edge ports	Enabled	<a href="#">98</a>
<code>spanning-tree &lt;port-list&gt; hello-time [ global   &lt;1 - 10&gt; ]</code>	Specifies the interval (in seconds) between periodic BPDU transmissions by the designated ports	2	<a href="#">98</a>
<code>spanning-tree &lt;port-list&gt; mcheck</code>	Forces a port to send RST/MST BPDUs for 3 seconds		<a href="#">98</a>

Command syntax	Description	Default value	CLI reference page
<code>spanning-tree &lt;port-list&gt; path-cost [ auto   &lt;1..20000000&gt; ]</code>	Assigns an individual port cost that the switch uses to determine which ports are forwarding ports in a given spanning tree	Auto	<a href="#">98</a>
<code>spanning-tree &lt;port-list&gt; point-to-point-mac [ true   false   auto ]</code>	Informs the switch of the type of device to which a specific port connects	True	<a href="#">99</a>
<code>spanning-tree &lt;port-list&gt; priority &lt;priority-multiplier&gt;</code>	Determines the priority of specified port(s) for use in forwarding		<a href="#">99</a>
<code>spanning-tree &lt;port-list&gt; root-guard</code>	Enables root guard on specified port(s)	Disabled	<a href="#">99</a>
<code>spanning-tree &lt;port-list&gt; tcn-guard</code>	Causes specified port(s) to stop propagating received topology change notifications and topology changes to other ports	Disabled	<a href="#">100</a>
<code>[no] spanning-tree [ &lt;port-list&gt;   all ] bpd-filter</code>	Enables or disables BPDU filtering	Disabled	<a href="#">100</a>
<code>spanning-tree show &lt;port&gt; configuration</code>	Displays BPDU filtering information		<a href="#">101</a>
<code>[no]spanning-tree &lt;port-list&gt; bpd-protection</code>	Enables or disables BPDU protection	Disabled	<a href="#">101</a>
<code>[no] spanning-tree &lt;port-list&gt; bpd-protection-timeout &lt;timeout&gt;</code>	Sets the duration of time (in seconds) when protected ports receiving unauthorized BPDUs will remain disabled	0	<a href="#">101</a>
<code>[no] spanning-tree trap errant-bpdu</code>	Enables and disables the	Disabled	<a href="#">101</a>



Command syntax	Description	Default value	CLI reference page
	sending of errant BPDU traps		
show spanning-tree bpdu-protection	Displays BPDU protection status		102
[no] spanning-tree <port-list> pvst-protection	Enables and disables PVST protection	Disabled	103
[no] spanning-tree <port-list> <pvst-filter>	Enables and disables PVST filtering	Disabled	103
[no] spanning-tree bpdu-protection-timeout <timeout>	Re-enables ports manually	0	103
show spanning-tree pvst-filter	Displays which ports have PVST filtering enabled		104
show spanning-tree pvst-protection	Displays which ports have PVST protection enabled		104
spanning-tree instance <1..16> vlan <vid> [<vid...vid>]	Configures MSTP instance parameters		104
spanning-tree instance <1..16> priority <priority-multiplier>	Sets the bridge priority for an instance		105
[no] spanning-tree instance <1..16> vlan <vid> [<vid...vid>]	Creates a new MST instance (MSTI) and moves the specified VLANs from the IST to the MSTI	instance (MSTPI): none	105
spanning-tree instance <ist / 1..16> <port-list> path-cost [ auto   <1..200000000> ]	Assigns an individual port cost for the specified MST instance	auto	105
spanning-tree instance <1..16> <port-list> priority <priority-multiplier>	Sets the switch (bridge) priority for the specified ports in the specified MST instance		106
spanning-tree <port-list> priority <priority-multiplier>	Sets the switch (bridge) priority for the specified ports for the IST (Instance 0) of the region in	priority: 32768 (multiplier: 8)	106

Command syntax	Description	Default value	CLI reference page
	which the switch resides		
[no] spanning-tree	Enables or disables MSTP spanning tree operation	Disabled	107
[no] spanning-tree pending [ apply   <config-name>   <config-revision>   <instance>   reset ]	Exchanges the currently active MSTP configuration with the current pending MSTP configuration		107
[no] spanning-tree instance <1..16> vlan <vid> [<vid..vid>]	Pre-configures VLANs in an MST instance		109
show spanning-tree	Displays MSTP statistics		112
show spanning-tree <port-list>			
show spanning-tree detail			
show spanning-tree <port-list> detail			
show spanning-tree instance [ ist   <1..16> ]			
show spanning-tree instance [ ist   <1..16> ] detail			
show spanning-tree <port-list> instance [ ist   <1..16> ] detail	Displays the MSTP configuration		115
show spanning-tree config			
show spanning-tree <port-list> config			
show spanning-tree config instance [ ist   <ist / 1..16> ]			
show spanning-tree <port-list> config instance [ ist   <1..16> ]			
show spanning-tree mst-config			
show spanning-tree pending [ instance   mst-config ] instance [ ist   <1..16> ]	Configures loop protection	send-disable	118
[no] loop-protect <port-list> [[ receiver-action send-disable no-disable ]   [transmit-interval <1-10>]   [ disable-timer <0-604800>]   [ trap loop-detected]   [ mode port vlan ]   [vlan <vid-list>]]			
show loop-protect <port-list>	Displays loop protection status		120
show spanning-tree root-history	Troubleshoots an MSTP configuration		124
show spanning-tree debug counters			
show spanning-tree debug-counters instance <instance-id>			

Command syntax	Description	Default value	CLI reference page
show spanning-tree debug-counters instance <instance-id> ports <port-list>			
[no] spanning-tree trap { errant-bpdu   loop-guard   new-root   root-guard }			

## Planning an MSTP application

Before configuring MSTP, keep in mind the following tips and considerations:

- Ensure that the VLAN configuration in your network supports all of the forwarding paths necessary for the desired connectivity. All ports connecting one switch to another within a region and one switch to another between regions should be configured as members of all VLANs configured in the region.
- Configure all ports or trunks connecting one switch to another within a region as members of all VLANs in the region. Otherwise, some VLANs could be blocked from access to the spanning tree root for an instance or for the region.
- Plan individual regions based on VLAN groupings. That is, plan on all MSTP switches in a given region supporting the same set of VLANs. Within each region, determine the VLAN membership for each spanning tree instance. (Each instance represents a single forwarding path for all VLANs in that instance.)
- Verify that there is one logical spanning tree path through the following:
  - Any inter-regional links
  - Any IST (Internal Spanning Tree) or MST instance within a region
  - Any legacy (802.1D or 802.1w) switch or group of switches. (Where multiple paths exist between an MST region and a legacy switch, expect the CST (Common Spanning Tree) to block all but one such path.)
- Determine the root bridge and root port for each instance.
- Determine the designated bridge and designated port for each LAN segment.
- Determine which VLANs to assign to each instance and use port trunks with 802.1Q VLAN tagging where separate links for separate VLANs would result in a blocked link preventing communication between nodes on the same VLAN. (See [“MSTP operation with 802.1Q VLANs” \(page 139\)](#).)
- Identify the edge ports connected to end nodes and enable the `admin-edge-port` setting for these ports. Leave the `admin-edge-port` setting disabled for ports connected to another switch, a bridge, or a half-duplex repeater.

## Configuring MSTP at a glance

The general steps for configuring MSTP via the CLI are:

1. Configure MSTP global parameters. This involves:
  - Selecting MSTP as the spanning tree mode: `spanning-tree mode mstp`
  - Clearing spanning tree debug counters:
 

```
spanning-tree clear-debug-counters
```
  - Specifying required parameters for MST region identity:
 

```
Region Name:spanning-tree config-name
Region Revision Number:spanning-tree config-revision
```
  - Optionally, specifying MSTP parameter changes for region settings:
 

HP recommends that you leave these parameters at their default settings for most networks. See the Caution below.

    - The maximum number of hops before the MSTP BPDU (Bridge Protocol Data Unit) is discarded: `spanning-tree max-hops` (default: 20)
    - Force-Version operation: `spanning-tree force-version`
    - Forward Delay: `spanning-tree forward-delay`
    - Hello Time (if it is the root device): `spanning-tree hello-time`
    - Maximum age to allow for STP packets before discarding: `spanning-tree maximum-age`
    - Device spanning tree priority. Specifies the priority value used along with the switch MAC address to determine which device is root. The lower a priority value, the higher the priority: `spanning-tree priority`
  - Enabling SNMP traps:
 

```
[no] spanning-tree trap { errant-bpdu | loop-guard | new-root |
root-guard }
```

---

**△ CAUTION:** When you enable MSTP on the switch, the default MSTP spanning tree configuration settings comply with the values recommended in the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) standard. Inappropriate changes to these settings can cause severely degraded network performance. Thus HP strongly recommends that changing these default settings be reserved only for experienced network administrators with a full understanding of IEEE 802.1D/w/s standards and operation.

---

2. Configure per port parameters. HP recommends that you use the default settings for these parameters and apply changes on a per-port basis only where a non-default setting is clearly indicated by the circumstances of individual links. Other features you might consider include BPDU Filtering or BPDU Protection—these provide additional per-port control over spanning tree operations and security on the switch.
3. Configure MST instances. Configure one instance for each VLAN group that you want to operate as an active topology within the region to which the switch belongs. When you create the instance, you must include a minimum of one VID. You can add more VIDs later if desired. Use the following command:
 

```
spanning-tree instance <n> vlan <vid>
```

To move a VLAN from one instance to another, first use `no spanning-tree instance <n> vlan <vid>` to unmap the VLAN from the current instance, then add the VLAN to the other instance. (While the VLAN is unmapped from an MSTI, it is associated with the region's IST instance.)
4. Configure the priority for each instance with the following command: `spanning-tree instance <n> priority <n>`

5. Configure MST instance port parameters. HP recommends that you apply changes on a per-port basis only where a non-default setting is clearly indicated by the circumstances of individual links. For example, you might want to set the path cost value for the instance or for the ports used by a specific MST instance. Use the following command:  

```
spanning-tree instance <ist / 1..16 port-list> path-cost  
[ <auto> | <1..200000000> ]
```

Alternatively, leaving this setting at the default (auto) allows the switch to calculate the path-cost from the link speed.
6. Enable spanning tree operation on the switch with the `spanning-tree` command.

## Configuring MSTP operation mode and global settings

The commands in this section apply at the switch (global) level. For configuring spanning tree settings on individual ports, see [“Configuring MSTP per-port parameters”](#) (page 97).

### Selecting MSTP as the spanning tree mode

**Syntax:**

```
spanning-tree mode mstp
```

Specifies that spanning tree will run in MSTP mode.

### Clearing spanning tree debug counters

**Syntax:**

```
spanning-tree clear-debug-counters
```

Clears spanning tree debug counters.

### Resetting the configuration name of the MST region in which a switch resides

**Syntax:**

```
[no] spanning-tree config-name <ascii-string>
```

Resets the configuration name of the MST region in which the switch resides. This name can include up to 32 nonblank characters and is case-sensitive. On all switches within a given MST region, the configuration names must be identical. For more than one MSTP switch in the same MST region, the identical region name must be configured on all such switches. If the default configuration name is retained on a switch, it cannot exist in the same MST region with another switch.

The default name is a text string using the hexadecimal representation of the switch's MAC address.

The `no` form of the command overwrites the currently configured name with the default name.

---

**NOTE:** This option is available only when the switch is configured for MSTP operation. There is no defined limit on the number of regions you can configure.

---

### Designating the revision number of the MST region for a switch

**Syntax:**

```
spanning-tree config-revision <revision-number>
```

Configures the revision number designated for the MST region in which you want the switch to reside. This setting must be the same for all switches residing in the

same region. Use this setting to differentiate between region configurations in situations such as the following:

- Changing configuration settings within a region where you want to track the configuration versions you use
- Creating a new region from a subset of switches in a current region and want to maintain the same region name.
- Using the `pending` option to maintain two different configuration options for the same physical region.

This setting must be the same for all MSTP switches in the same MST region.

Range: 0 - 65535

Default: 0

---

**NOTE:** This option is available only when the switch is configured for MSTP operation.

---

## Setting the spanning tree compatibility mode

### Syntax:

```
spanning-tree force-version[ stp-compatible | rstp-operation |  
mstp-operation ]
```

Sets the spanning tree compatibility mode. This command forces the switch to emulate behavior of earlier versions of spanning tree protocol, or return to MSTP behavior. The command is useful in test or debug applications and removes the need to reconfigure the switch for temporary changes in spanning tree operation.

<code>stp-compatible</code>	The switch applies 802.1D STP operation on all ports.
<code>rstp-operation</code>	The switch applies 802.1w operation on all ports except those ports where it detects a system using 802.1D Spanning Tree. RSTP is Rapid Spanning Tree Protocol.
<code>mstp-operation</code>	The switch applies 802.1s MSTP operation on all ports where compatibility with 802.1D or 802.1w spanning tree protocols is not required.

---

**NOTE:** Even when `mstp-operation` is selected, if the switch detects an 802.1D BPDU or an 802.1w BPDU on a port, it communicates with the device linked to that port using STP or RSTP BPDU packets. Also, if errors are encountered as described in [“Configuring MSTP at a glance” \(page 91\)](#), setting `force-version` to `stp-compatible` forces the MSTP switch to communicate out all ports using operations that are compatible with IEEE 802.1D STP.

**NOTE:** When using MSTP rapid state transitions

Under some circumstances the rapid state transitions employed by MSTP can increase the rates of frame duplication and misordering in the switched LAN. To allow MSTP switches to support applications and protocols that may be sensitive to frame duplication and misordering, setting the Force Protocol Version (`force-version`) parameter to `stp-compatible` allows MSTP to operate with rapid transitions disabled. The value of this parameter applies to all ports on the switch.

---

## Setting the time interval between listening, learning and forwarding states

### Syntax:

```
spanning-tree forward-delay
```

Sets the time the switch waits between transitioning from listening to learning and from learning to forwarding states.

Range: 4 - 30

Default: 15 seconds

## Setting spanning tree to operate in 802.1D legacy mode

### Syntax:

```
[no] spanning-tree legacy-mode
```

Forces spanning tree to operate in legacy (802.1D) mode.

Default: MSTP-operation.

The `no` form of this command returns the switch to the default 802.1s native mode (MSTP-operation)

## Setting spanning tree to operate with 802.1D legacy path cost values

### Syntax:

```
spanning-tree legacy-path-cost
```

Forces spanning tree to operate with legacy (802.1D) path cost values.

Default: 802.1t.

The `no` form of the command returns the switch to the default 802.1t (not legacy) path cost values.

## Specifying the time interval between BPDU transmissions

### Syntax:

```
spanning-tree hello-time <1..10>
```

If MSTP is running and the switch is operating as the CIST (Common and Internal Spanning Tree) root for your network, this command specifies the time in seconds between transmissions of BPDUs for all ports on the switch configured with the Global option (the default). This parameter applies in MSTP, RSTP and STP modes.

During MSTP operation, you can override this global setting on a per-port basis with this command: `spanning-tree <port-list> hello-time <1..10>`.

Default: 2 seconds.

## Setting the hop limit for BPDUs

### Syntax:

```
spanning-tree max-hops <hop-count>
```

Resets the number of hops allowed for BPDUs in an MST region. When an MSTP switch receives a BPDU, it decrements the hop-count setting the BPDU carries. If the hop-count reaches zero, the receiving switch drops the BPDU.

The switch does not change the message-age and maximum-age data carried in the BPDU as it moves through the MST region and is propagated to other regions.

Range: 1 - 40 Default: 20

## Setting the maximum age of received STP information

### Syntax:

```
spanning-tree maximum age
```

Sets the maximum age time for received STP information before it is discarded.

Default: 20 seconds

## Manipulating the pending MSTP configuration

### Syntax:

```
spanning-tree pending [ apply | <config-name> | <config-revision> |  
<instance> | reset ]
```

Manipulates the pending MSTP configuration. The command is useful in test or debug applications and enables rapid reconfiguration of the switch for changes in spanning tree operation.

**apply** Applies pending MSTP configuration (swaps active and pending configurations).

**<config-name>** Sets the pending MST region configuration name. Default is the switch's MAC address.

**<config-revision>** Sets the pending MST region configuration revision number. Default is 0.

**<instance>** Change pending MST instance configuration.

**reset** Copies the active configuration to pending.

## Setting the bridge priority for a region and determining the root switch

### Syntax:

```
spanning-tree priority <priority-multiplier>
```

Every switch running an instance of MSTP has a Bridge Identifier, which is a unique identifier that helps distinguish this switch from all others. The switch with the lowest Bridge Identifier is elected as the root for the tree.

The Bridge Identifier is composed of a configurable Priority component (2 bytes) and the bridge's MAC address (6 bytes). The ability to change the Priority component provides flexibility in determining which switch will be the root for the tree, regardless of its MAC address.

This command sets the switch (bridge) priority for the designated region in which the switch resides. The switch compares this priority with the priorities of other switches in the same region to determine the root switch for the region. The lower the priority value, the higher the priority. If there is only one switch in the region, then that switch is the root switch for the region. The root bridge in a region provides the path to connected regions for the traffic in VLANs assigned to the region's IST instance. Traffic in VLANs assigned to a numbered STP instance in a given region moves to other regions through the root switch for that instance.

The priority range for an MSTP switch is 0-61440. However, this command specifies the priority as a multiplier (0 - 15) of 4096. That is, when you specify a priority multiplier value of 0 - 15, the actual priority assigned to the switch is:

$(\text{priority-multiplier}) \times 4096$

For example, with 2 as the priority-multiplier on a given MSTP switch, the Switch Priority setting is 8,192.



---

**NOTE:** If multiple switches in the same MST region have the same priority setting, then the switch with the lowest MAC address becomes the root switch for that region.

---

## Enabling SNMP traps

### Syntax:

```
[no] spanning-tree trap { errant-bpdu | loop-guard | new-root | root-guard }
```

Enables or disables SNMP traps for errant-BPDU, loop guard, new root and root guard event notifications. This command is designed to be used with the `spanning-tree bpdu-filter` command (see [“Configuring BPDU filtering” \(page 100\)](#)) and the `bpdu-protection` command (see [“Enabling and disabling BPDU protection” \(page 101\)](#)).

`errant-bpdu` Enables SNMP notification when an errant BPDU is received. Designed for use with BPDU filtering (See [“Configuring BPDU filtering” \(page 100\)](#)).

`loop-guard` Enables SNMP notification when a loop guard inconsistency is detected. Designed for use with the Loop Guard option (See [“STP loop guard” \(page 121\)](#)).

`new-root` Enables SNMP notification when a new root is elected on any VLAN configured for MSTP on the switch.

`root-guard` Enables SNMP notification when a root guard inconsistency is detected. See [“Denying a port the role of root port” \(page 99\)](#).

Default for all of the above options: Disabled

The `no` form of the command disables traps on the switch.

## Configuring MSTP per-port parameters

In an MSTP topology, per-port parameters are set in the global configuration context. In most cases, HP recommends that you use the default settings for these parameters and apply changes on a per-port basis only where a non-default setting is clearly indicated by the circumstances of individual links. Some port parameters (such as `admin-edge-port`) affect all MSTI instances that consist of VLANs configured on the port. Other port parameters (such as `path-cost`) affect only the specified MST.

## Enabling immediate transition to forwarding on end nodes

### Syntax:

```
[no] spanning-tree <port-list> admin-edge-port
```

Enables `admin-edge-port` on ports connected to end nodes. During spanning tree establishment, ports with `admin-edge-port` enabled transition immediately to the forwarding state. If a bridge or switch is detected on the segment, the port automatically operates as non-edge, not enabled.

Default: Disabled

If `admin-edge-port` is disabled on a port and `auto-edge-port` has not been disabled, the `auto-edge-port` setting controls the behavior of the port.

The `no` form of this command disables edge port operation on the specified ports.

## Identifying edge ports automatically

### Syntax:

```
[no] spanning-tree <port-list> auto-edge-port
```

Enables the automatic identification of edge ports for faster convergence. When enabled, the port will look for BPDUs for the first 3 seconds. If there are none, the port will be classified as an edge port and it immediately start forwarding packets. If BPDUs are seen on the port, it will be classified as a non-edge port and normal STP operation will commence on that port.

If `admin-edge-port` is enabled for a port, the setting for `auto-edge-port` is ignored whether set to yes or no.

If `admin-edge-port` is set to no and `auto-edge-port` has not been disabled (set to no), then the `auto-edge-port` setting controls the behavior of the port.

Default: Enabled

The no form of this command disables `auto-edge-port` operation on the specified ports.

## Specifying the interval between BPDU transmissions

### Syntax:

```
spanning-tree <port-list> hello-time [ global | <1 - 10> ]
```

When the switch is the CIST root, this parameter specifies the interval (in seconds) between periodic BPDU transmissions by the designated ports. This interval also applies to all ports in all switches downstream from each port in the `<port-list>`.

A setting of `global` indicates that the ports in `<port-list>` on the CIST root are using the value set by the global spanning tree `hello-time` value.

When a given switch X is not the CIST root, the per-port `hello-time` for all active ports on switch X is propagated from the CIST root and is the same as the `hello-time` in use on the CIST root port in the currently active path from switch X to the CIST root. When switch X is not the CIST root, then the upstream CIST root's port `hello-time` setting overrides the `hello-time` setting configured on switch X.

Default Per-Port setting: Use Global.

Default Global Hello-Time: 2.

## Forcing a port to send RST/MST BPDUs

### Syntax:

```
spanning-tree <port-list> mcheck
```

Forces a port to send RST/MST BPDUs for 3 seconds. This tests whether all STP bridges on the attached LAN have been removed and the port can migrate to native MSTP mode and use RST/MST BPDUs for transmission.

## Determining which ports are forwarding ports by assigning port cost

### Syntax:

```
spanning-tree <port-list> path-cost [ auto | <1..200000000> ]
```

Assigns an individual port cost that the switch uses to determine which ports are forwarding ports in a given spanning tree. In the default configuration (auto) the switch determines a port's path cost by the port's type:

10 Mbps	2000000
100 Mbps	200000
1 Gbps	20000

See XXX—KH for information on compatibility with devices running 802.1D STP for the path cost values

Default: Auto

## Informing the switch of the device type to which a port connects

### Syntax:

```
spanning-tree <port-list> point-to-point-mac [ true | false | auto ]
```

Informs the switch of the type of device to which a specific port connects.

**true** (Default) Indicates a point-to-point link to a device such as a switch, bridge, or end-node.

**false** Indicates a connection to a half-duplex repeater (which is a shared LAN segment).

**auto** Causes the switch to set Force-False on the port if it is not running at full duplex.

## Determining which port to use for forwarding

### Syntax:

```
spanning-tree <port-list> priority <priority-multiplier>
```

MSTP uses this parameter to determine the port to use for forwarding. The port with the lowest priority number has the highest priority for use.

The range is 0 to 240 and is configured by specifying a multiplier from 0 - 15.

When you specify a priority multiplier of 0 - 15, the actual priority assigned to the switch is:

$(\text{priority-multiplier}) \times 16$

If you configure 2 as the priority multiplier on a given port, the actual Priority setting is 32. After specifying the port priority multiplier, the switch displays the actual port priority (and not the multiplier) in the `show spanning-tree` or `show spanning-tree <port-list>` displays.

You can view the actual multiplier setting for ports by executing `show running` and looking for an entry in this format:

```
spanning-tree <port-list> priority <priority-multiplier>
```

For example, configuring port A2 with a priority multiplier of 3 results in the following line in the `show running` output:

```
spanning-tree A2 priority 3
```

## Denying a port the role of root port

### Syntax:

```
spanning-tree <port-list> root-guard
```

When a port is enabled as `root-guard`, it cannot be selected as the root port even if it receives superior STP BPDUs. The port is assigned an "alternate" port role and enters a blocking state if it receives superior STP BPDUs.

A superior BPDU contains both "better" information on the root bridge and path cost to the root bridge, which would normally replace the current root bridge selection.

The superior BPDUs received on a port enabled as `root-guard` are ignored. All other BPDUs are accepted and the external devices may belong to the spanning tree as long as they do not claim to be the Root device.

Use this command on MSTP switch ports that are connected to devices located in other administrative network domains to:

- Ensure the stability of the core MSTP network topology so that undesired or damaging influences external to the network do not enter.
- Protect the configuration of the CIST root bridge that serves as the common root for the entire network.

Default: Disabled

## Denying a port propagation change information

### Syntax:

```
spanning-tree <port-list> tcn-guard
```

When enabled for a port, this causes the port to stop propagating received topology change notifications and topology changes to other ports.

Default: Disabled

## Configuring BPDU filtering

The STP BPDU filter feature allows control of spanning tree participation on a per-port basis. It can be used to exclude specific ports from becoming part of spanning tree operations. A port with the BPDU filter enabled will ignore incoming BPDU packets and stay locked in the spanning tree forwarding state. All other ports will maintain their role.

### Syntax:

```
[no] spanning-tree [ <port-list> | all] bpdu-filter
```

Enables or disables the BPDU filter feature on specified port(s). This forces a port to always stay in the forwarding state and be excluded from standard STP operation.

Sample scenarios in which this feature may be used are:

- To have STP operations running on selected ports of the switch rather than every port of the switch at a time.
- To prevent the spread of errant BPDU frames.
- To eliminate the need for a topology change when a port's link status changes. For example, ports that connect to servers and workstations can be configured to remain outside of spanning tree operations.
- To protect the network from denial of service attacks that use spoofing BPDUs by dropping incoming BPDU frames. For this scenario, BPDU protection offers a more secure alternative, implementing port shut down and a detection alert when errant BPDU frames are received.

---

**△ CAUTION:** Ports configured with the BPDU filter mode remain active (learning and forward frames); however, spanning tree cannot receive or transmit BPDUs on the port. The port remains in a forwarding state, permitting all broadcast traffic. This can create a network storm if there are any loops (that is, trunks or redundant links) using these ports. If you suddenly have a high load, disconnect the link and disable the `bpdu-filter` (using the `no` command).

---

## Example 62 Configuring BPDU filtering

To configure BPDU filtering on port a9, enter:

```
HP Switch(config)#: spanning-tree a9 bpdu-filter
```

## Viewing BPDU filtering

Syntax:

```
spanning-tree show <port> configuration
```

Displays the BPDU filter state.

## Example 63 Displaying BPDU filter status using the show spanning tree command

```
HP Switch(config)# show spanning-tree a9 config
```

Port	Type	Path Cost	Prio rity	Admin Edge	Auto Edge	Admin PtP	Hello Time	Root Guard	TCN Guard	BPDU Flt
A9	100/1000T	Auto	128	No	Yes	True	Global	No	No	Yes

Column showing BPDU filter status

## Example 64 Displaying BPDU filters using the show configuration command

This example shows how BPDU filters per port are displayed as separate entries of the spanning tree category within the configuration file.

```
HP Switch(config)# show configuration
```

```
...
spanning-tree
spanning-tree A9 bpdu-filter
spanning-tree C7 bpdu-filter
spanning-tree Trk2 priority 4
...
```

Rows showing ports with BPDU filters enabled

## Enabling and disabling BPDU protection

Syntax:

```
[no] spanning-tree <port-list> bpdu-protection
```

Enables or disables BPDU protection on specified port(s).

Syntax:

```
[no] spanning-tree <port-list> bpdu-protection-timeout <timeout>
```

Configures the duration in seconds when protected ports receiving unauthorized BPDUs will remain disabled. The default value of 0 (zero) sets an infinite timeout (that is, ports that are disabled by bpdu-protection are not, by default, re-enabled automatically).

Range: 0-65535 secondsDefault: 0

Syntax:

```
[no] spanning-tree trap errant-bpdu
```

Enables or disables the sending of errant BPDU traps.

- △ **CAUTION:** This command should only be used to guard edge ports that are not expected to participate in STP operations. Once BPDU protection is enabled, it will disable the port as soon as any BPDU packet is received on that interface.

### Example 65 Configuring BPDU protection

To configure BPDU protection on ports 1 to 10 with SNMP traps enabled, enter:

```
HP Switch(config)#: spanning-tree 1-10 bpdu protection
HP Switch(config)#: spanning-tree trap errant-bpdu
```

The following steps will then be set in progress:

1. When an STP BPDU packet is received on ports 1-10, STP treats it as an unauthorized transmission attempt and shuts down the port that the BPDU came in on.
2. An event message is logged and an SNMP notification trap is generated.
3. The port remains disabled until re-enabled manually by a network administrator using the interface `<port-list> enable` command.

**NOTE:** To re-enable the BPDU-protected ports automatically, configure a timeout period using the `spanning-tree bpdu-protection-timeout` command.

## Viewing BPDU protection status

Syntax:

```
show spanning-tree bpdu-protection
```

Displays a summary listing of ports with BPDU protection enabled. To display detailed per port status information, enter the specific port numbers as shown here.

Figure 18 Displaying BPDU protection status

```
HP Switch(config)# show spanning-tree bpdu-protection a1
Status and Counters - STP BPDU Protection Information
BPDU Protection Timeout (sec) : 0
Protected Ports : A1
```

Port	Type	Protection	State	Errant BPDUs
A1	100/1000T	Yes	Bpdu Error	1

Specifying the port displays additional status information for the designated ports.

BPDU protected ports are displayed as separate entries of the spanning tree category within the configuration file.

Figure 19 Displaying BPDU filters using the `show configuration` command

```
HP Switch(config)# show configuration
. . .
spanning-tree
spanning-tree A1 bpdu-protection
spanning-tree C7 bpdu-protection
spanning-tree Trk2 priority 4
. . .
```

Rows showing ports with BPDU protection enabled

# Configuring PVST

## Enabling and disabling PVST protection on ports

### Syntax:

```
[no] spanning-tree <port-list> pvst-protection
```

Enables or disables PVST protection on the port(s) specified. The command indicates which ports are not expected to receive any PVST BPDUs.

Default: Disabled on all ports.

### Example 66 Enabling PVST protection

---

To enable the PVST protection feature on ports 4 through 8, enter:

```
HP Switch(config)#: spanning-tree 4-8 pvst-protection
```

To disable the PVST protection feature on a port, for example, port 4, enter:

```
HP Switch(config)#: no spanning-tree 4 pvst-protection
```

---

## Enabling and disabling PVST filters on ports

### Syntax:

```
[no] spanning-tree <port-list> pvst-filter
```

Enables or disables PVST filters on the port(s) specified. The command indicates which ports are not expected to receive any PVST BPDUs.

Default: Disabled on all ports

### Example 67 Enabling PVST filtering on a port

---

```
HP Switch(config)#: spanning-tree 8 pvst-filter
```

Warning: The BPDU filter allows the port to go into a continuous forwarding mode and spanning-tree will not interfere, even if the port would cause a loop to form in the network topology.

If you suddenly experience high traffic load, disable the port and reconfigure the BPDU filter with the CLI command(s):

```
"no spanning-tree PORT_LIST bpdu-filter"  
"no spanning-tree PORT_LIST pvst-filter"
```

---

## Re-enabling a port manually

### Syntax:

```
[no] spanning-tree bpdu-protection-timeout <timeout>
```

Configures the duration of time protected ports remain disabled. The default value of 0 sets an infinite timeout, so ports that are disabled are not re-enabled automatically.

---

**NOTE:** This is a GLOBAL command.

---

Range: 0 - 65535 seconds Default: 0

You can also set the timeout in the MIB with this MIB object:

```
hpSwitchStpBpduProtectionTimeout
```

It is also possible to use the following automatic re-enable timer command:

```
HP Switch(config)#: spanning-tree bpdu-protection-timeout 120
```

## Displaying ports configured with PVST protection and filtering

### Example 68 Displaying all ports with PVST protection enabled

---

```
HP Switch(config)#: show spanning-tree pvst-protection

Status and Counters - PVST Port(s) BPDU Protection Information

BPDU Protection Timeout (sec) : 0
PVST Protected Ports : 5-6
```

---

### Example 69 Displaying all ports with PVST filtering enabled

---

```
HP Switch(config)#: show spanning-tree pvst-filter
Status and Counters - PVST Port(s) BPDU Filter Information
PVST Filtered Ports : 8
```

---

## Listing ports to see which have PVST protection or filtering enabled

### Syntax:

```
show spanning-tree <port-list> detail
```

### Example 70 Displaying if PVST protection is enabled (Yes)

---

```
.HP Switch(config)# show spanning-tree 7 detail
.
.
.
Port                : 7
  Status             : Down
  BPDU Protection    : Yes
  BPDU Filtering     : No
  PVST Protection    : Yes
  PVST Filtering     : No
  Errant BPDU Count  : 0
  Root Guard        : No
  TCN Guard         : No
.
.
.
```

## Configuring MST instances

### Configuring MST instance parameters

When you enable MSTP on the switch, a spanning tree instance is enabled automatically. The switch supports up to 16 configurable MST instances for each VLAN group that you want to operate as an active topology within the region to which the switch belongs. When creating an instance, you must include a minimum of one VID. You can add more VIDs later if desired.

### Syntax:

```
[no] spanning-tree instance <1..16> vlan <vid> [<vid..vid>]
```

Configuring MSTP on the switch automatically configures the IST instance and places all statically and dynamically configured VLANs on the switch into the IST instance.



This command creates a new MST instance (MSTI) and moves the VLANs you specify from the IST to the MSTI.

You must map at least one VLAN to an MSTI when you create it. You cannot map a VLAN ID to more than one instance. You can create up to 16 MSTIs in a region. The `no` form of the command removes one or more VLANs from the specified MSTI. If no VLANs are specified, the `no` form of the command deletes the specified MSTI.

When you remove a VLAN from an MSTI, the VLAN returns to the IST instance, where it can remain or be re-assigned to another MSTI configured in the region.

---

**NOTE:** Starting in software release 13.x.x, you can enter the `spanning-tree instance vlan` command before a static or dynamic VLAN is configured on the switch to preconfigure VLAN ID-to-MSTI mappings. No error message is displayed. Later, each newly configured VLAN that has already been associated with an MSTI is automatically assigned to the MSTI.

---

This new default behavior differs from automatically including configured (static and dynamic) VLANs in the IST instance and requiring the manual assigning of individual static VLANs to an MSTI.

---

**NOTE:** The valid VLAN IDs that you can map to a specified MSTI are from 1 to 4094. The VLAN ID-to-MSTI mapping does not require a VLAN to be already configured on the switch. The MSTP VLAN enhancement allows you to preconfigure MSTP topologies before the VLAN IDs associated with each instance exist on a switch.

---

## Setting the bridge priority for an instance

### Syntax:

```
spanning-tree instance <1..16> priority <priority-multiplier>
```

Sets the switch (bridge) priority for the designated instance. This priority is compared with the priorities of other switches in the same instance to determine the root switch. The lower the priority value, the higher the priority. If there is only one switch in the instance, then that switch is the root switch for the instance. The IST regional root bridge provides the path to instances in other regions that share one or more of the same VLANs.

The priority range for an MSTP switch is 0 - 61440. However, this command specifies the priority as a multiplier (0 - 15) of 4096. When a priority multiplier value is set from 0 - 15, the actual priority assigned to the switch for the specified MST instance is:  $(\text{priority-multiplier}) \times 4096$

For example, if you configure 5 as the priority-multiplier for MST Instance 1 on a given MSTP switch, the Switch Priority setting is 20,480 for that instance in that switch.

---

**NOTE:** If multiple switches in the same MST instance have the same priority setting, the switch with the lowest MAC address becomes the root switch for that instance.

---

## Configuring MST instance per-port parameters

### Assigning a port cost for an MST instance

#### Syntax:

```
spanning-tree instance <ist | 1..16> <port-list> path-cost [ auto  
| <1..200000000> ]
```

Assigns an individual port cost for the IST or for the specified MST instance.

For a given port, the path cost setting can be different for different MST instances to which the port may belong. The switch uses the path cost to determine which ports are the forwarding ports in the instance; that is, which links to use for the active topology of the instance and which ports to block.

The settings are either `auto` or in a range from 1 to 200,000,000. With the `auto` setting, the switch calculates the path cost from the link speed:

10 Mbps	2000000
100 Mbps	200000
1 Gbps	20000
Default	Auto

## Setting the priority for a port in a specified MST instance

### Syntax:

```
spanning-tree instance <1..16 port-list> priority <priority-multiplier>
```

Sets the priority for the specified ports in the specified MST instance.

For a given port, the priority setting can be different for different MST instances to which the port may belong. The priority range for a port in a given MST instance is 0 - 255. However, this command specifies the priority as a multiplier (0 - 15) of 16. When you specify a priority multiplier of 0 - 15, the actual priority assigned to the switch is: (priority-multiplier) x 16

### Example 71 Setting priority for a port in a specified MST instance

---

If you configure 2 as the priority multiplier on a given port in an MST instance, then the actual Priority setting is 32x. After you specify the port priority multiplier in an instance, the switch displays the actual port priority and not the multiplier in the `show spanning-tree instance <1..16>` or `show spanning-tree <port-list> instance <1..16>` displays.

You can view the actual multiplier setting for ports in the specified instance by executing `show running` and looking for an entry in the following format:

```
spanning-tree instance < 1..15 port-list> priority <priority-multiplier>
```

For example, configuring port A2 with a priority multiplier of 3 in instance 1, results in this line in the `show running` output:

```
spanning-tree instance 1 A2 priority 3
```

---

## Setting the priority for specified ports for the IST

### Syntax:

```
spanning-tree <port-list> priority <priority-multiplier>
```

Sets the priority for the specified ports for the IST (Instance 0) of the region in which the switch resides.

The priority component of the port's Port Identifier is set. The Port Identifier is a unique identifier that helps distinguish this switch's ports from all others. It consists of the priority value with the port number extension—PRIORITY:PORT\_NUMBER. A port with a lower value of Port Identifier is more likely to be included in the active topology.

This priority is compared with the priorities of other ports in the IST to determine which port is the root port for the IST instance. The lower the priority value, the

higher the priority. The IST root port (or trunk) in a region provides the path to connected regions for the traffic in VLANs assigned to the region's IST instance.

The priority range for a port in a given MST instance is 0 - 240. However, this command specifies the priority as a multiplier (0 - 15) of 16. When you specify a priority multiplier of 0 - 15, the actual priority assigned to the switch is: (priority-multiplier) x 16

### Example 72 Setting priority for specified ports for an IST

---

Configuring 5 as the priority multiplier on a given port in the IST instance for a region creates an actual priority setting of 80. After specifying the port priority multiplier for the IST instance, the switch displays the actual port priority, not the multiplier, in the `show spanning-tree instance ist` or `show spanning-tree <port-list> instance ist` displays. You can view the actual multiplier setting for ports in the IST instance by executing `show running` and looking for an entry in this format:

```
spanning-tree <port-list> priority <priority-multiplier>
```

So configuring port A2 with a priority multiplier of 2 in the IST instance, results in this line in the `show running` output:

```
spanning-tree A2 priority 2
```

---

## Enabling or disabling spanning tree operation

This command enables or disables spanning tree operation for any spanning tree protocol enabled on the switch. Before using to enable spanning tree, ensure that the right version is active on the switch.

### Syntax:

```
[no] spanning-tree
```

Enables or disables spanning tree. Enabling spanning tree with MSTP configured, implements MSTP for all physical ports on the switch according to the VLAN groupings for the IST instance and any other configured instances.

Disabling MSTP removes protection against redundant loops that can significantly slow or halt a network.

This command simply turns spanning tree on or off. It does not change the existing spanning tree configuration.

---

**NOTE:** The convergence time for implementing MSTP changes can be disruptive to your network. To minimize such disruption, consider using the `spanning-tree pending` command (see [“Enabling an entire MST region at once or exchanging one region configuration for another”](#) (page 107)).

---

## Enabling an entire MST region at once or exchanging one region configuration for another

This operation exchanges the currently active MSTP configuration with the currently pending MSTP configuration, making it possible to implement a new MSTP configuration with minimal network disruption or to exchange MSTP configurations for testing or troubleshooting purposes.

When configuring or reconfiguring MSTP, the switch recalculates the corresponding network paths. This can have a ripple effect throughout your network as adjacent MSTP switches recalculate network paths to support the configuration changes invoked in a single switch. Although MSTP employs rapid spanning tree operation, the convergence time for implementing MSTP changes can be disruptive to your network. However, by using the `spanning-tree pending` feature,

you can set up an MSTP on the switch and then invoke all instances of the new configuration at the same time, instead of one at a time.

### Syntax:

```
[no] spanning-tree pending[ apply | <config-name> | <config-revision>
| instance | reset ]
```

Exchanges the currently active MSTP configuration with the current pending MSTP configuration. Options are as follows:

<code>apply</code>	Exchanges the currently active MSTP configuration with the pending MSTP configuration.
<code>&lt;config-name&gt;</code>	Specifies the pending MST region name. Must be the same for all MSTP switches in the region. (Default: The switch's MAC address.)
<code>&lt;config-revision&gt;</code>	Specifies the pending MST region configuration revision number. Must be the same for all MSTP switches in the region. (Default: 0).
<code>instance &lt;1..16&gt; vlan [ vid   &lt;vid-range&gt; ]</code>	Creates the pending instance and assigns one or more VLANs to the instance.
<code>reset</code>	Copies the switch's currently active MSTP configuration to the pending configuration. This is useful when you want to experiment with the current MSTP configuration while maintaining an unchanged version.

## Creating a pending MSTP configuration

To create a pending MSTP configuration and exchange it with the active MSTP configuration:

1. Configure the VLANs to include in any instances in the new region. When you execute the `pending` command, all VLANs configured on the switch will be assigned to a single pending IST instance unless assigned to other, pending MST instances. The `pending` command creates the region's IST instance automatically.
2. Configure MSTP as the spanning tree protocol, then execute `write mem` and reboot. The `pending` option is available only with MSTP enabled.
3. Configure the pending region `<config-name>` to assign to the switch.
4. Configure the pending `<config-revision>` number for the region name.
5. If you want an MST instance other than the IST instance, configure the instance number and assign the appropriate VLANs (VIDs) using the `pending instance <1..16> vlan [ vid | <vid-range> ]` command.
6. Repeat step 5 for each additional MST instance necessary.
7. To review your pending configuration, use the `show spanning-tree pending` command.
8. To exchange the currently active MSTP configuration with the pending MSTP configuration, use the `spanning-tree pending apply` command.

# MSTP topologies

## Preconfiguring an MSTP regional topology

Starting in software release 13.X.X, the MSTP VLAN configuration enhancement allows you to preconfigure an MSTP regional topology and ensure that the same VLAN ID-to-MSTI assignments exist on each MSTP switch in the region.

- △ CAUTION:** When this software version is installed, the prior VLAN ID-to-MSTI mappings do not change. However, this enhancement is not backward-compatible. If you install a software version earlier than this version and you have configured MSTI entries instances mapped to VLANs, they will be removed from the configuration file when booting to the prior version of software. Do one of the following to install or reload a prior version of the software:
1. Remove all MSTP mappings from the configuration file, then reconfigure the instance mapping after running the desired software version.
  2. Save the current configuration file before updating the software to a new version. If you later reload this older version of the software, use this configuration file when you reload the older version. See [“Saving the current configuration before a software upgrade”](#) (page 111).

The default behavior of the `spanning-tree instance vlan` command changes so that, before a static VLAN is configured or a dynamic VLAN is learned on the switch, you can preconfigure its VLAN ID-to-MSTI mapping. Later, when the VLAN is created, it is automatically assigned to the MSTI to which it was previously mapped.

By supporting preconfigured VLAN ID-to-MSTI topologies, the VLAN configuration enhancement provides the following benefits:

- **Scalability:** In a network design in which you plan to use a large number of VLANs, you can preconfigure identical VLAN ID-to-MSTI mappings on all switches in a single, campus-wide MST region, regardless of the specific VLANs that you later configure on each switch. After the initial VLAN ID-to-MSTI mapping, you can decide on the exact VLANs that you need on each switch.  
All switches in a region must be configured with the same VLAN ID-to-MSTI mappings and the same MSTP configuration identifiers (region name and revision number).
- **Flexibility:** By preconfiguring identical VLAN ID-to-MSTI mappings on all switches in an MST region, you can combine switches that support different maximum numbers of VLANs.
- **Network stability:** You can reduce the interruptions in network connectivity caused by the regeneration of spanning trees in the entire network each time a configuration change in VLAN-to-MSTI mapping is detected on a switch. The negative impact on network performance is reduced if all newly created VLANs are pre-mapped to the correct MST instances. Later, VLAN creation and deletion are ignored by MSTP and no interruption in spanning tree traffic occurs.
- **Usability:** Dynamically learned GVRP VLANs can be mapped to MSTIs and support MSTP load balancing.

## Preconfiguring VLANs in an MST instance

When configuring an MSTP regional topology, multiple spanning tree instances are created. Each MST instance provides a fully connected active topology for a particular set of VLANs.

Each switch in an MSTP region is configured with the following set of common parameters:

- Region name (`spanning-tree config-name`)
- Region revision number (`spanning-tree config-revision`)
- Identical VLAN ID-to-MSTI mapping (`spanning-tree instance vlan`)

### Syntax:

```
[no] spanning-tree instance <1..16> vlan <vid> [<vid..vid>]
```

Configuring MSTP on the switch automatically configures the IST instance and places all statically and dynamically configured VLANs on the switch into the IST instance. This command creates a new MST instance (MSTI) and moves the VLANs specified from the IST to the MSTI.

You must map at least one VLAN to an MSTI when you create it. You cannot map a VLAN ID to more than one instance. You can create up to 16 MSTIs in a region.

The `no` form of the command removes one or more VLANs from the specified MSTI. If no VLANs are specified, the `no` form of the command deletes the specified MSTI.

When removing a VLAN from an MSTI, the VLAN returns to the IST instance, where it remains or is re-assigned to another MSTI configured in the region.

---

**NOTE:** The valid VLAN IDs to map to a specified MSTI are from 1 to 4094. The VLAN ID-to-MSTI mapping does not require a VLAN to be already configured on the switch. The MSTP VLAN enhancement allows preconfiguring MSTP topologies before the VLAN IDs associated with each instance exist on a switch.

---

When using preconfigured VLAN ID-to-MSTI topologies, ensure that MSTP switches remain in the same region by mapping all VLAN IDs used in the region to the same MSTIs on each regional switch.

Each MST instance supports a different set of VLANs. A VLAN that is mapped to an MST instance cannot be a member of another MST instance.

## Configuring MSTP instances with the VLAN range option (Example)

### Example 73 Mapping VLANs to MSTP Instance

If VLANs 1, 5 and 7 are currently present and you enter the following command, all the VLANs from 1 through 10 are included, even those VLANs that are not present.

```
HP Switch(config)#: spanning-tree instance 1 vlan 1-10
```

On HP switches other than those covered by this guide, only the VLANs that are present will be included, that is, only VLANs 1, 5 and 7. The switch will map these VLANs to MSTP Instance 1, which results in a Configuration Digest that is not the same as the Configuration Digest for the switches running this enhancement. (See [Example 74 “Mapping VLANs with the range option where all VLANs are included”](#) and [Example 75 “Mapping VLANs on other HP switches”](#))

[Example 74 “Mapping VLANs with the range option where all VLANs are included”](#) shows an example of an MSTP instance configured with the VLAN range option. All the VLANs are included in the instance whether they exist or not. [Example 75 “Mapping VLANs on other HP switches”](#) shows an example of an MSTP instance configured on another HP switch. Only VLANs 1, 5 and 7 are included in the instance.

### Example 74 Mapping VLANs with the range option where all VLANs are included

```
HP Switch(config)# show spanning-tree mst-config

MST Configuration Identifier Information
MST Configuration Name: MSTP1
MST Configuration Revision: 1
MST Configuration Digest: [0x51B7EBA6BEEED8702D2BA4497D4367517 ]

IST Mapped VLANs :

Instance ID Mapped VLANs
-----
1           1-10
```

The Configuration Digest value shown in [Example 75 “Mapping VLANs on other HP switches”](#) is not the same as in [Example 74 “Mapping VLANs with the range option where all VLANs are included”](#), indicating that these switches do not operate in the same instance.

The Common Spanning Tree (CST) will still have the correct root associations.

### Example 75 Mapping VLANs on other HP switches

```
HP Switch(config)# show spanning-tree mst-config

MST Configuration Identifier Information
MST Configuration Name: MSTP1
MST Configuration Revision: 1
MST Configuration Digest: [0x89D3ADV471668D6D832F6EC4AA9CF4AA ]

IST Mapped VLANs :

Instance ID Mapped VLANs
-----
1           1, 5, 7
```

See [“Operating notes for the VLAN configuration enhancement”](#) (page 141).

## Saving the current configuration before a software upgrade

Before updating to a new version of software, follow these steps:

1. Enter the `show config files` command to display your current configuration files:

```
HP Switch(config)#: show config files
```

Configuration files:

```
id | act pri sec | name
---+-----+-----
 1 | * * * | config1
 2 | | | | config2
 3 | | | |
```

2. To save a configuration file for software version K.12.43, enter this command:

```
HP Switch(config)#: copy config config1 config configK1243.cfg
```

Choose any name for the saved configuration file that you prefer.

3. Display the configuration files as shown in the following example. Note the newly created configuration file listed.

```
HP Switch(config)#: show config files
```

Configuration files:

```
id | act pri sec | name
---+-----+-----
 1 | * * * | config1
 2 | | | | config2
 3 | | | | configK1243.cfg
```

4. Update the switch to the desired version, for example, K.12.51. Enter the `show flash` command to see the results. The switch is now running the software version K.12.51.

```
HP Switch(config)#: show flash
```

```
Image          Size(Bytes)  Date    Version  Build #:
-----
Primary Image   : 6771179   04/17/08 K.12.51   304
Secondary Image : 7408949   11/06/08 K.12.43   123
Boot Rom Version: K.12.12
Default Boot    : Primary
```

5. To run the prior software version (K.12.43 in this example), enter this command:

```
HP Switch(config)#: boot system flash secondary config configK1243.cfg
```

After rebooting, the switch is running software version K.12.43 and is using the configuration file that you saved for this software version, `configK1243.cfg`.

You can also save the K.12.43 configuration file on a TFTP server. To reload the K.12.43 version of the software again, reload the configuration file before doing the reload.

## Displaying MSTP statistics

---

**NOTE:** SNMP MIB Support for MSTP is a superset of the STP/802.1D and RSTP/802.1w protocols and uses the MIB objects defined for these two protocols.

---

## Displaying global MSTP status

The following commands display the MSTP statistics for the connections between MST regions in a network.

### Syntax:

```
show spanning-tree
```

Displays the switch's global and regional spanning tree status, plus the per-port spanning tree operation at the regional level. Values for the following parameters



appear only for ports connected to active devices: Designated Bridge, Hello Time, PtP and Edge.

### Syntax:

```
show spanning-tree <port-list>
```

Displays the spanning tree status for the designated ports. You can list data for a series of ports and port trunks by specifying the first and last port or trunk of any consecutive series of ports and trunks. For example, to display data for port A20-A24 and trk1, you would use this command: `show spanning-tree a20-a24, trk1`

### Example 76 Displaying a common spanning tree status

```
HP Switch(config)# show spanning-tree
```

Multiple Spanning Tree (MST) Information

```

-----
| STP Enabled      : Yes
| Force Version   : MSTP-operation
| IST Mapped VLANs : 1,66
|
| Switch MAC Address : 0004ea-5e2000
| Switch Priority   : 32768
| Max Age         : 20
| Max Hops        : 20
| Forward Delay   : 15
|
| Topology Change Count : 0
| Time Since Last Change : 2 hours
|-----
| CST Root MAC Address : 00022d-47367f
| CST Root Priority     : 0
| CST Root Path Cost   : 4000000
| CST Root Port        : A1
|-----
| IST Regional Root MAC Address : 00883-028300
| IST Regional Root Priority     : 32768
| IST Regional Root Path Cost   : 200000
| IST Remaining Hops            : 19
|-----
| Protected Ports : A4
| Filtered Ports  : A7-A10
|-----

```

Switch's Spanning Tree Configuration and Identity of VLANs Configured in the Switch for the IST Instance

Identifies the overall spanning-tree root for the network.

Lists the switch's MSTP root data for connectivity with other regions and STP or RSTP devices.

Identifies the spanning-tree root for the IST Instance for the region.

Internal Spanning Tree Data (IST Instance) for the region in which the Switch Operates

Identifies the ports with BPDU protection and BPDU filtering enabled.

**Yes** means the switch is operating the port as if it is connected to switch, bridge, or end node (but *not* a hub).

Port	Type	Cost	Priority	State	Designated Bridge	Hello Time	PtP	Edge
A1	100/1000T	Auto	128	Forwarding	000883-028300	9	Yes	No
A2	100/1000T	Auto	128	Blocked	0001e7-948300	9	Yes	No
A3	100/1000T	Auto	128	Forwarding	000883-02a700	2	Yes	No
A4	100/1000T	Auto	128	Disabled				
A5	100/1000T	Auto	128	Disabled				
.	.	.	.	.				
.	.	.	.	.				

For Edge, No (admin-edge-port operation disabled) indicates the port is configured for connecting to a LAN segment that includes a bridge or switch. Yes indicates the port is configured for a host (end node) link. Refer to the **admin-edge-port** description under "Configuring MSTP Per-Port Parameters" on page 3-

### Displaying detailed port information

The following commands display the MSTP statistics for the connections between MST regions in a network.

### Syntax:

```
show spanning-tree detail
```

Displays additional parameters concerning the CST ports.

**Syntax:**

```
show spanning-tree <port-list> detail
```

Displays detailed spanning tree status for the designated ports.

**Example 77 Displaying port information**

```
HP Switch# show spanning-tree a9 detail

Status and Counters - CST Port(s) Detailed Information
-----
Port                : A9
Status              : Up
BPDU Filtering      : Yes
Errant BPUDUs received : 65
MST Region Boundary : Yes
External Path Cost  : 200000
External Root Path Cost : 420021
Administrative Hello Time : Use Global
Operational Hello Time : 2
AdminEdgePort       : No
OperEdgePort        : No
AdminPointToPointMAC : Force-True
OperPointToPointMAC : Yes
Aged BPDUs Count    : 0
Loop-back BPDUs Count : 0
TC ACK Flag Transmitted : 0
TC ACK Flag Received : 0

MST          MST          CFG          CFG          TCN          TCN
BPDUs Tx    BPDUs Rx    BPDUs Tx    BPDUs Rx    BPDUs Tx    BPDUs Rx
```

Gives information concerning the Common Spanning Tree (CST) only. Use the show spanning-tree instance commands to view counters pertaining to particular IST instances.

**NOTE:** This command gives information about the CST only. To view details of specific MST instances, use the show spanning tree instance commands.

**Displaying status for a specific MST instance**

The following commands display the MSTP statistics for a specified MST instance.

**Syntax:**

```
show spanning-tree instance [ ist | <1..16> ]
```

Displays the MSTP statistics for either the IST instance or a numbered MST instance running on the switch.

**Syntax:**

```
show spanning-tree instance [ ist | <1..16> ] detail
```

Displays status on all active ports for a specific instance of MSTP.

**Syntax:**

```
show spanning-tree <port-list> instance [ ist | <1..16> ] detail
```

Displays status on specified ports for a specific instance of MSTP.

## Example 78 Displaying status for a specific instance of an MSTP

This shows how to display detailed status for all active ports for a specific instance of MSTP.

```
HP Switch(config)#: show spanning-tree instance 11
```

```
MST Instance Information
  Instance ID : 11
  Mapped VLANs : 111,300
  Switch Priority      : 32768

  Topology Change Count : 2
  Time Since Last Change : 4 mins

  Regional Root MAC Address : 1cc1de-cfbc80
  Regional Root Priority    : 32768
  Regional Root Path Cost  : 400000
  Regional Root Port       : This switch is root
  Remaining Hops           : 20
```

Port	Type	Cost	Priority	Role	State	Designated Bridge
1	10/100TX	200000	128	Root	Forwarding	1cc1de-cfbc80
2	10/100TX	200000	128	Designated	Forwarding	1cc1de-02a700
3	10/100TX	Auto	112	Designated	Forwarding	1cc1de-02a700
4	10/100TX	Auto	128	Disabled	Disabled	
.	.	.	.	.	.	.

## Displaying the MSTP configuration

### Displaying the global MSTP configuration

This command displays the switch's basic and MST region spanning tree configuration, including basic port connectivity settings.

#### Syntax:

```
show spanning-tree config
```

The upper part of this output shows the switch's global spanning tree configuration that applies to the MST region. The port listing shows the spanning tree port parameter settings for the spanning tree region operation configured by the `spanning-tree <port-list>` command. For information on these parameters, see [“Configuring MSTP per-port parameters” \(page 97\)](#).

#### Syntax:

```
show spanning-tree <port-list> config
```

This command shows the same data as the above command, but lists the spanning tree port parameter settings for only the specified port or trunk. You can list data for a series of ports and port trunks by specifying the first and last port or trunk of any consecutive series of ports and trunks. For example, to display data for port A20-A24 and trunk 1, use the command: `show spanning-tree a20-a24, trk1 config`

Figure 20 Displaying the switch's global spanning tree configuration

```
Switch-2(config)# show spanning-tree config
```

Multiple Spanning Tree (MST) Configuration Information

STP Enabled [No] : Yes  
Force Version [MSTP-operation] : MSTP-operation

MST Configuration Name : REGION\_1  
MST Configuration Revision : 1  
Forward Delay [15] : 15  
Max Age [20] : 20

Switch Priority : 32768  
Hello Time [2] : 2  
Max Hops [20] : 20

Port	Type	Cost	Priority	Edge	Point-to-Point	MCheck	Hello Time
A3	10/100TX	Auto	128	Yes	Force-True	Yes	Use Global
A4	10/100TX	Auto	128	Yes	Force-True	Yes	Use Global
:	:	Per-Port Priority	:	:	:	:	:
A20	10/100TX	Auto	128	Yes	Force-True	Yes	Use Global
A21	10/100TX	Auto	128	Yes	Force-True	Yes	Use Global
A22	10/100TX	Auto	128	Yes	Force-True	Yes	Use Global
A23	10/100TX	Auto	128	Yes	Force-True	Yes	Use Global
A24	10/100TX	Auto	128	Yes	Force-True	Yes	Use Global
Trk1		Auto	128	Yes	Force-True	Yes	Use Global

### Displaying per-instance MSTP configurations

These commands display the per-instance port configuration and current state, along with instance identifiers and regional root data.

#### Syntax:

```
show spanning-tree config instance [ ist | <1..16> ]
```

The upper part of this output shows the instance data for the ist or for the specified instance. The lower part of the output lists the spanning tree port settings for the specified instance.

#### Syntax:

```
show spanning-tree <port-list> config instance [ ist | <1..16> ]
```

This command shows the same data as the preceding command, but lists the spanning tree port parameter settings for only the specified port or trunk. You can list data for a series of ports and port trunks by specifying the first and last port or trunk of any consecutive series of ports and trunks.

## Example 79 Displaying port data

```
Switch-2(config)# show spanning-tree config instance 1

MST Instance Configuration Information
-----
Instance ID : 1
Switch Priority : 32768
Mapped VLANs : 11,22
-----
Port Type      | Cost      | Priority
-----+-----+-----
A3  10/100TX   | Auto      | 128
A4  10/100TX   | Auto      | 128
A5  10/100TX   | Auto      | 128
.    .         | .         | .
.    .         | .         | .
A23 10/100TX   | Auto      | 128
A24 10/100TX   | Auto      | 128
Trk1 100000    | 100000    | 128
-----+-----+-----
```

Annotations in the image:

- An arrow points from a grey box labeled "Instance-Specific Data" to the first three lines of the output (Instance ID, Switch Priority, Mapped VLANs).
- An arrow points from a grey box labeled "Port Settings for the specified instance." to the table of port configurations.

To display data for ports A20-A24 and trk1, you would use the command:

```
HP Switch(config)#: show spanning-tree a20-a24,trk1 config instance 1
```

## Displaying the region-level configuration

This command is useful for quickly verifying the allocation of VLANs in the switch's MSTP configuration and for viewing the configured region identifiers.

**Syntax:**

```
show spanning-tree mst-config
```

**NOTE:** The switch computes the MSTP Configuration Digest from the VID to MSTI configuration mappings on the switch itself. As required by the 802.1s standard, all MSTP switches within the same region must have the same VID to MSTI assignments and any given VID can be assigned to either the IST or one of the MSTIs within the region. Thus, the MSTP Configuration Digest must be identical for all MSTP switches intended to belong to the same region. When comparing two MSTP switches, if their Digest identifiers do not match, they cannot be members of the same region. (See [Example 80 \(page 118\)](#).)

## Example 80 Displaying a region-level configuration

---

```
HP Switch(config)#: show spanning-tree net-config

MST Configuration Identifier Information

MST Configuration Name : REGION_1
MST Configuration Revision : 1
MST Configuration Digest : 0xDAD6A13EC5141980B7EBDA71D8991E7C

IST Mapped VLANs : 1,66

Instance ID Mapped VLANs
-----
1          11,22
2          33,44,55
```

---

## Displaying the pending MSTP configuration

This command displays the MSTP configuration the switch will implement if you execute the `spanning tree pending apply` command. See [“Enabling an entire MST region at once or exchanging one region configuration for another”](#) (page 107).

### Syntax:

```
show spanning-tree pending [ instance | mst-config ]
    instance [ <1..16> | ist ] Lists region, instance ID and VLAN
                                information for the specified, pending
                                instance.
    mst-config Lists region, IST instance VLANs, numbered
                instances and assigned VLAN information
                for the pending MSTP configuration.
```

## Example 81 Displaying a pending configuration

---

```
HP Switch(config)#: show spanning-tree pending instance 3

Pending MST Instance Configuration Information

MST Configuration Name : New-Version_01
MST Configuration Revision : 1
Instance ID : 3
Mapped VLANs : 3

Switch(config)#: show spanning-tree pending mst-config

Pending MST Configuration Identifier Information

MST Configuration Name : New-Version_01
MST Configuration Revision : 1

IST Mapped VLANs : 1,2,4-4094

Instance ID Mapped VLANs
-----
3          3
```

---

## Configuring loop protection

Loop protection provides protection against loops by transmitting loop protocol packets out of ports on which loop protection has been enabled. When the switch sends out a loop protocol packet

and then receives the same packet on a port that has a `receiver-action` of `send-disable` configured, it shuts down the port from which the packet was sent.

### Syntax:

```
[no] loop-protect <port-list> [[receiver-action [[<send-disable>] |  
[<no-disable>]]] | [transmit-interval <1-10>] | [disable-timer  
<0-604800>] | [trap loop-detected]][mode][[port] | [vlan]][vlan <vid-list>]
```

Configures per-port loop protection on the switch.

<code>receiver-action</code>	Sets the action to be taken when a loop is detected on the specified ports. The port that receives the loop protection packet determines what action is taken. If <code>send-disable</code> is configured, the port that transmitted the packet is disabled. If <code>no-disable</code> is configured, the port is not disabled when a loop is detected.
------------------------------	--

`send-disable | no-disable`

---

**NOTE:** The port will not transmit loop protection packets unless it is a member of an untagged VLAN. If a port is only a member of tagged VLANs, the loop protection packets are not transmitted.

---

Default: `send-disable`

`trap loop-detected`

Configures loop protection traps for SNMP indicating when a loop has been detected on a port.

`disable-timer <0-604800>`

Configures how long (in seconds) a port is disabled when a loop has been detected. A value of zero disables the auto re-enable function.

Default: Timer is disabled

`transmit-interval <1-10>`

Configures the time in seconds between the transmission of loop protection packets.

Default: 5 seconds

`mode port | vlan`

Configures loop protection in port or VLAN mode.

`vlan <vlan-id-list>`

Configures the VLANs on which `loop-protect` is enabled. Maximum number of loop-protected VLANs is 32.

## Enabling loop protection in port mode

Follow these steps.

1. Configure port mode with this command:

```
HP Switch(config)#: loop-protect mode port
```

2. Enter the `loop-protect` command and specify the ports on which loop protection should be enabled. For example:

```
HP Switch(config)#: loop-protect 1-2
```

3. Optionally specify receiver-action of send-disable to shut down the port in the event of a loop. For example:

```
HP Switch(config)#: loop-protect 1-2 receiver-action send-disable
```

## Enabling loop protection in VLAN mode

VLANs can be configured for loop protection only when operating in VLAN mode. When loop-protect is enabled for a VLAN and a loop-protect enabled interface is a member of that VLAN, loop protect packets are sent on that VLAN to detect loops.

To enable loop protection in VLAN mode:

1. Configure VLAN mode with the command:

```
HP Switch(config)#: loop-protect mode vlan
```

2. Enter the loop-protect command and specify the VLANs on which loop protection should be enabled. For example:

```
HP Switch(config)#: loop-protect vlan 20,30
```

## Changing modes for loop protection

When changing from VLAN mode to port mode, the following prompt appears. The VLANs are then no longer configured for loop protection.

### Example 82 Changing modes for loop protection

---

```
HP Switch(config)#: loop-protect mode port
Any Loop Protect enabled VLAN will be deleted. Do you want to continue [Y/N]?
N
```

---

## Displaying loop protection status

Syntax:

```
show loop-protect <port-list>
```

Displays the loop protection status for VLANs. If no ports are specified, the information is displayed only for ports with loop protection enabled.

### Example 83 Displaying loop protection information for port mode

---

```
HP Switch(config)#: show loop-protect 1-2
```

Status and Counters - Loop Protection Information

```
Transmit Interval (sec)      : 5
Port Disable Timer (sec)    : 5
Loop Detected Trap          : Enabled
Loop Protect Mode           : Port
Loop Protect Enabled VLANs :
```

Port	Loop Protect	Loop Detected	Detected on VLAN	Loop Count	Time Since Last Loop	Rx Action	Port Status
1	Yes	Yes		1	5s	send-disable	Down
2	Yes	No		0		send-disable	Up

---

## Displaying loop protection status in VLAN mode

Syntax:

```
show loop-protect <port-list>
```



Displays the loop protection status for VLANs. If no ports are specified, the information is displayed only for the ports that have loop protection enabled.

### Example 84 Displaying loop protection information for VLAN mode

```
HP Switch(config)#: show loop-protect 1-2
```

```
Status and Counters - Loop Protection Information
```

```
Transmit Interval (sec)      : 5
Port Disable Timer (sec)    : 5
Loop Detected Trap          : Enabled
Loop Protect Mode           : Vlan
Loop Protect Enabled VLANs  : 20,30
```

Port	Loop Protect	Loop Detected	Detected on VLAN	Loop Count	Time Since Last Loop	Rx Action	Port Status
1	Yes	Yes	20	1	45s	send-disable	Down
2	Yes	No		0		send-disable	Up

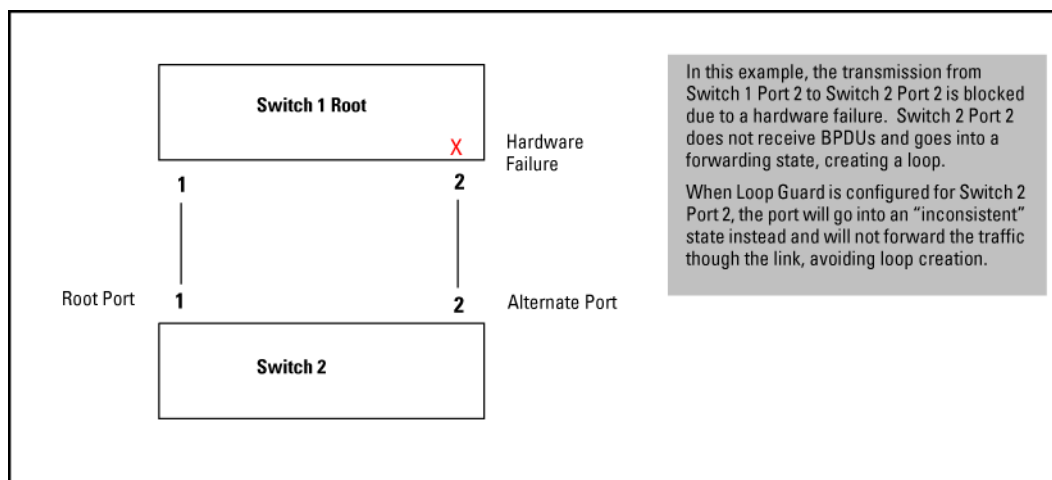
For more information, see “Loop protection” (page 143).

### STP loop guard

Spanning Tree (STP) is used to ensure a loop-free topology over the LAN. Occasionally a hardware or software failure can cause STP to fail, creating STP/forwarding loops that can cause network failures where unidirectional links are used. The non-designated port transitions in a faulty manner because the port is no longer receiving STP BPDUs.

STP Loop Guard causes the non-designated port to go into the STP loop inconsistent state instead of the forwarding state. In the loop-inconsistent state the port prevents data traffic and BPDU transmission through the link, therefore avoiding the loop creation. When BPDUs again are received on the inconsistent port, it resumes normal STP operation automatically. STP loop guard is best applied on blocking or forwarding ports.

Figure 21 Loop creation with transmission failure



### Syntax:

```
[no] spanning-tree <port-list> loop-guard
```

Enables STP loop guard on a particular port or ports. The `no` form of the command disables STP loop guard.

Default: Disabled.

## Example 85 Enabling spanning tree loop guard on Port 2 and displaying the port's status

```
HP Switch(config)#: spanning-tree 2 loop-guard
HP Switch(config)#: show spanning-tree
```

### Multiple Spanning Tree (MST) Information

```
STP Enabled      : Yes
Force Version    : MSTP-operation
IST Mapped VLANs : 1-4094
Switch MAC Address : 0024a8-d13a40
Switch Priority   : 32768
Max Age          : 20
Max Hops         : 20
Forward Delay    : 15
```

```
Topology Change Count : 1
Time Since Last Change : 20 mins
```

```
CST Root MAC Address : 001083-847000
CST Root Priority     : 0
CST Root Path Cost   : 60000
CST Root Port        : 1
```

```
IST Regional Root MAC Address : 0024a8-d13a40
IST Regional Root Priority     : 32768
IST Regional Root Path Cost   : 0
IST Remaining Hops            : 20
```

```
Root Guard Ports      :
Loop Guard Ports      : 2
TCN Guard Ports       :
BPDU Protected Ports  :
BPDU Filtered Ports   :
PVST Protected Ports  :
PVST Filtered Ports   :
```

Port	Type	Cost	Priority	State	Designated Bridge	Hello Time	PtP	Edge
1	100/1000T	20000	128	Forwarding	001871-cdea00	2	Yes	No
2	100/1000T	Auto	128	Inconsistent				
3	100/1000T	Auto	128	Disabled				
4	100/1000T	Auto	128	Disabled				
5	100/1000T	Auto	128	Disabled				
6	100/1000T	Auto	128	Disabled				
7	100/1000T	Auto	128	Disabled				
8	100/1000T	Auto	128	Disabled				

## Example 86 Displaying summary spanning tree configuration information

```
HP Switch(config)#: show spanning-tree config
```

```
Multiple Spanning Tree (MST) Configuration Information
```

```
STP Enabled [No] : Yes
Force Version [MSTP-operation] : MSTP-operation
Default Path Costs [802.1t] : 802.1t
MST Configuration Name : 0024a8d13a40
MST Configuration Revision : 0          Switch Priority : 32768
Forward Delay [15] : 15                Hello Time [2] : 2
Max Age [20] : 20                      Max Hops [20] : 20
```

Port	Type	Path Cost	Prio	Admin Edge	Auto Edge	Admin PtP	Hello Time	Root Guard	Loop Guard	TCN Guard	BPDU Flt
1	100/1000T	Auto	128	No	Yes	True	Global	No	No	No	No
2	100/1000T	Auto	128	No	Yes	True	Global	No	Yes	No	No
3	100/1000T	Auto	128	No	Yes	True	Global	No	No	No	No
4	100/1000T	Auto	128	No	Yes	True	Global	No	No	No	No
5	100/1000T	Auto	128	No	Yes	True	Global	No	No	No	No
6	100/1000T	Auto	128	No	Yes	True	Global	No	No	No	No
.											
.											
.											

## Example 87 Displaying detailed spanning tree configuration information

```
HP Switch(config)#: show spanning-tree detail
```

```
Status and Counters - CST Port(s) Detailed Information
```

```
Port : 1
Status : Up
```

```
.
```

```
Port : 2
Status : Up
BPDU Protection : No
BPDU Filtering : No
PVST Protection : No
PVST Filtering : No
Errant BPDU Count : 0
Root Guard : No
Loop Guard : Yes
TCN Guard : No
MST Region Boundary : Yes
External Path Cost : 20000
External Root Path Cost : 40000
Administrative Hello Time: Global
Operational Hello Time : 2
AdminEdgePort : No
Auto Edge Port : Yes
OperEdgePort : No
AdminPointToPointMAC : True
OperPointToPointMAC : Yes
Aged BPDUs Count : 0
Loop-back BPDUs Count : 0
TC ACK Flag Transmitted : 0
TC ACK Flag Received : 1
```

MST BPDUs Tx	MST BPDUs Rx	CFG BPDUs Tx	CFG BPDUs Rx	TCN BPDUs Tx	TCN BPDUs Rx
3	0	24354	1682	0	13

## Example 88 Displaying spanning tree configuration information for a single port

```
HP Switch(config)#: show spanning-tree 2
```

### Multiple Spanning Tree (MST) Information

```
STP Enabled      : Yes
Force Version    : MSTP-operation
IST Mapped VLANs : 1-4094
Switch MAC Address : 0024a8-d13a40
Switch Priority   : 32768
Max Age          : 20
Max Hops         : 20
Forward Delay    : 15

Topology Change Count : 1
Time Since Last Change : 58 mins

CST Root MAC Address : 001083-847000
CST Root Priority     : 0
CST Root Path Cost   : 60000
CST Root Port        : 1

IST Regional Root MAC Address : 0024a8-d13a40
IST Regional Root Priority     : 32768
IST Regional Root Path Cost   : 0
IST Remaining Hops            : 20

Root Guard Ports      :
Loop Guard Ports      : 2
TCN Guard Ports       :
BPDU Protected Ports :
BPDU Filtered Ports  :
PVST Protected Ports  :
PVST Filtered Ports   :
```

Port	Type	Cost	Priority	State	Designated Bridge	Hello Time	PtP Edge
2	100/1000T	Auto	128	Inconsistent			

## Troubleshooting an MSTP configuration

This section describes the `show spanning-tree` commands to use to monitor, troubleshoot and debug the operation of a multiple-instance spanning tree configuration in a network.

The `show spanning-tree` commands described in this section allow for focusing on increasingly specific levels of operation. For example, you can display debug information for:

- All MST instances
- All ports used in one MST instance
- A specific port or several ports used in one MST instance

Also, you can display the change history for the root (bridge) switch used as the single forwarding path for:

- All MST regions, STP bridges and RSTP bridges in an STP network
- All VLANs on MSTP switches in a region
- All VLANs on MSTP switches in an mst instance

## Displaying the change history of root bridges

The `show spanning-tree root-history` command lets you display change history information (up to 10 history entries) for a specified root bridge in any of the following MSTP topologies:

- **Common Spanning Tree (cst):**  
Provides connectivity in a bridged network between MST regions, STP LANs and RSTP LANs.
- **Internal Spanning Tree (ist):**  
Provides connectivity within an MST region for VLANs associated with the default Common and Internal Spanning Tree (CIST) instance in your network (VLANs that have not been mapped to an MST instance).
- **MST Instance (mst):**  
Connects all static and (from release 13.x.y ) dynamic VLANs assigned to a multiple spanning tree instance.

### Syntax:

```
show spanning tree root-history [ <cst | ist | mst > <instance-id> >
```

Displays the change history for the root bridge in the specified MSTP topology.

`cst` Displays the change history for the root bridge of a spanning tree network, including MST regions and STP and RSTP bridges.

`ist` Displays the change history for the root bridge in the IST instance of an MST region.

`mst <instance-id>` Displays the change history for the root bridge in an MST instance, where `<instance-id>` is an ID number from 1 to 16.

Use the `show spanning-tree root-history` command to view the number and dates of changes in the assignment of a root bridge. Possible intrusion into your MST network may occur if an unauthorized external device gains access to a spanning tree by posing as the root device in a topology. To prevent an MST port connected to the device from being selected as the root port in a topology, use the `spanning-tree root-guard` command.

## Example 89 Sample output of the `show spanning-tree root-history` command for different MSTP topologies

The following examples show sample output of the `show spanning-tree root-history` command for different MSTP topologies. In each example, the root bridge ID is displayed in the format: `<priority>: <mac-address>`

Where:

- `<priority>` is the MSTP switch priority calculated for one of the following:
  - The IST (regional) root switch using the `spanning-tree priority` command
  - An MSTI root switch using the `spanning-tree instance priority` command
- `<mac-address>` is the MAC address of the root (bridge) switch.

## Example 90 Displaying `show spanning-tree root-history CST` output

```
HP Switch(config)# show spanning-tree root-history cst

Status and Counters - CST Root Changes History

MST Instance ID      : 0
Root Changes Counter : 2
Current Root Bridge ID : 32768:000883-024500

Root Bridge ID      Date      Time
-----
32768:000883-024500 02/09/07 17:40:59
36864:001279-886300 02/09/07 17:40:22
```

Identifies the root bridge of the common spanning tree in a bridged network that connects different MST regions and STP or RSTP devices.

## Example 91 Displaying `show spanning-tree root-history IST` output

```
HP Switch(config)# show spanning-tree root-history ist

Status and Counters - IST Regional Root Changes History

MST Instance ID      : 0
Root Changes Counter : 2
Current Root Bridge ID : 32768:000883-024500

Root Bridge ID      Date      Time
-----
32768:000883-024500 02/09/07 17:40:59
36864:001279-886300 02/09/07 17:40:22
```

Identifies the root bridge of the internal spanning tree in an MST region.

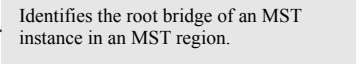
## Example 92 Displaying show spanning-tree root-history MSTI output

```
HP Switch(config)# show spanning-tree root-history mst 2

Status and Counters - MST Instance Regional Root Changes History

MST Instance ID      : 2
Root Changes Counter : 2
Current Root Bridge ID : 32770:000883-024500

Root Bridge ID      Date      Time
-----
32770:000883-024500 02/09/07 17:40:59
32770:001279-886300 02/09/07 17:40:22
```



### Displaying debug counters for all MST instances

The `show spanning-tree debug-counters` command allows you to display the aggregate values of all MSTP debug counters that are maintained on a switch. These aggregate values are a summary of the information collected from all ports and from all spanning tree instances that forward traffic on switch ports.

Use the displayed diagnostic information to globally monitor MSTP operation on a per-switch basis.

#### Syntax:

```
show spanning-tree debug-counters
```

Displays debug counters for MSTP activity on all ports configured for VLANs used in spanning tree instances.

## Example 93 Displaying output for debug counters

The following example shows sample output of the `show spanning-tree debug-counters` command for all ports.

```
HP Switch(config)#: show spanning-tree debug-counters
```

```
Status and Counters - MSTP Bridge Common Debug Counters Information
```

Counter Name	Aggregated Value	Collected From
Invalid BPDUs	0	CIST
Errant BPDUs	170927	CIST
MST Config Error BPDUs	0	CIST
Looped-back BPDUs	0	CIST
Starved BPDUs/MSTI MSGs	0	CIST/MSTIs
Exceeded Max Age BPDUs	0	CIST
Exceeded Max Hops BPDUs/MSTI MSGs	0	CIST/MSTIs
Topology Changes Detected	2	CIST/MSTIs
Topology Changes Tx	6	CIST/MSTIs
Topology Changes Rx	4	CIST/MSTIs
Topology Change ACKs Tx	0	CIST
Topology Change ACKs Rx	0	CIST
TCN BPDUs Tx	0	CIST
TCN BPDUs Rx	0	CIST
CFG BPDUs Tx	0	CIST
CFG BPDUs Rx	0	CIST
RST BPDUs Tx	0	CIST
RST BPDUs Rx	0	CIST
MST BPDUs/MSTI MSGs Tx	10	CIST/MSTIs
MST BPDUs/MSTI MSGs Rx	341802	CIST/MSTIs

## Displaying debug counters for one MST instance

The `show spanning-tree debug-counters instance` command lets you display the aggregate values of all MSTP debug counters maintained on a switch for a specified spanning tree instance. These aggregate values are a summary of information collected from all ports that have VLANs assigned to the specified instance.

Use this command to troubleshoot the global MSTP diagnostic information displayed in `show spanning-tree debug-counters` command output when you suspect unauthorized MSTP activity in a specific MST instance.

### Syntax:

```
show spanning-tree debug-counters instance <instance-id>
```

Displays debug counters for MSTP activity on all ports configured for VLANs in the specified MST instance.

The valid values for `instance <instance-id>` are 0 to 16, where 0 specifies the default MST (CIST) instance and 1 to 16 specify a multiple spanning tree (MST) instance.



## Example 94 Displaying debug counters for a CIST instance

The following example shows sample output of the `show spanning-tree debug-counters instance` command when applied to the Common and Internal Spanning Tree (CIST) instance (default MST instance 0) in the network.

```
HP Switch(config)#: show spanning-tree debug-counters instance 0
```

```
Status and Counters - CIST Common Debug Counters Information
```

```
MST Instance ID : 0
```

Counter Name	Aggregated Value	Collected From
Invalid BPDUs	0	Ports
Errant BPDUs	172603	Ports
MST Config Error BPDUs	0	Ports
Looped-back BPDUs	0	Ports
Starved BPDUs	0	Ports
Exceeded Max Age BPDUs	0	Ports
Exceeded Max Hops BPDUs	0	Ports
Topology Changes Detected	1	Ports
Topology Changes Tx	3	Ports
Topology Changes Rx	2	Ports
Topology Change ACKs Tx	0	Ports
Topology Change ACKs Rx	0	Ports
TCN BPDUs Tx	0	Ports
TCN BPDUs Rx	0	Ports
CFG BPDUs Tx	0	Ports
CFG BPDUs Rx	0	Ports
RST BPDUs Tx	0	Ports
RST BPDUs Rx	0	Ports
MST BPDUs Tx	5	Ports
MST BPDUs Rx	172577	Ports

## Displaying debug counters for ports in an MST instance

The `show spanning-tree debug-counters instance ports` command displays the aggregate values of all MSTP debug counters maintained on one or more ports used by a specified spanning tree instance. These aggregate values are a summary of information collected from the specified ports that have VLANs assigned to the specified instance.

Use this command to troubleshoot at a finer level the more general MSTP diagnostic information displayed in the `show spanning-tree debug-counters instance` command output, when you suspect unauthorized MSTP activity on one or more MST ports in an MST instance.

### Syntax:

```
show spanning-tree debug-counters instance <instance-id> ports  
<port-list>
```

Displays debug counters for MSTP activity on the specified ports configured for VLANs in the specified MST instance.

`instance <instance-id>` The valid values for `<instance-id>` are from 0 to 16, where 0 specifies the default MST (CIST) instance and 1 to 16 specify an MST instance.

`ports <port-list>` Specifies one or more MST ports or trunk ports. In the port list, enter a series of ports by separating the first and last ports in the series with a dash (-); for example, a2-a8 or

trk1-trk3. Separate individual ports and series of ports with a comma; for example, a2-a8, a20, trk1, trk4-trk5.

### Example 95 Displaying debug counters for a CIST and MST instance

---

The following example shows sample output of the `show spanning-tree debug-counters instance ports` command for both the CIST (default MST instance 0) and an MST instance (instance 2) on port A15.

```
HP Switch(config)#: show spanning-tree debug-counters instance 0 ports a15
```

```
Status and Counters - CIST Port(s) Debug Counters Information
```

```
MST Instance ID : 0  
Port : A15
```

Counter Name	Value	Last Updated
Invalid BPDUs	0	
Errant BPDUs	0	
MST Config Error BPDUs	0	
Looped-back BPDUs	0	
Starved BPDUs	0	
Exceeded Max Age BPDUs	0	
Exceeded Max Hops BPDUs	0	
Topology Changes Detected	1	02/09/07 17:40:59
Topology Changes Tx	3	02/09/07 17:41:03
Topology Changes Rx	2	02/09/07 17:41:01
Topology Change ACKs Tx	0	
Topology Change ACKs Rx	0	
TCN BPDUs Tx	0	
TCN BPDUs Rx	0	
CFG BPDUs Tx	0	
CFG BPDUs Rx	0	
RST BPDUs Tx	0	
RST BPDUs Rx	0	
MST BPDUs Tx	5	02/09/07 17:41:03
MST BPDUs Rx	173540	02/13/07 18:05:34

## Example 96 Displaying debug counters output for one port in an MST instance

The following example shows spanning tree debug-counters instance ports command output for one port in an MST instance.

```
HP Switch(config)#: show spanning-tree debug-counters instance 2 ports a15
```

```
Status and Counters - MSTI Port(s) Debug Counters Information
```

```
MST Instance ID : 2  
Port : A15
```

Counter Name	Value	Last Updated
Starved MSTI MSGs	0	
Exceeded Max Hops MSTI MSGs	0	
Topology Changes Detected	1	02/09/07 17:40:59
Topology Changes Tx	3	02/09/07 17:41:03
Topology Changes Rx	2	02/09/07 17:41:01
MSTI MSGs Tx	5	02/09/07 17:41:03
MSTI MSGs Rx	173489	02/13/07 18:03:52

### Field descriptions in MSTP debug command output

The following table contains descriptions of the debugging information displayed in the output of show spanning-tree debug-counters commands.

**Table 13 MSTP debug command output: field descriptions**

Field	Displays the number of...
Invalid BPDUs	Received BPDUs that failed standard MSTP (802.1Q-REV/D5.0 14.4) validation checks and were dropped. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
Errant BPDUs	Received BPDUs that were dropped on a port that is configured to not expect BPDU packets. This counter is maintained by the CIST (MST instance, 0 default MST instance 0 in the network) on a per-port basis and is incremented each time a BPDU packet is received on a port configured with the BPDU filter to ignore incoming BPDU packets (spanning-tree bpdu-filter command) or the BPDU protection feature to disable the port when BPDU packets are received (spanning-tree bpdu-protection command).
MST Config Error BPDUs	BPDUs received from a neighbor bridge with inconsistent MST configuration information. For example, BPDUs from a transmitting bridge may contain the same MST configuration identifiers (region name and revision number) and format selector as the receiving bridge, but the value of the Configuration Digest field (VLAN ID assignments to regional IST and MST instances) is different. This difference indicates a probable configuration error in MST region settings on the communicating bridges. The received BPDU is still processed by MSTP.  This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
Looped-back BPDUs	Times a port has received self-sent BPDU packets as the result of an external loop condition in which the BPDUs were looped back to the originating transmission port. The received BPDU is still processed by MSTP and the port changes to a blocked state.  This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
Starved BPDUs	Times that no BPDUs are received within the scheduled interval (three times the Hello Time value configured with the spanning-tree hello-time command) from a downstream CIST-designated peer port on the CIST root, alternate, or backup port. As a result, the "starved" port triggers a spanning tree topology regeneration.  This counter is maintained by the CIST (default MST instance 0) on a per-port basis.

**Table 13 MSTP debug command output: field descriptions** *(continued)*

Field	Displays the number of...
Starved MSTI MSGs	<p>Times that no BPDUs are received within the scheduled interval (three times the Hello Time value configured with the <code>spanning-tree hello-time</code> command) from a downstream MSTI-designated peer port on the MSTI root, alternate, or backup port. As a result, the "starved" port triggers a spanning tree topology regeneration.</p> <p>This counter is maintained by the CIST (default MST instance 0) on a per-port basis.</p>
Exceeded Max Age BPDUs	<p>Times that a BPDU packet is received from a bridge external to the MST region with a Message Age value greater than the configured value of the Max Age parameter (<code>spanning-tree maximum age</code> command). This may occur if the receiving bridge is located too far from the root bridge (beyond the configured size of the spanning tree domain on the root bridge) or if a BPDU packet with invalid root information is continuously circulating between bridges in a spanning tree domain and needs to be aged out.</p> <p>This counter is maintained by the CIST (default MST instance 0) on a per-port basis.</p>
Exceeded Max Hops BPDUs	<p>Times that a BPDU packet is received from a bridge internal to the MST region with a CIST Remaining Hops value less than or equal to 1. This may occur if the receiving bridge is located too far from the CIST regional root bridge (beyond the configured size of the MST region on the CIST regional root bridge) or if a BPDU packet with invalid CIST regional root bridge information is continuously circulating between bridges in the MST Region and needs to be aged out.</p> <p>This counter is maintained by the CIST (default MST instance 0 in the region) on a per-port basis.</p>
Exceeded Max Hops MSTI MSGs	<p>Times that an MSTI MSG packet is received from a bridge internal to the MST region with an MSTI Remaining Hops value less than or equal to 1. This may occur if the receiving bridge is located too far from the MSTI regional root bridge (beyond the configured size of the MST region on the MSTI regional root bridge) or if a BPDU packet with invalid MSTI regional root bridge information is continuously circulating between bridges in an MST region and needs to be aged out. This counter is maintained on a per-MSTI per-port basis.</p>
Topology Changes Detected	<p>Times that a Topology Change event is detected by the CIST or MSTI port and the port triggers a topology change propagation throughout the network. A Topology Change event occurs when a non-edge port enters forwarding state. This counter is maintained on a per-CIST per-port and on a per-MSTI per-port basis.</p>
Topology Changes Tx	<p>Times that Topology Change information is propagated (sent out) through the port to the rest of the network.</p> <p>For a CIST port, the counter is the number of times that a CFG, RST or MST BPDU with the TC flag set is transmitted out of the port.</p> <p>For an MSTI port, the counter is the number of times that a MSTI configuration message with the TC flag set is transmitted out of the port.</p> <p>This counter is maintained on a per-CIST per-port and on a per-MSTI per-port bases.</p>
Topology Changes Rx	<p>Times that Topology Change information is received from the peer port.</p> <p>For a CIST port, the counter is the number of times that a CFG, RST or MST BPDU with the TC flag set is received.</p> <p>For an MSTI port, the counter is the number of times that an MSTI configuration message with the TC flag set is received.</p> <p>This counter is maintained on a per-CIST per-port and on a per-MSTI per-port basis.</p>
Topology Change ACKs Tx	<p>Times that the Topology Change acknowledgement is transmitted through the port (number of CFG, RST or MST BPDUs transmitted with the Topology Change Acknowledge flag set). This counter is maintained by the CIST (default MST instance 0) on a per-port basis.</p>
Topology Change ACKs Rx	<p>Times the Topology Change acknowledgement is received on the port (number of CFG, RST or MST BPDUs received with the Topology Change Acknowledge flag set). This counter is maintained by the CIST (default MST instance 0) on a per-port basis.</p>

**Table 13 MSTP debug command output: field descriptions** (continued)

Field	Displays the number of...
TCN BPDUs Tx	Topology Change Notification BPDUs that are transmitted through the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
TCN BPDUs Rx	Topology Change Notification BPDUs that are received on the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
CFG BPDUs Tx	802.1D Configuration BPDUs that are transmitted through the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
CFG BPDUs Rx	802.1D Configuration BPDUs that are received on the port. This counter maintained by the CIST (default MST instance 0) on a per-port basis.
RST BPDUs Tx	802.1w RST BPDUs that are transmitted through the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
RST BPDUs Rx	802.1w RST BPDUs that are received on the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
MST BPDUs Tx	802.1s MST BPDUs that are transmitted through the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
MST BPDUs Rx	802.1s MST BPDUs that are received on the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
MSTI MSGs Tx	Times that a configuration message for a specific MSTI was encoded in (802.1s) MST BPDUs that are transmitted through the port. This counter is maintained on a per-MSTI per-port basis.
MSTI MSGs Rx	Times that the MSTI detected a configuration message destined to the MSTI in (802.1s) MST BPDUs received on the port. This counter is maintained on a per-MSTI per-port basis.

## Troubleshooting MSTP operation

**Table 14 Troubleshooting MSTP operation**

Problem	Possible cause
Duplicate packets on a VLAN, or packets not arriving on a LAN at all.	The allocation of VLANs to MSTIs may not be identical among all switches in a region.
A switch intended to operate in a region does not receive traffic from other switches in the region.	An MSTP switch intended for a particular region may not have the same configuration name or region revision number as the other switches intended for the same region. The MSTP configuration name ( <code>spanning-tree config-name</code> command) and MSTP configuration revision number ( <code>spanning-tree config-revision</code> command) must be identical on all MSTP switches intended for the same region.  Another possible cause is that the set of VLANs and VLAN ID-to-MSTI mappings ( <code>spanning-tree instance vlan</code> command) configured on the switch may not match the set of VLANs and VLAN ID-to-MSTI mappings configured on other switches in the intended region.

## About MSTP

### Overview

**NOTE:** For information on configuring RPVST+, see the *Rapid per-VLAN spanning tree operation* chapter in this guide.

Without spanning tree, having more than one active path between a pair of nodes causes loops in the network, which can result in duplication of messages leading to a "broadcast storm" that can bring down the network.

---

**NOTE:**

MSTP cannot protect against loops when there is an unmanaged device on the network that drops spanning tree packets, or may fail to detect loops where this is an edge port configured with client authentication (802.1X, Web and MAC authentication). To protect against the formation of loops in these cases, you can use the loop protection feature (see [“Configuring loop protection”](#) (page 118)).

---

Multiple-Instance spanning tree operation (802.1s) ensures that only one active path exists between any two nodes in a spanning tree instance. A spanning tree instance comprises a unique set of VLANs and belongs to a specific spanning tree region. A region can comprise multiple spanning tree instances (each with a different set of VLANs) and allows one active path among regions in a network. Applying VLAN tagging to the ports in a multiple-instance spanning tree network enables blocking of redundant links in one instance while allowing forwarding over the same links for non-redundant use by another instance.

**Example 97 VLAN/Instance groupings**

---

Suppose there are three switches in a region configured with VLANs grouped into two instances, as follows:

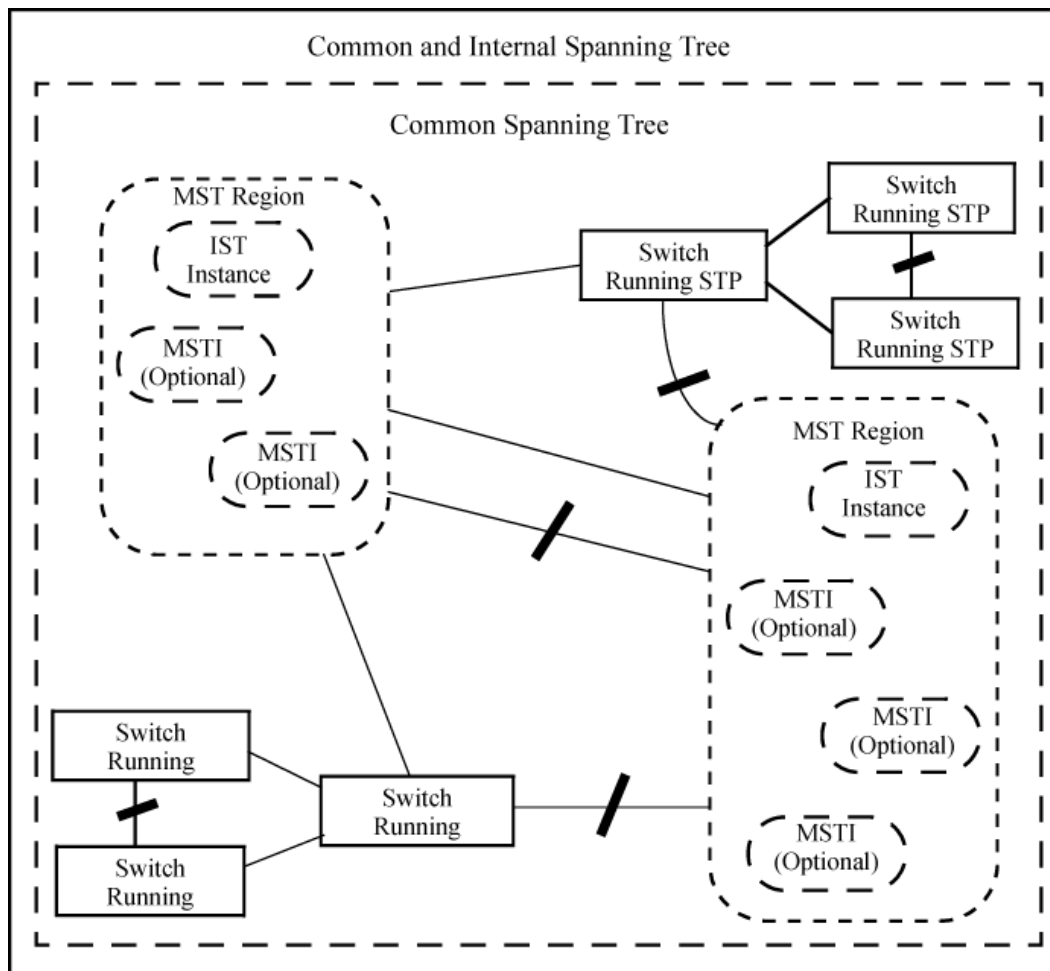
VLANs	Instance 1	Instance 2
10, 11, 12	Yes	No
20, 21, 22	No	Yes

---

The logical and physical topologies resulting from these VLAN/Instance groupings result in blocking on different links for different VLANs:



Figure 22 An MSTP network with legacy STP and RSTP devices connected



### How MSTP operates

In the factory default configuration, spanning tree operation is off. Also, the switch retains its currently configured spanning tree parameter settings when disabled. Thus, if you disable spanning tree, then later re-enable it, the parameter settings will be the same as before spanning tree was disabled. The switch also includes a "Pending" feature that enables you to exchange MSTP configurations with a single command. (See ["Enabling an entire MST region at once or exchanging one region configuration for another"](#) (page 107).)

**NOTE:** The switch automatically senses port identity and type and automatically defines spanning tree parameters for each type, as well as parameters that apply across the switch. Although these parameters can be adjusted, HP strongly recommends leaving these settings in their default configurations unless the proposed changes have been supplied by an experienced network administrator who has a strong understanding of the IEEE 802.1D/w/s standards and operation.

### 802.1s Multiple Spanning Tree Protocol (MSTP)

The switches covered in this guide use the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) standard.

The 802.1D and 802.1w spanning tree protocols operate without regard to a network's VLAN configuration and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology. The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.



While the per-VLAN spanning tree approach adopted by some vendors overcomes the network utilization problems inherent in using STP or RSTP, using a per-VLAN technology with multiple VLANs can overload the switch's CPU. MSTP on the switches covered in this guide complies with the IEEE 802.1s standard and extends STP and RSTP functionality to map multiple independent spanning tree instances onto a physical topology. With MSTP, each spanning tree instance can include one or more VLANs and applies a separate, per-instance forwarding topology. Thus, where a port belongs to multiple VLANs, it may be dynamically blocked in one spanning tree instance, but forwarding in another instance. This achieves load-balancing across the network while keeping the switch's CPU load at a moderate level (by aggregating multiple VLANs in a single spanning tree instance). MSTP provides fault tolerance through rapid, automatic reconfiguration if there is a failure in a network's physical topology.

With MSTP-capable switches, you can create a number of MST regions containing multiple spanning tree instances. This requires the configuration of a number of MSTP-capable switches. However, it is not necessary to do this. You can just enable MSTP on an MSTP-capable switch and a spanning tree instance is created automatically. This instance always exists by default when spanning tree is enabled and is the spanning tree instance that communicates with STP and RSTP environments. The MSTP configuration commands operate exactly like RSTP commands and MSTP is backward-compatible with the RSTP-enabled and STP-enabled switches in your network.

**△ CAUTION:** Spanning tree interprets a switch mesh as a single link. Because the switch automatically gives faster links a higher priority, the default MSTP parameter settings are usually adequate for spanning tree operation. Because incorrect MSTP settings can adversely affect network performance, do not change the MSTP settings from their default values unless you have a strong understanding of how spanning tree operates.

In a mesh environment, the default MSTP timer settings (Hello Time and Forward Delay) are usually adequate for MSTP operation. Because a packet crossing a mesh may traverse several links within the mesh, using smaller-than-default settings for the MSTP Hello Time and Forward Delay timers can cause unnecessary topology changes and end-node connectivity problems. For MSTP information beyond what is provided in this manual, see the IEEE 802.1s standard.

### MST regions

All MSTP switches in a given region must be configured with the same VLANs and each MSTP switch within the same region must have the same VLAN-to-instance assignments. In addition, a VLAN can belong to only one instance within any region. Within a region:

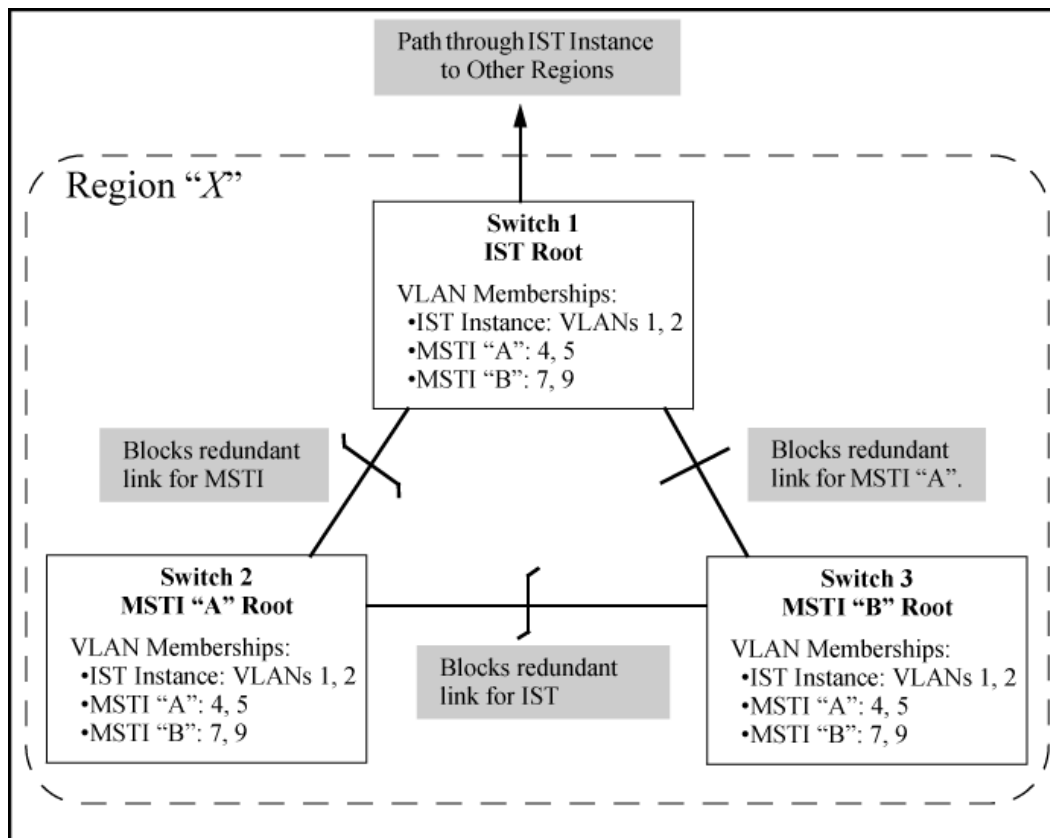
- All of the VLANs belonging to a given instance compose a single, active spanning tree topology for that instance.
- Each instance operates independently of other regions.

Between regions there is a single, active spanning tree topology.

### How separate instances affect MSTP

Assigning different groups of VLANs to different instances ensures that those VLAN groups use independent forwarding paths. For example, in [Figure 23 \(page 138\)](#) each instance has a different forwarding path.

**Figure 23 Active topologies built by three independent MST instances**



While allowing only one active path through a given instance, MSTP retains any redundant physical paths in the instance to serve as backups (blocked) paths in case the existing active path fails. Thus, if an active path in an instance fails, MSTP automatically activates (unblocks) an available backup to serve as the new active path through the instance for as long as the original active path is down. Note also that a given port may simultaneously operate in different states (forwarding or blocking) for different spanning tree instances within the same region. This depends on the VLAN memberships to which the port is assigned. For example, if a port belongs to VLAN 1 in the IST instance of a region and also belongs to VLAN 4 in MSTI "x" in the same region, the port may apply different states to traffic for these two different instances.

Within a region, traffic routed between VLANs in separate instances can take only one physical path. To ensure that traffic in all VLANs within a region can travel between regions, all of the boundary ports for each region should belong to all VLANs configured in the region. Otherwise, traffic from some areas within a region could be blocked from moving to other regions.

All MSTP switches (as well as STP and RSTP switches) in a network use BPDUs (Bridge Protocol Data Units) to exchange information from which to build multiple, active topologies in the individual instances within a region and between regions. From this information:

- The MSTP switches in each LAN segment determine a designated bridge and designated port or trunk for the segment.
- The MSTP switches belonging to a particular instance determine the root bridge and root port or trunk for the instance.
- For the IST instance within a region, the MSTP switches linking that region to other regions (or to STP or RSTP switches) determine the IST root bridge and IST root port or trunk for the region. (For any Multiple spanning tree instance—MSTI—in a region, the regional root may be a different switch that is not necessarily connected to another region.)
- The MSTP switches block redundant links within each LAN segment, across all instances and between regions, to prevent any traffic loops.

As a result, each individual instance (spanning tree) within a region determines its regional root bridge, designated bridges and designated ports or trunks.

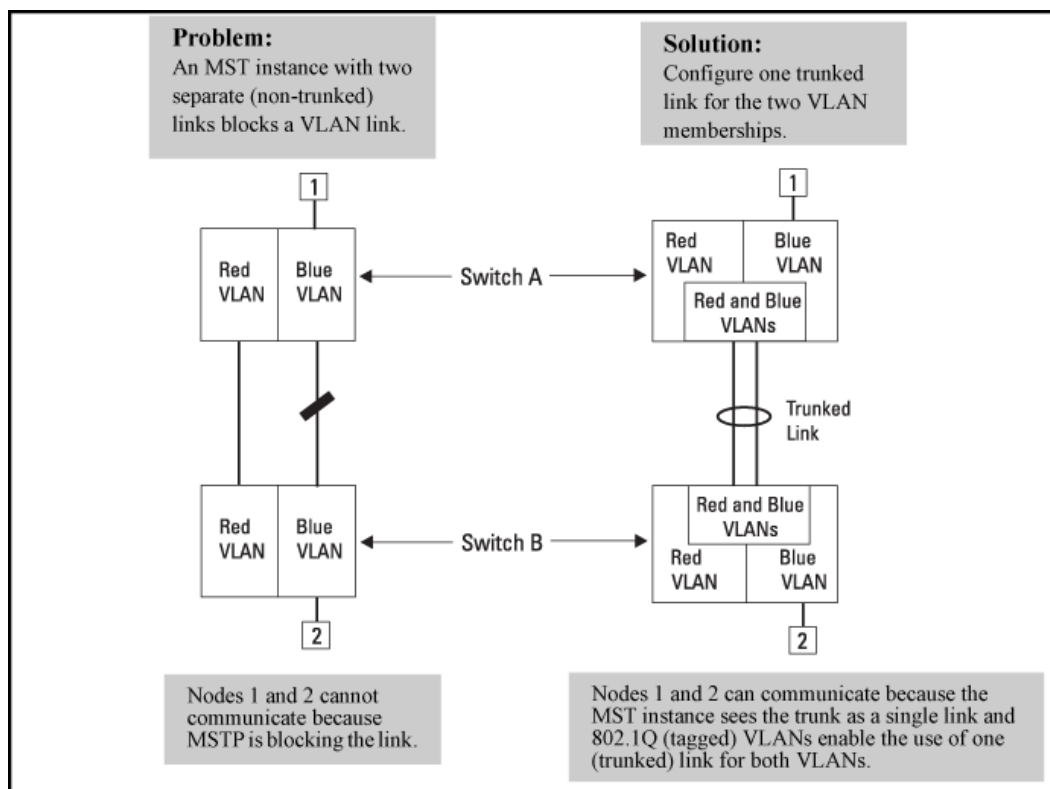
### Regions, legacy STP and RSTP switches and the Common Spanning Tree (CST)

The IST instance and any MST instances in a region exist only within that region. Where a link crosses a boundary between regions (or between a region and a legacy STP or RSTP switch), traffic is forwarded or blocked as determined by the Common Spanning Tree (CST). The CST ensures that there is only one active path between any two regions, or between a region and a switch running STP and RSTP. (See [Figure 22 \(page 136\)](#).)

### MSTP operation with 802.1Q VLANs

As indicated in the preceding sections, within a given MST instance, a single spanning tree is configured for all VLANs included in that instance. Thus if redundant physical links exist in separate VLANs within the same instance, MSTP blocks all but one of those links. However, you can prevent the bandwidth loss caused by blocked redundant links for different VLANs in an instance by using a port trunk. The following example shows how you can use a port trunk with 802.1Q (tagged) VLANs and MSTP without unnecessarily blocking any links or losing any bandwidth.

### Example 99 Using a trunked link to support multiple VLAN connectivity within the same MST instance



**NOTE:** All switches in a region should be configured with the VLANs used in that region and all ports linking MSTP switches together should be members of all VLANs in the region. Otherwise, the path to the root for a given VLAN will be broken if MSTP selects a spanning tree through a link that does not include that VLAN.

### Types of Multiple Spanning Tree Instances

A multiple spanning tree network comprises separate spanning tree instances existing in an MST region. (There can be multiple regions in a network.) Each instance defines a single forwarding topology for an exclusive set of VLANs. By contrast, an STP or RSTP network has only one spanning

tree instance for the entire network and includes all VLANs in the network. (An STP or RSTP network operates as a single-instance network.) A region can include two types of STP instances:

- Internal spanning tree Instance (IST Instance)

This is the default spanning tree instance in any MST region. It provides the root switch for the region and comprises all VLANs configured on the switches in the region that are not specifically assigned to Multiple Spanning Tree Instances (MSTIs, described below).

Within a region, the IST instance provides a loop-free forwarding path for all VLANs associated with it. VLANs that are not associated with an MSTI are, by default, associated with the IST instance. Note that the switch automatically places dynamic VLANs (resulting from GVRP operation) in the IST instance. Dynamic VLANs cannot exist in an MSTI (described below).

- Multiple Spanning Tree Instance (MSTI)

This type of configurable spanning tree instance comprises all static VLANs you specifically assign to it and must include at least one VLAN. The VLANs you assign to an MSTI must initially exist in the IST instance of the same MST region. When you assign a static VLAN to an MSTI, the switch removes the VLAN from the IST instance. (Thus, you can assign a VLAN to only one MSTI in a given region.) All VLANs in an MSTI operate as part of the same single spanning tree topology. (The switch does not allow dynamic VLANs in an MSTI.)

---

**△ CAUTION:** When you enable MSTP on the switch, the default MSTP spanning tree configuration settings comply with the values recommended in the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) standard. Inappropriate changes to these settings can result in severely degraded network performance. For this reason, HP strongly recommends that changing these default settings be reserved only for experienced network administrators who have a strong understanding of the IEEE 802.1D/w/s standards and operation.

---

## Operating rules

- All switches in a region must be configured with the same set of VLANs, as well as the same MST configuration name and MST configuration number.
- Within a region, a VLAN can be allocated to either a single MSTI or to the region's IST instance.
- All switches in a region must have the same VID-to-MST instance assignment.
- There is one root MST switch per configured MST instance.
- Because boundary ports provide the VLAN connectivity between regions, all boundary ports on a region's root switch should be configured as members of all static VLANs defined in the region.
- There is one root switch for the Common and Internal Spanning Tree (CIST). At any given time, all switches in the network will use the per-port `hello-time` parameter assignments configured on the CIST root switch.
- Where multiple MST regions exist in a network, there is only one active, physical communication path between any two regions, or between an MST region and an STP or RSTP switch. MSTP blocks any other physical paths as long as the currently active path remains in service.
- Within a network, an MST region appears as a virtual RSTP bridge to other spanning tree entities (other MST regions and any switches running 802.1D or 802.1w spanning tree protocols).
- Within an MSTI, there is one physical communication path between any two nodes, regardless of how many VLANs belong to the MSTI. Within an IST instance, there is also one spanning tree across all VLANs belonging to the IST instance.
- An MSTI comprises a unique set of VLANs and forms a single spanning tree instance within the region to which it belongs.

- A dynamic VLAN learned by GVRP will always be placed in the IST instance and cannot be moved to any configured MST instance.  
Starting in software release 13.X.X, dynamically learned GVRP VLANs can be mapped to MSTIs and support MSTP load balancing.
- In software release 13.X.X and later, you can preconfigure static and dynamic VLAN ID-to-MSTI mappings before the VLAN is created on the switch. Later, when the static VLAN ID is configured or a dynamic GVRP VLAN is learned, the VLAN is automatically associated with the preconfigured MSTI. For more information, see [“Configuring MST instance parameters” \(page 104\)](#).
- Communication between MST regions uses a single spanning tree.
- If a port on a switch configured for MSTP receives a legacy (STP/802.1D or RSTP/802.1w) BPDU, it automatically operates as a legacy port. In this case, the MSTP switch interoperates with the connected STP or RSTP switch as a separate MST region.
- Within an MST region, there is one logical forwarding topology per instance and each instance comprises a unique set of VLANs. Where multiple paths exist between a pair of nodes using VLANs belonging to the same instance, all but one of those paths will be blocked for that instance. However, if there are different paths in different instances, all such paths are available for traffic. Separate forwarding paths exist through separate spanning tree instances.
- A port can have different states (forwarding or blocking) for different instances (which represent different forwarding paths).
- MSTP interprets a switch mesh as a single link.

### Operating notes for the VLAN configuration enhancement

- Configuring MSTP on the switch automatically configures the Internal Spanning Tree (IST) instance and places all statically and dynamically configured VLANs on the switch into the IST instance. The spanning tree instance vlan command creates a new MST instance and moves the VLANs you specify from the IST to the MSTI.  
You must map a least one VLAN ID to an MSTI when you create it. You cannot map a VLAN ID to more than one instance. You can create up to 16 MSTIs in a region.
- The no form of the spanning tree instance vlan command removes one or more VLANs from the specified MSTI. If no VLANs are specified, the no form of the command deletes the specified MSTI.  
When you remove a VLAN from an MSTI, the VLAN returns to the IST instance, where it can remain or be reassigned to another MSTI configured in the region.
- If you enter the spanning tree instance vlan command before a static or dynamic VLAN is configured on the switch to preconfigure VLAN ID-to-MSTI mappings, no error message is displayed. Later, each newly configured VLAN that has already been associated with an MSTI is automatically assigned to the MSTI.  
This new default behavior differs from automatically including configured (static and dynamic) VLANs in the IST instance and requiring you to manually assign individual static VLANs to an MSTI.
- Valid VLAN IDs that you can map to a specified MSTI are numbered from 1 to 4094. The VLAN ID-to-MSTI mapping does not require a VLAN to be already configured on the switch. The MSTP VLAN enhancement lets you preconfigure MSTP topologies before the VLAN IDs associated with each instance exist on a switch.

- When you use preconfigured VLAN ID-to-MSTI topologies, ensure that MSTP switches remain in the same region by mapping all VLAN IDs used in the region to the same MSTIs on each regional switch.
- When you upgrade switch software to release x.13.yy and later, the existing MSTP topology configuration is automatically saved. All existing VLAN ID-to-MSTI assignments are maintained on a switch for uninterrupted MSTP network operation.

## MSTP compatibility with RSTP or STP

IEEE 802.1s MSTP includes RSTP functionality and is designed to be compatible with both IEEE 802.1D and 802.1w spanning tree protocols. Using the default configuration values, your switches will interoperate effectively with RSTP and STP devices. MSTP automatically detects when the switch ports are connected to non-MSTP devices in the spanning tree and communicates with those devices using 802.1D or 802.1w STP BPDU packets, as appropriate.

To enable effective interoperation with STP (802.1D) configured devices, however, you may need to adjust the default configuration values. Here are two such examples:

- The rapid state transitions employed by MSTP may result in an increase in the rates of frame duplication and misordering in the switched LAN. To allow the switch to support applications and protocols that may be sensitive to frame duplication and misordering, you can disable rapid transitions by setting the Force Protocol Version parameter to STP-compatible. The value of this parameter applies to all ports on the switch. See information on force version on [“Setting the spanning tree compatibility mode”](#) (page 94).
- One of the benefits of MSTP is the implementation of a larger range of port path costs, which accommodates higher network speeds. However, this can create some incompatibility between devices running the older 802.1D STP. You can adjust to this incompatibility by implementing the global spanning tree legacy-path cost command (see [“Setting spanning tree to operate with 802.1D legacy path cost values”](#) (page 95)). See also the Note on Path Cost below (page 142).

---

**NOTE:** RSTP and MSTP implement a greater range of path costs than 802.1D STP and use different default path cost values to account for higher network speeds. These values are shown below.

Port type	802.1D STP path cost	RSTP and MSTP path cost
10 Mbps	100	2 000 000
100 Mbps	10	200 000
1 Gbps	5	20 000

Because the maximum value for the path cost allowed by 802.1D STP is 65535, devices running that version of spanning tree cannot be configured to match the values defined by MSTP, at least for 10 Mbps and 100 Mbps ports. In LANs where there is a mix of devices running 802.1D STP, RSTP and MSTPs, you should reconfigure the devices so the path costs match for ports with the same network speeds.

---

## PVST protection and filtering

**NOTE:** These options are available for switches that support the MSTP protocol only. They are not supported for switches running RSTP.

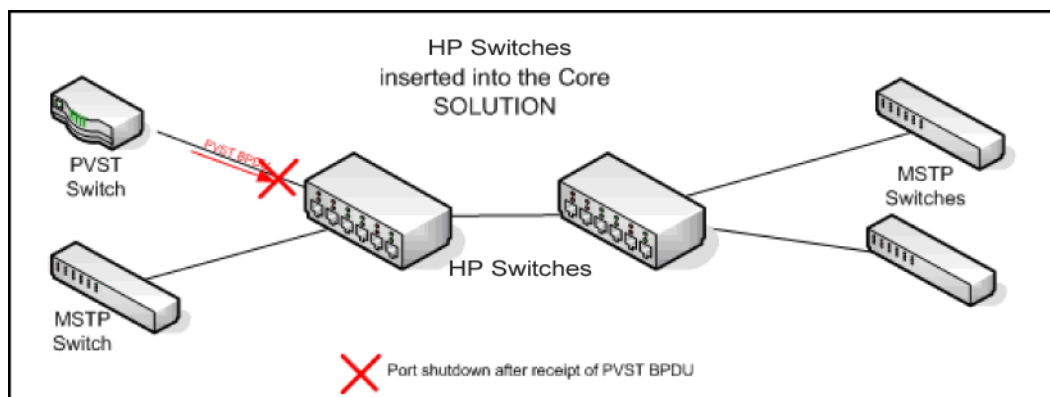
---

## PVST protection

If an HP switch in the core of a network receives Per Vlan Spanning Tree (PVST) BPDUs and forwards the unrecognized PVST BPDUs on to MSTP-only switches, those switches then disconnect themselves from the network. This can create instability in the network infrastructure.

When the PVST protection feature is enabled on a port and a PVST BPDU is received on that port, the interface on which the PVST BPDU arrived is shut down, which isolates the sending switch from the rest of the network. An event message is logged and an SNMP notification trap is generated. The errant BPDU counter `hpSwitchStpPortErrantBpduCounter` is incremented. The PVST protection feature is enabled per-port.

**Figure 24 PVST switch being isolated after sending a PVST BPDU**



**NOTE:** This is similar to the BPDU Guard feature where BPDU protection is applied to edge ports connected to end user devices that do not run STP. If STP BPDU packets are received on a protected port, the feature will disable that port and alert the network manager via an SNMP trap.

## PVST filtering

If you configure a port for PVST filtering instead of PVST protection, the port remains in operation but traps are still generated and the BPDU counter `hpSwitchStpPortErrantBpduCounter` is incremented.

**CAUTION:** Enabling the PVST filter feature allows the port to continuously forward packets without spanning tree intervention, which could result in loop formation. If this occurs, disable the port and then reconfigure it with these commands:

```
no spanning-tree <port-list> bpdu-filter
no spanning-tree <port-list> pvst-filter
```

## Loop protection

In cases where spanning tree cannot be used to prevent loops at the edge of the network, loop protection may provide a suitable alternative. Loop protection operates in two modes:

**Untagged** The default mode. This mode can be used to find loops in untagged downlinks.  
**Tagged VLAN** Finds loops on tagged VLANs. This mode can be used to detect loops in tagged-only uplinks where STP cannot be enabled.

The cases where loop protection might be chosen ahead of spanning tree to detect and prevent loops are as follows:

**On ports with client authentication** When spanning tree is enabled on a switch that use 802.1X, Web authentication and MAC authentication, loops may go undetected. For example, spanning tree packets that are looped back to an edge port will not be processed because

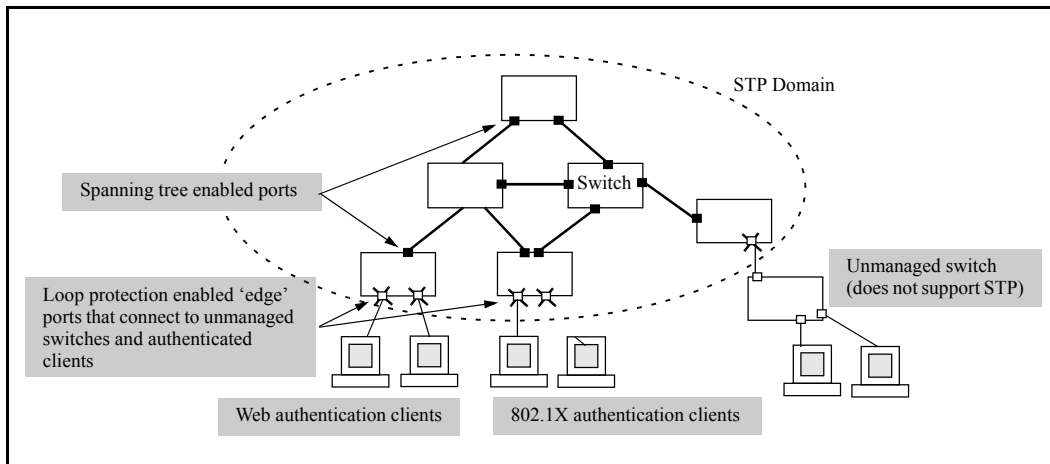


they have a different broadcast/multicast MAC address from the client-authenticated MAC address. To ensure that client-authenticated edge ports get blocked when loops occur, you should enable loop protection on those ports.

On ports connected to unmanaged devices

Spanning tree cannot detect the formation of loops where there is an unmanaged device on the network that does not process spanning tree packets and simply drops them. Loop protection has no such limitation and can be used to prevent loops on unmanaged switches.

### Example 100 Loop protection enabled in preference to STP



### Operating notes

- The `receiver-action` option can be configured on a per-port basis and can only be enabled after loop protection has been enabled on the port. All other configuration options (`disable-timer`, `trap loop-detected` and `transmit interval`) are global.
- The `trap` option refers to a SNMP trap.
- Regardless of how the `receiver-action` and `trap` options are configured, all detected loops will be logged in the switch's event log.
- The `no loop-protect port` command will not remove a receive-action configuration line from the running configuration unless this option is set to `receive-action send-disable`.
- If `loop-protect` is enabled in port mode, it cannot also be enabled in VLAN mode and vice-versa.



## 5 Quality of Service: Managing bandwidth effectively

Command Syntax	Description	Default value	CLI page reference
<code>show qos &lt;global-classifier&gt;</code>	Displays a global QoS configuration		150
<code>qos [ &lt;udp-port&gt;   &lt;tcp-port&gt; ][ ipv4   ipv6   ip-all ][ &lt;port-number&gt;   range &lt;start / end&gt; ]priority &lt;0 - 7&gt;</code>	Assigns an 802.1p priority	Disabled	150
<code>show qos tcp-udp-port-priority</code>	Displays a list of all TCP and UDP QoS classifiers		151
<code>qos dscp-map &lt;codepoint&gt; priority &lt;0 - 7&gt;</code>	Creates a DSCP policy	No override	151
<code>show qos resources</code>	Displays resource usage for policies		155
<code>qos device-priority [ &lt;ipv4-address&gt;   [ipv4] &lt;ipv4-address/mask-length&gt; ] priority &lt;0 - 7&gt;</code>	Assigns a priority for a global IP-device classifier		156
<code>qos device-priority [ &lt;ipv6-address&gt;   ipv6 &lt;ipv6-address/mask-length&gt; ] priority &lt;0 - 7&gt;</code>			
<code>qos dscp-map &lt;codepoint&gt; priority &lt;0 - 7&gt;</code>	Creates a policy based on IP address		158
<code>qos device-priority [ &lt;ipv4-address&gt;   [ipv4] &lt;ipv4-address/mask-length&gt; ] dscp &lt;codepoint&gt;</code>			
<code>qos device-priority &lt;ipv6-address&gt;   [ipv6] &lt;ipv6-address/mask-length&gt; dscp &lt;codepoint&gt;</code>			
<code>qos type-of-service ip-precedence</code>	Assigns an 802.1p priority for a global IP-precedence classifier	Disabled	162
<code>qos type-of-service diff-services &lt;codepoint&gt;</code>	Uses a global IP-Diffserv classifier to mark matching packets with an 801.p priority		163
<code>qos type-of-service diff-services &lt;current-codepoint&gt; dscp &lt;new-codepoint&gt;</code>	Uses a global IP-Diffserv classifier to mark matching packets with a new DSCP policy		164
<code>qos protocol [ ip   ipx   arp   appletalk   sna   netbeui ]priority &lt;0 - 7&gt;</code>	Assigns a priority for a global layer-3 protocol classifier	No-override	167

Command Syntax	Description	Default value	CLI page reference
<code>vlan &lt;vid&gt; qos priority &lt;0 - 7&gt;</code>	Assigns a priority for a global VLAN-ID classifier		168
<code>qos dscp-map &lt;codepoint&gt; priority &lt;0 - 7&gt;</code>	Creates a policy based on a VLAN-ID classifier	No-override	170
<code>interface &lt;port-list&gt; qos priority &lt;0 - 7&gt;</code>	Assigns a DSCP policy for a global source-port classifier	No-override	173
<code>qos dscp-map &lt;codepoint&gt; priority&lt;0 - 7&gt;</code>	Creates a policy based on source-port classifiers	No-override	173
Global configuration context: <code>[no] class [ ipv4   ipv6   &lt;classname&gt; ]</code>	Configures classifier-based QoS		177
Class configuration context: <code>[no] [&lt;seq-number&gt;][ match   ignore ]&lt;ip-protocol&gt; &lt;source-address&gt; &lt;destination-address&gt;[dscp &lt;codepoint&gt;] [precedence &lt;precedence-value&gt;][tos &lt;tos-value&gt; ][vlan &lt;vlan-id&gt; ]</code>			
Global configuration context: <code>[no] policy qos &lt;policy-name&gt;</code>			
Policy configuration context: <code>[no][ &lt;seq-number&gt;] class [ ipv4   ipv6   &lt;classname&gt; action &lt;qos-action&gt;][action &lt;qosaction ...&gt;]</code>			
Global configuration context: <code>[no][&lt;seq-number&gt;]class [ ipv4   ipv6 ] &lt;classname&gt; action &lt;qos-action&gt;[ action &lt;qosaction ...&gt;]</code>	Configures QoS actions in a policy		180
Global configuration context: <code>qos dscp-map &lt;codepoint&gt; priority &lt;0 - 7&gt;</code>	Reconfigures the 802.1p priority value currently assigned to a DSCP codepoint		183
Policy configuration context: <code>class ipv4   ipv6 &lt;classname&gt; action dscp &lt;codepoint&gt; priority &lt;0 - 7&gt;</code>			
<code>show class ipv4 &lt;classname&gt;</code>	Displays a classifier-based QoS configuration		184
<code>show class ipv6 &lt;classname&gt;</code>			
<code>show class config</code>			
<code>qos dscp-map &lt;codepoint&gt; priority &lt;0 - 7&gt; [ name &lt;ascii-string&gt; ]</code>	Configures Differentiated Services Codepoint (DSCP) mapping		188

Command Syntax	Description	Default value	CLI page reference
qos queue-config [ 2-queues   4-queues   8-queues ]	Configures QoS queues	8 queues	190
show qos queue-config	Displays the QoS queue configuration		191

## Overview

A Quality of Service (QoS) network policy refers to the network-wide controls available to:

- Ensure uniform and efficient traffic-handling throughout your network, while keeping the most important traffic moving at an acceptable speed, regardless of current bandwidth usage.
- Exercise control over the priority settings of inbound traffic arriving in and travelling through your network.

Adding bandwidth can be a good idea, but is not always feasible and does not completely eliminate the potential for network congestion. There will always be points in the network where multiple traffic streams merge or where network links change speed and capacity. The impact and number of these congestion points will increase over time as more applications and devices are added to the network.

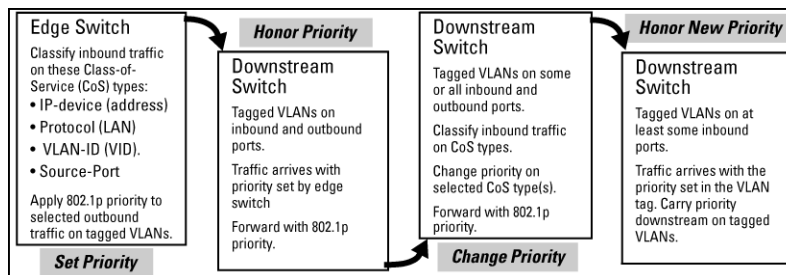
When network congestion occurs, it is important to move traffic on the basis of relative importance. However, without Quality of Service (QoS) prioritization, less important traffic consumes network bandwidth and slows down or halts the delivery of more important traffic. Without QoS, most traffic received by the switch is forwarded with the same priority it had upon entering the switch. In many cases, such traffic is normal priority and competes for bandwidth with all other normal-priority traffic, regardless of its relative importance to your organization's mission.

## Using QoS to classify and prioritize network traffic

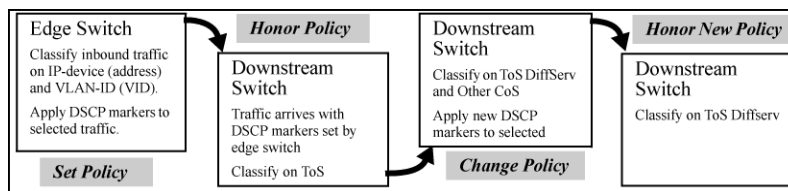
Quality of Service is used to classify and prioritize traffic throughout a network. QoS enables you to establish an end-to-end traffic-priority policy to improve the control and throughput of important data. You can manage available bandwidth so that the most important traffic goes first. For example, you can use Quality of Service to:

- Upgrade or downgrade traffic from various servers.
- Control the priority of traffic from dedicated VLANs or applications.
- Change the priorities of traffic from various segments of your network as your business needs change.
- Set priority policies in edge switches in your network to enable traffic-handling rules across the network.

**Figure 25 802.1p priority based on CoS (Class-of-Service) types and use of VLAN tags**



**Figure 26 Application of Differentiated Services Codepoint (DSCP) policies**



## Applying QoS to inbound traffic at the network edge

At the edge switch, QoS classifies certain traffic types and in some cases applies a DSCP policy. At the next hop (downstream switch) QoS honors the policies established at the edge switch. Further downstream, another switch may reclassify some traffic by applying new policies and yet other downstream switches can be configured to honor the new policies.

## Preserving QoS in outbound traffic in a VLAN

QoS is implemented in the form of rules or policies that are configured on the switch. Although you can use QoS to prioritize traffic only while it moves through the switch, you derive the maximum benefit by using QoS in an 802.1Q VLAN environment (with 802.1p priority tags) or in an untagged VLAN environment (with DSCP policies in which QoS sets priorities that downstream devices can support without reclassifying the traffic).

## Using QoS to optimize existing network resources

By prioritizing traffic, QoS supports traffic growth on the network while optimizing the use of existing resources—and delaying the need for further investments in equipment and services. QoS enables you to:

- Specify which traffic has higher or lower priority, regardless of current network bandwidth or the relative priority setting of the traffic when it is received on the switch.
- Change (upgrade or downgrade) the priority of outbound traffic.
- Override "illegal" packet priorities set by upstream devices or applications that use 802.1Q VLAN tagging with 802.1p priority tags.

## Using classifier-based QoS to provide additional policy actions and aid migration in networks with legacy and OEM devices

The classifier-based configuration model is a single, simplified procedure and command syntax for cross-feature usage, which offers:

- Finer granularity than globally-configured QoS for classifying IPv4 and IPv6 traffic
- Additional actions for managing selected traffic, such as rate limiting and IP precedence marking
- The application of QoS policies to inbound traffic flows on specific port and VLAN interfaces (instead of using only globally-configured, switch-wide QoS settings)
- The use of configured traffic classes by different software features, such as QoS or port mirroring

Classifier-based QoS is designed to work with existing globally-configured, switch-wide QoS policies by allowing you to zoom in on a subset of port or VLAN traffic to further manage it. Classifier-based policies take precedence over and may override globally-configured, switch-wide QoS settings.

Classifier-based QoS policies provide greater control for managing network traffic. Using multiple match criteria, you can finely select and define the classes of traffic that you want to manage. QoS-specific actions determine how you can handle the selected traffic.

## Configuring QoS globally

To globally configure a QoS policy on the switch, follow these steps:

1. Determine the global QoS policy to implement on the switch by analyzing the types of traffic flowing through the network and identifying one or more traffic types to prioritize. The order of precedence in which global QoS classifiers are applied, from **a** (highest) to **h** (lowest), is as follows:
  - a.** TCP/UDP applications.
  - b.** Device priority—IP source or destination address. Destination has precedence over source, see [Table 15 \(page 149\)](#).
  - c.** IP precedence bit set (leftmost three bits in the ToS/Traffic Class field of IP packets).
  - d.** IP differentiated services bit set (leftmost six bits in the ToS/Traffic Class field of IP packets).
  - e.** Layer-3 protocol.
  - f.** VLAN ID. At least one tagged VLAN is required on the network.
  - g.** Source port.
  - h.** Incoming 802.1p priority (requires at least one tagged VLAN on the network).  
Default: In a tagged VLAN environment, the incoming 802.1p priority is used as the default QoS classifier if no global QoS classifier with a higher precedence matches.
2. Select the global QoS classifier to use. The following table shows the types of QoS marking (802.1p priority or DSCP codepoint) supported by each global QoS classifier.

**Table 15 QoS marking supported by global QoS classifiers**

Global QoS classifiers	Type of QoS marking used to prioritize outbound traffic	
	802.1p Priority <sup>1</sup> only	DSCP policy <sup>2</sup> — DSCP codepoint with 802.1p priority
UDP/TCP	Supported	Supported
IP Device	Supported	Supported
IP Precedence	Supported <sup>3</sup>	Not Supported
IP DiffServ	Supported	Supported
L3 Protocol	Supported	Not Supported
VLAN ID	Supported	Supported
Source Port	Supported	Supported

- <sup>1</sup> When you configure only the 802.1p priority to mark packets that match a global QoS classifier, the selected traffic is prioritized and sent to the corresponding outbound port queue on the switch (see [Table 18 \(page 195\)](#)). VLAN-tagged ports are necessary to carry the 802.1p priority in a packet header to downstream devices.
- <sup>2</sup> When you configure a DSCP policy to mark packets that match a global QoS classifier, the selected traffic is also prioritized according to the associated 802.1p priority and sent to the corresponding outbound port queue on the switch. VLAN-tagged ports carry the 802.1p priority in a packet header to downstream devices. In addition, you can configure downstream devices to read the DSCP value in IP packets and implement the service policy implied by the codepoint.
- <sup>3</sup> When using a global QoS IP Precedence classifier, the 802.1p priority is automatically assigned to matching packets based on the IP precedence bit set in the packet header.

3. For 802.1p priority settings to be included in outbound packets, ensure that tagged VLANs are configured on the appropriate downstream links.

4. Determine the global QoS policy required for each QoS-capable device in the network and configure the necessary settings.

For downstream devices to recognize and use DSCP codepoints in IP packets sent from the switch, enable ToS (Type-of-Service) Differentiated Service mode on the devices and configure the appropriate DSCP policies. Note that certain DSCP policies have a default 802.1p priority automatically assigned (see [Table 26 \(page 211\)](#)).

---

**NOTE:** For more information on how to use global QoS classifiers, see “[Global QoS restrictions](#)” ([page 198](#)).

---

## Viewing a global QoS configuration

To display the existing switch-wide configurations for a global QoS classifier, use one of the following `show qos` commands.

### Syntax:

```
show qos <global-classifier>
```

`device-priority`

Displays the current device (IP address) priority configuration, see [Example 103 \(page 158\)](#).

`port-priority`

Displays the current source-port priority configuration, see [Figure 39 \(page 173\)](#).

`protocol-priority`

Displays the current protocol priority configuration.

`tcp-udp-port-priority`

Displays the current TCP/UDP port priority configuration, see [Figure 28 \(page 155\)](#).

`type-of-service`

Displays the current type-of-service priority configuration. The display output differs according to the option used for IP Precedence, see [Figure 31 \(page 163\)](#). See also [Figure 32 \(page 164\)](#).

`vlan-priority`

Displays the current VLAN priority configuration.

## Assigning an 802.1p priority for a global TCP/UDP classifier

To mark matching TCP or UDP packets with an 802.1p priority, enter the following command:

### Syntax:

```
qos [ udp-port | tcp-port ] [ ipv4 | ipv6 | ip-all ]  
[ <port-number> | range <start end> ] priority <0 - 7>
```

Marks an 802.1p priority in outbound packets with the specified TCP or UDP application-port number, where:

`ipv4` Marks only IPv4 packets (default).

`ipv6` Marks only IPv6 packets.

`ip-all` Marks all IP traffic (both IPv4 and IPv6 packets).

`port-number` TCP/UDP port number from 1 to 65535.

<code>range &lt;start end&gt;</code>	Marks a range of TCP/UDP ports. See <a href="#">“Operating notes on using TCP/UDP port ranges” (page 201)</a> . If you specify a range, the minimum port number must precede the maximum port number in the range.
<code>priority &lt;0 - 7&gt;</code>	Marks the specified 802.1p priority in matching TCP or UDP packets.

The 802.1p priority determines the packet's queue in the outbound port on the switch. If the packet leaves the switch on a tagged VLAN port, it carries the 802.1p priority with it to the next downstream device.

Default: Disabled — No 802.1p priority is assigned.

The `no` form of the command deletes the specified UDP or TCP port number or range of port numbers as a QoS classifier.

---

**NOTE:** If you have specified a range of port numbers, you must specify the entire range in the `no` command; you cannot remove part of a range.

---

## Displaying a list of all TCP and UDP QoS classifiers

Syntax:

```
show qos tcp-udp-port-priority
```

Displays a listing of all TCP and UDP QoS classifiers currently in the running-config file.

## Assigning a DSCP policy for a global TCP/UDP classifier

This global QoS packet-marking option assigns a previously configured or default DSCP policy (codepoint and 802.1p priority) to TCP or UDP packets having the specified port number or range of port numbers. When assigning a DSCP policy, the switch performs the following actions:

1. Selects an incoming IP packet if the TCP or UDP port number it carries matches the port number specified in the TCP or UDP classifier (as shown in [Figure 48 \(page 201\)](#), above).
2. Overwrites (re-marks) the packet's DSCP with the new DSCP configured for matching packets.
3. Assigns the 802.1p priority associated with the new DSCP. (See [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#).)
4. Forwards the packet through the appropriate outbound port queue.

## Creating a DSCP policy based on TCP/UDP port number classifiers

The following procedure creates a DSCP policy for IP packets carrying the selected TCP or UDP port-number classifier.

1. Identify the TCP or UDP port-number classifier you want to use for assigning a DSCP policy.
2. Determine the DSCP policy for packets carrying the selected TCP or UDP port number or range of port numbers.
  - a. Determine the DSCP you want to assign to the selected packets. (This codepoint will be used to overwrite (re-mark) the DSCP carried in packets received from upstream devices.)
  - b. Determine the 802.1p priority you want to assign to the DSCP.
3. If necessary, use the `qos dscp-map <codepoint> priority <0 - 7>` command to configure the DSCP policy (codepoint and associated 802.1p priority) that you want to use to mark matching packets.

---

**NOTE:** Prerequisite: A DSCP codepoint must have a preconfigured 802.1p priority (0 - 7) before you can use the codepoint to mark matching packets. If a codepoint you want to use shows `No-override` in the Priority column of the DSCP Policy table (`show qos dscp-map` command), you must first configure a priority for the codepoint before proceeding (`qos dscp-map priority` command). See [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#).

---

**Syntax:**

`qos dscp-map <codepoint> priority <0 - 7>`

Optional: This command is required only if an 802.1p priority is not already assigned to the specified `<codepoint>` in the DSCP Policy table (see [Table 16 \(page 189\)](#)).

Valid values for a DSCP codepoint are as follows:

- A binary value for the six-bit codepoint from 000000 to 111111.
- A decimal value from 0 (low priority) to 63 (high priority) that corresponds to a binary DSCP bit set
- An ASCII standard (hexadecimal) name for a binary DSCP bit set

af11 (001010)	af42 (100100)
af12 (001100)	af43 (100110)
af13 (001110)	ef (101110)
af21 (010010)	cs1 (001000) = precedence 1
af22 (010100)	cs2 (010000) = precedence 2
af23 (010110)	cs3 (011000) = precedence 3
af31 (011010)	cs4 (100000) = precedence 4
af32 (011100)	cs5 (101000) = precedence 5
af33 (011110)	cs6 (110000) = precedence 6
af41 (100010)	cs7 (111000) = precedence 7
default (000000)	

Enter `?` to display the list of valid codepoint entries.

When the switch applies the specified DSCP policy to a packet, the priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. For IP packets, the DSCP will be replaced by the codepoint specified in this command.

Default: No-override for most codepoints. See [“The default DSCP policy table” \(page 189\)](#).



4. Configure the switch to assign the DSCP policy to packets with the specified TCP or UDP port number or range of port numbers.

**Syntax:**

```
qos [ <udp-port> | <tcp-port> ] [ ipv4 | ipv6 | ip-all ]  
[ <port-number> | range <start end> ] dscp <codepoint>
```

Assigns a DSCP policy to outbound packets having the specified TCP or UDP application-port number or port range and overwrites the DSCP in these packets with the assigned *<codepoint>* value, where:

- *ipv4* marks only IPv4 packets (default).
- *ipv6* marks only IPv6 packets.
- *ip-all* marks all IP traffic (both IPv4 and IPv6 packets).
- *port-number* specifies a TCP/UDP port-number from 1 to 65535.
- *range start end* specifies a range of TCP/UDP ports; see [“Operating notes on using TCP/UDP port ranges” \(page 201\)](#). If you specify a range, the minimum port number must precede the maximum port number in the range.
- *dscp codepoint* overwrites the DSCP codepoint in the IPv4 ToS byte or IPv6 Traffic Class byte of matching packets with the specified value.

Valid values for the DSCP codepoint are as follows:

- A binary value for the six-bit codepoint from 000000 to 111111.
- A decimal value from 0 (low priority) to 63 (high priority) that corresponds to a binary DSCP bit set
- An ASCII standard name for a binary DSCP bit set

Enter **?** to display the list of valid codepoint entries.

The DSCP value you enter must be currently associated with an 802.1p priority in the DSCP Policy table (see [Table 24 \(page 208\)](#)). The 802.1p priority and determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device.

The default DSCP codepoint is *No-override*. The DSCP codepoint is not overwritten in matching packets.

The *no* form of the command deletes the specified UDP or TCP port number or range of port numbers as a QoS classifier. If you configured a range of port numbers as the QoS classifier, you must enter the entire range in the *no* command; you cannot remove part of a range.

**Syntax:**

```
show qos tcp-udp-port-priority
```

Displays a listing of all TCP and UDP QoS classifiers currently in the running-config file.

## Assigning DSCP policies to packets matching specified TCP and UDP port applications (Example)

Port Applications	DSCP Policies	
	DSCP	Priority
23-UDP	000111	7
80-TCP	000101	5
914-TCP	000010	1
1001-UDP	000010	1

1. Determine whether the DSCP codepoints that you want to use to mark matching packets already have an 802.1p priority assigned, which could indicate use by existing applications (`show qos dscp-map` command).

**NOTE:** A DSCP codepoint must also have a priority configured before you can use it to mark matching packets.

### Example 101 Displaying the current DSCP-map configuration

```
HP Switch(config)#: show qos dscp-map
```

```
DSCP -> 802.p priority mappings
```

```
NOTE: 'qos type-of-service diff-services' must be configured  
before DSCP is honored on inbound traffic.
```

```
DSCP CodePoint DSCP Value 802.1p tag DSCP Policy name  
-----  
000000         0           0           cs0  
000001         1           No-override  
000010         2           No-override  
000011         3           No-override  
000100         4           No-override  
000101         5           No-override  
000110         6           No-override  
000111         7           No-override  
001000         8           1           cs1  
001001         9           No-override
```

2. Configure the DSCP policies for the codepoints you want to use.

**Figure 27 Assigning priorities to the selected DSCPs**

```
HP Switch(config)# qos dscp-map af11 priority 3  
HP Switch(config)# qos dscp-map 13 priority 3  
HP Switch(config)# qos dscp-map af13 priority 3  
HP Switch(config)# write memory  
  
HP Switch(config)# show config  
HP Switch configuration:  
  
; J9146 Configuration Editor; Created on release W.14.XX  
  
hostname "Switch"  
time daylight-time-rule None  
qos dscp-map af11 priority 3  
qos dscp-map 13 priority 3  
qos dscp-map af13 priority 3  
.  
.  
.
```

Configure these three codepoints with non-default priorities.

Show config lists the non default codepoint settings.

- Assign the DSCP policies to the selected TCP/UDP port applications and display the result.

**Figure 28 Configuring a DSCP policy for global TCP/UDP port classifiers**

```

HP Switch(config)# qos udp-port 23 dscp 000111
HP Switch(config)# qos tcp-port 80 dscp 000101
HP Switch(config)# qos tcp-port 914 dscp 000010
HP Switch(config)# qos udp-port range 1001 2000 dscp 000010

TCP/UDP port based priorities

Protocol | IP Packet Application | DSCP | Priority
-----+-----+-----+-----+-----+
UDP      | IPV4      23          | DSCP 8 | 7
TCP      | IPV4      80          | DSCP 6 | 5
TCP      | IPV4      914         | DSCP 3 | 1
UDP      | IPV4      1001-2000   | DSCP 3 | 1
  
```

Global TCP/UDP port-number classifiers

DSCP Policy: DSCP codepoint (3) and 802.1p priority (1) mapping (Note: DSCP 3 is the decimal equivalent of binary 000010.)

The switch applies the DSCP policies in [Figure 28 \(page 155\)](#) to IP packets with the specified TCP/UDP port applications that are received in the switch. The switch manages the packets as follows:

- Overwrites the original DSCPs in the selected packets with the new DSCPs specified in the above policies.
- Assigns the 802.1p priorities in the above policies to the selected packets.

## Displaying resource usage for QoS policies

When configuring global QoS classifiers using TCP/UDP and a Layer 4 Application port number or port range, the switch automatically assigns two QoS resources for each policy—one for traffic to the TCP/UDP destination port and one for traffic to the TCP/UDP source port.

The `show qos resources` command displays the number of hardware resources currently in use by QoS policies as well as other software features.

## Example 102 Displaying the hardware resources used by currently configured QoS policies

```
HP Switch(config)#: show qos resources
```

```
Resource usage in Policy Enforcement Engine
```

Slots	Rules Available	Rules Used							
		ACL	QoS	IDM	VT	Mirror	PBR	Other	
A	3014	15	11	0	1	0	0	3	

Slots	Meters Available	Meters Used							
		ACL	QoS	IDM	VT	Mirror	PBR	Other	
A	250		5	0				0	

Slots	Application Port Ranges Available	Application Port Ranges Used							
		ACL	QoS	IDM	VT	Mirror	PBR	Other	
A	14	2	0	0		0	0	0	

```
0 of 8 Policy Engine management resources used.
```

Key:

ACL = Access Control Lists

QoS = Device & Application Port Priority, QoS Policies, ICMP rate limits

IDM = Identity Driven Management

VT = Virus Throttling blocks

Mirror = Mirror Policies, Remote Intelligent Mirror endpoints

PBR = Policy Based Routing Policies

Other = Management VLAN, DHCP Snooping, ARP Protection, Jumbo IP-MTU, Transparent Mode.

Resource usage includes resources actually in use, or reserved for future use by the listed feature. Internal dedicated-purpose resources, such as port bandwidth limits or VLAN QoS priority, are not included.

**NOTE:** ACLs and QoS policies share the same application port ranges. If a new QoS policy specifies a port range that is already configured for one or more ACLs, the QoS column increases by 1, but the **Application Port Ranges Available** column remains unchanged. Likewise, if an ACL is configured for a port range on which a QoS policy is already applied, the ACL column increases by 1, while the **Available** column remains unchanged.

Similarly, when you remove a port range, the **Application Port Ranges Available** column increases only if the port range is not configured for an existing ACL or QoS policy on the switch.

## Assigning a priority for a global IP-device classifier

This global QoS packet-marking option assigns an 802.1p priority to all IP packets that have the specified IP address as either a source or destination. If both the source and destination addresses match, the priority configured for the IP destination address has precedence.

**Syntax:**

```
qos device-priority[ <ipv4-address> | [ipv4 ]<ipv4-address/mask-length>
]
priority <0 - 7>
qos device-priority[ <ipv6-address> | ipv6 <ipv6-address/mask-length>
]
```

`priority <0 - 7>`

Marks an 802.1p priority in outbound packets with the specified IP address or subnet mask in the source or destination field in a packet header, where:

- `<ipv4-address>` or `<ipv6-address>` is an IPv4 or IPv6 address used to match the source or destination address in packet headers.

---

**NOTE:** An IPv6 local-link address (such as `fe80::110:252%vlan20`) that is automatically generated on a VLAN interface is not supported as an `ipv6-address` value.

---

- `[ipv4] <ipv4-address/mask-length>` is the subnet identified by the IPv4 mask for the specified address that is used to match the IPv4 in the source or destination field of packet headers.
- `ipv6 <ipv6-address/prefix-length>` is the subnet identified by the IPv6 prefix-length for the specified address that is used to match the IPv6 address in the source or destination field of packet headers.

Enter the IPv4 mask or IPv6 prefix length with an address in CIDR format by using the number of significant bits (for example, `2001:db8::1:262:a03:e102:127/64` or `10.28.31.1/24`).

- `priority <0 - 7>` marks the specified 802.1p priority in matching IP packets.

The 802.1p priority determines the packet's queue in the outbound port on the switch. If the packet leaves the switch on a tagged VLAN port, it carries the 802.1p priority with it to the next downstream device.

The `no` form of the command deletes the specified IP address or subnet mask as a QoS classifier and resets the priority for the VLAN to `No-override`.

`show qos device-priority`

Displays a listing of all IP device-priority QoS configurations currently in the running-config file.

## Example 103 Configuring and displaying 802.1p priority

This example shows how to configure and display the 802.1p priority used to mark packets that match each global IP-device classifier:

IP Address / Mask or Prefix Length	802.1p Priority
10.28.31.1	7
10.28.31.130	5
10.28.31.100/24	1
2001:db8:2:1:212:79ff:fe88:a100	3
2001:db8:3:3::/64	1

```
HP Switch(config)#: qos device-priority 10.28.31.1 priority 7
HP Switch(config)#: qos device-priority 10.28.31.130 priority 5
HP Switch(config)#: qos device-priority ipv4 10.28.32.100/24 priority 1
HP Switch(config)#: qos device-priority 2001:db8:2:1:212:79ff:fe88:a100 priority
HP Switch(config)#: qos device-priority ipv6 2001:db8:3:3::/64 priority 1
HP Switch(config)#: show qos device-priority
```

Device priorities

Device Address	Apply rule	DSCP	Priority
10.28.31.1	Priority		7
10.28.31.130	Priority		5
10.28.32.100/24	Priority		1
2001:db8:2:1:212:79ff:fe88:a100	Priority		3
2001:db8:3:3::/64	Priority		1

## Assigning a DSCP policy for a global IP-device classifier

This global QoS packet-marking option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to outbound IP packets having the specified IP address or subnet mask in the source or destination field of their packet header. The switch:

1. Selects an incoming IPv4 or IPv6 packet on the basis of the source or destination IP address or subnet mask it carries.
2. Overwrites the DSCP in matching packets with the globally configured DSCP codepoint and assigns the 802.1p priority associated with the new DSCP. For more information, see [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#).
3. Forwards the packet through the appropriate outbound port queue.

## Creating a policy based on IP address

This procedure creates a DSCP policy for IP packets carrying the selected IP address (source or destination).

1. Identify the IPv4 or IPv6 address to use as a classifier for assigning a DSCP policy.
2. Determine the DSCP policy for packets carrying the selected IP address:
  - a. Determine the DSCP you want to assign to the selected packets. (This codepoint will be used to overwrite the DSCP carried in packets received from upstream devices.)
  - b. Determine the 802.1p priority you want to assign to the DSCP.
3. If necessary, use the `qos dscp-map <codepoint> priority <0 - 7>` command to configure the DSCP policy (codepoint and associated 802.1p priority) that you want to use to mark matching packets.

Prerequisite: A DSCP codepoint must have a preconfigured 802.1p priority (0 - 7) to use the codepoint to mark matching packets. If a codepoint shows `No-override` in the Priority

column of the DSCP Policy table (`show qos dscp-map` command), first configure a priority for the codepoint before proceeding (`qos dscp-map priority` command). See [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#).

#### Syntax:

```
qos dscp-map <codepoint> priority <0 - 7>
```

Optional: this command is required only if an 802.1p priority is not already assigned to the specified `<codepoint>` in the DSCP Policy table, see [Table 16 \(page 189\)](#).

When the switch applies this policy to a packet, the priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. For IP packets, the DSCP will be replaced by the codepoint specified in this command.

Default: No-override for most codepoints. See [“The default DSCP policy table” \(page 189\)](#).

4. Configure the switch to assign the DSCP policy to packets with the specified IP address or subnet mask.

#### Syntax:

```
qos device-priority [ <ipv4-address> | [ipv4  
<ipv4-address/mask-length>]]
```

```
dscp <codepoint>
```

```
qos device-priority [ <ipv6-address> | ipv6  
<ipv6-address/mask-length> ]
```

```
dscp <codepoint>
```

Assigns a DSCP policy in packets with the specified IP address or subnet mask in the source or destination field in a packet header, where:

- *<ipv4-address>* or *<ipv6-address>* is an IPv4 or IPv6 address used to match the source or destination address in packet headers.

---

**NOTE:** An IPv6 local-link address (such as `fe80::110:252%vlan20`) that is automatically generated on a VLAN interface is not supported as an *ipv6-address* value.

---

- `[ipv4] <ipv4-address/mask-length>` is the subnet identified by the IPv4 mask for the specified address that is used to match the IPv4 in the source or destination field of packet headers.
- `ipv6 ipv6-address/prefix-length` is the subnet identified by the IPv6 prefix-length for the specified address that is used to match the IPv6 address in the source or destination field of packet headers.

Enter the IPv4 mask or IPv6 prefix length with an address in CIDR format by using the number of significant bits (for example, `2001:db8:2:1:262:a03:e102:127/64` or `10.28.31.1/24`).

- `dscp <codepoint>` overwrites the DSCP codepoint in the IPv4 ToS byte or IPv6 Traffic Class byte of matching packets with the specified value. Valid values for the DSCP codepoint are as follows:
  - A binary value for the six-bit codepoint from `000000` to `111111`.
  - A decimal value from `0` (low priority) to `63` (high priority) that corresponds to a binary DSCP bit set
  - An ASCII standard name for a binary DSCP bit set Enter `?` to display the list of valid codepoint entries.

The DSCP value you enter must be currently associated with an 802.1p priority in the DSCP Policy table (see [Table 24 \(page 208\)](#)). The 802.1p priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. The default DSCP codepoint is `No-override`. The DSCP codepoint is not overwritten in matching packets.

The `no` form of the command deletes the specified IP address or subnet mask as a QoS classifier. If you configured a subnet mask as match criteria, you must enter the entire IP address and mask-length in the `no` command.

#### Syntax:

```
show qos device-priority
```



Displays a listing of all IP addresses and subnet masks used as QoS classifiers currently in the running-config file.

## Assigning DSCP policies to packets matching specified global classifiers

This example shows how to assign the following DSCP policies to the packets that match the specified global IP-device classifiers:

IP address	DSCP Policy	
	DSCP codepoint	802.1p priority
10.28.31.1	000111	7
10.28.31.130	000101	5
10.28.31.100/24	000010	1
2001:db8:2:1:212:79ff:fe88:a100	000101	3
2001:db8:3:3::/64	000010	1

1. Determine whether the DSCP codepoints that you want to use to mark matching packets already have an 802.1p priority assigned, which could indicate use by existing applications (`show qos dscp-map` command). This is not a problem if the configured priorities are acceptable for all applications that use the same DSCP (see [“Notes on changing priority settings” \(page 210\)](#)).

Note that a DSCP codepoint must have an associated priority before you can use it to mark matching packets.

**Figure 29 Display the current DSCP-map configuration**

```
HP Switch(config)# show qos dscp-map
DSCP -> 802.p priority mappings
DSCP CodePoint DSCP Value 802.1p tag DSCP Policy name
-----
000000          0          No-override
000001          1          No-override
000010          2          No-override
000011          3          No-override
000100          4          No-override
000101          5          No-override
000110          6          No-override
000111          7          No-override
.
```

2. Configure the priorities for the DSCPs you want to use to mark packets.

**Figure 30 Assigning 802.1p priorities to the selected DSCPs**

```
HP Switch(config)# qos dscp-map 000111 priority 7
HP Switch(config)# qos dscp-map 000101 priority 5
HP Switch(config)# qos dscp-map 000010 priority 1
HP Switch(config)# show qos dscp-map
DSCP -> 802.p priority mappings
DSCP CodePoint DSCP Value 802.1p tag DSCP Policy name
-----
000000          0          No-override
000001          1          No-override
000010          2          1
000011          3          No-override
000100          4          No-override
000101          5          5
000110          6          No-override
000111          7          7
.
```

### 3. Assign the DSCP policies to the specified IP-device addresses and display the result.

```
HP Switch(config)#: qos device-priority 10.28.31.1 dscp 000111
HP Switch(config)#: qos device-priority 10.28.31.130 dscp 000101
HP Switch(config)#: qos device-priority ipv4 10.28.32.100/24 dscp 000010
HP Switch(config)#: qos device-priority 2001:db8:2:1:212:79ff:fe88:a100 dscp 000
HP Switch(config)#: qos device-priority ipv6 2001:db8:3:3/64 dscp 000010
HP Switch(config)#: show qos device-priority
```

Device priorities

Device Address	Apply rule	DSCP	Priority
10.28.31.1	Priority	000111	7
10.28.31.130	Priority	000101	5
10.28.32.100/24	Priority	000010	1
2001:db8:2:1:212:79ff:fe88:a100	Priority	000101	3
2001:db8:3:3/64	Priority	000010	1

The switch applies the DSCP policies in [Figure 30 \(page 161\)](#) to IP packets with the specified IP addresses and subnet masks (source or destination) received in the switch. The switch manages the packets as follows:

- Overwrites the original DSCPs in the selected packets with the new DSCPs specified in the above policies.
- Assigns the 802.1p priorities in the above policies to the appropriate packets.

## Assigning an 802.1p priority for a global IP-precedence classifier

If a device or application upstream of the switch sets the precedence bits in the ToS/Traffic Class byte of IPv4/IPv6 packets, you can use this global packet-marking option to prioritize packets for outbound port queues. If the outbound packets are in a tagged VLAN, this priority is carried as an 802.1p value to the adjacent downstream devices.

### Syntax:

```
qos type-of-service ip-precedence
```

Causes the switch to automatically assign an 802.1p priority to all IP packets (IPv4 and IPv6) by computing a packet's 802.1p priority from the precedence bits the packet carries. This priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device.

ToS IP Precedence Default: Disabled

```
no qos type-of-service
```

Disables all ToS classifier operation, including prioritization using the precedence bits.

```
show qos type-of-service
```

When the IP-precedence mode is enabled (or if neither Type-of-Service option is configured), this command displays the ToS configuration status. If the Diff-serv mode is enabled, codepoint data is displayed as described in ["Assigning a DSCP policy for a global IP-Diffserv classifier"](#) (page 164).

Using the IP-precedence classifier, prioritization of outbound packets relies on the IP-Precedence bit setting that IP packets carry with them from upstream devices and applications. To configure and verify this option:

**Figure 31 Enabling ToS IP-precedence prioritization**

```
HP Switch(config)# qos type-of-service ip-precedence
HP Switch(config)# show qos type-of-service
Type of Service [Disabled] : IP Precedence
```

To change from IP-precedence to IP-Diffserv mode, follow the procedure in [“Assigning a priority for a global IP-device classifier” \(page 156\)](#), which automatically disables IP-Precedence. To disable IP-Precedence without enabling the IP-Diffserv option, enter the `no qos type-of-service` command.

## Using a global IP-Diffserv classifier to mark matching packets with an 802.1p priority

1. Identify a DSCP used to set a policy in packets received from an upstream or edge switch.
2. Determine the 802.1p priority (0 - 7) you want to apply to packets carrying the identified DSCP. (You can either maintain the priority assigned in the upstream or edge switch, or assign a new priority.)
3. If necessary, use the `qos dscp-map <codepoint> priority <0 - 7>` command to configure the DSCP policy (codepoint and associated 802.1p priority) that you want to use to mark matching packets.
4. Enable IP-Diffserv mode by entering the `qos type-of-service diff-services` command.

### Syntax:

```
qos type-of-service diff-services <codepoint>
```

Causes the switch to read the *<codepoint>* (DSCP) of an incoming IP packet and, when a match occurs, assign the associated 802.1p priority in the DSCP Policy table (see [“The default DSCP policy table” \(page 189\)](#)).

```
no qos type-of-service
```

Disables all ToS classifier operation.

```
no qos dscp-map <codepoint>
```

Disables direct 802.1p priority assignment to packets carrying the *<codepoint>*, by reconfiguring the codepoint priority assignment in the DSCP table to `No-override`. Note that if this codepoint is in use as a DSCP policy for another Diffserv codepoint, you must disable or redirect the other Diffserv codepoint's DSCP policy before you can disable or change the codepoint. For example, in [Figure 32 \(page 164\)](#) you cannot change the priority for the 000000 codepoint until you redirect the DSCP policy for 000001 from using 000000 as a policy.

For more information see [“Notes on changing priority settings” \(page 210\)](#) and [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#).

```
show qos type-of-service
```

Displays the current Type-of-Service configuration. In IP-Diffserv mode it also shows the current direct 802.1p assignments and the current DSCP assignments covered later in this section.

## Examples

### Example 104 show qos type-of-service

An edge switch A in an untagged VLAN assigns a DSCP of 000110 on IP packets it receives on port A6 and handles the packets with high priority (7). When these packets reach interior switch B you want the switch to handle them with the same high priority. To enable this operation you would configure an 802.1p priority of 7 for packets received with a DSCP of 000110 and then enable `diff-services`:

Figure 32 Displaying the codepoints available for 802.1p priority assignments

```
HP Switch(config)# show qos type-of-service
Type of Service : Differentiated Services

Codepoint DSCP Policy | Priority
-----+-----
000000      | 1
000001      | 1
000010      | No-override
000011      | No-override
000100      | 5
000101      | No-override
000110      | No-override
000111      | No-override
001000      | No-override
001001      | 5
.           | .
.           | .
.           | .
```

If ToS Diff-Serv is enabled, executing this command displays the current ToS configuration and shows that the selected DSCP is not currently in use.

The 001100 codepoint is unused, and thus available for directly assigning an 802.1p priority without changing the packet's DSCP.

Note: All codepoints without a "DSCP Policy" entry are available for direct 802.1p priority assignment.

Figure 33 Type-of-Service configuration that enables both 802.1p priority and DSCP policy assignment

```
HP Switch(config)# qos dscp-map 000110 priority 7
HP Switch(config)# show qos type-of-service
Type of Service : Differentiated Services

Codepoint DSCP Policy | Priority
-----+-----
000000      | 1
000001      | 1
000010      | No-override
000011      | No-override
000100      | 5
000101      | No-override
000110      | 7
000111      | No-override
001000      | No-override
001001      | 5
001010      | 1
.           | .
.           | .
.           | .
```

Outbound IP packets with a DSCP of 000110 will have a priority of 7.

Notice that codepoints 000000 and 001001 are named as DSCP policies by other codepoints (000001 and 000100 respectively). This means they are not available for changing to a different 802.1p priority.

## Assigning a DSCP policy for a global IP-Diffserv classifier

The preceding section describes how to forward an 802.1p priority level set by an edge (or upstream) switch. This section describes how to use a global IP-Diffserv classifier to mark matching packets with a new DSCP policy. A DSCP policy consists of a DSCP codepoint and an associated 802.1p priority.

You can use a global IP-Diffserv classifier to mark a DSCP policy at the same time with a global IP-Diffserv classifier that marks an 802.1p priority if different DSCP codepoints are configured with each classifier.

To use a global IP-Diffserv classifier to mark matching packets with a new DSCP policy, follow these steps:

1. Identify the DSCP used to set a policy in packets received from an upstream or edge switch.
2. Create a new policy by using the `qos dscp-map code-point priority <0 - 7>` command to configure an 802.1p priority for the codepoint you will use to overwrite the DSCP that the packet carries from upstream.

3. Use the `qos type-of-service diff-services <incoming-DSCP> dscp <outgoing-DSCP>` command to change the policy on packets coming from the edge or upstream switch with the specified incoming DSCP.

Figure 51 (page 214) illustrates this scenario.

#### Syntax:

```
qos type-of-service diff-services
    Enables ToS Diff-services.
```

#### Syntax:

```
qos type-of-service diff-services <current-codepoint> dscp
<new-codepoint>
```

Configures the switch to select an incoming IP packet carrying the `<current-codepoint>` and then use the `<new-codepoint>` to assign a new, previously configured DSCP policy to the packet. The policy overwrites the `<current-codepoint>` with the `<new-codepoint>` and assigns the 802.1p priority specified by the policy.

Valid values for a DSCP codepoint are as follows:

- A binary value for the six-bit codepoint from 000000 to 111111.
- A decimal value from 0 (low priority) to 63 (high priority) that corresponds to a binary DSCP bit set
- An ASCII standard (hexadecimal) name for a binary DSCP bit set

Enter ? to display the list of valid codepoint entries.

To reconfigure the 802.1p priority currently assigned to a DSCP codepoint, use the `qos dscp-map` command as described in [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#).

#### Syntax:

```
no qos type-of-service
    Disables all ToS classifier operation. Current ToS DSCP policies and priorities remain in the configuration and will become available if you re-enable ToS Diff-services.
```

#### Syntax:

```
no qos type-of-service [diff-services <codepoint>]
    Deletes the DSCP policy assigned to the <codepoint> and returns the <codepoint> to the 802.1p priority setting it had before the DSCP policy was assigned, which is either a value from 0 - 7 or No-override.
```

#### Syntax:

```
show qos type-of-service
    Displays a listing of codepoints with any corresponding DSCP policy reassignments for outbound packets. Also displays the 802.1p priority for each codepoint that does not have a DSCP policy assigned to it.
```

## Example 105 Configuring new DSCP policies

The following example shows how to configure new DSCP policies on matching packets with the specified DSCP codepoints.

Received DSCP	Policy DSCP	802.1p Priority	Policy Name (Optional)
001100	000010	6	Level 6
001101	000101	4	Level 4

1. Determine if the DSCP codepoints that you want to use to mark matching packets already have an 802.1p priority assigned, which could indicate use by existing applications (`show qos dscp-map` command). This is not a problem as long as the configured priorities are acceptable for all applications using the same DSCP, see [“Notes on changing priority settings” \(page 210\)](#).

Also, note that a DSCP codepoint must have a preconfigured 802.1p priority (0 - 7) before you can use the codepoint to mark matching packets. If a codepoint you want to use shows No-override in the Priority column of the DSCP Policy table (`show qos dscp-map` command), you must first configure a priority for the codepoint before proceeding (`qos dscp-map priority` command). See [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#).

**Figure 34 Displaying the current DSCP-map configuration**

```
HP Switch(config)# show qos dscp-map
DSCP -> 802.p priority mappings
DSCP CodePoint DSCP Value 802.1p tag DSCP Policy name
-----
000000        0          No-override
000001        1          No-override
000010        2          No-override
000011        3          No-override
000100        4          No-override
000101        5          No-override
000110        6          No-override
000111        7          No-override
```

The DSCPs for this example have not yet been assigned an 802.1p priority level.

2. Configure the desired policies (codepoint and associated 802.1p priority) in the DSCP table:

## Example 106 Configuring DSCP policies in the DSCP table

```
HP Switch(config)#: qos dscp-map 000010 priority 6 name 'Level 6'
HP Switch(config)#: qos dscp-map 000101 priority 4 name 'Level 4'
HP Switch(config)#: show qos dscp-map
DSCP -> 802.p priority mappings
DSCP policy 802.1p tag Policy name
-----
000000        No-override
000001        No-override
000010        6          Level 6
000011        No-override
000100        No-override
000101        4          Level 4
000110        No-override
000111        No-override
```

- Assign the new policies to mark matching packets with the specified codepoints.

**Figure 35 Assigning DSCP policies to outbound packets based on the DSCP codepoint from upstream devices**

```

HP Switch(config)# qos type-of-service diff-services 001100 dscp 000010
HP Switch(config)# qos type-of-service diff-services 001101 dscp 000101
HP Switch(config)# show qos type-of-service
Type of Service : Differentiated Services

Codepoint DSCP Policy | Priority
-----+-----
000000 | No-override
000001 | No-override
000010 | 6
000011 | No-override
000100 | No-override
000101 | 4
000110 | No-override
000111 | No-override
001000 | No-override
001001 | No-override
001010 | No-override
001011 | No-override
001100 | 6
001101 | 4
001110 | No-override

```

### Assigning a priority for a global layer 3 protocol classifier

This global QoS packet-marking option assigns an 802.1p priority to outbound packets having the specified Layer-3 protocol.

#### Syntax:

```

qos protocol [ ip | ipx | arp | appletalk | sna | netbeui ]
priority <0 - 7>

```

Configures an 802.1p priority for outbound packets having the specified protocol. This priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. You can configure one QoS classifier for each protocol type.

Default: No-override

```

no qos protocol ip | ipx | arp | appletalk | sna | netbeui
priority <0 - 7>

```

Disables use of the specified protocol as a QoS classifier and resets the protocol priority to No-override.

```

show qos protocol

```

Lists the QoS protocol classifiers with their priority settings.

## Example 107 Configuring global Layer-3 protocol classifiers

To configure the following global Layer-3 protocol classifiers:

1. Configure QoS protocol classifiers with IP at 0 (normal), ARP at 5 (medium) and AppleTalk at 7 (high) and display the QoS protocol configuration.
2. Disable the QoS IP protocol classifier, downgrade the ARP priority to 4 and again display the QoS protocol configuration.

The following example shows the necessary configuration commands.

Figure 36 Adding, displaying, removing and changing QoS protocol classifiers

```
HP Switch(config)# qos protocol ip priority 0
HP Switch(config)# qos protocol appletalk priority 7
HP Switch(config)# qos protocol arp priority 5
HP Switch(config)# show qos protocol

Protocol priorities
-----
Protocol  Priority
-----
IP        0
IPX       No-override
ARP       5
AppleTalk 7
SNA       No-override
Net BEUI  No-override

HP Switch(config)# no qos protocol ip
HP Switch(config)# qos protocol arp priority 4
HP Switch(config)# show qos protocol

Protocol priorities
-----
Protocol  Priority
-----
IP        No-override
IPX       No-override
ARP       4
AppleTalk 7
SNA       No-override
Net BEUI  No-override
```

Configures IP, Appletalk, and ARP as QoS classifiers.

Removes IP as QoS classifier.

Changes the priority of the ARP QoS classifier.

Displays the results of these changes.

## Assigning a priority for a global VLAN-ID classifier

This global QoS packet-marking option assigns a priority to all outbound packets having the specified VLAN-ID (VID). You can configure this option by either specifying the VLAN-ID ahead of the `qos` command or moving to the VLAN context for the VLAN you want to configure for priority.

### Syntax:

```
vlan <vid> qos priority <0 - 7>
```

Configures an 802.1p priority for outbound packets belonging to the specified VLAN. This priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. You can configure one QoS classifier for each VLAN-ID.

Default: No-override

```
no vlan <vid> qos
```

Removes the specified VLAN-ID as a QoS classifier and resets the priority for that VLAN to No-override.

```
show qos vlan-priority
```

Displays a listing of the QoS VLAN-ID classifiers currently in the running-config file, with their priority data.



## Example 108 Displaying the VLANs available for QoS prioritization

In this example, 802.1p priorities are assigned to packets received in VLANs 1, 20, 30 and 40.

```
HP Switch(config)# show vlans

Status and Counters - VLAN Information

Maximum VLANs to support : 256
Primary VLAN : DEFAULT_VLAN
Management VLAN :

VLAN ID Name | Status | Voice | Jumbo
-----+-----+-----+-----
1  DEFAULT_VLAN | Port-based | No | No
20  VLAN_20 | Static | No | No
30  VLAN_30 | Static | No | No
40  VLAN_40 | Static | No | No
```

Mark VLAN 1 packets with priority 2.

Mark VLAN 20 and 30 packets with priority 5.

Mark VLAN 40 packets with priority 7.

Enter the following commands to mark VLAN packets that match the specified VLAN IDs with an 802.1p priority:

```
HP Switch(config)#: vlan 1 qos priority 2
HP Switch(config)#: vlan 20 qos priority 5
HP Switch(config)#: vlan 30 qos priority 5
HP Switch(config)#: vlan 40 qos priority 7
HP Switch(config)#: show qos vlan
```

VLAN priorities

VLAN ID	Apply rule	DSCP	Priority
1	Priority		2
20	Priority		5
30	Priority		5
40	Priority		7

## Example 109 Returning a QoS-prioritized VLAN to "No-override" status

If later it is necessary to remove VLAN 20 from QoS prioritization, enter the following command:

```
HP Switch(config)# no vlan 20 qos
HP Switch(config)# show qos vlan-priority

VLAN priorities

VLAN ID Apply rule | DSCP | Priority
-----+-----+-----+-----
1  Priority | | 2
20  No-override | | No-override
30  Priority | | 5
40  Priority | | 7
```

In this instance, **No-override** indicates that VLAN 20 is not prioritized by QoS.

## Assigning a DSCP policy for a global VLAN-ID classifier

This global QoS packet-marking option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to outbound IP packets having the specified VLAN-ID (VID). The switch:

1. Selects an incoming IP packet on the basis of the VLAN-ID it carries.
2. Overwrites the packet's DSCP with the DSCP configured for matching packets.

3. Assigns the 802.1p priority associated with the new DSCP. (See [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\).](#))
4. Forwards the packet through the appropriate outbound port queue.

## Creating a policy based on the VLAN-ID classifier

1. Determine the VLAN-ID classifier to which you want to assign a DSCP policy.
2. Determine the DSCP policy for packets carrying the selected VLAN-ID.
  - a. Determine the DSCP you want to assign to the selected packets. (This codepoint will be used to overwrite the DSCP carried in packets received from upstream devices.)
  - b. Determine the 802.1p priority you want to assign to the DSCP.
3. If necessary, use the `qos dscp-map <codepoint> priority <0 - 7>` command to configure the DSCP policy (codepoint and associated 802.1p priority) that you want to use to mark matching packets.

Prerequisite: A DSCP codepoint must have a preconfigured 802.1p priority (0 - 7) before you can use the codepoint to mark matching packets. If a codepoint you want to use shows `No-override` in the Priority column of the DSCP Policy table (`show qos dscp-map` command), you must first configure a priority for the codepoint before proceeding (`qos dscp-map priority` command). See [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\).](#)

4. Configure the switch to assign the DSCP policy to packets with the specified VLAN-ID.

### Syntax:

```
qos dscp-map <codepoint>priority <0 - 7>
```

This command is optional if a priority has already been assigned to the `<codepoint>`. The command creates a DSCP policy by assigning an 802.1p priority to a specific DSCP.

When the switch applies this priority to a packet, the priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. For IP packets, the DSCP codepoint in the packet header is replaced by the codepoint specified in this command.

Default: For most codepoints, No-override. See [Table 16 \(page 189\).](#)

### Syntax:

```
vlan <vid> qos dscp <codepoint>
```

Assigns a DSCP policy to IP packets carrying the specified VLAN ID and overwrites the DSCP in these packets with the assigned `<codepoint>` value.

- A binary value for the six-bit codepoint from 000000 to 111111.
- A decimal value from 0 (low priority) to 63 (high priority) that corresponds to a binary DSCP bit set
- An ASCII standard name for a binary DSCP bit set.

Enter ? to display the list of valid codepoint entries.

The DSCP policy includes an 802.1p priority and determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device.

Default: No-override

## Syntax:

```
no vlan <vid> qos
```

Removes a global QoS classifier for the specified VLAN.

## Syntax:

```
show qos device-priority
```

Displays a listing of all QoS VLAN-ID classifiers currently in the running-config file.

### Example 110 Assigning DSCP policies to packets

This example assigns the following DSCP policies (codepoint and associated 802.1p priority) to packets with the specified VLAN IDs:

VLAN-ID	DSCP	Priority
40	000111	7
30	000101	5
20	000010	1
1	000010	1

1. Determine if the DSCP codepoints that you want to use to mark matching packets already have an 802.1p priority assigned, which could indicate use by existing applications (`show qos dscp-map` command). This is not a problem as long as the configured priorities are acceptable for all applications using the same DSCP (see [“Notes on changing priority settings”](#) (page 210)).

A DSCP codepoint must also have a priority configured before you can use it to mark matching packets.

**Figure 37** Displaying the current DSCP-priority mapping in the DSCP policy table

```
HP Switch(config)# show qos dscp-map
```

DSCP	CodePoint	DSCP Value	802.1p tag	DSCP Policy name
000000		0		No-override
000001		1		No-override
000010		2		No-override
000011		3		No-override
000100		4		No-override
000101		5		No-override
000110		6		No-override
000111		7		No-override

The DSCPs for this example have not yet been assigned an 802.1p priority level.

2. Configure the priorities for the DSCPs.

**Figure 38** Assign priorities to the selected DSCPs

```
HP Switch(config)# qos dscp-map 000110 priority 7
HP Switch(config)# qos dscp-map 000101 priority 5
HP Switch(config)# qos dscp-map 000010 priority 1
HP Switch(config)# show qos dscp-map
```

Codepoint	DSCP Policy	Priority
000000	No-override	
000001	No-override	
000010	1	
000011	No-override	
000100	No-override	
000101	5	
000110	7	
000111	No-override	
001000	No-override	

802.1p priorities are configured in this step.

### 3. Assign the DSCP policies to the selected VLAN IDs and display the result.

```
HP Switch(config)#: vlan 1 qos dscp 000010
HP Switch(config)#: vlan 20 qos dscp 000010
HP Switch(config)#: vlan 30 qos dscp 000101
HP Switch(config)#: vlan 40 qos dscp 000111

HP Switch(config)#: show qos vlan-priority
```

VLAN priorities

VLAN ID	Apply rule	DSCP	Priority
1	DSCP	000010	1
20	DSCP	000010	1
30	DSCP	000101	5
40	DSCP	000111	7

The switch will now apply the DSCP policies to packets received on the switch with the specified VLAN-IDs. This means the switch will:

- Overwrite the original DSCPs in the selected packets with the new DSCPs specified in the above policies.
- Assign the 802.1p priorities in the above policies to the appropriate packets.

## Assigning a priority for a global source-port classifier

This global QoS packet-marking option assigns a priority to all outbound packets having the specified source-port.

This option can be configured by either specifying the source-port ahead of the `qos` command or moving to the port context for the port you want to configure for priority. For configuring multiple source-ports with the same priority, it is easier to use the `interface <port-list>` command to go to the port context instead of individually configuring the priority for each port.

### Syntax:

```
interface <port-list> qos priority <0 - 7>
```

Configures an 802.1p priority for packets entering the switch through the specified (source) ports. This priority determines the packet queue in the outbound ports to which traffic is sent. If a packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. You can configure one QoS classifier for each source-port or group of source-ports.

Default: No-override

### Syntax:

```
no interface <port-list>
```

Disables use of the specified source-ports for QoS classifiers and resets the priority for the specified source-ports to No-override.

### Syntax:

```
show qos port-priority
```

Lists the QoS port-priority classifiers with their priority data.

## Example 111 Prioritizing inbound traffic on source-ports

This example shows how to prioritize inbound traffic on the following source-ports:

Source-Port	Priority
A1 - A3	2
A4	3
B1, B4	5
C1-C3	6

Enter the following commands to prioritize packets received from the specified source ports:

**Figure 39 Configuring and displaying source-port QoS priorities**

```
HP Switch(config)# interface 1-3 qos priority 6
HP Switch(config)# interface 4-5 qos priority 5
HP Switch(config)# interface 6-7 qos priority 3

Switch(config)# show qos port-priority
```

Port	Apply rule	DSCP	Priority	Radius	Override
1	Priority		6	No-override	
2	Priority		6	No-override	
3	Priority		6	No-override	
4	Priority		5	No-override	
5	Priority		5	No-override	
6	Priority		3	No-override	
7	Priority		3	No-override	
8	No-override		No-override	No-override	
9	No-override		No-override	No-override	
10	No-override		No-override	No-override	

If you later decided to remove source-port A1 from QoS prioritization, you would enter the following command:

**Figure 40 Returning a QoS-prioritized VLAN to "No-override" status**

```
HP Switch(config)# no interface 1 qos
HP Switch(config)# show qos port-priority
```

Port	Apply rule	DSCP	Priority	Radius	Override
1	Priority		No-override	No-override	
2	Priority		6	No-override	
3	Priority		6	No-override	
4	Priority		5	No-override	

In this instance, **No-override** indicates that port 1 is not prioritized by QoS.

## Assigning a DSCP policy for a global source-port classifier

This global QoS packet-marking option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to outbound IP packets received from the specified source-ports. The switch:

1. Selects an incoming IP packet on the basis of its source-port.
2. Overwrites the packet's DSCP with the DSCP configured for matching packets.
3. Assigns the 802.1p priority associated with the new DSCP. (See ["Using Differentiated Services Codepoint \(DSCP\) mapping"](#) (page 188).)
4. Forwards the packet through the appropriate outbound port queue.

For more on DSCP, see ["About QoS"](#) (page 192).

## Creating a policy based on source-port classifiers

Only one DSCP per source-port may be used to mark matching packets.

Configuring a new DSCP for a source-port automatically overwrites any previous DSCP or 802.1p priority configuration for that source-port classifier.

1. Identify the source-port classifier to which you want to assign a DSCP policy.
2. Determine the DSCP policy for packets having the selected source-port:
  - a. Determine the DSCP you want to assign to the selected packets. (This codepoint will be used to overwrite the DSCP carried in packets received through the source-port from upstream devices.)
  - b. Determine the 802.1p priority you want to assign to the DSCP.
3. If necessary, use the `qos dscp-map <codepoint> priority <0 - 7>` command to configure the DSCP policy (codepoint and associated 802.1p priority) that you want to use to mark matching packets.

---

**NOTE:** Prerequisite: A DSCP codepoint must have a preconfigured 802.1p priority (0 - 7) before you can use the codepoint to mark matching packets. If a codepoint you want to use shows `No-override` in the Priority column of the DSCP Policy table (`show qos dscp-map` command), you must first configure a priority for the codepoint before proceeding (`qos dscp-map priority` command). See [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#).

---

#### Syntax:

```
qos dscp-map <codepoint> priority <0 - 7>
```

This command is optional if a priority has already been assigned to the `<codepoint>`.

The command creates a DSCP policy by assigning an 802.1p priority to a specific DSCP. When the switch applies this priority to a packet, the priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. For IP packets, the DSCP codepoint in the packet header is replaced by the codepoint specified in this command.

Default: For most codepoints, `No-override`. See [Table 16 \(page 189\)](#).

4. Configure the switch to assign the DSCP policy to packets from the specified source-port.

#### Syntax:

```
interface <port-list> qos dscp <codepoint>
```

Assigns a DSCP policy to IP packets from the specified source-ports and overwrites the DSCP in these packets with the assigned codepoint value.

- A binary value for the six-bit codepoint from 000000 to 111111.
- A decimal value from 0 (low priority) to 63 (high priority) that corresponds to a binary DSCP bit set
- An ASCII standard name for a binary DSCP bit set.  
Enter ? to display the list of valid codepoint entries.

#### Syntax:

```
interface <port-list> qos dscp <codepoint>
```

The DSCP policy includes an 802.1p priority and determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device.

Default: No-override

#### Syntax:

```
no interface [e] <port-list> qos
```

Removes a QoS classifier for the specified source-ports.

#### Syntax:

```
show qos source-port
```

Displays a listing of all source-port QoS classifiers currently in the running-config file.

### Example 112 Assigning DSCP policies (codepoint and associated 802.1p priority) to matching packets

In this example, the following DSCP policies (codepoint and associated 802.1p priority) are assigned to matching packets with the specified source-ports:

Source-Port	DSCP	Priority
A2	000111	7
B1-B3	000101	5
B4, C2	000010	1

1. Determine if the DSCP codepoints that you want to use to mark matching packets already have an 802.1p priority assigned, which could indicate use by existing applications (`show qos dscp-map` command). This is not a problem as long as the configured priorities are acceptable for all applications using the same DSCP.

Also, note that a DSCP must have an 802.1p priority configured before you can use it to mark matching packets. If necessary, use the `qos dscp-map <codepoint> priority <0 - 7>` command to configure the DSCP policy (codepoint and associated 802.1p priority) that you want to use to mark matching packets.

#### Figure 41 Displaying the current DSCP-priority mapping in the DSCP policy table

```

HP Switch(config)# show qos dscp-map

DSCP -> 802.p priority mappings

NOTE: 'qos type-of-service diff-services' must be configured
before DSCP is honored on inbound traffic.

DSCP CodePoint DSCP Value 802.ip tag DSCP Policy name
-----
000000 0 0 cs0
000001 1 No-override
000010 2 No-override
000011 3 No-override
000100 4 No-override
000101 5 No-override
000110 6 No-override
000111 7 No-override
001000 8 1 cs1
001001 9 No-override
001010 10 No-override af11
001011 11 No-override
001100 12 No-override af12
001101 13 No-override
001110 14 No-override af13
001111 15 No-override
010000 16 2 cs2
010001 17 No-override
. . .
. . .

```

The DSCPs for this example have not yet been assigned an 802.1p priority level.

2. Configure the priorities for the DSCPs that you want to use to mark matching packets.

**Figure 42 Assigning priorities to the specified DSCP codepoints**

```

HP Switch(config)# qos dscp-map 2 priority 7
HP Switch(config)# qos dscp-map 3 priority 5

HP Switch(config)# show qos dscp-map

DSCP -> 802.p priority mappings

NOTE: 'qos type-of-service diff-services' must be configured
before DSCP is honored on inbound traffic.

DSCP CodePoint DSCP Value 802.ip tag DSCP Policy name
-----
000000 0 0 cs0
000001 1 No-override
000010 2 7
000011 3 5
000100 4 No-override
000101 5 No-override
000110 6 No-override
000111 7 No-override
001000 8 1 cs1
001001 9 No-override
001010 10 No-override af11
001011 11 No-override
001100 12 No-override af12
001101 13 No-override
001110 14 No-override af13
001111 15 No-override
010000 16 2 cs2
010001 17 No-override
. . .
. . .

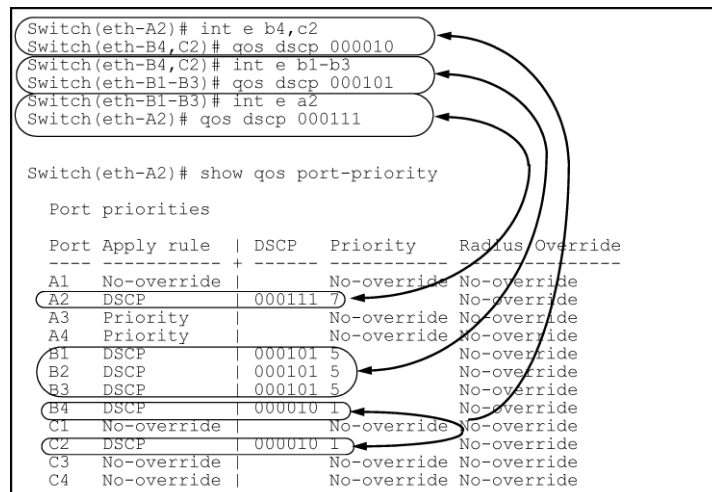
```

DSCP Policies Configured in this Step



- Assign the DSCP policies to the selected source-ports and display the result.

**Figure 43 Displaying global source-port classifier with DSCP-priority marking**



## Configuring classifier-based QoS

To use the classifier-based model to configure a QoS policy and apply it to a selected class of traffic on a port or VLAN interface, follow these steps:

- Evaluate the types of traffic in your network and identify the traffic types that you want to prioritize or rate limit.
- Create an IPv4 or IPv6 traffic class using the `class` command to select the packets you want to manage.

Context: Global configuration

### Syntax:

```
[no] class ipv4 | ipv6 <classname>
```

Defines the name of a traffic class and specifies whether a policy is to be applied to IPv4 or IPv6 packets, where `<classname>` is a text string (64 characters maximum). After you enter the `class` command, you enter the class configuration context to specify match criteria. A traffic class contains a series of `match` and `ignore` commands, which specify the criteria used to classify packets.

A traffic class consists of match criteria, which consist of `match` and `ignore` commands.

- The `match` commands define the values that header fields must contain for a packet to belong to the class and be managed by policy actions.
- The `ignore` commands define the values which, if contained in header fields, exclude a packet from the policy actions configured for the class.

**NOTE:** Enter `match/ignore` statements in the precise order in which you want their criteria to be used to check packets.

The following match criteria are supported in `match/ignore` statements for inbound IPv4/IPv6 traffic:

- IP source address (IPv4 and IPv6)
- IP destination address (IPv4 and IPv6)
- Layer 2 802.1Q VLAN ID

- Layer 3 IP protocol
- Layer 3 IP precedence bits
- Layer 3 DSCP codepoint
- Layer 4 TCP/UDP application port
- VLAN ID

3. Enter one or more `match` or `ignore` commands from the class configuration context to filter traffic and determine the packets on which policy actions will be performed.

Context: Class configuration

### Syntax:

```
[no] [<seq-number>] [ match | ignore ]<ip-protocol> <source-address>
<destination-address> [dscp <codepoint>] [precedence
<precedence-value>] [tos <tos-value> ] [vlan <vlan-id>]
```

4. Create a QoS policy to perform QoS actions on selected packets by entering the `policy qos` command from the global configuration context.

Context: Global configuration

### Syntax:

```
[no] policy qos <policy-name>
```

Defines the name of a QoS policy and enters the policy configuration context.

A traffic policy consists of one or more classes and one or more QoS actions configured for each class of traffic. The configured actions are executed on packets that match a `match` statement in a class. No policy action is performed on packets that match an `ignore` statement.

---

**NOTE:** Be sure to enter each class and its associated QoS actions in the precise order in which you want packets to be checked and processed by QoS actions.

---

To configure the QoS actions that you want to execute on packets that match the criteria in a specified class, enter one or more `class action` commands from the policy configuration context:

Context: Class configuration

### Syntax:

```
[no ] [<seq-number>] class [ ipv4 | ipv6 ] <classname> action
<qos-action> [ action <qos action ...>]
```

Defines the QoS actions to be applied on a pre-configured IPv4 or IPv6 traffic class when a packet matches the `match` criteria in the traffic class. You can enter multiple action statements for the same traffic class.

```
[no] [ <seq-number> ] class [ ipv4 | ipv6 ] <classname>
<seq-number>
```

(Optional) Sequentially orders the QoS actions that you enter in a policy configuration. Actions are executed on matching packets in numerical order.

Default: QoS action statements are numbered in increments of 10, starting at 10.

```
class [ipv4 | ipv6]
<classname>
```

Defines the preconfigured traffic class on which the QoS actions in the policy are

executed and specifies whether the QoS policy is applied to IPv4 or IPv6 traffic in the class. The `classname` is a text string (64 characters maximum).

---

**NOTE:** Multiple `class action` statements can be configured for different traffic classes in the same policy. The execution of QoS actions is performed in the order in which the actions are numerically listed in the policy.

---

`action < qos-action > [action < qos-action > ...]` Configures the QoS action specified by the `< qos-action >` replaceable. The action is executed on any packet that matches the `match` criteria in the class. The action is not executed on packets that match `ignore` criteria.

The complete `no` form of the `class action` command or the `no < seq-number >` command removes a QoS action from the policy configuration.

The following QoS commands are supported by the `< qos-action >` replaceable:

- `rate-limit < kbps >`
- `priority < priority-value >`
- `ip-precedence < precedence-value >`
- `dscp < dscp-value >`

For information on the complete syntax of each QoS command, see [“Configuring QoS actions in a policy” \(page 180\)](#).

To manage packets that do not match the `match` or `ignore` criteria in any class in the policy and therefore have no QoS actions performed on them, enter an optional default class. The default class is placed at the end of a policy configuration and specifies the QoS actions to perform on packets that are neither matched nor ignored.

5. (Optional) To configure a default class in a policy, enter the `default-class` command at the end of a policy configuration and specify one or more QoS actions to be executed on packets that are not matched and not ignored.

Context: Class configuration

### Syntax:

`[no] default-class action < qos-action > [action < qos-action ... >]`

Configures a default class that allows one or more QoS actions to be executed on packets that are not matched or ignored by any of the class configurations in a QoS policy. The `default-class` supports the same QoS commands as the `class ipv4 | ipv6 action` command: `rate-limit`, `priority`, `ip-precedence` and `dscp`.

6. Apply the QoS policy to inbound traffic on a port (`interface service-policy in` command) or VLAN (`vlan service-policy in` command) interface.

The following restrictions apply to a QoS service policy:

- Only one QoS policy is supported on a port or VLAN interface.
- If you apply a QoS policy to a port or VLAN interface on which a QoS policy is already configured, the new policy replaces the existing one.
- A QoS policy is supported only on inbound traffic.

Because only one QoS policy is supported on a port or VLAN interface, ensure that the policy you want to apply contains all the required classes and actions for your configuration.

To apply a QoS policy on a port or VLAN interface, enter one of the following commands from the global configuration context.

Context: Global configuration

### Syntax:

```
interface <port-list> service-policy <policy-name>
```

Configures specified ports with a QoS policy that is applied to inbound traffic on each interface.

Separate individual port numbers in a series with a comma; for example, a1, b4, d3.

Enter a range of ports by using a dash; for example, a1-a5.

The QoS policy name you enter must be the same as the policy name you configured with the `policy qos` command in Step 2.

### Syntax:

```
vlan <vlan-id> service-policy <policy-name> in
```

Configures a QoS policy on the specified VLAN that is applied to inbound traffic on the VLAN interface.

Valid VLAN ID numbers range from 1 to 4094.

The QoS policy name you enter must be the same as the policy name you configured with the `policy` command in Step 2.

7. Determine the additional QoS configurations that you need to apply to each QoS-capable device in your network and configure the appropriate policy.

Optional: For 802.1p (CoS) priority settings to be included in outbound packets, configure tagged VLANs on the appropriate downstream links.

## Configuring QoS actions in a policy

In QoS policy-configuration mode, you define the actions to be applied to a pre-configured IPv4 or IPv6 traffic class when a packet matches the `match` criteria in the class. Note: Actions are not executed on packets that match `ignore` criteria. You can enter multiple action statements in a traffic class, including the default class.

The following commands are supported in a QoS policy configuration:

<code>rate-limit</code>	Configures the rate limit for matching packets.
<code>ip-precedence</code>	Configures (marks) the IP precedence bits in the ToS byte of IPv4 packet headers and Traffic Class byte of IPv6 headers.
<code>dscp</code>	Configures the DSCP bits in the IPv4 ToS byte and IPv6 Traffic Class byte of packet headers.

`priority` Configures the 802.1p class of service (CoS) priority in Layer 2 frame headers.

For information on the difference between the DSCP bits and precedence bits in the ToS byte of an IPv4 header and the Traffic Class byte of an IPv6 header.

Context: Global configuration

### Syntax:

```
[no] [<seq-number> ]class [ ipv4 | ipv6 ] <classname> action <gos-action> [ action <gosaction ...> ]
```

In a QoS policy configuration, the `<gos-action>` parameter can be any of the following commands:

`rate-limit <kbps>`

Configures the maximum transmission rate for matching packets in a specified traffic class. All packets that exceed the configured limit are dropped.

The rate limit is specified in kilobits per second, where `<kbps>` is a value from 0 to 10000000.

#### Rate limiting usage

- Rate limit values below 13 kbps may result in unpredictable rate limiting behavior.
- Configuring a rate limit of 0 (zero) kilobits on a port blocks all traffic on the port. If blocking all traffic is the desired behavior, HP recommends that you configure deny ACL instead configuring a rate limit of 0.
- A rate limit that you apply with a classifier-based policy overrides any globally-configured per-port rate limit on the selected packets.

For more information on per-port rate limiting, see “Port Traffic Controls” in the *Management and Configuration Guide*.

#### Rate limiting restrictions

- A rate limit is calculated on a per-module or per port-bank basis. If trunked ports or VLANs with a configured rate limit span multiple modules or port-banks, the configured rate limit is not guaranteed.
- A QoS policy that uses the `class action rate-limit` command is not supported on a port interface on which ICMP rate limiting has already been globally configured. To apply the QoS policy, you must first disable the ICMP rate limiting configuration.

In cases where you want to maintain an ICMP rate limiting configuration, configure a class in which you specify the necessary match statements for ICMP traffic and a QoS policy in which you configure the rate limit action for the class.

For information on globally-configured ICMP, see “Configuring ICMP section in the Configuring IP Parameters for Routing Switches” in the *Multicast and Routing Guide*.

`priority <priority-value>`

Configures the 802.1p class of service (CoS) bits in Layer 2 frames of matching packets in a specified traffic class. Valid CoS values range from 0 to 7.

The 802.1p CoS value controls the outbound port-queue priority for traffic leaving the switch. In an 802.1Q VLAN network, downstream devices may honor or change the 802.1p priority in incoming packets. For more information, see [“Layer 2 802.1p prioritization” \(page 195\)](#).

[Table 18 \(page 195\)](#) shows how the Layer 2 802.1p priority value determines to which outbound port queue a packet is sent both on the switch and on a downstream device.

The 802.1p CoS numeric value (from 0 to 7) corresponds to the hexadecimal equivalent of the three binary 0 and 1 bit settings in the Layer 2 header. For example if the CoS bit values are 1 1 1, the numeric value is 7 (1+2+4). Similarly, if the CoS bits are 0 1 1, the numeric value is 3 (1+2+0).

---

**NOTE:** If you want the 802.1p CoS priority settings included in outbound packets to be honored on downstream devices, configure tagged VLANs on the appropriate inbound and outbound ports.

---

`ip-precedence`  
`<precedence-value>`

Configures the IP precedence value in the IPv4 ToS byte or IPv6 Traffic Class byte of matching packets in a specified traffic class. Valid IP precedence values are either a numeric value from 0 (low priority) to 7 (high priority) or its corresponding name:

0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet (for inter-network control)
7	network (for network control)

[Table 18 \(page 195\)](#) shows how the Layer 2 802.1p priority value determines to which outbound port queue a packet is sent.

[Table 23 \(page 205\)](#) shows the 802.1p priority value (0 to 7) associated, by default, with each IP Precedence three-bit setting and automatically assigned by the switch to the Layer 2 header of matching packets.

`dscp <dscp-value>`

Configures the DSCP codepoint in the IPv4 ToS byte or IPv6 Traffic Class byte of matching packets in a specified traffic class.

Valid values for the DSCP codepoint are any of the following:

- A binary eight-bit set (such as 100110 )
- A decimal value from 0 (low priority) to 63 (high priority) that corresponds to a binary DSCP bit set
- The ASCII standard name for a binary DSCP bit set:

af11 (001010)	af42 (100100)
af12 (001100)	af43 (100110)
af13 (001110)	ef (101110)
af21 (010010)	cs1 (001000) = <i>precedence 1</i>
af22 (010100)	cs2 (010000) = <i>precedence 2</i>
af23 (010110)	cs3 (011000) = <i>precedence 3</i>
af31 (011010)	cs4 (100000) = <i>precedence 4</i>
af32 (011100)	cs5 (101000) = <i>precedence 5</i>
af33 (011110)	cs6 (110000) = <i>precedence 6</i>
af41 (100010)	cs7 (111000) = <i>precedence 7</i>
default (000000)	

Prerequisite: The DSCP value you enter must already be configured with an 802.1p priority in the DSCP Policy table (“[The default DSCP policy table](#)” (page 189)) before you can use it to mark matching packets.

**NOTE:** DSCP-802.1p Mapping: The 802.1p priority currently associated with each DSCP codepoint is stored in the DSCP Policy table (displayed with the `show qos dscp-map` command and shown in “[The default DSCP policy table](#)” (page 189)). Note that certain DSCP codepoints have 802.1p priorities assigned by default. The 802.1p priority mapped to a DSCP codepoint is automatically applied in matching packets whose codepoint is reset with the `class action dscp` command in a QoS policy.

## Reconfiguring the 802.1p priority value currently assigned to a DSCP codepoint

To reconfigure the 802.1p priority value currently assigned to a DSCP codepoint, enter one of the following commands:

- Global configuration context:  
`qos dscp-map <<codepoint>> priority <<0 - 7> >`
- Policy configuration context:  
`class [ ipv4 | ipv6 ] <classname> action dscp <codepoint> priority <0 - 7>`

If you do not enter a `priority` value with the `class action dscp` command in a QoS policy, one of the following occurs:

- The switch refers to the DSCP Policy table to assign the 802.1p value that is currently configured for the specified DSCP codepoint to remark matching packets.
- If the specified DSCP codepoint is not associated with an 802.1p priority in the DSCP Policy table, an error message is displayed and the `class action dscp <codepoint>` command is not executed. You are prompted to reenter the command with an 802.1p priority: `class action dscp <codepoint> priority <0 - 7>`.

To ensure that the desired 802.1p priority is assigned to matching packets, you may need to first remap the priority to the new codepoint before you configure the policy, by using the `qos dscp-map <codepoint> priority <0 - 7>` command.

**NOTE:** After you reconfigure the 802.1p priority for a DSCP codepoint, the switch immediately applies the new 802.1p priority value to packets transmitted with the associated codepoint as a result of:

- Globally-configured QoS commands
- `class action dscp` commands in other QoS policies

---

### Example 113 Applying classifier-based QoS policy to inbound traffic on VLAN

---

In the following example, a classifier-based QoS policy (`dscp-remap`) that assigns a new DSCP codepoint (`af43`) and associated 802.1p priority (5) to matching packets with a specified DSCP codepoint (`af11`) is applied to the inbound traffic on a VLAN.

```
HP Switch(config)#: qos dscp-map af43 priority 5
HP Switch(config)#: class ipv4 dscp5
HP Switch(config-class)#: match ip any any dscp af11
HP Switch(config-class)#: exit
HP Switch(config)#: policy qos dscp-remap
HP Switch(config-policy)#: class ipv4 dscp5 action dscp af43
HP Switch(config-policy)#: exit
HP Switch(config)#: vlan 3 service-policy dscp-remap in
```

**NOTE:** In this example, the desired 802.1p priority is mapped to the specified DSCP codepoint by using the `qos dscp-map <codepoint> priority <0 - 7>` command before the QoS policy is configured.

---

## Viewing a classifier-based QoS configuration

Use the following `show` commands to display information about a classifier-based QoS configuration and statistics or resource usage on QoS policies.

### Syntax:

```
show class config
show class ipv4 classname
show class ipv6 classname
```

<code>config</code>	Displays all classes, both IPv4 and IPv6 and lists the statements that make up each class.
<code>ipv4 <i>classname</i></code>	Lists the statements that make up the IPv4 class identified by <i>classname</i> .
<code>ipv6 <i>classname</i></code>	Lists the statements that make up the IPv6 class identified by <i>classname</i> .

Additional variants of the `show class` command provide information on classes that are members of policies that have been applied to ports or VLANs.



## Example 114 Displaying `show class` output for a QoS policy

---

```
HP Switch(config)#: show class ipv4 gnutella
Statements for Class ipv4 "gnutella"
 10 match tcp 0.0.0.0 255.255.255.255 range 6346 6347 0.0.0.0 255.255.255.255
 20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 6346 6347
 30 match udp 0.0.0.0 255.255.255.255 range 6346 6347 0.0.0.0 255.255.255.255
 40 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 6346 6347
```

```
HP Switch(config)#: show class ipv4 kazaa
Statements for Class ipv4 "kazaa"
 10 match tcp 0.0.0.0 255.255.255.255 eq 1214 0.0.0.0 255.255.255.255
 20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 1214
 30 match udp 0.0.0.0 255.255.255.255 eq 1214 0.0.0.0 255.255.255.255
 40 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 1214
```

```
HP Switch(config)#: show class ipv4 http
Statements for Class ipv4 "http"
 10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 80
 20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443
 50 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 8080
```

---

### Syntax:

`show policy policy-name`

`show policy config`

- |                          |  |
|--------------------------|--|
| <code>policy-name</code> | Lists the statements that make up the specified policy.  |
| <code>config</code>      | Displays the names of all policies defined for the switch and lists the statements that make up each policy. |

Additional variants of the `show policy` command provide information on policies that have been applied to ports or VLANs.

## Example 115 Displaying `show policy` output for a QoS policy

---

```
HP Switch(config)#: show policy suspect-traffic
Statements for Policy "suspect-traffic"
 10 class ipv4 "http" action rate-limit kbps 2000 action priority 3
 20 class ipv4 "kazaa" action rate-limit kbps 1000 action priority 2
 30 class ipv4 "gnutella" action rate-limit kbps 1000 action priority 2
```

---

### Syntax:

[ `show` | `clear` ] `statistics policy <policy-name> port <port-num>`

[ `show` | `clear` ] `statistics policy <policy-name> vlan <vid> in`

- |                               |   |
|-------------------------------|---|
| <code>show</code>             | Displays the statistics for a specified policy applied to a specified port or VLAN.                           |
| <code>clear</code>            | Clears statistics for the specified policy and port or VLAN.  |
| <code>policy-name</code>      | Specifies the name of the policy.   |
| <code>&lt;port-num&gt;</code> | Specifies the number of the port on which the policy is applied (single port only, not a range).              |
| <code>&lt;vid&gt;</code>      | Specifies the number or name of the vlan on which the policy is applied. VLAN ID numbers range fro 1 to 4094. |
| <code>in</code>               | Specifies that statistics are shown for inbound traffic only.   |

## Example 116 Displaying show statistics policy output for a QoS policy

```
HP Switch# show statistics policy suspect-traffic vlan 300 in
HitCounts for Policy suspect-traffic

10 class ipv4 "http" action rate-limit kbps 2000 action priority 3 [ Meter 975000
kilo bits]
(150) 10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 80
(0) 20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443
(200) 30 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 8000
(0) 40 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 8001
(300) 50 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 8080

20 class ipv4 "kazaa" action rate-limit kbps 1000 action priority 2 [ Meter 0
kilo bits]
(0) 10 match tcp 0.0.0.0 255.255.255.255 eq 1214 0.0.0.0 255.255.255.255
(0) 20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 1214
(0) 30 match udp 0.0.0.0 255.255.255.255 eq 1214 0.0.0.0 255.255.255.255
(0) 40 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 1214

30 class ipv4 "gnutella" action rate-limit kbps 1000 action priority 2 [ Meter 0
kilo bits]
(0) 10 match tcp 0.0.0.0 255.255.255.255 range 6346 6347 0.0.0.0
255.255.255.255
(0) 20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 6346
6347
(0) 30 match tcp 0.0.0.0 255.255.255.255 range 6346 6347 0.0.0.0
255.255.255.255
(0) 40 match udp 0.0.0.0 255.255.255.255 range 6346
```

Number of packets (in parentheses) that have matched the criteria in the match/ignore statement in each class in the QoS policy and have been processed by the action configured for the class

### Syntax:

`show policy resources`

Displays the number of hardware resources (rules, meters and application port ranges) used by classifier-based QoS policies that are currently applied to interfaces on the switch, as well as mirroring policies and other software features.

**NOTE:** The information displayed is the same as the output of `show qos resources` (see [Example 102 \(page 156\)](#)) and `show access-list resources` commands. For a detailed explanation of the information displayed with the `show [qos | <access-list> | <policy>] <resources>` command, see the "[Monitoring Resources](#)" appendix of the Management and Configuration Guide.

## Example 117 Displaying show policy resources output for all currently configured QoS policies

```
HP Switch(config)#: show policy resources
```

```
Resource usage in Policy Enforcement Engine
```

Slots	Rules	Rules Used							
	Available	ACL	QoS	IDM	VT	Mirror	PBR	Other	
A	3014	15	11	0	1	0	0	3	

Slots	Meters	Meters Used							
	Available	ACL	QoS	IDM	VT	Mirror	PBR	Other	
A	250		5	0				0	

Slots	Application	Application Port Ranges Used							
	Port Ranges	ACL	QoS	IDM	VT	Mirror	PBR	Other	
A	14	2	0	0		0	0	0	

```
0 of 8 Policy Engine management resources used.
```

Key:

ACL = Access Control Lists

QoS = Device & Application Port Priority, QoS Policies, ICMP rate limits

IDM = Identity Driven Management

VT = Virus Throttling blocks

Mirror = Mirror Policies, Remote Intelligent Mirror endpoints

PBR = Policy Based Routing Policies

Other = Management VLAN, DHCP Snooping, ARP Protection, Jumbo IP-MTU, Transparent Mode.

Resource usage includes resources actually in use, or reserved for future use by the listed feature. Internal dedicated-purpose resources, such as port bandwidth limits or VLAN QoS priority, are not included.

## Configuring a QoS policy for Voice over IP and Data traffic (Example)

In this example, an administrator would like to configure the following Layer 2 802.1p CoS and Layer 3 DSCP values to prioritize how VoIP traffic from different phones is handled compared to data traffic:

Softphone traffic	DSCP 46; 802.1p CoS priority 6
Avaya phone traffic	DSCP 34; 802.1p CoS priority 3
Miscellaneous phone traffic	DSCP 26; 802.1p CoS priority 3
Data traffic	DSCP 000000; 802.1p CoS priority 0

The following QoS configuration creates and assigns a QoS policy to VLAN 1 that prioritizes VoIP and data traffic in this way:

**Figure 44 A QoS policy for voice over IP and data traffic**

```
HP Switch(config)# class ipv4 DataTraffic
HP Switch(config-class)# match ip any any dscp 0
HP Switch(config-class)# exit
HP Switch(config)# class ipv4 softphoneTraffic
HP Switch(config-class)# match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
ip-dscp 46
HP Switch(config-class)# exit
HP Switch(config)# class ipv4 DigiPhoneTr
HP Switch(config-class)# match ip 12.255.100.10/24 any ip-dscp 34
HP Switch(config-class)# match ip 10.255.100.12/24 any ip-dscp 26
HP Switch(config-class)# exit
HP Switch(config)# policy qos prioritizeVoIP
HP Switch(config-policy)# class ipv4 DataTraffic action priority 0
HP Switch(config-policy)# class ipv4 softphoneTraffic action priority 6
HP Switch(config-policy)# class ipv4 DigiPhoneTraffic action priority 3
HP Switch(config-policy)# exit
HP Switch(config)# vlan 2 service-policy prioritizeVoIP in
```

These match statements select traffic that satisfies multiple criteria; for example, a TCP port range and a DSCP value or a source IP address and a DSCP value.

## Configuring a QoS policy for layer 4 TCP/UDP traffic (Example)

The following example shows how to configure a rate limiting policy for TCP/UDP application streams and apply the policy on all inbound switch ports.

```
HP Switch(config)#: class ipv4 http
HP Switch(config-class)#: match tcp any any eq 80
HP Switch(config-class)#: match tcp any any eq 443
HP Switch(config-class)#: match tcp any any eq 8080
HP Switch(config-class)#: exit
HP Switch(config)#: class ipv4 kazaa
HP Switch(config-class)#: match tcp any eq 1214 any
HP Switch(config-class)#: match tcp any any eq 1214
HP Switch(config-class)#: exit
HP Switch(config)#: class ipv4 gnutella
HP Switch(config-class)#: match tcp any range 6346 6347 any
HP Switch(config-class)#: match tcp any any range 6346 6347
HP Switch(config-class)#: match udp any range 6346 6347 any
HP Switch(config-class)#: match udp any any range 6346 6347
HP Switch(config-class)#: exit
HP Switch(config)#: policy qos PrioritizeSuspectTraffic
HP Switch(config-policy)#: class ipv4 http action rate-limit kbps 7000
HP Switch(config-policy)#: class ipv4 kazaa action rate-limit kbps 2920
HP Switch(config-policy)#: class ipv4 gnutella action rate-limit kbps 2920
HP Switch(config-policy)#: exit
HP Switch(config)#: interface all service-policy PrioritizeSuspectTraffic in
```

## Configuring a QoS policy for subnet traffic (Example)

The next example shows how to configure a QoS policy that prioritizes inbound traffic sent to and received from a specified subnet (15.29.16.0/10) and TCP port range on VLAN 5.

**Figure 45 A QoS policy for IPv4 and IPv6 subnet traffic on a VLAN interface**

```
HP Switch# class ipv4 adminTraffic
HP Switch(config-class)# match ip 15.29.16.1/10 any
HP Switch(config-class)# match ip any 15.29.16.1/10
HP Switch(config-class)# match tcp ::/0 ::/0 range 100 200 ip-dscp 46
HP Switch(config-class)# exit
HP Switch# policy prioritizeAdminTraffic
HP Switch(config-policy)# class ipv4 adminTraffic action priority 7
HP Switch(config-policy)# exit
```

Match statement with IPv6 source and destination addresses.

## Using Differentiated Services Codepoint (DSCP) mapping

The DSCP Policy Table associates an 802.1p priority with a DSCP codepoint in an IPv4/IPv6 packet. Using DSCP codepoints in your network lets you set a LAN policy that operates independently of 802.1Q VLAN-tagging.

In the default state, most of the 64 codepoints do not assign an 802.1p priority, as indicated by No-override in [Table 16 \(page 189\)](#). However, some codepoints, such as Assured Forwarding and Expedited Forwarding, have a default 802.1p priority setting.

Use the following commands to display the DSCP Policy table, configure the codepoint-priority assignments and assign optional names to the codepoints.

**Syntax:**

`show qos dscp-map`  
Displays the DSCP Policy table.

`qos dscp-map <codepoint> priority <0 - 7> [name <ascii-string>]`  
Configures an 802.1p priority for the specified codepoint and an optional (DSCP policy) name.

`no qos dscp-map <codepoint>`  
Removes the currently configured 802.1p priority that is associated with the specified <codepoint> and displays the No-override setting. The codepoint policy name, if configured, is also removed.

`no qos dscp-map <codepoint> name`  
Deletes only the policy name, if configured, for the specified codepoint.

**Table 16 The default DSCP policy table**

DSCP Policy	802.1p Priority	DSCP Policy	802.1p Priority	DSCP Policy	802.1p Priority
000000	No-override	010110	3 <sup>1</sup>	101011	No-override
000001	No-override	010111	No-override	101100	No-override
000010	No-override	011000	No-override	101101	No-override
000011	No-override	011001	No-override	101110	7 <sup>2</sup>
000100	No-override	011010	4 <sup>1</sup>	101111	No-override
000101	No-override	011011	No-override	110000	No-override
000110	No-override	011100	4 <sup>1</sup>	110001	No-override
000111	No-override	011101	No-override	110010	No-override
001000	No-override	011110	5 <sup>1</sup>	110011	No-override
001001	No-override	011111	No-override	110100	No-override
001010	1 <sup>1</sup>	100000	No-override	110101	No-override
001011	No-override	100001	No-override	110110	No-override
001100	1 <sup>1</sup>	100010	6 <sup>1</sup>	110111	No-override
001101	No-override	100011	No-override	111000	No-override
001110	2 <sup>1</sup>	100100	6 <sup>1</sup>	111001	No-override
001111	No-override	100101	No-override	111010	No-override
010000	No-override	100110	7 <sup>1</sup>	111011	No-override
010001	No-override	100111	No-override	111100	No-override
010010	0 <sup>1</sup>	101000	No-override	111101	No-override
010011	No-override	101001	No-override	111110	No-override
010100	0 <sup>1</sup>	101010	No-override	111111	No-override
010101	No-override				

<sup>1</sup> Assured Forwarding codepoints; configured by default on the switches covered in this guide.

<sup>2</sup> Expedited Forwarding codepoint configured by default.

## Displaying non-default codepoint settings (Example)

### Default priority settings for selected codepoints

In a few cases, such as 001010 and 001100, a default DSCP policy (implied by the DSCP standards for Assured-Forwarding and Expedited-Forwarding) is used. You can change the priorities for the default policies by using the `qos dscp-map <codepoint> priority <0 - 7>` command.

The currently configured DSCP policies (codepoint and associated 802.1p priority) are not enabled until you configure a global or classifier-based QoS policy to mark matching packets or configure a global IP-Diffserv classifier.

Table 16 (page 189) displays the switch's default codepoint-priority assignments. If you change the priority of any codepoint to a non-default value and then enter the `write memory` command, the switch will list the non-default setting in the `show config` display.

The default configuration has the following DSCP-priority settings:

Codepoint	Default Priority
001100	1
001101	No-override
001110	2

If you reconfigure these three codepoints to a priority of 3 and then enter the `write memory` command, the switch displays the changes in the `show config` listing:

**Figure 46** Displaying non-default priority settings in the DSCP table

```
HP Switch(config)# qos dscp-map 001100 priority 3
HP Switch(config)# qos dscp-map 001101 priority 3
HP Switch(config)# qos dscp-map 001110 priority 3
HP Switch(config)# write memory

HP Switch(config)# show config

Startup configuration:

; J9625A Configuration Editor; Created on release #K.15.XX
; Ver #01:01:00

hostname "HP E2620-24-PoEP Switch"
qos dscp-map 001100 priority 3
qos dscp-map 001101 priority 3
qos dscp-map 001110 priority 3
```

Configures three codepoints with non-default priorities.

The "show config" command lists the non-default codepoint settings.

## Changing the priority setting on a policy when classifiers are currently using the policy (Example)

In this example, the codepoint 000001 is in use by one or more global QoS policies. If you try to modify the priority currently associated with the codepoint, an error message similar to the following is displayed:

```
HP Switch(config)#: qos dscp-map 1 priority 2
Cannot modify DSCP Policy 1 - in use by other qos rules.
```

In this case, follow these steps to change the priority:

## Configuring QoS queues

QoS queue configuration reduces the number of outbound queues that all switch ports use to buffer packets for 802.1p user priorities.

Use the following commands to change the number of queues per port and display the current priority queue configuration on the switch.

## Syntax:

```
qos queue-config <2-queues | 4-queues | 8-queues>
```

Configures the number of outbound priority queues for all ports on the switch using one of the following options: 2-queues, 4-queues, or 8-queues.

The new configuration will:

- Remove any previously configured bandwidth-min output settings
- Set the new number of outbound port queues

If you select anything but yes for this operation, the operation is aborted and a message `Operation aborted` appears.

---

**△ CAUTION:** This command executes a `write memory` followed by an immediate reboot, replacing the Startup configuration with the content of the current Running configuration.

In addition to setting the number of outbound port queues, the new configuration will remove any previously configured `bandwidth-min` output settings.

---

## Viewing the QoS queue configuration

### Syntax:

```
show qos queue-config
```

Displays the current priority queue configuration and memory allocations per queue. For example:

```
HP Switch#: show qos queue-config
```

Queue	802.1p Priority	Memory %
----	-----	-----
1	1-2	10
2	0,3	70
3	4-5	10
4	6-7	10

## Using the outbound queue monitor

---

**NOTE:** Outbound queue monitoring is not supported on HP 3800 switches.

---

When QoS is used to prioritize traffic, different kinds of traffic can be assigned to different egress queues. If there is a great deal of traffic, it is desirable to be able determine if some traffic to the lower priority queues was dropped. This feature allows the egress queues for one port to be monitored for dropped packets.

### Syntax:

```
[no] qos watch-queue <port> out
```

Configures the switch to start monitoring the specified port for the dropped packets for each queue. Disabling and then re-enabling monitoring on a port clears the per-queue dropped packet counters. For example:

```
HP Switch(config)#: qos watch-queue 5 out
```

The `no` form of the command stops the collection of dropped traffic information. (Default: disabled)

## Displaying per-queue counts

The `show interface queues` command displays the number of dropped packets for each queue for the configured port. The port must have been configured with the `qos watch-queue` command. Ports that have not been configured display zero values for the queue counts.

### Example 118 Monitoring egress queues on a port

---

```
HP Switch(config)#: show interface queues 5
```

```
Status and Counters - Queue Counters for port 5
```

```
Name :
MAC Address      : 001c2e-95ab3f
Link Status      : Up
Port Totals (Since boot or last clear) :
  Rx Ucast Pkts  : 142,181          Tx Ucast Pkts  : 552
  Rx B/Mcast Pkts : 10,721,488       Tx B/Mcast Pkts : 11,765
  Rx Bytes       : 1,267,216,218   Tx Bytes       : 2,652,372
  Rx Drop Packets : 0              Tx Drop Packets : 0
Egress Queue Totals (Since boot or last clear) :
Queue CoS  Dropped Packets
1          1-2  123456789012345
2          0,3  12345678
3          4-5  1234
4          6-7  0
```

---

## About QoS

### QoS operation

On the switches covered in this guide, QoS operation may be configured through a combination of the following methods:

- Globally-configured, switch-wide QoS settings
- Classifier-based per-port and per-VLAN QoS policies.

Classifier-based QoS policies are designed to work with existing globally-configured, switch-wide QoS settings by allowing you to zoom in on a subset of port or VLAN traffic to further manage it. You can use multiple match criteria to more finely select and define the classes of traffic that you want to manage. QoS policy actions determine how you can handle the selected traffic.

---

**NOTE:** While providing greater control for implementing QoS policies, classifier-based QoS policies may override globally-configured QoS settings. For more information, see [“Viewing a classifier-based QoS configuration” \(page 184\)](#).

Carefully plan your QoS strategies in advance, identifying the network traffic that you can globally configure and the traffic on which you want to execute customized, classifier-based QoS actions.

---

### Globally-configured QoS

Globally-configured QoS operation supports the following types of packet classification and traffic marking on outbound port and VLAN traffic. For information on how to configure and use global QoS settings, see [“Configuring QoS globally” \(page 149\)](#).

- Globally configured packet classification criteria include:
  - IPv4 device: source and destination address
  - Layer 2 802.1p priority (VLAN header)
  - Layer 3 protocol (such as ARP, IP, IPX, RIP)
  - Layer 3 IPv4 Type of Service (ToS) byte: IP precedence or DSCP bits



- Layer 3 IPv6 Traffic Class byte: IP precedence or DSCP bits
- Layer 4 UDP/TCP application port
- Source port on the switch
- VLAN ID
- Traffic marking options are as follows:
  - Setting the Layer 2 802.1p priority value in VLAN-tagged and untagged packet headers
  - Setting the Layer 3 Differentiated Services Codepoint (DSCP) bits in the ToS byte of IPv4 packet headers and Traffic Class byte of IPv6 headers.

## Classifier-based QoS

Classifier-based QoS feature	Default	Page reference
Classifier-Based QoS Configuration Procedure		177
Override of Global QoS Settings		208
Viewing a Classifier-Based QoS Configuration		184
Classifier-Based QoS Restrictions		209
Classifier-Based QoS Configuration Examples		187
DSCP Policy Table	Various	188
Queue Configuration	8 Queues	190

Starting in release K.14.01, classifier-based QoS operation provides additional QoS actions on a per-port and per-VLAN basis.

- Classifier-based match criteria on inbound IPv4/IPv6 traffic include:
  - IP source address (IPv4 and IPv6)
  - IP destination address (IPv4 and IPv6)
  - IP protocol (such as ICMP or SNMP)
  - Layer 3 IP precedence bits
  - Layer 3 DSCP codepoint
  - Layer 4 UDP/TCP application port
  - VLAN ID
- Classifier-based QoS policy actions on matching IPv4/IPv6 packets are as follows:
  - Setting Layer 2 802.1p priority value (class of service) in VLAN-tagged and untagged packet headers
  - Setting the Layer 3 IP precedence bits
  - Setting the Layer 3 Differentiated-Services Codepoint (DSCP) bits
  - Rate limiting inbound traffic on port and VLAN interfaces

For information on operation with globally-configured QoS settings, see [“Advanced classifier-based QoS”](#) (page 207).

## QoS packet classification

To manage network traffic using QoS features, you must first classify (select) the packets you want to manage. You can use any combination of the following packet classification methods to select packets for QoS management:

- Globally configured, switch-wide classification criteria
- Classifier-based match criteria applied to inbound traffic on specific port and VLAN interfaces

**NOTE:** Starting in software release K.14.01, global and classifier-based QoS policies support IPv6 and IPv4 packet classification.

### Using multiple global criteria

**NOTE:** HP recommends that you configure a minimum number of global QoS classifiers to prioritize a specific packet type. Increasing the number of enabled global QoS classifiers increases the complexity of possible outcomes and consumes switch resources.

The switches covered in this guide provide six types of globally-configured QoS classifiers (match criteria) to select packets for QoS traffic marking.

When multiple, global QoS classifiers are configured, a switch uses the highest-to-lowest search order shown in the following table to identify the highest-precedence classifier to apply to any given packet. When a match between a packet and a classifier is found, the switch applies the QoS policy configured for the classifier and the packet is handled accordingly.

**Table 17 Globally-configured packet classification: search order and precedence**

Search order	Precedence	Global QoS classifier
1	1 (highest)	UDP/TCP application type (port)
2	2	Device priority (destination or source IP address)
3	3	IP type of service: precedence and DSCP bit sets (IP packets only)
4	4	IP protocol (IP, IPX, ARP, AppleTalk, SNA and NetBeui)
5	5	VLAN ID
6	6	Incoming source-port on the switch
Default	7 (lowest)	The incoming 802.1p priority (present in tagged VLAN environments) is preserved if no global QoS classifier with a higher precedence matches.

**NOTE:** On the switches covered in this guide, if the switch is configured with multiple global classifiers that match the same packet, the switch only applies the QoS marking configured for the QoS classifier with the highest precedence. In this case, the QoS configuration for another, lower-precedence classifier that matches is ignored.

For example, if QoS assigns a high priority to packets belonging to VLAN 100 and normal priority to all IP protocol packets, because the IP protocol priority (4) has precedence over the VLAN priority (5), IP protocol packets on VLAN 100 are set to normal priority.

### Classifier-based match criteria

In classifier-based packet classification, match criteria provide a way to select the packets on which you want to execute QoS actions, such as rate limiting or 802.1p prioritization.

Match criteria are configured by creating a class of IPv4 or IPv6 traffic, which contains one or more match or ignore statements. A traffic class may be used by any classifier-based software feature, such as QoS or port mirroring.

By using classifier-based QoS, you can configure multiple match criteria that search multiple fields in packet headers to select the exact traffic you want to rate limit or prioritize for a port or VLAN interface. A classifier-based QoS policy is especially useful when you want to manage different types of traffic in the same way (for example, to prioritize both IP subnet and voice traffic).

## QoS traffic marking

As described in [“QoS operation” \(page 192\)](#), when you apply or reconfigure QoS actions for selected packets, QoS supports different types of traffic marking in globally-configured QoS settings and classifier-based per-port or per-VLAN QoS policies.

### Globally-configured traffic marking

If a packet matches one of the globally-configured packet classifiers, QoS applies one of the following types of traffic marking to the outbound packet:

Layer 2 802.1p prioritization	Controls the outbound port-queue priority for traffic leaving the switch and (if traffic exits through a VLAN-tagged port) sends the priority setting with the individual packets to downstream devices.
Layer 3 DSCP marking	Enables the switch to set, change and honor prioritization policies by using the Differentiated Services (diff-serv) bits in the IPv4 ToS byte and IPv6 Traffic Class byte of packet headers.

#### Layer 2 802.1p prioritization

By setting a new 802.1p priority value, QoS lets you control the priority of outbound packets moving through the switch. The Layer 2 802.1p priority setting in a packet header determines the outbound port queue to which the packet is sent.

By default, the switches covered in this guide have eight outbound traffic queues (0 through 7). A lower-numbered queue has a lower outbound priority; a higher-numbered queue has a higher outbound priority. Packets are transmitted from the switch port on the basis of their queue assignment and whether any higher queues are empty. (To increase bandwidth, you can reconfigure the switch to use four or two outbound queues. See [“Configuring QoS queues” \(page 190\)](#).)

Configuring a new 802.1p priority value allows you to set the outbound priority queue to which a packet is sent. For example, you can configure an 802.1p priority of 0 through 7 for an outbound packet. When the packet is sent to a port, the QoS priority determines the outbound queue to which the packet is assigned as shown in the following table.

**Table 18 802.1p priority settings and outbound queue assignment**

802.1p priority setting	Outbound port queue
1 and 2	Low priority (1, 2)
0 or 3	Normal priority (3, 4)
4 and 5	Medium priority (5, 6)
6 and 7	High priority (7, 8)

If a packet is transmitted in an untagged-VLAN environment, the 802.1p priority settings in the preceding table control only the outbound queue to which the packet is sent on the local switch. Because no VLAN tag is used, an 802.1p priority value is not added to the 802.1Q field in the packet header for use by downstream devices.

However, if your network uses only one VLAN and does not require VLAN-tagged ports, you can preserve 802.1p priority settings in outbound traffic by configuring the ports on links between devices on which you want 802.1p priorities to be honored as tagged VLAN members.

If a packet is transmitted in an 802.1Q VLAN-tagged environment, the QoS-configured 802.1p setting is also added to the VLAN packet header as an 802.1p priority for use by downstream devices and applications.

In an 802.1Q VLAN environment with VLAN-tagged ports, if QoS is not configured on the switch but is configured on an upstream device, the priorities carried in the packets determine the outbound port queue on which packets are forwarded.

**Table 19 Mapping 802.1p priorities to outbound port queues on the switch and downstream devices**

Configured 802.1p priority	Outbound port queue in the switch	802.1p priority added to tagged VLAN packets exiting the switch	Queue assignment in downstream devices with:		
			8 queues	4 queues	2 queues
1	Queue 1	1 (low priority)	Queue 1	Queue 1	Queue 1
2	Queue 2	2	Queue 2		
0	Queue 3	0 (normal priority)	Queue 3	Queue 2	
3	Queue 4	3	Queue 4		
4	Queue 5	4 (medium priority)	Queue 5	Queue 3	
5	Queue 6	5	Queue 6		
6	Queue 7	6 (high priority)	Queue 7	Queue 4	
7	Queue 8	7	Queue 8		

**NOTE:** You can reconfigure the QoS queue setting to change the number of outbound port queues in the switch from eight (default) to four or two queues. For more information, see [“Configuring QoS queues” \(page 190\)](#).

### Layer 3 DSCP marking

By changing or honoring the settings of the DSCP codepoint in IP packet headers, QoS allows you to control the DSCP and associated 802.1p priority values in outbound IP packets that are sent to downstream devices.

You can later configure downstream devices to read and use the DSCP policy that QoS sets. When marking the DSCP bits in IP packets, a QoS policy is not dependent on VLAN-tagged ports to carry 802.1p packet priorities to downstream devices (as shown in [“QoS traffic marking supported in tagged and untagged VLANs” \(page 197\)](#)).

When configuring a Layer 3 DSCP policy, specify:

- Bit values for the DSCP codepoint (the upper six bits in the ToS/Traffic Class byte in IP packet headers), entered in either binary format, the decimal equivalent, or an ASCII standard (hexadecimal) name
- An 802.1p priority value that is associated with the new DSCP bit values

Certain DSCP codepoints (such as Assured Forwarding and Expedited Forwarding) have default 802.1p priorities as shown in [“The default DSCP policy table” \(page 189\)](#).

A DSCP policy assigns a DSCP codepoint and 802.1p priority value to IPv4 and IPv6 packets. As shown in [“Application of Differentiated Services Codepoint \(DSCP\) policies” \(page 148\)](#), you can classify traffic on an edge switch and use Layer 3 DSCP-marking (instead of only 802.1p priority) to assign and preserve QoS policies on downstream devices. In this case, if you reconfigure the 802.1p priority associated with the DSCP codepoint, the new 802.1p assignment takes effect starting on the switch on which it is configured and is used in packets sent to downstream devices.

If you configure a different 802.1p priority for a DSCP codepoint, the new DSCP policy overrides the 802.1p priority value in packets which enter the switch with the specified codepoint. The Layer 2 802.1p priority setting (0 through 7) determines the outbound port queue to which a packet is sent (as shown in [Table 18 \(page 195\)](#)).

## VLAN and untagged VLAN environments

QoS operates in VLAN-tagged and untagged environments. If your network does not use multiple VLANs, you can still implement the 802.1Q VLAN capability to allow packets to carry an 802.1p priority to the next downstream device. To do so, configure the ports on links to other network devices as VLAN-tagged members.

In a tagged or untagged VLAN, you can also ensure that IPv4/IPv6 packets carry an 802.1p priority to downstream devices by configuring DSCP marking in the ToS/Traffic Class byte.

The following table summarizes the QoS options for traffic-marking in VLAN-tagged and untagged environments.

**Table 20 QoS traffic marking supported in tagged and untagged VLANs**

QoS marking supported on outbound packets	Port membership in VLANs	
	Tagged	Untagged
Assign an 802.1p priority that determines the outbound port queue to which a packet is sent	Supported	Supported
Carry the 802.1p priority to the next downstream device	Supported	Not Supported
Carry a DSCP policy (DSCP codepoint <sup>1</sup> and associated 802.1p priority <sup>2</sup> ) to downstream devices	Supported	Supported

<sup>1</sup> DSCP marking (DSCP codepoint and associated 802.1p priority) are not supported on non-IP packets and packets selected using the following global QoS classifiers: Layer 3 Protocol and IP-Precedence. Also, in order for DSCP policy marking to be honored on a downstream device, the device must be configured to use the DSCP policy in IP packet headers.

<sup>2</sup> The 802.1p priority associated with a DSCP codepoint (see [“The default DSCP policy table” \(page 189\)](#)) is used to determine the packet's outbound port queue. When used in a VLAN-tagged environment, an 802.1p priority is also carried in the 802.1Q field of outbound packet headers.

## Classifier-based traffic marking

Classifier-based per-port or per-VLAN QoS policies support the following traffic-marking actions. Note that in addition to globally-configured QoS traffic marking (802.1p and DSCP prioritization), classifier-based QoS policies also support IP precedence and rate limiting.

Layer 2 802.1p prioritization	Controls the outbound port queue priority for traffic leaving the switch and (if traffic exits through a VLAN-tagged port) sends the priority setting in packet headers to downstream devices.
Layer 3 IP precedence-bitmarking	Enables the switch to set, change and honor prioritization policies by using the IP precedence bits in the ToS byte of IPv4 packet headers and Traffic Class byte of IPv6 headers.
Layer 3 DSCP marking	Enables the switch to set, change and honor prioritization policies by using the Differentiated Services (Diffserv) bits in the ToS byte of IPv4 headers and Traffic Class byte of IPv6 headers.
Rate limiting	Enables a port or VLAN interface to allow only the specified amount of bandwidth to be used for inbound traffic. When traffic exceeds the configured limit, it is dropped.

For information on how to configure and use classifier-based QoS policies, see [“Configuring classifier-based QoS” \(page 177\)](#).

**NOTE:** After you apply a classifier-based QoS policy on a port or VLAN interface:

- The 802.1p (CoS) priority and DSCP codepoint marking applied to classified packets override any 802.1p and DSCP codepoint values that are globally-configured using the QoS commands, described in [“Configuring QoS globally” \(page 149\)](#).
- The rate limit applied to classified packets overrides any globally configured rate limit globally-configured with the commands described in the Port Traffic Controls chapter in the *Management and Configuration Guide*.

For more information on how classifier-based traffic marking overrides globally-configured traffic marketing, see [“Override of global QoS settings” \(page 208\)](#).

## No override

By default, the `show qos` output for following global QoS classifiers may display `No-override` for QoS marking: IP Precedence, IP Diffserv, Layer-3 Protocol, VLAN ID and Source-port (see [“Displaying show qos output” \(page 198\)](#)). `No-override` means that the global QoS policy used to mark matching packets does not assign an 802.1p value.

- IP packets received through a VLAN-tagged port are managed using the 802.1p priority they carry in the 802.1Q field in their headers.
- VLAN-tagged packets received through an untagged port are handled by the switch with normal priority.

### Example 119 Show QoS command output

[“Displaying show qos output” \(page 198\)](#) shows the global QoS configurations on the switch that are configured with the VLAN ID classifier. Note that non-default 802.1p priorities have been configured for VLAN IDs 22 and 33; packets received on VLAN 1 are managed with the default settings, as described in the two bulleted items above.

### Figure 47 Displaying show qos output



## Global QoS restrictions

This table shows the packet types supported by different global QoS classifiers and DSCP marking.

**Table 21 Restrictions for global QoS support**

Type of packets supported	Global QoS classifiers							DSCP overwrite (re-marking)
	TCP/UDP	IP Device	IP Type-of-Service	Layer 3 Protocol	VLAN ID	Source Port	Incoming 802.1p	
IP packets (IPv4 and IPv6 <sup>1</sup> ) only	Yes	Yes	Yes	No	No	No	No	Yes
Layer-2 SAP encapsulation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

<sup>1</sup> Globally-configured QoS supports IPv6 packets starting in release K.14.01.

## All switches

For explicit QoS support of IP subnets, HP recommends forcing IP subnets onto separate VLANs and then configuring VLAN-based classifiers for those VLANs.

## For devices that do not support 802.1Q VLAN-tagged ports

For communication between these devices and the switch, connect the device to a switch port configured as `Untagged` for the VLAN in which you want the device's traffic to move.

## Port tagging rules

For a port on the switch to be a member of a VLAN, the port must be configured as either `Tagged` or `Untagged` for that VLAN. A port can be an untagged member of only one VLAN of a given protocol type. Otherwise, the switch cannot determine which VLAN should receive untagged traffic. For more on VLANs, see [“Static Virtual LANs \(VLANs\)” \(page 10\)](#).

## Maximum global QoS remarking entries

The switches covered in this guide accept the maximum number of configured outbound 802.1p priority and DSCP entries shown in the following table.

**Table 22 Maximum number of QoS entries.**

Switch	Maximum QoS remarking	Notes
3800 Switches	250 <sup>1</sup> configured entries	<ul style="list-style-type: none"> <li>Each IP Device (IP address) QoS configuration uses two entries.</li> <li>Each TCP/UDP Port QoS configuration uses two entries.</li> <li>All other global QoS classifier configurations use one entry each.</li> </ul>
Switch 8212zl Series 5400zl Series 5300yl		

<sup>1</sup> Configuring IP Device (IP address) and TCP/UDP global QoS classifiers reduces this maximum. For more information, see the Notes column.

If the global QoS configurations on a switch exceed the maximum number of entries shown in [Table 22 \(page 199\)](#), the following error message is displayed:

```
Unable to add this QoS rule. Maximum number (<entry-#:>) already reached.
```

## Not supported

Use of an inbound 802.1p packet priority as a classifier for remapping a packet's outbound priority to different 802.1p priority. For example, where inbound packets carry an 802.1p priority of 1, QoS cannot be configured use this priority as a classifier for changing the outbound priority to 0.

## Fragmented packets and TCP/UDP

QoS is not performed on fragmented packets under TCP/UDP.

## Monitoring shared resources

The QoS feature shares internal switch resources with several other features. The switch provides ample resources for all features. However, if the internal resources become fully subscribed, additional QoS provisions cannot be configured until the necessary resources are released from other uses. For information on determining the current resource availability and usage, see the appendix titled Monitoring Resources in the Management and Configuration Guide for your switch.

## Global QoS classifiers

### Global TCP/UDP classifier

#### Global QoS classifier precedence: 1

When you use TCP or UDP and a Layer 4 Application port number as a global QoS classifier, traffic carrying the specified TCP/UDP port numbers is marked with a specified priority level, without regard for any other QoS classifiers in the switch. You can configure up to 50 TCP/UDP application port numbers as QoS classifiers.

---

**NOTE:** Starting in software release K.14.01, global TCP/UDP classifiers are supported on IPv4, IPv6, or both IPv4 and IPv6 packets. In previous releases, only IPv4 packets were supported.

---

#### Options for assigning priority

The packet-marking options for global TCP/UDP port-number classifiers include:

- 802.1p priority
- DSCP policy (Assigning a new DSCP and an associated 802.1p priority; inbound packets can be IPv4 or IPv6.)

For a given TCP or UDP port number, you can use only one of the above options at a time. However, for different port numbers, you can use different options.

#### TCP/UDP port number ranges

There are three ranges:

- Well-Known Ports: 0 - 1023
- Registered Ports: 1024 - 49151
- Dynamic and Private Ports: 49152 - 65535

For more information, including a listing of UDP/TCP port numbers, go to the Internet Assigned Numbers Authority (IANA) website at:

[www.iana.org](http://www.iana.org)

Then click on:

**Protocol Number Assignment Services**  
**P** under **Directory of General Assigned Numbers**)  
**Port Numbers**



## Operating notes on using TCP/UDP port ranges

- Only 6 concurrent policies are possible when using unique ranges. The number of policies allowed is less if ACLs are also using port ranges.
- No ranges allowed that include any port numbers configured as part of another QoS application port number policy.
- An error message is generated if there are not enough hardware resources available when configuring a policy.
- The entire range of configured port numbers must be specified when using the `no` form of the command, for example:

```
HP Switch(config)#: qos udp-port range 1300 1399 dscp 001110
HP Switch(config)#: no qos range 1300 1399
```

## Example 120 Configuration for TCP and UDP port prioritization

The following example displays the following configuration for TCP and UDP port prioritization:

TCP/UDP port	802.1p priority for TCP	802.1p priority for UDP
TCP Port 23 (Telnet)	7	7
UDP Port 23 (Telnet)	7	7
TCP Port 80 (World Wide Web HTTP)	2	2
UDP Port 80 (World Wide Web HTTP)	1	1

**Figure 48 Configuring 802.1p priority assignments on TCP/UDP ports**

```
HP Switch(config)# qos tcp-port 23 priority 7
HP Switch(config)# qos tcp-port 80 priority 2
HP Switch(config)# qos udp-port 23 priority 7
HP Switch(config)# qos udp-port 80 priority 1
HP Switch(config)# qos udp-port range 100 199 priority 3
HP Switch(config)# show qos tcp-udp-port-priority
```

TCP/UDP port based priorities					
Protocol	IP Packet Type	Application Port	Apply rule	DSCP	Priority
TCP	IPV4	23	Priority		7
TCP	IPV4	80	Priority		2
UDP	IPV4	23	Priority		7
UDP	IPV4	80	Priority		1
UDP	IPV4	100-199	Priority		3

Values in these two columns define the QoS classifiers used to select the packets to prioritize.

Indicates that 802.1p priority assignments are in use for packets with 23, 80 or 100-199 as a TCP or UDP port number.

Displays the 802.1p priority assignment for packets with the indicated QoS classifiers.

## About global IP-device classifier

### Global QoS classifier precedence: 2

The global IP-device classifier enables you to configure up to 300 IP addresses to select IP packets according to source or destination address.

---

**NOTE:** IPv6 Support: Starting in software release K.14.01, IP device classifiers are supported on IPv4,IPv6 and IPv4/IPv6 subnets. In previous releases, only IPv4 packets are supported.

---

When a globally-configured IP-device address has the highest precedence in the switch for traffic addressed to or from the device, traffic received on the switch with the configured IP address is marked with the specified priority level. You can configure different IP-device classifiers with different priority levels.

**NOTE:** QoS IP-Device Restriction: The configuration of a QoS IP-device priority on the Management VLAN IP address (if configured) is not supported. If no Management VLAN is configured, the configuration of a QoS IP-device priority on the default VLAN IP address is not supported.

---

## Options for assigning priority

The packet-marking options for global IP-device classifiers include:

- 802.1p priority
- DSCP policy: Assigning a new DSCP and 802.1p priority

For information on global QoS operation when other global classifiers apply to the same traffic, see to [“Using multiple global criteria” \(page 194\)](#).

For a given IP address or subnet mask, you can assign only one of the above options at a time. However, for different IP addresses, you can use different options.

## Global IP type-of-service classifier

### Global QoS classifier precedence: 3

The global IP Type-of-Service classifier enables you to classify and mark IP packets according to the following modes:

IP-precedence mode

All IP packets generated by upstream devices and applications include a precedence bit set in the ToS/Traffic Class byte. In IP-precedence mode, the switch uses the precedence bits to compute and assign the corresponding 802.1p priority.

IP Differentiated Services (Diffserv) Mode

The Diffserv mode uses the codepoints set in IP packets by upstream devices and applications to assign an 802.1p priority to packets. You can use Diffserv mode to mark packets in the following ways:

Assign a new DSCP policy: A policy includes both a codepoint and a corresponding 802.1p priority. This option selects an incoming IP packet on the basis of its codepoint and assigns a new codepoint and corresponding 802.1p priority. (Use the `qos dscp-map` command to specify a priority for any codepoint; see [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#).)

Assign an 802.1p priority: This option reads the DSCP of an incoming IP packet and, without changing this codepoint, assigns the 802.1p priority to the packet, as configured in the DSCP Policy Table (see [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#)). Thus a priority value of 0 - 7 must be configured for a DSCP before the switch can perform a QoS match on the packet's DSCP bits.

---

**NOTE:** Prerequisite: A DSCP codepoint must have a preconfigured 802.1p priority (0 - 7) before you can use the codepoint to mark matching packets. If a codepoint you want to use shows No-override in the Priority column of the DSCP Policy table (`show qos dscp-map` command), you must first configure a priority for the codepoint before proceeding (`qos dscp-map priority` command). See [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#). Note that some 802.1p priorities are assigned by default to well-known DSCP codepoints, such as the "Assured Forwarding" and "Expedited Forwarding" codepoints (see [“The default DSCP policy table” \(page 189\)](#)).

---

Unless IP-Precedence mode and Diffserv mode are both disabled (the default setting), enabling one automatically disables the other. For more information on Type-of-Service operation, see [“IPv4 ToS/IPv6 traffic class byte” \(page 204\)](#).

## Global Layer-3 protocol classifier

### Global QoS Classifier Precedence: 4

When a global Layer-3 Protocol classifier is configured as the highest-precedence classifier and the switch receives traffic carrying the specified protocol, matching packets are assigned the priority configured for the classifier. (For information on QoS operation when other global QoS classifiers match the same traffic, see [“Using multiple global criteria” \(page 194\)](#).)

## Global VLAN-ID classifier

### Global QoS Classifier Precedence: 5

The global VLAN-ID (VID) classifier allows you to use up to 4094 VLAN IDs to match packets. When a particular VLAN-ID classifier has the highest precedence in the switch, traffic received in the VLAN is marked with the configured priority level. You can configure different global VLAN-ID classifiers to mark packets with different priority levels.

### Options for assigning priority

The global QoS packet-marking options for packets that carry a specified VLAN-ID include:

- 802.1p priority
- DSCP policy (Assigning a new DSCP and an associated 802.1p priority; inbound packets must be IPv4.)

For information on QoS operation when other global QoS classifiers match the same traffic, see to [“Using multiple global criteria” \(page 194\)](#).

---

**NOTE:** A global VLAN-ID classifier marks priority levels only in packets received on static VLANs. Packets received in a dynamic VLAN created by GVRP operation are not marked by a global VLAN-ID classifier.

The VLAN ID used as a global QoS classifier must currently exist on the switch. If you remove a VLAN from the switch, all global QoS configurations that use the VLAN ID for packet marking are also removed.

---

## Global source-port classifier

### Global QoS Classifier Precedence: 6

The global QoS source-port classifier allows you to use a packet's source-port on the switch to mark packets. When a global source-port classifier has the highest precedence in the switch for traffic entering through a port, traffic received on the port is marked with the configured priority level. Different source-port classifiers can have different priority levels.

## Options for assigning priority on the switch

The global QoS packet-marking options for matching packets from a specified source-port include:

- 802.1p priority
- DSCP policy: Assigning a new DSCP and an associated 802.1p priority

For information on QoS operation when other global QoS classifiers match the same traffic, see to [“Using multiple global criteria” \(page 194\)](#).

## Options for assigning priority from a RADIUS server

You can use a RADIUS server to assign a QoS source-port priority during an 802.1X port-access authentication session. See the RADIUS chapter in the *Access Security Guide* for your switch.

## Radius override field

During a client session authenticated by a RADIUS server, the server can impose a port priority that applies only to that client session. For more information, see the RADIUS chapter in the *Access Security Guide* for your switch.

## IPv4 ToS/IPv6 traffic class byte

IPv4 packet headers contain a Type of Service (ToS) byte; IPv6 packet headers contain a Traffic Class byte. In an IPv6 packet, the Traffic Class byte is used in the same way as the ToS byte in an IPv4 packet. A ToS/Traffic Class byte includes a DSCP codepoint and precedence bits:

- Differentiated Services Codepoint (DSCP)  
Consists of the upper six bits of the ToS/Traffic Class byte. There are 64 possible codepoints. In the switches covered in this guide, the default QoS configuration includes some codepoints, such as Assured Forwarding and Expedited Forwarding, that are preconfigured with an 802.1p priority setting. All other codepoints are not configured with an 802.1p priority and display `No-override` as shown in the default DSCP Policy table ([“The default DSCP policy table” \(page 189\)](#)).  
Use the `qos dscp map` command to configure the switch to assign different 802.1p priorities to IP packets with different codepoints. Also, you can configure the switch to assign a new codepoint with its associated priority level (0-7) to matching packets as follows:
  1. Configure a DSCP codepoint with the desired priority in an edge switch.
  2. Configure the local switch to mark specified inbound traffic with the DSCP (and thus create a policy for that traffic type).
  3. Configure the internal switches in your LAN to honor the policy.

For example, you could configure an edge switch to assign a codepoint of 000001 to all packets received from a specific VLAN and then handle all traffic with that codepoint at high priority.

For a codepoint listing and the commands for displaying and changing the DSCP Policy table, see [“Using Differentiated Services Codepoint \(DSCP\) mapping” \(page 188\)](#).

- Precedence Bits  
A subset of the DSCP codepoint, consisting of the upper three bits of the ToS/Traffic Class byte. When a global IP-Precedence classifier is configured, the switch uses the precedence bit set to determine the priority for selected packets as shown in the following table. (The switch does not change the setting of the precedence bits.)

**Table 23 IP precedence-to-802.1p priority mapping**

ToS/Traffic Class Byte: IP Precedence Bits	Corresponding 802.1p Priority	Service Priority Level
000	1	Lowest
001	2	Low
002	0	Normal
003	3	
004	4	
005	5	
006	6	
007	7	Highest

**NOTE:** Using a global IP-Precedence classifier to prioritize IP packets relies on priorities set in upstream devices and applications.

Figure 49 (page 205) shows the difference between the diffserv bits and precedence bits in an IPv4 ToS byte and an IPv6 Traffic Class byte. Note that:

- Precedence bits are a subset of the Differentiated Services bits.
- The right-most two bits are reserved.

**Figure 49 IPv4 ToS/IPv6 traffic class byte with DSCP codepoint and precedence bits**

<b>IPv4 Fields:</b>	Destination MAC Address	Source MAC Address	802.1Q Field	Type and Version	Type-of-Service Byte	...
<b>Sample IPv4 Packet:</b>	FF FF FF FF FF FF	08 00 09 00 00 16	08 00	45	E 0	...
<b>IPv6 Fields:</b>	Destination MAC Address	Source MAC Address	...	...	Traffic Class Byte	...
<b>Sample IPv6 Packet:</b>	FF FF FF FF FF FF	2001:db8:260:0212::01b4	...	...	E 0	...

Differentiated Services Codepoint						
Precedence Bits			Delay Throughput Reliability Bits			Rsvd.
1	1	1	0	0	0	0 0
E			0			

## Comparing global IP type-of-service classifiers

The next table shows the difference in how global IP-Precedence and IP-Diffserv classifiers are implemented in the switch.

Outbound port	IP Type-of-Service classifiers	
	IP-Precedence mode	IP differentiated services mode
IP Packet Sent Out an Untagged Port in a VLAN	<p>Based on the IP Precedence bit set in a packet's ToS/Traffic Class field, the packet is sent to one of eight outbound port queues in the switch:</p> <ul style="list-style-type: none"> <li>• 1 - 2 = low priority (queue 1, 2)</li> <li>• 0 - 3 = normal priority (queue 3, 4)</li> <li>• 4 - 5 = medium priority (queue 5, 6)</li> <li>• 6 - 7 = high priority (queue 7, 8)</li> </ul>	<p>Based on the DSCP codepoint that the switch has been configured to detect, one of the following actions is taken:</p> <ul style="list-style-type: none"> <li>• The codepoint is re-marked according to the configured DSCP policy and the 802.1p priority currently configured for the codepoint in the DSCP Policy see (Table 23 (page 205)).</li> <li>• The codepoint is not changed, but the 802.1p priority is marked with the currently configured value for the codepoint in the DSCP Policy table.</li> </ul> <p>Based on the new 802.1p priority marking, the packet leaves the switch through one of the following queues:</p> <ul style="list-style-type: none"> <li>• 1 - 2 = low priority (queue 1, 2)</li> <li>• 0 - 3 = normal priority (queue 3, 4)</li> <li>• 4 - 5 = medium priority (queue 5, 6)</li> <li>• 6 - 7 = high priority (queue 7, 8)</li> </ul> <p>If <i>No-override</i> (the default) is configured for the 802.1p priority associated with a codepoint, the priority in the packet header is not re-marked by the global IP-Diffserv classifier and, by default, is sent to the "normal priority" outbound port queue.</p>
IP Packet Sent Out a Tagged Port in a VLAN	<p>Based on the IP Precedence bit set in a packet's ToS/Traffic Class field:</p> <ul style="list-style-type: none"> <li>• The packet is sent to one of eight outbound port queues in the switch as described above.</li> <li>• The IP Precedence value (0 - 7) is used to set the corresponding 802.1p priority in the VLAN tag carried by the packet to the next downstream device (see Table 23 (page 205)).</li> </ul>	<p>Based on the DSCP codepoint that the switch has been configured to detect, one of the following actions is taken:</p> <ul style="list-style-type: none"> <li>• The codepoint is re-marked according to the configured DSCP policy and the 802.1p priority currently configured for the codepoint in the DSCP Policy Table (Table 23 (page 205)).</li> <li>• The codepoint is not changed, but the 802.1p priority is marked with the currently configured value for the codepoint in the DSCP Policy Table (Table 23 (page 205)).</li> </ul> <p>Based on the new 802.1p priority marking, the packet leaves the switch through one of the outbound port queues described above.</p> <p>In addition, the priority value (0 - 7) is used to set the 802.1p priority in the VLAN tag carried by the packet to the next downstream device. If the priority is configured as <i>No-override</i> in the DSCP Policy table, the VLAN tag carries a "0" (normal priority) 802.1p setting if not prioritized by other global QoS classifiers.</p>

## Advanced classifier-based QoS

Starting in software release K.14.01, in addition to the packet classification and prioritization methods described in [“Configuring QoS globally” \(page 149\)](#), QoS configuration also supports advanced classifier-based functions. Advanced classifier-based QoS introduces:

- A finer granularity than globally-configured QoS for classifying IPv4 and IPv6 traffic
- Additional actions for managing selected traffic, such as rate limiting and IP precedence marking
- The application of QoS policies to inbound traffic flows on specific port and VLAN interfaces (instead of using only globally-configured, switch-wide QoS settings)
- The ability to re-use traffic classes in different software-feature configurations, such as QoS and port mirroring

Classifier-based QoS is designed to work with existing globally-configured, switch-wide QoS policies by allowing you to zoom in on a subset of port or VLAN traffic to further manage it. Classifier-based policies take precedence over and may override, globally-configured QoS settings that apply to all traffic on the switch.

Classifier-based QoS policies provide greater control for managing network traffic. Using multiple match criteria, you can finely select and define the classes of traffic that you want to manage. QoS-specific policy actions determine how you can handle the selected traffic.

For more information, see the "Classifier-Based Software Configuration" chapter in the *Advanced Traffic Management Guide*.

## Classifier-based QoS model

Classifier-based QoS configuration consists of the following general steps:

1. Classify the traffic that you want to manage by configuring a class.
2. Configure a QoS policy in which you specify the QoS actions to execute on each class of traffic.
3. Assign the QoS policy to a port or VLAN (inbound only) interface.

**NOTE:** Classifier-based QoS operation supports all globally-configured packet classification criteria (except for Source-port and Layer-3 protocol) and traffic marking functions and provides additional QoS actions on a per-port and per-VLAN basis.

- Classifier-based match criteria on inbound IPv4/IPv6 traffic include:
  - IP source address (IPv4 and IPv6)
  - IP destination address (IPv4 and IPv6)
  - IP protocol (such as ICMP or SNMP)
  - Layer 3 IP precedence bits
  - Layer 3 DSCP codepoint
  - Layer 4 TCP/UDP application port (including TCP flags)
  - VLAN ID
- Classifier-based QoS policy actions on matching IPv4/IPv6 packets are as follows:
  - Setting the Layer 2 802.1p priority value (class of service) in VLAN-tagged and untagged packet headers
  - Setting the Layer 3 IP precedence bits
  - Setting the Layer 3 Differentiated Services Codepoint (DSCP) bits
  - Rate limiting inbound traffic on port and VLAN interfaces

## Override of global QoS settings

After you apply a QoS policy to an interface, the classifier-based settings configured by QoS actions in the policy override any 802.1p CoS or DSCP codepoint values that were globally-configured on the switch to mark packets using the QoS commands described in [“Configuring QoS globally”](#) (page 149).

If you use a classifier-based QoS configuration along with globally-configured QoS commands, the order of precedence in which 802.1p priority, IP precedence and DSCP settings mark selected packets is as follows, from highest (1) to lowest (9):

**Table 24 Order of precedence for classifier-based QoS over global QoS**

Precedence order	QoS feature	Reference
1	Classifier-based port-specific policy	(page 177)
2	Classifier-based VLAN-specific policy	(page 177)
3	Globally-configured TCP/UDP priority	(page 200)
4	Globally-configured IP-device priority	(page 201)
5	Globally-configured IP Type-of-Service priority	(page 202)
6	Globally-configured Layer 3-Protocol priority	(page 203)
7	Globally-configured VLAN-ID priority	(page 168)
8	Globally-configured Source-Port priority	(page 203)
9	802.1p CoS in Layer 2 VLAN header <sup>1</sup>	(page 194)



<sup>1</sup> In a tagged VLAN environment, the incoming 802.1p priority is used as the default QoS classifier to determine how a packet is handled if no global or classifier-based QoS match criterion with a higher precedence matches.

## Effect of No-override

If you configure a global IP-Diffserv classifier and `No-override` is displayed for the 802.1p priority associated with a codepoint, DSCP marking cannot be performed on matching outbound packets. However, QoS does not affect the packet-queuing 802.1p priority or VLAN tagging carried in the packet.

In this case, the packets are handled as follows (as long as no other QoS classifier marks a new 802.1p priority on the matching packets):

802.1Q status	Outbound 802.1p priority
Received and forwarded on a tagged-port member of a VLAN	Unchanged
Received on an untagged-port member of a VLAN; forwarded on a tagged-port member of a VLAN	0 (zero) normal
Forwarded on an untagged-port member of a VLAN	None

## Classifier-based QoS restrictions

The following restrictions apply to QoS policies configured with the classifier-based model:

- A classifier-based QoS policy cannot be applied on a port or VLAN interface on which a classifier-based QoS policy is already configured. It is possible to apply a classifier-based policy of a different type, such as port mirroring.
- A QoS policy that uses the `rate-limit` command is not supported on a port interface on which ICMP rate limiting has already been globally configured. To apply the QoS policy, you must first disable the ICMP rate limiting configuration. See “ICMP section in the Configuring IP Parameters for Routing Switches” in the *Multicast and Routing Guide*.

In cases where an ICMP rate limiting configuration is to be maintained, configure a QoS policy by adding the necessary `match` statements for the ICMP traffic in a class configuration, then configure a `rate-limit` action for the class in the policy configuration.

- In a QoS policy that uses the `class action rate-limit` command, the rate limit is calculated on a per-module or per port-bank basis. If trunked ports or VLANs with a configured rate limit span multiple modules or port-banks, the configured rate limit is not guaranteed.
- In a QoS policy that uses the `class action dscp` command, the DSCP value entered must be already configured with an 802.1p priority in the DSCP Policy table (see “[The default DSCP policy table](#)” (page 189)).

## Interaction with other software features

After applying a QoS policy to an interface, an error message appears if there are not sufficient hardware resources to support the policy. In this case, use the `show resources` command to verify the amount of resources that are currently in use and the resources available on the switch. QoS policies share the same hardware resources with other software features, such as mirroring policies, ACLs, virus throttling, the management VLAN, and so on.

Use the displayed information to decide whether to re-prioritize current resource usage by reconfiguring or disabling software features to free the resources reserved for less important features.

For more information, see “[Displaying resource usage for QoS policies](#)” (page 155) and the Monitoring Resources chapter in the *Management and Configuration Guide*.

## Notes on changing priority settings

If you try to modify the priority associated with a DSCP codepoint in a DSCP policy using the `qos dscp-map priority` command, and if the DSCP policy is currently used by one or more global QoS or classifier-based QoS policies, the following error message is displayed:

```
Cannot modify DSCP Policy codepoint - in use by other qos rules.
```

In this case, enter the following QoS show commands to identify in which global and classifier-based QoS configurations the DSCP policy is currently used:

```
show policy <qos-policy>
show qos tcp-udp-port-priority
show qos device-priority
show qos type-of-service
show qos protocol
show qos vlan
show qos port-priority
```

After determining the QoS configurations in which the DSCP-priority mapping is used, you can either delete a QoS configuration and reset the DSCP-priority mapping to `No-override`, or change either the 802.1p priority or the codepoint used in the QoS configuration.

### Example 121 Changing the priority of a codepoint

---

If codepoint 000001 is currently mapped to priority 6, and several global QoS policies use this codepoint to assign a priority to their respective types of matching traffic, you can change the priority associated with the codepoint using the following procedure.

1. Identify the global and classifier-based QoS policies that use the codepoint.
  2. Do one of the following:
    - a. Reconfigure each QoS policy by re-entering a different DSCP codepoint or a different 802.1p priority associated with the codepoint.
    - b. Enter the `no qos <classifier>` or `no policy <qos-policy>` command to remove the current DSCP policy with codepoint 000001 and reset the priority to `No-override`.
  3. Use the `qos dscp-map 000001 priority 0 - 7` command to remap DSCP 000001 to the desired priority.
  4. Do one of the following:
    - a. Reconfigure codepoint 000001 in the QoS policies in which you want to use the new DSCP-priority mapping to mark matching packets.
    - b. Leave a QoS policy in which you use DSCP 000001 to mark matching packets with the associated `No-override` priority mapping.
- 

### Error messages for DSCP policy changes

See the error messages in the following table to troubleshoot an error condition that results from reconfiguring a DSCP policy.

**Table 25 Error messages generated by DSCP policy changes**

Error message	Description
DSCP Policy <i>&lt;decimal-codepoint&gt;</i> not configured	You have tried to configure a codepoint in a global or classifier-based QoS policy for which there is no associated priority (No-override). Use the <code>qos dscp-map</code> command to configure a priority for the codepoint, then re-enter the codepoint in the QoS configuration.
Cannot modify DSCP Policy <i>&lt;codepoint&gt;</i> - in use by other qos rules.	You have tried to configure a codepoint in a global or classifier-based QoS policy that is already in use by other QoS policies. Before remapping the codepoint to a new priority, you must first reconfigure the other QoS policies so that they do not use the current codepoint-priority mapping. You can have multiple QoS policies that use the same codepoint to mark packets as long as it is acceptable for all such policies to use the same 802.1p priority.

## QoS queue configuration

### Mapping of outbound port queues

This table shows the mapping of 802.1p priorities to outbound port queues.

**Table 26 Mapping 802.1p priorities to outbound port queues**

802.1p priority	8 Queues (default)	4 Queues	2 Queues
1 (lowest)	1	1	1
2	2		
0 (normal)	3	2	
3	4		
4	5	3	2
5	6		
6	7	4	
7 (highest)	8		

## Impact of QoS queue configuration on guaranteed minimum bandwidth (GMB)

Changing the number of queues removes any `bandwidth-min` output settings in the startup configuration, and automatically re-allocates the GMB per queue as shown in the following table.

**Table 27 Default GMB percentage allocations per QoS queue configuration**

802.1p priority	8 Queues (default)		4 Queues		2 Queues	
	Queue	GMB	Queue	GMB	Queue	GMB
1 (lowest)	1	2%	1	8%	1	20%
2	2	3%				
0 (normal)	3	30%				
3	4	10%				
4	5	10%	3	30%	2	80%
5	6	10%				
6	7	15%	4	45%		
7 (highest)	8	20%				

**NOTE:** See "Port Traffic Controls" in the *Management and Configuration Guide* for your switch.

## Setting minimum guaranteed bandwidth with 8 queues

When 10 Mbps ports on an 8200zl or 5400zl switch are configured in QoS for eight outbound queues (the default), and the guaranteed minimum bandwidth is set for 5 Mbps or less for a given queue, then packets in the lower-priority queues may be discarded on ports that are oversubscribed for extended periods of time. If the oversubscription cannot be corrected, HP recommends reconfiguring the switch to operate with four outbound queues. The command to do this is:

```
HP Switch(config)#: qos queue-config 4-queues
```

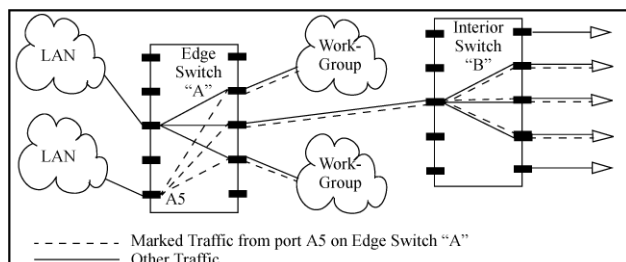
This issue applies to 8200zl and 5400zl switches operating with any of the following modules installed.

HP device	Product number	Minimum supported software version
HP Switch 24-port 10/100/1000 PoE+v2 zl Module	J9534A	K.15.02.0004
HP Switch 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module	J9535A	K.15.02.0004
HP Switch 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module	J9536A	K.15.02.0004
HP Switch 24-port SFP v2 zl Module	J9537A	K.15.02.0004
HP Switch 8-port 10-GbE SFP+ v2 zl Module	J9538A	K.15.02.0004
HP 24-port 10/100 PoE+ v2 zl Module	J9547A	K.15.02.0004
HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module	J9548A	K.15.02.0004
HP 20-port Gig-T / 4-port SFP v2 zl Module	J9549A	K.15.02.0004
HP 24-port Gig-T v2 zl Module	J9550A	K.15.02.0004
HP 12-port Gig-T / 12-port SFP v2 zl Module	J9637A	K.15.02.0004

## Assigning an 802.1p priority for a global IP-diffserv classifier

One of the best uses for this global QoS packet-marking option is on an interior switch to honor (continue) a policy set on an edge switch. The IP-diffserv classifier enables selecting incoming packets having a specific DSCP and forwards these packets with the desired 802.1p priority. For example, if an edge switch A marks all packets received on port A5 with a particular DSCP, you can configure a downstream (interior) switch B to handle such packets with the desired priority (regardless of whether 802.1Q-tagged VLANs are in use).

**Figure 50 Interior switch B honors the policy established in edge switch A**



To do so, assign the desired 802.1p priority to the same codepoint that the upstream or edge switch assigns to the selected packets. When the downstream switch receives an IP packet carrying one of these codepoints, it assigns the configured priority to the packet and sends it out the appropriate outbound port queue. (The packet retains the codepoint it received from the upstream or edge switch). You can use this option concurrently with the diffserv DSCP Policy option, as long as the DSCPs specified in the two options do not match.

**NOTE:** Different applications may use the same DSCP in their IP packets. Also, the same application may use multiple DSCPs if the application originates on different clients, servers, or other devices. Using an edge switch enables you to select the desired packets and mark them with predictable DSCPs that can be used by downstream switches to honor policies set in the edge switch.

When enabled, the switch applies direct 802.1p prioritization to all packets having codepoints that meet these prerequisites:

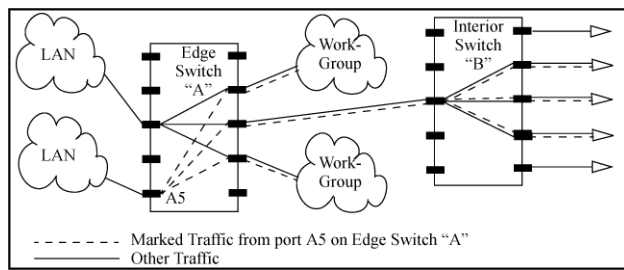
- The codepoint is configured with an 802.1p priority in the DSCP table. (Codepoints configured with `No-override` are not used.)
- The codepoint is not configured for a new DSCP policy assignment.

Thus, the switch does not allow the same incoming codepoint (DSCP) to be used simultaneously for directly assigning an 802.1p priority and also assigning a DSCP policy. For a given incoming codepoint, if you configure one option and then the other, the second overwrites the first.

## Assigning an 802.1p priority for a global IP-diffserv classifier

One of the best uses for this global QoS packet-marking option is on an interior switch to honor (continue) a policy set on an edge switch. The IP-diffserv classifier enables selecting incoming packets having a specific DSCP and forwards these packets with the desired 802.1p priority. For example, if an edge switch A marks all packets received on port A5 with a particular DSCP, you can configure a downstream (interior) switch B to handle such packets with the desired priority (regardless of whether 802.1Q-tagged VLANs are in use).

**Figure 51 Interior switch B honors the policy established in edge switch A**



To do so, assign the desired 802.1p priority to the same codepoint that the upstream or edge switch assigns to the selected packets. When the downstream switch receives an IP packet carrying one of these codepoints, it assigns the configured priority to the packet and sends it out the appropriate outbound port queue. (The packet retains the codepoint it received from the upstream or edge switch). You can use this option concurrently with the diffserv DSCP Policy option, as long as the DSCPs specified in the two options do not match.

**NOTE:** Different applications may use the same DSCP in their IP packets. Also, the same application may use multiple DSCPs if the application originates on different clients, servers, or other devices. Using an edge switch enables you to select the desired packets and mark them with predictable DSCPs that can be used by downstream switches to honor policies set in the edge switch.

When enabled, the switch applies direct 802.1p prioritization to all packets having codepoints that meet these prerequisites:

- The codepoint is configured with an 802.1p priority in the DSCP table. (Codepoints configured with `No-override` are not used.)
- The codepoint is not configured for a new DSCP policy assignment.

Thus, the switch does not allow the same incoming codepoint (DSCP) to be used simultaneously for directly assigning an 802.1p priority and also assigning a DSCP policy. For a given incoming codepoint, if you configure one option and then the other, the second overwrites the first.

## Viewing logging output

The `show logging` command troubleshoots problems in stacking.

### Syntax

```
show logging [a|r|m|p|w|i|d|substring]
```

The options `a|r|substring` can be used in combination with an event class option.

`a` Instructs the switch to display all recorded log events, which includes events from previous boot cycles.

`r` Instructs the switch to display recorded log events in reverse order (most recent first.)

`substring` Instructs the switch to display only those events that match the substring.

The remaining event class options are listed in order of severity with lowest severity first. The output of the command is confined to event classes of equal or higher severity.

Only one of options `d|i|w|e|p|m` can be used in the command at a time.

`m` Displays major type of messages.

`p` Displays major and error type of messages.

`w` Displays major, error and warning type of messages.

`i` Displays major, error, warning and information.

d Displays major, error, warning, information and debug messages.

### Example 122 Logging output

---

```
HP Stack 3800 #: show logging -r -s  
I 10/02/00 00:46:56 02558 chassis: ST1-STBY: Stack port 3 is now on-line.  
I 10/02/00 00:46:56 02558 chassis: ST2-CMDR: Stack port 2 is now on-line.
```

---

# 6 BYOD-redirect

## Introduction

The HP BYOD (bring-your-own-device) solution lets you design, manage, and control a BYOD network when you configure the BYOD-redirect feature on your switches.

Where BYOD-redirect is enabled on a switch, the device's client credentials are sent to the BYOD server for registration. The BYOD server stores the registration information for each client's device (such as the device MAC-address), which gives that client's device access to the network.

The HP BYOD solution includes:

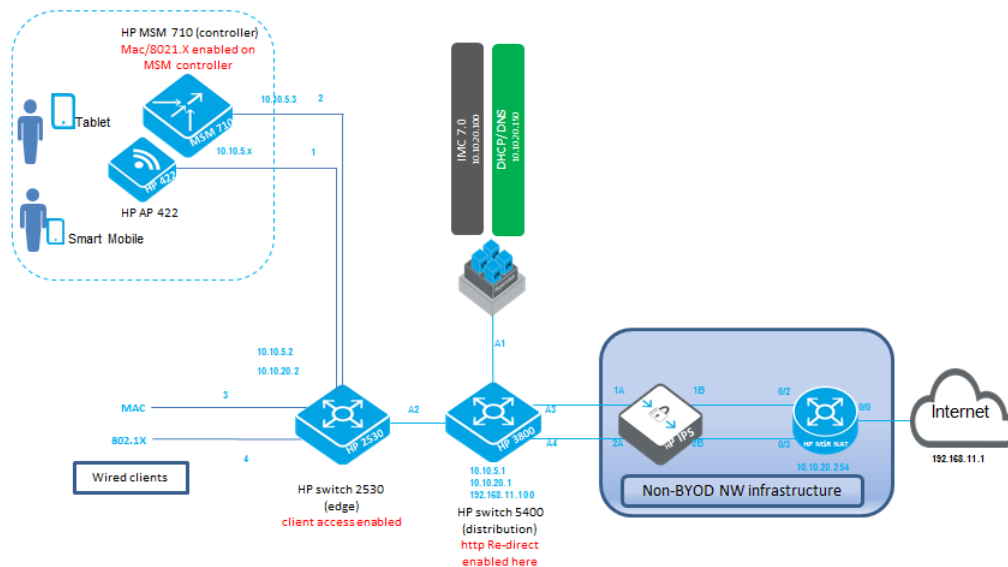
- secure user authentication
- centralized authentication process
- authorization and accounting
- unified monitoring and network management services
- ease-of-use self-registration (on-boarding) process

### Example 123 BYOD solution

Figure 52 (page 216) illustrates a BYOD solution that includes the following:

- Access point and wireless controller: manages wireless SSIDs.
- BYOD (IMC) server: manages BYOD policy and centralized user management.
- HP switches: re-directs user registration traffic to IMC and grants port.
- BYOD Redirect feature: supported on HP ProVision switches.

Figure 52 BYOD solution



## Features

When BYOD-redirect is enabled on a VLAN, the BYOD feature intercepts HTTP traffic and blocks all other traffic for which free rules are not enabled. Most BYOD-redirect implementation is platform independent, except installing free rules to mitigate risks.

Communication between clients and the IMC server is tunneled by the edge switch:



1. A client request is read by the HTTP task.
2. The HTTP task always redirects, after embedding client IP addresses, a URL trying to access the redirected URL.
3. The redirect response includes URL parameters: **user ip address** and **url user is trying to access**.
4. The client receives a redirect response from the switch and makes an HTTP request to redirect the URL.

**Figure 53 The BYOD-redirect function**

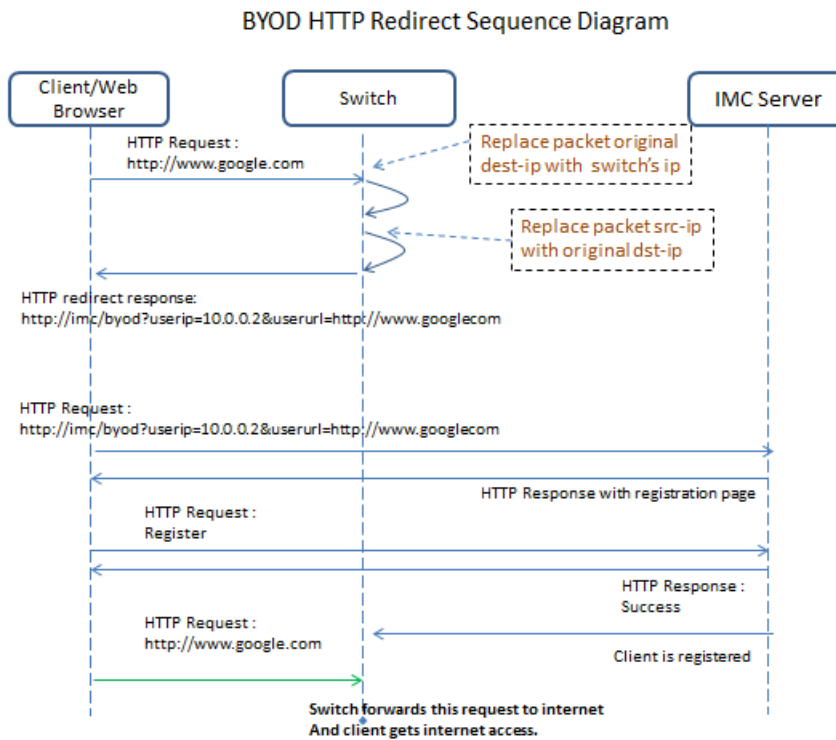
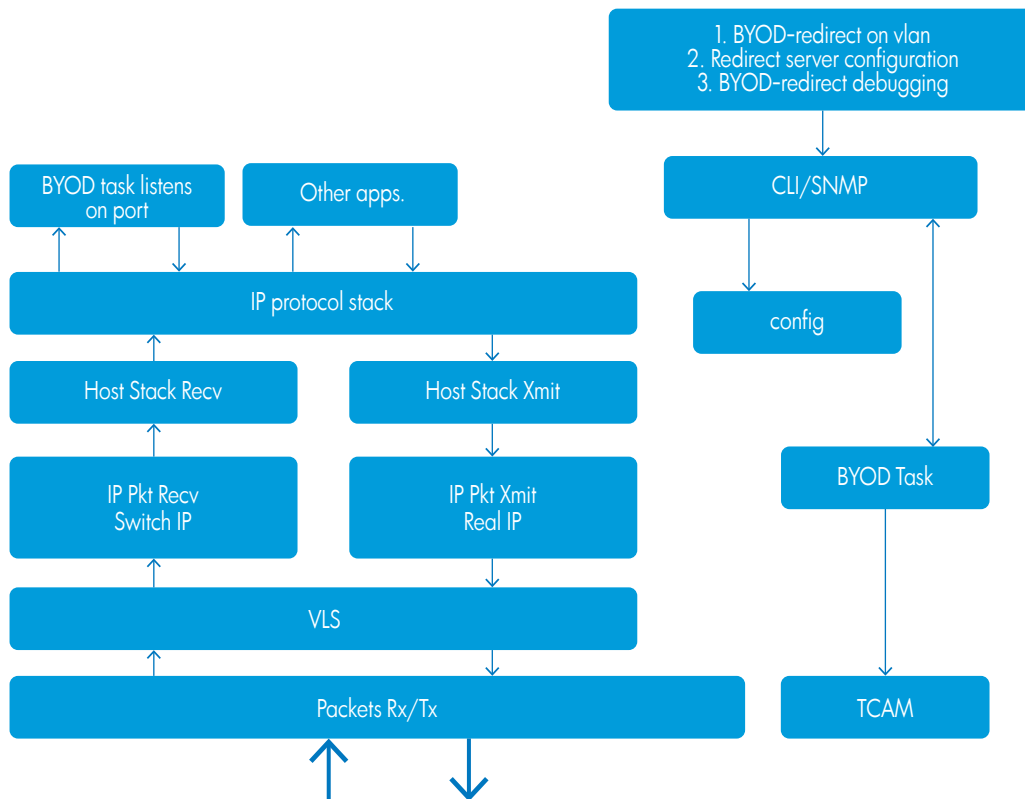


Figure 54 BYOD-redirect on VLAN



## SNMP Interactions

BYOD updates server details using the BYOD VLAN map and TCAM rules from an SNMP communication, handling dynamic re-configuration events by BYOD task:

1. To configure a BYOD server:  
Internal data structure is updated, including the server URL, server IP, port and other parameters.
2. To enable BYOD-redirect on a VLAN:  
The following TCAM rules are installed:
  - Steal and hardware drop for http traffic (80).
  - Drop (IP traffic) all rules to be installed.
  - Install hardware forward rule for http packets to the BYOD server.
  - Allow ARP packets any to any.
3. Configure free rules to allow traffic to DNS, DHCP and other traffic.

## Interoperability with other switch features

The following rules can help avoid conflicts when BYOD-redirect has been deployed on a switch with other features:

1. **MAFR and BYOD-redirect are mutually exclusive** – MAFR and BYOD-redirect solve similar problems.
2. **DNS sentinel and BYOD-redirect** – When a DNS sentinel is enabled, the switch tunnels packets to the controller. Packets are re-injected to the switch only if the controller classifies DNS packets as permitted. When BYOD-redirect is enabled, the user should configure an ACL rule to pass through DNS packets to the switch. If SDN controller policy classifies a DNS packet originating from a client as drop, then BYOD-redirect does not work.

3. **IP sentinel and BYOD-redirect** – When IP sentinel is enabled for the IP flows configured by the SDN controller, the switch tunnels the IP packets to the controller. The IP packets are re-injected to the switch only if the controller classifies the IP traffic as not malicious. If the SDN controller policy classifies the client’s IP traffic as malicious, then BYOD-redirect fails.
4. **OpenFlow and BYOD-redirect** – If an OpenFlow instance is enabled on a VLAN, then all traffic is given to the OpenFlow packet processing task. BYOD-redirect requires intercepting IP (HTTP) packets. If BYOD-redirect inter-operates with OpenFlow, traffic should be copied to both Openflow and BYOD-redirect; otherwise, the switch cannot enable BYOD-redirect and OpenFlow on the same VLAN.
5. **Other TCAM rules** – If any other user has configured TCAM rules that override TCAM entries installed for BYOD-redirect, BYOD redirect does not work.

## Interoperability with other vendors

Because BYOD policy integrates several logical components including MSM, UAM, and RADIUS, the redirected URL in the BYOD-redirect feature on a switch must include the `byod-server-url` and `user-ip` information to work with the IMC server.

BYOD-redirect configuration command syntax for ProVision software matches Comware server command syntax.

## Restrictions

BYOD-redirect has the following restrictions:

1. BYOD-redirect is a per-VLAN configuration; up to three VLANs can be enabled with BYOD-redirect.
2. BYOD-redirect supports up to three redirection servers configured on a switch. When a redirection server URL is configured, the BYOD module maintains separate data structures to store the re-directed URL on the VLAN where BYOD-redirect is enabled. BYOD-redirect statistics are maintained for each server.

## Configuring

### Creating a BYOD server

Configure a portal redirect web-server.

#### Syntax

```
[no] portal web-server [web-server-name] url [url-string]
```

Term	Meaning
portal	Configure the BYOD redirect feature.
web-server	Configure portal redirect web-server.
url	Configure the URL of the BYOD server.
<i>url-string</i>	A URL redirecting the client to the BYOD server must be in ASCII.

### Associating a BYOD server

Associate a BYOD server with a specific VLAN to redirect clients to the assigned URL page.

## Syntax

```
[no] vlan [vlan-id] <portal web-server [web-server-name] >
```

Term	Meaning
vlan	Add, delete, edit VLAN configuration or enter a VLAN context.
<i>vlan-id</i>	VLAN identifier or VLAN name.
portal	Configure the BYOD redirect feature on a VLAN.
web-server	Specify the BYOD web-server.
<i>web-server-name</i>	BYOD web-server name in ASCII.

## Creating a BYOD ACL rule

Configure a BYOD-free rule.

### Syntax

```
[no] portal free-rule [rule-number] vlan [VLAN-ID] destination  
<<ip-address> | mask <mask-length> | any tcp <des-tcp-port>  
| udp <des-udp-port> | source <ip-address> | mask  
<mask-length> | any tcp <src-tcp-port> |udp <src-udp-port>>
```

Term	Meaning
portal	Configure the BYOD redirect feature.
free-rule	Configure a BYOD-free rule.
rule-number	Free rule number as an INTEGER<1-6>.
vlan	Free rule source VLAN ID.
VLAN-ID	VLAN identifier or VLAN name.
destination	Free rule destination.
<i>ip-address</i>	IP address
mask	Mask
mask-length	Mask length.
tcp	TCP protocol
udp	UDP Protocol
des-udp-port	tcp port destination
source	Free rule source.
<src/des-tcp/udp-port>	TCP or UDP port number, as an integer<1-65534>.
any	Free rule source any.
ip	Free rule source IP.
IP	Free rule destination IP.
any	Free rule source or destination any.

## Implementing BYOD-redirect configuration

BYOD enables employees to register and access corporate resources with personally-owned devices. Though BYOD provides flexibility to employees, it can bring challenges to IT departments. BYOD-redirect is designed to help manage and control personal devices and policies at the enterprise network level.

Before implementing BYOD-redirect ensure that:

- BYOD-redirect is configured on a VLAN.
- BYOD-redirect is supported on up to three VLANs.
- BYOD-redirect is supported with Mac and 802.1X authentications.
- BYOD-redirect works with IMC 7.0 UAM module.
- The switch supports Radius CoA Access-Accept (RFC 3576/5176).
- The client URL and DHCP IP are included in the Re-direct URL to the IMC.

---

**NOTE:** Until the registration process has been completed, a client device cannot access the internet or the enterprise network. Any traffic from this unauthorized device is redirected to the BYOD server.

---

### Implementing BYOD-redirect configuration examples

The following examples show how to implement BYOD-redirect for both wired and wireless solutions.

## Example 124 BYOD configuration on a distribution switch

---

To facilitate the BYOD-redirect function, complete the following tasks on the distribution switch:

1. Configure DNS and make FQDN solution successful: `ip dns server-address priority 1 <DNS-server-IP>`.

---

**NOTE:** The argument to the URL can be an FQDN or IP address. If you use the IP address as an argument, this step is not necessary.

---

2. Configure BYOD web-server URL: `portal web-server "byod" url http://imc.com:8080/byod`.
3. Enable BYOD-redirect on a VLAN: `vlan 101 portal web-server "byod."`
4. Configure BYOD-redirect free-rules on the on-boarding VLAN 101 to permit client traffic transit through DNS and DHCP servers using the following commands.

To permit DNS traffic to/from a DNS server to a client through on-boarding VLAN:

- a. `portal free-rule 1 vlan 101 source any udp 0 destination any udp 53`
- b. `portal free-rule 2 vlan 101 source any udp 53 destination any udp 0`

To permit DHCP traffic to/from DHCP server to client through on-boarding VLAN:

- a. `portal free-rule 3 vlan 101 source any udp 68 destination any udp 67`
- b. `portal free-rule 4 vlan 101 source any udp 67 destination any udp 68`

5. Register device in IMC on the on-boarding VLAN. When registration is successful, client traffic is placed into different VLAN (guest/corporate) configurations.
- 

## Example 125 Client authentication configuration on edge switch

---

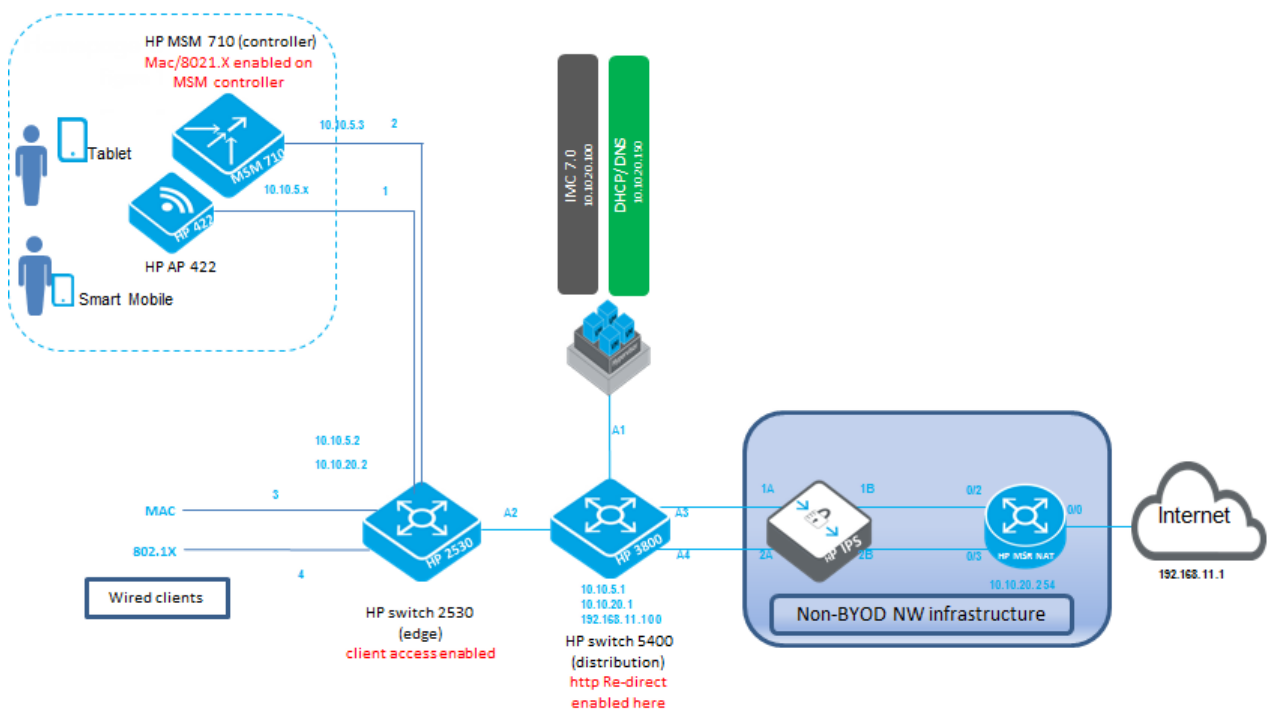
Enable MAC authentication on edge switch port 1-2 using the following commands:

- `# enable mac authentication on ports 1-2`
  - `aaa port-access mac-based 1-2`
  - `# configure number of client limits on port 1 and port2`
  - `aaa port-access mac-based 1 addr-limit 32`
  - `aaa port-access mac-based 2 addr-limit 32`
  - `radius-server host <radius ip> dyn-authorization`
  - `radius-server host <radius ip> time-window 0`
-

**Table 28 Wired and wireless components configured in a network topology**

Access Type	Edge Switch	Distribution Switch	Configuration Procedure Note
Wired Access	HP 2530 switch	HP 5400 switch	<ol style="list-style-type: none"> <li>1. Register the HP 2530 switch in HP IMC.</li> <li>2. Create the configuration on HP 2530 switch.</li> <li>3. Create the configuration on HP 5400 switch.</li> </ol>
Wireless Access			<ol style="list-style-type: none"> <li>1. Make the HP MSM controller reachable by HP IMC.</li> <li>2. Ensure that access points (HP 422) are managed by the MSM controller.</li> <li>3. Configure MAC or 802.1X authentication on the MSM controller.</li> <li>4. Create the configuration on the HP 5400 switch.</li> </ol>

**Figure 55 Wired and wireless components configured in a network topology**



**Table 29 Wired clients solution**

Access Type	Edge Switch	Distribution Switch	Configuration Procedure
Wired Access	HP 2530 switch	HP 3800 switch	<ol style="list-style-type: none"> <li>1. Register the HP 2530 switch and HP 3800 switch in IMC.</li> <li>2. Ensure that both HP 2530 switch and HP 3800 switch can reach the DHCP and DNS server.</li> <li>3. Create the configuration on HP 2530 switch.</li> <li>4. Create the configuration on HP 3800 switch.</li> </ol>

Figure 56 Wired clients solution

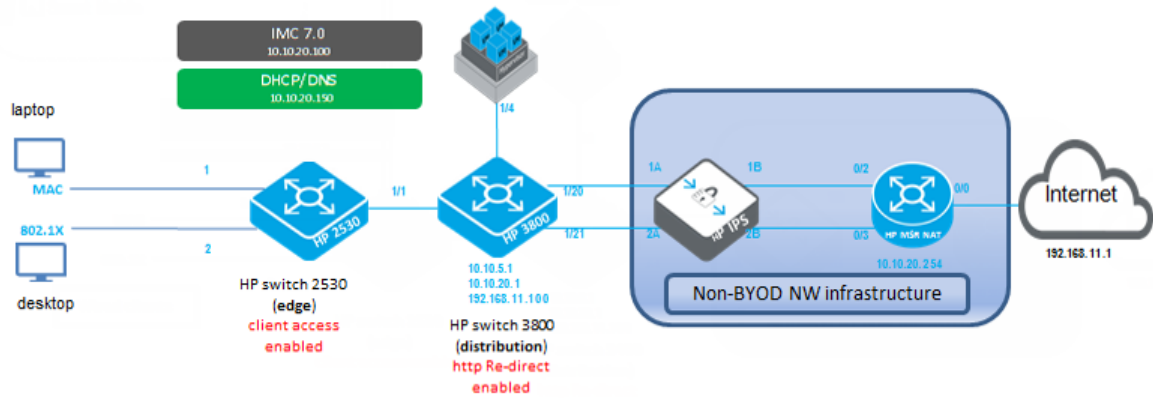
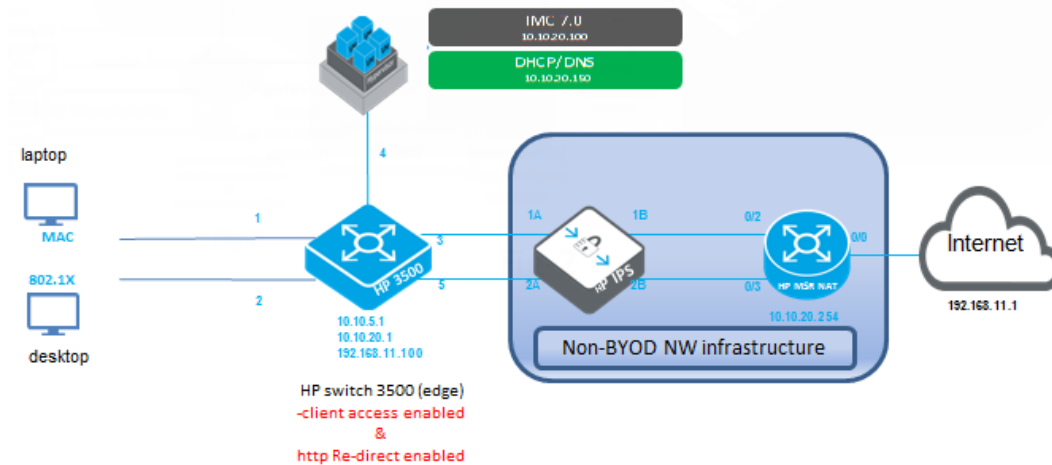


Table 30 Configuration and access for wired clients on an edge switch

Access Type	Edge Switch	Distribution Switch	Configuration Procedure
Wired Access	HP 3500 switch	N/A	<ol style="list-style-type: none"> <li>1. Register the HP 3500 switch in HP IMC.</li> <li>2. Ensure that the HP 3500 switch is reachable by the DHCP and DNS server.</li> <li>3. Create the configuration on the HP 3500 switch.</li> <li>4. Create the following configuration on the HP 3500 switch.</li> </ol>

Figure 57 Configuration and access for wired clients on an edge switch



## Show commands

### Show portal server

Display all BYOD servers and their attributes or specify a BYOD web-server-name to display its details.



## Syntax

```
show portal web-server [web-server-name]
```

Term	Meaning
portal	Display BYOD server details..
web-server	Specify the BYOD web-server.
<i>web-server name</i>	Enter BYOD web-server name in ASCII.

## Sample output

```
Portal Server:
1) imc:
Resolved IP      : 15.146.197.224
VPN Instance    : n/a
URL              : http://15.146.197.224:80/byod
VLAN            : 101
DNS Cache Status : 20 seconds
```

## Show portal redirect statistics

Show redirect statistics of a BYOD.

## Syntax

```
show portal redirect statistics
```

Term	Meaning
portal	Display BYOD server details.
redirect	Display redirect statistics
statistics	Display the statistics.

## Example 126 Sample output

```
show portal redirect statistics
Status and Counters - Portal Redirect Information
Total Opens          : 0
Resets Connections   : 0
Current Opens        : 0
Packets Received     : 14997
Packets Sent         : 12013
  HTTP Packets Sent  : 3002
Current Connection States :
SYN_RECV             : 0
ESTABLISHED          : 0
```

## Show portal free rule

Display all BYOD free rules and their attributes; the user can specify a BYOD rule to display its free rule.

## Syntax

```
show portal free-rule [free-rule-number]
```

Term	Meaning
portal	Display BYOD server details.
free-rule	Display BYOD-free rule.
<i>free-rule-number</i>	Free rule number as an integer <0-50>.

## Example 127 Sample output

```
Rule-Number   : 2
Vlan          : 0
Source:
Protocol      : UDP
Port         : 12345
IP           : 0.0.0.0
Mask        : 0.0.0.0
MAC         : n/a
Interface    : n/a
Destination:
Protocol      : UDP
Port         : 123
IP           : 0.0.0.0
Mask        : 0.0.0.0
```

## Associating with the BYOD server on a specified VLAN

Associate a BYOD server with a specific VLAN to redirect clients to the assigned URL page.

## Syntax

```
[no] vlan <VLAN-ID > [portal web-server < web-server-name>]
```

Term	Meaning
portal	Configure the BYOD redirect feature on the VLAN.
web-server	Specify the BYOD web-server.
ASCII-STR	BYOD web server name.
vlan	Add, delete, edit VLAN configuration or enter a VLAN context.
VLAN-ID	Enter a VLAN identifier or a VLAN name.

---

# 7 Support and other resources

## Intended audience

This guide is intended for network administrators with intermediate-to-advanced knowledge of computer networking.

## Related documentation

The following sources provide related information:

- *HP Basic Operation Guide*
- *HP Management and Configuration Guide*
- *HP Access Security Guide*
- *HP Multicast and Routing Guide*
- *HP IPv6 Configuration Guide*
- *Power over Ethernet (PoE/PoE+) Planning and Implementation Guide*
- *HP Switch Software Feature Index — Extended*
- *HP Switch 620 Redundant and External Power Supply Installation and Getting Started Guide*
- *HP Switch 630 Redundant and/or External Power Supply Installation and Getting Started Guide*

You can also find the documents referenced in this guide on the Manuals page of the HP Business Support Center website: <http://www.hp.com/support/manuals>.

## Contacting HP

### HP technical support

For worldwide technical support information, see the HP support website:

<http://www.hp.com/networking/support>.

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

### Subscription service

HP recommends that you register your product at the Subscriber's choice for business website:

<http://www.hp.com/go/e-updates>

After registering, you will receive email notifications of product enhancements, new driver versions, firmware updates and other product resources.

## Related information

### HP websites

- HP: <http://www.hp.com>
- HP Networking: <http://www.hp.com/go/networking>
- HP Partner Locator: [http://www.hp.com/service\\_locator](http://www.hp.com/service_locator)
- HP Software Downloads: <http://www.hp.com/support/downloads>

## Typographical conventions

**Table 31 Document conventions**

Convention	Element
Blue text: Table 26	Cross-reference links and email addresses
Blue underlined text: <a href="http://www.hp.com">http://www.hp.com</a>	Website addresses
<b>Bold</b> text	<ul style="list-style-type: none"><li>• Keys that are pressed</li><li>• Text entered into a GUI element, such as a box</li><li>• GUI elements that are clicked or selected, such as menu□ and list items, buttons, tabs and check boxes</li></ul>
<i>Italic</i> text	Text emphasis
Monospace text	<ul style="list-style-type: none"><li>• File and directory names</li><li>• System output</li><li>• Code</li><li>• Commands, their arguments and argument values</li></ul>
Monospace italic text	<ul style="list-style-type: none"><li>• Code variables</li><li>• Command variables</li></ul>
Monospace bold text	Emphasized monospace text
. . . .	Indication that example continues

## HP customer support services

If you are having trouble with your switch, Hewlett-Packard offers support 24 hours a day, seven days a week through the use of a number of automated electronic services. See the Customer Support/Warranty booklet that came with your switch for information on how to use these services to get technical support. HP provides up-to-date customer care, support and warranty information at <http://www.hp.com/networking/support>.

Your HP authorized network reseller can also provide assistance, both with services that they offer and with services offered by HP.

## Before calling support

Before calling your networking dealer or HP Support, to make the support process most efficient, first retrieve the following information:

Information item	Information location
<ul style="list-style-type: none"><li>• Product identification, including mini-GBICs</li></ul>	The front of the switch and on labels on the mini-GBICs
<ul style="list-style-type: none"><li>• Details about the switch's status including the software (OS) version, a copy of the switch configuration, a copy of the switch Event Log and a copy of the switch status and counters information</li></ul>	Switch console: show tech command
<ul style="list-style-type: none"><li>• Copy of your network topology map, including network addresses assigned to the relevant devices</li></ul>	Your network records

# Index

## Symbols

- 802.1p priority
  - classifier, 197
  - determining outbound port queue, 180
  - mapped to DSCP codepoint, 188
    - DSCP policy table, 183
  - packet marking, 182, 195, 197, 208
    - global QoS, 150, 156, 162, 167, 168, 172
  - priority, 197
- 802.1Q VLAN tagging, 65

## A

- alias
  - with show VLAN commands, 23

## B

- Bootp
  - gateway ignored, 53
- BYOD-redirect
  - Associate VLAN, 226
  - configuration
    - distribution switch, 222
- Configuring
  - creating a BYOD server, 219
- configuring, 219
  - associating a BYOD server, 219
  - client authentication on edge switch, 222
  - creating a BYOD ACL rule, 220
- Features
  - VLAN, 216
- features, 216
  - interoperability, 218
- implementing
  - BYOD-redirect configuration, 221
  - BYOD-redirect configuration example, 221
- interoperability, 218
  - Comware, 219
- Introduction, 216
- restrictions, 219
- show commands, 224
- show portal free-rule, 225
- show portal redirect statistics, 225
- show portal server, 224
- SNMP interactions, 218
- VLAN
  - SNMP, 218

## C

- classifier
  - benefits, 148, 207
  - class configuration, 177
    - match criteria, 194, 208
  - class configuration match criteria, 193
  - override of global QoS configuration, 198, 207, 208
  - packet marking

- rate limiting, 208
- policy configuration
  - applying to an interface, 180
  - marking packets, 193
- QoS configuration, 184, 207, 209
- resource usage, 186
- restrictions, 180
  - QoS rate limiting, 181
- classifier-based
  - classifier, 178
  - match criteria
    - classifier-based QoS, 194
- classifier-based QoS
  - classifier, 182, 208, 209
  - marking packets, 197
    - DSCP codepoint, 197
- Command Syntax
  - show
    - logging, 214
- Command syntax**
  - disable layer3 vlan**
    - <vid>, 32
  - gvrp**, 65
  - interface <port-list>**
    - <tagged|untagged|...>, 35
    - unknown-vlans <learn | ...>, 65
  - ip-recv-mac-address**, 10
    - <mac-address> [interval], 43
  - loop-protect <port-list>**
    - receiver-action, 119
  - management-vlan**, 10
    - [<vlan-id>|<vlan-name>], 38
  - max-vlans**, 10, 24
  - no vlan**
    - <vid>, 29
  - portal free-rule, 220
  - portal web-server, 219
  - primary-vlan**, 10
    - vid, 25
  - qos**
    - <udp/tcp-port> ipv4/ipv6/ip-all ... range..dscp, 153
    - device-priority <ipv4...> codepoint, 160
    - device-priority <ipv4...> priority, 156
    - dscp-map <codepoint> priority, 159
    - dscp-map <codepoint> priority ..., 152
    - type-of-service, 165
    - type-of-service diff-services, 163, 165, 167
    - type-of-service diff-services <codepoint>, 165
    - type-of-service ip-precedence, 162
    - udp/tcp-port ipv4/ipv6 ip-all, 150
  - show**
    - gvrp, 62, 63
    - ip-recv-mac-address, 10, 43
    - loop-protect <port-list>, 120
    - qos <global-classifier>, 150
    - qos <qos> device-priority, 160

- qos tcp-udp-port-priority, 151, 153
- qos type-of-service, 165
- spanning-tree, 112
- spanning-tree <port-list>, 113
- spanning-tree <port-list> config, 115
- spanning-tree <port-list> detail, 104, 114
- spanning-tree <port-list> instance, 114
- spanning-tree bpdu-protection, 102
- spanning-tree config, 115
- spanning-tree config instance, 116
- spanning-tree debug-counters, 127
- spanning-tree debug-counters instance, 128, 129
- spanning-tree detail, 113
- spanning-tree instance ...detail, 114
- spanning-tree instance *ist*, 114
- spanning-tree mst-config, 117
- spanning-tree pending instance, 118
- spanning-tree root-history, 125
- vlan ports, 19
- vlangs, 10, 18, 66
- vlangs <vlan-id>, 20
- vlangs custom, 10, 22
- vlangs ports, 10
- show portal free-rule, 226
- show portal tcp-cheat statistics, 225
- show portal web-server, 225
- spanning-tree**, 107
  - 802.ID legacy path, 95
  - bpdu-protection-timeout <timeout>, 103
  - clear-debug-counters, 93
  - config-name, 93
  - config-revision, 93
  - force-version, 94
  - hello-time, 95, 98
  - instance ... path-cost auto, 105
  - instance <...> vlan <vid>, 110
  - instance <..> vlan <vid>, 104
  - instance <port-list> priority ..., 105
  - legacy-mode, 95
  - legacy-path-cost, 95
  - max-hops, 95
  - maximum age, 96
  - mode mstp, 93
  - MSTP forward delay, 94
  - pending, 96
  - pending <config>, 108
  - priority, 96
  - show <port> configuration, 101
  - SNMP traps, 97
  - trap, 97
  - trap errant-bpdu, 101
- spanning-tree** <port-list>
  - ... | all ] bpdu-filter, 100
  - admin-edge-port, 97
  - auto-edge-port, 98
  - bpdu-protection, 101
  - bpdu-protection-timeout, 101
  - loop-guard, 121
  - mcheck, 98
  - path-cost, 98
  - point-to-point-mac, 99
  - priority, 99, 106
  - pvst-filter, 103
  - pvst-protection, 103
  - root-guard, 99
  - tcn-guard, 100
- static-vlan**, 10
  - <vlan-id>, 30
- vlan**
  - <vid>, 30
  - <vid> qos priority, 42
  - vid, 10, 28
- vlan portal web-server, 220, 226
- vlan vid**
  - qos priority, 10
- vlangs**
  - show, 18
- configuration
  - factory default, 16, 17

## D

- default class
  - classifier, 179
  - configuration, 179
- default settings
  - ip-recv-mac-address interval, 43
  - management VLAN, 38
  - MSTP, 92
  - VLAN name, 18, 28
  - VLAN qos priority, 42
- default VLAN, 17
- delete
  - Multiple VLANs, 35
- DHCP
  - gateway ignored, 53
- DSCP codepoint, 202
  - classifier, 197
  - defined, 204
  - in ToS byte, 205
  - in Traffic Class byte, 205
  - mapped to 802.1p priority, 188
  - match criteria, classifier, 178
  - packet marking, 182, 196, 197, 208
    - global QoS, 151, 169, 173
  - Quality of Service, 196

## G

- gateway
  - manual config priority, 53
- global QoS
  - marking packets, 196
  - priority, 195
- guaranteed minimum bandwidth
  - with 8 QoS queues, 212
- GVRP
  - advertisement, 68, 71
  - advertisement responses, 69
  - benefits, 67

- converting dynamic to static, 69
- converting to static VLAN, 67
- dynamic VLAN and reboots, 68
- dynamic VLANs always tagged, 61
- IP addressing, 69
- learn, 66
- maximum VLANs, , 68
- non-GVRP aware device, 68
- operating notes, 68
- port control options, 72
- port-leave from dynamic, 72
- recommended tagging, 72
- tagged, dynamic VLAN, 61
- unknown VLAN, 72
- unknown VLAN options, 69
- VLAN behavior, 17
- VLAN, dynamic adds, 26
- with QoS, 203

GVRP block

- disabling, 66

## H

- honored in downstream devices
  - downstream device (QoS)
    - effect of 802.1p priority settings, 196

## I

IP

- gateway, 53

IP address

- match criteria classifier, 177

IP precedence bits, 178, 202

- defined, 204
- in ToS byte, 205
- in Traffic Class byte, 205

IPv4

- ARP VLAN requirement, 46
- protocol VLAN ARP requirement, 28

IPv6

- management VLAN , 55
- match criteria
  - classifier, 148, 177, 193, 194, 207
  - global QoS, 199, 202
- match criteria in classifier-based QoS, 157

## J

- jumbo frames
  - GVRP, 65

## L

Layer-3 protocol

- match criteria classifier, 178

loop protection

- MSTP
  - trap transmit interval, 119
- used for unmanaged devices, 134

## M

MAC address

- duplicate, 48
- per switch, 48
- per VLAN, 48
- same for all VLANs, 57
- single forwarding database, 48

marking packets

- 802.1p priority, 195
- classifier-based QoS, 197
- global QoS, 195
- rate limit, 197

match criteria

- classifier, 178
- classifier-based QoS, 177, 208
- global QoS, 202
  - IP address, 201
  - source port, 203
  - VLAN ID, 203
- IP precedence bits, 202
- Type of Service, 202

match criteria, global QoS

- DSCP codepoint, 202

mesh

- management VLAN, 55

message

- VLAN already exists, 31

MSTP see spanning tree (MSTP)

Multiple Instance Spanning Tree see spanning tree (MSTP)

## O

outbound port queue (QoS)

- determined by 802.1p priority, 147
- determined by DSCP policy, 147

## P

packet marking

- 802.1p priority, 182, 197, 208
- classifier-based QoS, 197
- DSCP codepoint, 182, 196, 197, 208
- global QoS, 195
- precedence bits, 182, 197, 208
- rate limit, 197

path costs

- configuring 802.1D STP values, 86

policy configuration

- marking packets, 178, 208

port

- monitoring, 58

port trunk

- VLAN, 58

precedence bits

- classifier, 197

precedence bits (QoS)

- packet marking, 182, 197, 208

priority

- number of queues, 190
- queues per port, 190

priority (QoS)

- IP address source and destination match, 156
- match criteria, 194



VID, effect of eliminating, 203

protocol

ARP requirement, 46

limit, 17

PVST

enabling, disabling , 103

manually re-enabling port , 103

show configured ports, 104

## Q

QoS policy, 178

Quality of Service

802.1p priority, 196

basic operation, 192

classifier-based configuration, 207

classifier-based override of global configuration, 198, 208

determining outbound port queue, 206

DSCP policy table, 189

feature description, 147

global configuration, 149

GVRP not supported, 203

in VLAN- and untagged-VLAN environments, 197

inbound traffic on network edge, 148

marking packets, 195

match criteria, 177, 178, 200, 201, 202, 203

maximum remarking entries, 199

no-override in DSCP policy table, 209

number of priority queues, 190

outbound VLAN traffic, 148

packet classification, 194

global configuration, 149

packet marking, 197, 208

802.1p priority, 195

classifier-based QoS, 197

global QoS, 150, 195

IP precedence, 197

QoS policy

classifier-based, 193

globally-configured, 192

queue configuration, 190

resource usage

show resources command, 155

restrictions, 209

global QoS, 198

show resources command, 209

viewing configuration, 150

## R

rate limit

classifier, 197

rate limiting

classifier-based QoS, 181, 197, 208

restrictions, 181

resources used

show resources command, 209

restrictions

classifier-based QoS, 180

QoS configuration, 209

routing

non-routable VLAN, 55

## S

source port

classifier, 203

spanning tree

MSTP

active path, 138

BPDU, 92, 95, 98, 138

broadcast storm, 133

change VLAN instance, 92

CIST, 95

CIST root, 98

compatibility with RSTP or STP, 142

compatibility mode, 94

configuration steps, 91

CST, 139

CST status, 113

debug counters, 127, 128, 129

default settings, 92

display statistics and configuration, 112

enabling a region, 107

enabling, disabling, 107

fault tolerance, 137

forward delay, 94

forwarding state, 97

general operation, 134

hop count, 95

in a switch mesh, 137

instance, 92, 104

instance mapping, 110

instance status, 114

instance types, 139

instance VLAN, 109

IST instance, 104, 110

IST port priority, 106

loop protection, 143

MIB support, 112

MSTI port priority, 106

operating rules, 140

operation, 136

pending configuration, 118

pending option, 94

per-port parameters, 97

planning for, 91

port states, 138

preconfigure VLANs in instance, 109

priority, 92

priority resolution, 105

priority, device, 96

PVST filtering , 143

PVST protection , 143

redundant links, 138

region, 134

region configuration, 117

region name, 93

regions, 137

root history, 125

- root switch instance, 105
  - routed traffic, 138
  - saving current configuration, 111
  - troubleshooting, 124
  - trunked link, 115, 139
  - viewing global configuration, 115
  - VLAN instance assigned, 105
  - VLAN membership, 139
  - VLAN range option, 111
  - with legacy STP and RSTP, 139
  - with VLANs, 139
- SNMP
  - traps, 97
  - VLAN effect on, 57
- subnet address, 11
- SVLAN
  - delete multiple, 35
- T**
- TCP/UDP
  - match criteria, 200
  - match criteria classifier, 178
  - packet classification, 200
- Traffic Class byte
  - compared to IPv4 ToS byte, 205
- Type of Service
  - determining outbound port queue, 206
  - match criteria
    - global QoS, 202
  - ToS byte compared to IPv6 Traffic Class byte, 205
- U**
- untagged
  - VLAN, 17
- V**
- VLAN
  - already exists message, 31
  - broadcast domain, 13
  - configuration, 17
  - convert dynamic to static, 30
  - customizing output, 22
  - dedicated management, 53
  - default VLAN, 53
  - default VLAN name change, 53
  - default VLAN VID, 53
  - delete multiple, 35
  - deleting, 28, 29, 46
  - deleting with member ports, 28
  - duplicate MAC address, 48
  - dynamic, 11, 13, 17, 30
  - effect on spanning tree, 57
  - external protocol router, 58
  - gateway IP, 53
  - GVRP, auto, 17
  - heartbeat packets, 59
  - IP interface relationship, 57
  - layer-2 broadcast domain, 13
  - layer-3 broadcast domain, 13
  - limit, 16, 17
  - MAC address verification, 43
  - match criteria classifier, 177, 178
  - maximum capacity, 34
  - missing VLAN, 34
  - multiple forwarding database, 48
  - multiple VLANs on port, 51
  - non-routable, 55
  - number allowed, including dynamic, 26
  - port configuration, 52
  - port monitoring, 58
  - port trunk, 58
  - port-based, 13
  - primary, 25, 27, 53
  - primary VLAN not allowed, 25
  - primary with DHCP, 45
  - protocol, 13, 15, 19, 20, 28, 46, 51, 57
    - capacity per VLAN, 46
    - example, 52
    - forbid, 31
    - IPv4 routing, 12
    - non-routable, 12, 49
    - primary VLAN not allowed, 53
    - router, external, 13
    - routing, 13
    - tagged member, 12
    - tagging, 13
    - traffic separation, 11
    - untagged packet forwarding, 46
  - protocol compared to port-based, 12
  - protocol routing, 58
  - restrictions, 58
  - routing between VLANs, 13
  - show VLAN ports detail, 19
  - single forwarding database, 48
  - static, 11, 17, 53
  - status, 18
  - subnet, 13
  - tagged, 17
  - tagging, 49, 51
  - untagged, 34
  - untagged legacy VLAN, 43
  - untagged operation, 47
  - untagged,, 17
  - VID, 50, 51
  - voice, 14, 18, 19, 20, 46
  - voice configuration, 29
- Voice VLANs, 56
- VoIP
  - operating rules, 46
- W**
- write memory
  - converting dynamic to static VLAN, 68