This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

Publication Number
5991-6197
August 2006

Applicable Products
ProCurve Switch 2900-24G (J9049A)
ProCurve Switch 2900-48G (J9050A)

Trademark Credits
Microsoft, Windows, and Microsoft Windows NT are US registered trademarks of Microsoft Corporation.

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

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

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.

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

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

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types of Static VLANs Available in the Switch</td>
<td>2-5</td>
</tr>
<tr>
<td>Port-Based VLANs</td>
<td>2-5</td>
</tr>
<tr>
<td>Protocol-Based VLANs</td>
<td>2-5</td>
</tr>
<tr>
<td>Designated VLANs</td>
<td>2-5</td>
</tr>
<tr>
<td>Terminology</td>
<td>2-6</td>
</tr>
<tr>
<td>Static VLAN Operation</td>
<td>2-7</td>
</tr>
<tr>
<td>VLAN Environments</td>
<td>2-8</td>
</tr>
<tr>
<td>VLAN Operation</td>
<td>2-9</td>
</tr>
<tr>
<td>Routing Options for VLANs</td>
<td>2-10</td>
</tr>
<tr>
<td>Overlapping (Tagged) VLANs</td>
<td>2-10</td>
</tr>
<tr>
<td>Per-Port Static VLAN Configuration Options</td>
<td>2-12</td>
</tr>
<tr>
<td>VLAN Operating Rules</td>
<td>2-14</td>
</tr>
<tr>
<td>General Steps for Using VLANs</td>
<td>2-17</td>
</tr>
<tr>
<td>Multiple VLAN Considerations</td>
<td>2-18</td>
</tr>
<tr>
<td>Single Forwarding Database Operation</td>
<td>2-19</td>
</tr>
<tr>
<td>Example of an Unsupported Configuration and How To Correct It</td>
<td>2-20</td>
</tr>
<tr>
<td>Multiple Forwarding Database Operation</td>
<td>2-21</td>
</tr>
<tr>
<td>Configuring VLANs</td>
<td>2-22</td>
</tr>
<tr>
<td>Menu: Configuring Port-Based VLAN Parameters</td>
<td>2-22</td>
</tr>
<tr>
<td>To Change VLAN Support Settings</td>
<td>2-23</td>
</tr>
<tr>
<td>Adding or Editing VLAN Names</td>
<td>2-24</td>
</tr>
<tr>
<td>Adding or Changing a VLAN Port Assignment</td>
<td>2-26</td>
</tr>
<tr>
<td>CLI: Configuring Port-Based and Protocol-Based VLAN Parameters</td>
<td>2-28</td>
</tr>
<tr>
<td>Web: Viewing and Configuring VLAN Parameters</td>
<td>2-39</td>
</tr>
<tr>
<td>802.1Q VLAN Tagging</td>
<td>2-40</td>
</tr>
<tr>
<td>Special VLAN Types</td>
<td>2-45</td>
</tr>
<tr>
<td>VLAN Support and the Default VLAN</td>
<td>2-45</td>
</tr>
<tr>
<td>The Primary VLAN</td>
<td>2-45</td>
</tr>
<tr>
<td>The Secure Management VLAN</td>
<td>2-46</td>
</tr>
<tr>
<td>Preparation</td>
<td>2-48</td>
</tr>
<tr>
<td>Configuration</td>
<td>2-49</td>
</tr>
<tr>
<td>Deleting the Management VLAN</td>
<td>2-50</td>
</tr>
<tr>
<td>Operating Notes for Management VLANs</td>
<td>2-50</td>
</tr>
<tr>
<td>Voice VLANs</td>
<td>2-51</td>
</tr>
</tbody>
</table>
Operating Rules for Voice VLANs .............................................. 2-51
Components of Voice VLAN Operation ..................................... 2-52
Voice VLAN QoS Prioritizing (Optional) ................................. 2-52
Voice VLAN Access Security .................................................. 2-53

Effect of VLANs on Other Switch Features ...................... 2-53
  Spanning Tree Operation with VLANs ................................. 2-53
  IP Interfaces ......................................................................... 2-54
  VLAN MAC Address .......................................................... 2-54
  Port Trunks .......................................................................... 2-54
  Port Monitoring .................................................................... 2-54
  Jumbo Packet Support ......................................................... 2-55

VLAN Restrictions ................................................................. 2-55

3 GVRP

Contents .................................................................................. 3-1
Overview ................................................................................. 3-2
Introduction ........................................................................... 3-3
General Operation ................................................................. 3-4
Per-Port Options for Handling GVRP “Unknown VLANs” ........ 3-7
Per-Port Options for Dynamic VLAN Advertising and Joining . 3-9
GVRP and VLAN Access Control ............................................ 3-11
  Advertisements and Dynamic Joins ....................................... 3-11
  Port-Leave From a Dynamic VLAN ...................................... 3-11
Planning for GVRP Operation ............................................... 3-12
Configuring GVRP On a Switch ............................................. 3-13
  Menu: Viewing and Configuring GVRP ................................ 3-13
  CLI: Viewing and Configuring GVRP ................................... 3-14
  Web: Viewing and Configuring GVRP .................................. 3-18
GVRP Operating Notes ........................................................... 3-18
### 4 Multiple Instance Spanning-Tree Operation

**Contents**

- Overview .............................................. 4-2
- 802.1s Multiple Spanning Tree Protocol (MSTP) ................. 4-5
  - MSTP Structure .................................... 4-6
  - How MSTP Operates ................................ 4-9
    - MST Regions ..................................... 4-9
    - Regions, Legacy STP and RSTP Switches, and the
      Common Spanning Tree (CST) .................... 4-11
    - MSTP Operation with 802.1Q VLANs ........... 4-11
  - Terminology ...................................... 4-13
  - Operating Rules .................................. 4-14
  - Transitioning from STP or RSTP to MSTP .............. 4-15
  - Tips for Planning an MSTP Application ............. 4-16
  - Steps for Configuring MSTP ...................... 4-17
  - Configuring MSTP Operation Mode and Global Parameters .................. 4-19
  - Configuring Basic Port Connectivity Parameters ........ 4-22
  - Configuring MST Instance Parameters ................ 4-25
  - Configuring MST Instance Per-Port Parameters ........ 4-28
  - Enabling or Disabling Spanning Tree Operation .... 4-31
  - Enabling an Entire MST Region at Once or
    Exchanging One Region Configuration for Another ........ 4-31
  - Displaying MSTP Statistics and Configuration .......... 4-33
    - Displaying MSTP Statistics ..................... 4-33
    - Displaying the MSTP Configuration .......... 4-36
  - Operating Notes .................................. 4-40
  - Troubleshooting .................................. 4-40

### 5 Quality of Service (QoS): Managing Bandwidth More Effectively

**Contents**

- Introduction ......................................... 5-3
- Terminology ........................................ 5-6
- Overview ........................................... 5-7
- Classifiers for Prioritizing Outbound Packets ........... 5-10
Packet Classifiers and Evaluation Order .................................. 5-10

**Preparation for Configuring QoS** ........................................... 5-11
Preserving 802.1p Priority .................................................. 5-11
Steps for Configuring QoS on the Switch ................................ 5-11

**Using QoS Classifiers To Configure**
**Quality of Service for Outbound Traffic** ................................. 5-13
Viewing the QoS Configuration .............................................. 5-14
No Override ........................................................................... 5-14
QoS UDP/TCP Priority .......................................................... 5-15
  Assigning an 802.1p Priority Based on TCP or UDP Port Number ........................................ 5-16
  Assigning a DSCP Policy Based on TCP or UDP Port Number .............................................. 5-18
QoS IP-Device Priority .......................................................... 5-21
  Assigning a Priority Based on IP Address ........................................ 5-22
  Assigning a DSCP Policy Based on IP Address .............................................. 5-23
QoS IP Type-of-Service (ToS) Policy and Priority ......................... 5-27
  Assigning an 802.1p Priority to IPv4 Packets on the Basis of the ToS Precedence Bits .......... 5-28
  Assigning an 802.1p Priority to IPv4 Packets on the Basis of Incoming DSCP ..................... 5-29
  Assigning a DSCP Policy on the Basis of the DSCP in IPv4 Packets Received from Upstream Devices .............................................. 5-33
  Details of QoS IP Type-of-Service ........................................... 5-36
Assigning a Priority Based on Layer-3 Protocol .......................... 5-39
QoS VLAN-ID (VID) Priority .................................................. 5-41
  Assigning a Priority Based on VLAN-ID ........................................ 5-41
  Assigning a DSCP Policy Based on VLAN-ID (VID) .............................................. 5-43
QoS Source-Port Priority ........................................................ 5-47
  Assigning a Priority Based on Source-Port ........................................ 5-47
  Assigning a DSCP Policy Based on the Source-Port .............................................. 5-49
Differentiated Services Codepoint (DSCP) Mapping ..................... 5-52
  Default Priority Settings for Selected Codepoints .............................................. 5-54
  Quickly Listing Non-Default Codepoint Settings .............................................. 5-54
Note On Changing a Priority Setting ........................................ 5-55
  Example of Changing the Priority Setting on a Policy ........................................... 5-56
IP Multicast (IGMP) Interaction with QoS ........................................ 5-59
QoS Messages in the CLI ................................................................. 5-60
QoS Operating Notes and Restrictions ........................................... 5-61

6 Stack Management

Contents ......................................................................................... 6-1

Introduction to Stack Management .................................................. 6-3
  Stacking Support on ProCurve Switches ..................................... 6-3
  Components of ProCurve Stack Management ......................... 6-5
  General Stacking Operation ......................................................... 6-5
  Operating Rules for Stacking ....................................................... 6-7
    General Rules ........................................................................ 6-7
    Specific Rules ....................................................................... 6-8

Configuring Stack Management ....................................................... 6-9
  Overview of Configuring and Bringing Up a Stack ..................... 6-9
    General Steps for Creating a Stack ......................................... 6-11
  Using the Menu Interface To View Stack Status
    and Configure Stacking ......................................................... 6-13
      Using the Menu Interface To View and Configure a
        Commander Switch ......................................................... 6-13
      Using the Menu To Manage a Candidate Switch ................. 6-15
  Using the Commander To Manage The Stack ............................ 6-17
    Using the Commander To Access Member Switches for
      Configuration Changes and Monitoring Traffic .................. 6-23
      Converting a Commander or Member to a Member
        of Another Stack ............................................................. 6-25
  Monitoring Stack Status ............................................................... 6-25
    Using the CLI To View Stack Status and Configure Stacking ... 6-30
      Using the CLI To View Stack Status ................................... 6-32
      Using the CLI To Configure a Commander Switch ............. 6-34
      Adding to a Stack or Moving Switches Between Stacks ....... 6-36
      Using the CLI To Remove a Member from a Stack ............. 6-41
      Using the CLI To Access Member Switches for Configuration
        Changes and Traffic Monitoring ...................................... 6-43
    SNMP Community Operation in a Stack ................................. 6-44
Using the CLI To Disable or Re-Enable Stacking ............... 6-45
Transmission Interval .................................................. 6-45
Stacking Operation with Multiple VLANs Configured ........ 6-45
Status Messages ......................................................... 6-46

Index ................................................................. 1
About Your Switch Manual Set

The switch manual set includes the following documentation:

- *Read Me First*—a printed guide shipped with your switch. Provides software update information, product notes, and other information.

- *Installation and Getting Started Guide*—a printed guide shipped with your switch. This guide explains how to prepare for and perform the physical installation and connect the switch to your network.

- *Management and Configuration Guide*—a PDF on the ProCurve Networking Web Site that describes how to configure, manage, and monitor basic switch operation.

- *Advanced Traffic Management Guide*—a PDF on the ProCurve Networking Web Site that explains how to configure traffic management features such as VLANs, MSTP, and QoS.

- *Multicast and Routing Guide*—a PDF on the ProCurve Networking Web Site that explains how to configure IGMP and IP routing.

- *Access Security Guide*—a PDF on the ProCurve Networking Web Site that explains how to configure access security features and user authentication on the switch.

- *Release Notes*—posted on the ProCurve Networking Web Site to provide information on software updates. The release notes describe new features, fixes, and enhancements that become available between revisions of the main product guide.

**Note**

For the latest version of all ProCurve switch documentation, including Release Notes covering recently added features, visit the ProCurve Networking web site at [www.procurve.com](http://www.procurve.com), click on [Technical support](http://www.procurve.com), and then click on [Product manuals (all)](http://www.procurve.com).
Feature Index

For the manual set supporting your switch model, the following feature index indicates which manual to consult for information on a given software feature.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1Q VLAN Tagging</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.1p Priority</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.1X Port-Based Authentication</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>ACLs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>AAA Authentication</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Authorized IP Managers</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Authorized Manager List (web, telnet, TFTP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto MDIX Configuration</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>BOOTP</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Config File</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Console Access</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Copy Command</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>CoS (Class of Service)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Debug</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>DHCP Configuration</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>DHCP Option 82</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>DHCP/Bootp Operation</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Diagnostic Tools</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Downloading Software</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Eavesdrop Protection</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Event Log</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Factory Default Settings</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow Control (802.3x)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Management</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Transfers</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friendly Port Names</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guaranteed Minimum Bandwidth (GMB)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GVRP</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Identity-Driven Management (IDM)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface Access (Telnet, Console/Serial, Web)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Addressing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Routing</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jumbos Support</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LACP</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LLDP</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LLDP-Med</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Address Management</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Lockdown</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Lockout</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC-based Authentication</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC authentication RADIUS support</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management VLAN</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Monitoring and Analysis</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast Filtering</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple Configuration Files</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Management Applications (SNMP)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------</td>
<td>----------------------------</td>
<td>-----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>OpenView Device Management</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passwords and Password Clear Protection</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCM</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Configuration</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Monitoring</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Security</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Status</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Trunking (LACP)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port-Based Access Control</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port-Based Priority (802.1Q)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol Filters</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol VLANS</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality of Service (QoS)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS Authentication and Accounting</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS-Based Configuration</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMON 1,2,3,9</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routing</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routing - IP Static</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Copy</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SFLOW</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SFTP</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMPv3</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Downloads (SCP/SFTP, TFPT, Xmodem)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source-Port Filters</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanning Tree (MSTP)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSHv2 (Secure Shell) Encryption</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------</td>
<td>------------------------------</td>
<td>-----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>SSL (Secure Socket Layer)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stack Management</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Syslog</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Information</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>TACACS+ Authentication</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Telnet Access</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>TFTP</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Time Protocols (TimeP, SNTP)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Traffic/Security Filters</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>UDP Forwarder</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Virus Throttling (connection-rate filtering)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VLANs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VLAN Mirroring (1 static VLAN)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Voice VLAN</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Web Authentication RADIUS Support</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Web-based Authentication</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Web UI</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Xmodem</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Getting Started

Contents

Introduction .......................................................... 1-2
Conventions .......................................................... 1-2
  Feature Descriptions by Model ................................ 1-2
  Command Syntax Statements .................................... 1-3
  Command Prompts ................................................ 1-3
  Screen Simulations ................................................. 1-4
  Port Identity Examples .......................................... 1-4
  Configuration and Operation Examples ....................... 1-4
  Keys ................................................................. 1-4
Sources for More Information ..................................... 1-5
  Getting Documentation From the Web ....................... 1-7
  Online Help ......................................................... 1-7
Need Only a Quick Start? ........................................... 1-8
  IP Addressing ........................................................ 1-8
To Set Up and Install the Switch in Your Network ........... 1-9
  Physical Installation ............................................. 1-9
Introduction

This Management and Configuration Guide is intended for use with the following switches:

- ProCurve Switch 2900-24G
- ProCurve Switch 2900-48G

This guide describes how to use the command line interface (CLI), Menu interface, and web browser to configure, manage, monitor, and troubleshoot switch operation.

For an overview of other product documentation for the above switches, refer to “Product Documentation” on page xi.


Caution

Use only the supported genuine ProCurve mini-GBICs with your switch. Non-ProCurve mini-GBICs are not supported.

Conventions

This guide uses the following conventions for command syntax and displayed information.

Feature Descriptions by Model

In cases where a software feature is not available in all of the switch models covered by this guide, the section heading specifically indicates which product or product series offer the feature.

For example, (the switch is highlighted here in bold italics):

“QoS Pass-Through Mode on the 2900 Switches”.
Command Syntax Statements

Syntax: ip default-gateway < ip-addr >

Syntax: show interfaces [port-list]

■ Vertical bars ( | ) separate alternative, mutually exclusive elements.
■ Square brackets ([ ]) indicate optional elements.
■ Braces (< >) enclose required elements.
■ Braces within square brackets ([<>]) indicate a required element within an optional choice.
■ Boldface indicates use of a CLI command, part of a CLI command syntax, or other displayed element in general text. For example:
  “Use the copy tftp command to download the key from a TFTP server.”
■ Italics indicate variables for which you must supply a value when executing the command. For example, in this command syntax, you must provide one or more port numbers:
  Syntax: aaa port-access authenticator < port-list >

Command Prompts

In the default configuration, your switch displays a CLI prompt similar to the following:

ProCurve 2900-24G#

To simplify recognition, this guide uses ProCurve to represent command prompts for all models. For example:

ProCurve#

(You can use the hostname command to change the text in the CLI prompt.)
Screen Simulations

**Displayed Text.** Figures containing simulated screen text and command output look like this:

```
ProCurve> show version
Image stamp: /sw/code/build/info
August 1, 2006 13:43:13
T.11.01
139

ProCurve>
```

**Figure 1-1. Example of a Figure Showing a Simulated Screen**

In some cases, brief command-output sequences appear without figure identification. For example:

```
ProCurve(config)# clear public-key
ProCurve(config)# show ip client-public-key
show_client_public_key: cannot stat keyfile
```

**Port Identity Examples**

This guide describes software applicable to both chassis-based and stackable ProCurve switches. Where port identities are needed in an example, this guide uses the chassis-based port identity system, such as “A1, “B3-B5”, “C7”, etc. However, unless otherwise noted, such examples apply equally to the stackable switches, which typically use only numbers, such as “1”, “3-5”, “15”, etc. for port identities.

**Configuration and Operation Examples**

Unless otherwise noted, examples using a particular switch model apply to all switch models covered by this guide.

**Keys**

Simulations of actual keys use a bold, sans-serif typeface with square brackets. For example, the Tab key appears as [Tab] and the “Y” key appears as [Y].
Sources for More Information

For additional information about switch operation and features not covered in this guide, consult the following sources:

- **Feature Index**—For information on which product manual to consult for a given software feature, refer to the “Feature Index” on page xii.

**Note**

For the latest version of all ProCurve switch documentation, including Release Notes covering recently added features, visit the ProCurve Networking Web Site at [www.procurve.com](http://www.procurve.com), click on **Technical support**, and then click on **Product Manuals (all)**.

- **Software Release Notes**—Release notes are posted on the ProCurve Networking web site and provide information on new software updates:
  - new features and how to configure and use them
  - software management, including downloading software to the switch
  - software fixes addressed in current and previous releases

To view and download a copy of the latest software release notes for your switch, refer to “Getting Documentation From the Web” on page 1-7.

- **Product Notes and Software Update Information**—The printed *Read Me First* shipped with your switch provides software update information, product notes, and other information. For the latest version, refer to “Getting Documentation From the Web” on page 1-7.

- **Installation and Getting Started Guide**—Use the Installation and Getting Started Guide shipped with your switch to prepare for and perform the physical installation. This guide also steps you through connecting the switch to your network and assigning IP addressing, as well as describing the LED indications for correct operation and trouble analysis. You can download a copy from the ProCurve Networking web site. (See “Getting Documentation From the Web” on page 1-7.)
Getting Started
Sources for More Information

- **Management and Configuration Guide**—Use this guide for information on topics such as:
  - various interfaces available on the switch
  - memory and configuration operation
  - interface access
  - IP addressing
  - time protocols
  - port configuration, trunking, and traffic control
  - SNMP, LLDP, and other network management topics
  - file transfers, switch monitoring, troubleshooting, and MAC address management

- **Advanced Traffic Management Guide**—Use this guide for information on topics such as:
  - VLANs: Static port-based and protocol VLANs, and dynamic GVRP VLANs
  - spanning-Tree: 802.1s (MSTP)
  - Quality-of-Service (QoS)

- **Multicast and Routing Guide**—Use this guide for information topics such as:
  - IGMP
  - IP routing

- **Access Security Guide**—Use this guide for information on topics such as:
  - Local username and password security
  - Web-Based and MAC-based authentication
  - RADIUS and TACACS+ authentication
  - SSH (Secure Shell) and SSL (Secure Socket Layer) operation
  - 802.1X access control
  - Port security operation with MAC-based control
  - Authorized IP Manager security
  - Key Management System (KMS)
Getting Documentation From the Web

1. Go to the ProCurve Networking Web Site at www.procurve.com
2. Click on Technical support.
3. Click on Product manuals.
4. Click on the product for which you want to view or download a manual.

Online Help

If you need information on specific parameters in the menu interface, refer to the online help provided in the interface. For example:

```
Default Gateway : 10.35.204.1
Default TTL     : 64
IP Address       : 10.35.204.104
Subnet Mask      : 255.255.240.0
Actions-> Cancel   Edit   Save Help

Display help information.
Use arrow keys to change action selection and <Enter> to execute action.
```

If you need information on a specific command in the CLI, type the command name followed by “help”. For example:
Need Only a Quick Start?

IP Addressing

If you just want to give the switch an IP address so that it can communicate on your network, or if you are not using VLANs, ProCurve recommends that you use the Switch Setup screen to quickly configure IP addressing. To do so, do one of the following:

- Enter `setup` at the CLI Manager level prompt.
  
  `Procurve# setup`

- In the Main Menu of the Menu interface, select

  **8. Run Setup**

For more on using the Switch Setup screen, see the *Installation and Getting Started Guide* you received with the switch.
To Set Up and Install the Switch in Your Network

Physical Installation

Use the ProCurve Installation and Getting Started Guide (shipped with the switch) for the following:

■ Notes, cautions, and warnings related to installing and using the switch and its related modules
■ Instructions for physically installing the switch in your network
■ Quickly assigning an IP address and subnet mask, set a Manager password, and (optionally) configure other basic features.
■ Interpreting LED behavior.

For the latest version of the Installation and Getting Started Guide for your switch, refer to “Getting Documentation From the Web” on page 1-7.
Getting Started
To Set Up and Install the Switch in Your Network

—This page is intentionally unused—
Static Virtual LANs (VLANs)

Contents

Overview ................................................................. 2-3

Introduction .............................................................. 2-4
  General VLAN Operation ............................................ 2-4
  Types of Static VLANs Available in the Switch ................ 2-5
    Port-Based VLANs ................................................ 2-5
    Protocol-Based VLANs ......................................... 2-5
    Designated VLANs .............................................. 2-5

Terminology .............................................................. 2-6

Static VLAN Operation .................................................. 2-7
  VLAN Environments ................................................. 2-8
  VLAN Operation ..................................................... 2-9
  Routing Options for VLANs ....................................... 2-10
  Overlapping (Tagged) VLANs ..................................... 2-10
  Per-Port Static VLAN Configuration Options .................. 2-12

VLAN Operating Rules .................................................. 2-14

General Steps for Using VLANs ...................................... 2-17

Multiple VLAN Considerations ...................................... 2-18
  Single Forwarding Database Operation ........................ 2-19
  Example of an Unsupported Configuration and How To Correct It 2-20
  Multiple Forwarding Database Operation ...................... 2-21

Configuring VLANs ...................................................... 2-22
  Menu: Configuring Port-Based VLAN Parameters .............. 2-22
    To Change VLAN Support Settings ............................ 2-23
    Adding or Editing VLAN Names ............................... 2-24
    Adding or Changing a VLAN Port Assignment .............. 2-26
  CLI: Configuring Port-Based and Protocol-Based VLAN Parameters 2-28
### Contents

- **Web: Viewing and Configuring VLAN Parameters** ........................................ 2-39

#### 802.1Q VLAN Tagging

- **Special VLAN Types** .................................................................................. 2-40
  - 802.1Q VLAN Tagging .................................................................................. 2-41
- **VLAN Support and the Default VLAN** ...................................................... 2-45
- **The Primary VLAN** .................................................................................... 2-45
- **The Secure Management VLAN** ............................................................... 2-46
  - Preparation .................................................................................................. 2-48
  - Configuration ............................................................................................... 2-49
- **Deleting the Management VLAN** ............................................................. 2-50
- **Operating Notes for Management VLANs** ............................................. 2-50
- **Voice VLANs** ............................................................................................ 2-51
  - Operating Rules for Voice VLANs ............................................................... 2-51
  - Components of Voice VLAN Operation ...................................................... 2-52
  - Voice VLAN QoS Prioritizing (Optional) ..................................................... 2-52
  - Voice VLAN Access Security ..................................................................... 2-53

#### Effect of VLANs on Other Switch Features

- Spanning Tree Operation with VLANs ......................................................... 2-53
- IP Interfaces .................................................................................................. 2-54
- VLAN MAC Address ..................................................................................... 2-54
- Port Trunks .................................................................................................... 2-54
- Port Monitoring ............................................................................................. 2-54
- Jumbo Packet Support .................................................................................. 2-55

#### VLAN Restrictions

- ....................................................................................................................... 2-55
Overview

This chapter describes how to configure and use static, port-based and protocol-based VLANs on the switches covered in this guide.

For general information on how to use the switch’s built-in interfaces, refer to these chapters in the Management and Configuration Guide for your switch:

- Chapter 3, “Using the Menu Interface”
- Chapter 4, “Using the Command Line Interface (CLI)”
- Chapter 5, “Using the Web Browser Interface”
- Chapter 6, “Switch Memory and Configuration”
Introduction

VLAN Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>view existing VLANs</td>
<td>n/a</td>
<td>page 2-23 thru 2-28</td>
<td>page 2-29</td>
<td>page 2-39</td>
</tr>
<tr>
<td>configuring static VLANs</td>
<td>default VLAN with VID = 1</td>
<td>page 2-23 thru 2-28</td>
<td>page 2-28</td>
<td>page 2-39</td>
</tr>
</tbody>
</table>

VLANs enable you to group users by logical function instead of physical location. This helps to control bandwidth usage within your network by allowing you to group high-bandwidth users on low-traffic segments and to organize users from different LAN segments according to their need for common resources and/or their use of individual protocols. You can also improve traffic control at the edge of your network by separating traffic of different protocol types. VLANs can also enhance your network security by creating separate subnets to help control in-band access to specific network resources.

General VLAN Operation

A VLAN is comprised of multiple ports operating as members of the same subnet (broadcast domain). Ports on multiple devices can belong to the same VLAN, and 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 in the same VLAN on another device.)

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, refer to chapter 3, “GVRP”.)

By default, the switches covered in this guide are 802.1Q VLAN-enabled and allow up to 256 static and dynamic VLANs. (The default static VLAN setting is 8). 802.1Q compatibility enables you to assign each switch port to multiple VLANs, if needed.
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 comprised 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. Refer to table 2-1 on page 2-7.

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 only, they can provide improved security and availability for management traffic.

- **The Default VLAN:** This port-based VLAN is always present in the switch and, in the default configuration, includes all ports as members (page 2-45).
- **The 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, you can designate another, port-based, non-default VLAN, as the Primary VLAN (page 2-45).
- **The Secure Management VLAN:** This optional, port-based VLAN establishes an isolated network for managing the ProCurve switches that support this feature. Access to this VLAN and to the switch’s management functions are available only through ports configured as members (page 2-46).
- **Voice VLANs:** This optional, port-based VLAN type enables you to separate, prioritize, and authenticate voice traffic moving through your network, and to avoid the possibility of broadcast storms affecting VoIP (Voice-over-IP) operation (page 2-51).
In a multiple-VLAN environment that includes some 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 some cabling and VLAN restrictions. For more on this topic, refer to “Multiple VLAN Considerations” on page 2-18.

Terminology

**Dynamic VLAN:** An 802.1Q VLAN membership temporarily created on a port linked to another device, where both devices are running GVRP. (See also Static VLAN.) For more information, refer to chapter 3, “GVRP”.

**Static VLAN:** A port-based or protocol-based VLAN configured in switch memory. (See also Dynamic VLAN.)

**Tagged Packet:** A packet that carries an IEEE 802.1Q VLAN ID (VID), which is a two-byte extension that precedes the source MAC address field of an ethernet frame. A VLAN tag is layer 2 data and is transparent to higher layers.

**Tagged VLAN:** A VLAN that complies with the 802.1Q standard, including priority settings, and allows a port to join multiple VLANs. (See also Untagged VLAN.)

**Untagged Packet:** A packet that does not carry an IEEE 802.1Q VLAN ID (VID).

**Untagged VLAN:** A VLAN that does not use or forward 802.1Q VLAN tagging, including priority settings. A port can be a member of only one untagged VLAN of a given type (port-based and the various protocol-based types). (See also Tagged VLAN.)

**VID:** The acronym for a VLAN Identification Number. Each 802.1Q-compliant VLAN must have its own unique VID number, and that VLAN must be given the same VID in every device in which it is configured.
Static VLAN Operation

A group of networked ports assigned to a VLAN form a broadcast domain that is separate from other VLANs that may be configured on the switch. On a given switch, packets arebridged 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 2-1. Comparative Operation of Port-Based and Protocol-Based VLANs

<table>
<thead>
<tr>
<th></th>
<th>Port-Based VLANs</th>
<th>Protocol-Based VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Addressing</strong></td>
<td>Usually configured with at least one unique IP address. You can create a port-based VLAN without an IP address. However, this limits the switch features available to ports on that VLAN. (Refer to “How IP Addressing Affects Switch Operation” in the chapter on configuring IP addressing in the Management and Configuration Guide for the switch.) You can also use multiple IP addresses to create multiple subnets within the same VLAN. (For more on this topic, refer to the chapter on configuring IP addressing in the Management and Configuration Guide for the switch.)</td>
<td>You can configure IP addresses on all protocol VLANs. However, IP addressing is used only on IPv4 and IPv6 protocol VLANs.</td>
</tr>
<tr>
<td><strong>Untagged VLAN Membership</strong></td>
<td>A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged.</td>
<td>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 protocol VLANs. 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 VLANs. A port’s untagged VLAN memberships can include up to four different protocol types. This means that a port can be an untagged member of one of the following: • Four single-protocol VLANs • Two protocol VLANs where one VLAN includes a single protocol and the other includes up to three protocols • One protocol VLAN where the VLAN includes four protocols</td>
</tr>
</tbody>
</table>
### VLAN Environments

You can configure different VLAN types in any combination. Note that the default VLAN will always be present. (For more on the default VLAN, refer to “VLAN Support and the Default VLAN” on page 2-45.)

**Table 2-2. VLAN Environments**

<table>
<thead>
<tr>
<th>VLAN Environment</th>
<th>Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>The default VLAN (port-based; VID of “1”) Only</td>
<td>In the default VLAN configuration, all ports belong to VLAN 1 as untagged members.</td>
</tr>
<tr>
<td></td>
<td>VLAN 1 is a port-based VLAN, for IPv4 traffic.</td>
</tr>
<tr>
<td>Multiple VLAN Environment</td>
<td>In addition to the default VLAN, the configuration can include one or more port-based VLANs and one or more protocol VLANs. (The switches covered in this guide allow up to 256 VLANs of all types.) Using VLAN tagging, ports can belong to multiple VLANs of all types.</td>
</tr>
<tr>
<td></td>
<td>Enabling routing on the switch enables the switch to 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 protocol(s).</td>
</tr>
</tbody>
</table>
VLAN Operation

The Default VLAN. In figure 2-1, all ports belong to the default VLAN, and devices connected to these ports are in the same broadcast domain. Except for an IP address and subnet, no configuration steps are needed.

![Figure 2-1. Example of a Switch in the Default VLAN Configuration](image1)

Multiple Port-Based VLANs. In figure 2-2, routing within the switch is disabled (the default). This means that 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 VLAN, is also present, but not shown. (The default VLAN cannot be deleted from the switch. However, ports assigned to other VLANs can be removed from the default VLAN, if desired.) If internal (IP) routing is enabled on the switch, then the external router is not needed for traffic to move between port-based VLANs.

![Figure 2-2. Example of Multiple VLANs on the Switch](image2)
Protocol VLAN Environment. Figure 2-2 can also be applied to a protocol VLAN environment. 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. However, routable, non-IP traffic always requires an external router.

Routing Options for VLANs

<table>
<thead>
<tr>
<th>Table 2-3. Options for Routing Between VLAN Types in the Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-Based</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>Port-Based</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>IPX</td>
</tr>
<tr>
<td>IPv4</td>
</tr>
<tr>
<td>IPv6</td>
</tr>
<tr>
<td>ARP</td>
</tr>
<tr>
<td>AppleTalk</td>
</tr>
<tr>
<td>SNA²</td>
</tr>
<tr>
<td>NETbeui²</td>
</tr>
</tbody>
</table>

¹Requires an external router to route between VLANs.
²Not a routable protocol type. End stations intended to receive traffic in these protocols must be attached to the same physical network.

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

Introducing Tagged VLAN Technology into Networks Running Legacy (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. This means that on the 802.1Q-compliant device, separate ports (configured as untagged) must be used to connect separate VLANs to non-802.1Q devices.
Static Virtual LANs (VLANs)

Static VLAN Operation

The legacy (non-802.1Q compliant) switch requires a separate link for each VLAN.

VLAN tagging enables the Link to carry Red VLAN and Blue VLAN Traffic.

Non-802.1Q Switch

Red VLAN

Red Server

ProCurve Switch

ProCurve Switch

Blue Server

Blue VLAN

Red VLAN

Red VLAN

ProCurve Switch

Blue VLAN

Blue VLAN

Red VLAN

Blue VLAN

Figure 2-5. Example of Tagged and Untagged VLAN Technology in the Same Network

For more information on VLANs, refer to:

- “Overview of Using VLANs” (page 2-45)
- “Menu: Configuring VLAN Parameters (page 2-22)
- “CLI: Configuring VLAN Parameters” (page 2-22)
- “Web: Viewing and Configuring VLAN Parameters” (page 2-39)
- “VLAN Tagging Information” (page 2-40)
- “Effect of VLANs on Other Switch Features” (page 2-53)
- “VLAN Restrictions” (page 2-55)

Per-Port Static VLAN Configuration Options

The following figure and table show the options you can use to assign individual ports to a static VLAN. Note that GVRP, if configured, affects these options and VLAN behavior on the switch. The display below shows the per-port VLAN configuration options. Table 2-4 briefly describes these options.
Example of Per-Port VLAN Configuration with GVRP Disabled (the default)

<table>
<thead>
<tr>
<th>Port</th>
<th>DEFAULT_VLAN</th>
<th>VLAN-22</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Untagged</td>
<td>Forbid</td>
</tr>
<tr>
<td>A2</td>
<td>No</td>
<td>Tagged</td>
</tr>
<tr>
<td>A3</td>
<td>No</td>
<td>Tagged</td>
</tr>
<tr>
<td>A4</td>
<td>Forbid</td>
<td>Tagged</td>
</tr>
<tr>
<td>A5</td>
<td>Untagged</td>
<td>No</td>
</tr>
</tbody>
</table>

Example of Per-Port VLAN Configuration with GVRP Enabled

<table>
<thead>
<tr>
<th>Port</th>
<th>DEFAULT_VLAN</th>
<th>VLAN-22</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Untagged</td>
<td>Forbid</td>
</tr>
<tr>
<td>A2</td>
<td>Auto</td>
<td>Tagged</td>
</tr>
<tr>
<td>A3</td>
<td>Auto</td>
<td>Tagged</td>
</tr>
<tr>
<td>A4</td>
<td>Forbid</td>
<td>Tagged</td>
</tr>
<tr>
<td>A5</td>
<td>Untagged</td>
<td>Auto</td>
</tr>
</tbody>
</table>

Enabling GVRP causes “No” to display as “Auto”.

Figure 2-6. Comparing Per-Port VLAN Options With and Without GVRP

Table 2-4. Per-Port VLAN Configuration Options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Effect on Port Participation in Designated VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tagged</td>
<td>Allows the port to join multiple VLANs.</td>
</tr>
<tr>
<td>Untagged</td>
<td>Allows VLAN connection to a device that is configured for an untagged VLAN instead of a tagged VLAN. A port can be an untagged member of only one port-based VLAN. A port can also be an untagged member of only one protocol-based VLAN for any given protocol type. 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.</td>
</tr>
<tr>
<td>No</td>
<td><strong>No</strong>: Appears when the switch is not GVRP-enabled; prevents the port from joining that VLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>- or - Auto</strong>: Appears when GVRP is enabled on the switch; allows the port to dynamically join any advertised VLAN that has the same VID</td>
</tr>
<tr>
<td>Forbid</td>
<td>Prevents the port from joining the VLAN, even if GVRP is enabled on the switch.</td>
</tr>
</tbody>
</table>
VLAN Operating Rules

- **DHCP/Bootp:** If you are using DHCP/Bootp to acquire the switch’s configuration, packet time-to-live, and TimeP information, you must designate the VLAN on which DHCP is configured for this purpose as the Primary VLAN. (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:** A protocol-based VLAN can include up to four protocol types. In protocol VLANs using the IPv4 protocol, ARP must be one of these protocol types (to support normal IP network operation). Otherwise, IP traffic on the VLAN is disabled. If you configure an IPv4 protocol VLAN that does not already include the ARP VLAN protocol, the switch displays this message:

  ```
  ProCurve(config)# vlan 97 protocol ipv4
  Caution: IPv4 assigned without ARP undeliverable IP packets.
  ```

- **Deleting Static VLANs:** On the switches covered in this guide you can delete a VLAN regardless of whether there are currently any ports belonging to that VLAN. (The ports are moved to the default VLAN.)
- **Adding or Deleting VLANs**: Changing the number of VLANs supported on the switch requires a reboot. (From the CLI, you must perform a `write memory` command before rebooting.) Other VLAN configuration changes are dynamic.

- **Inbound Tagged Packets**: 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. 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.

- **Untagged Packet Forwarding**: 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. That is, when a port receives an incoming, untagged packet, it processes the packet according to the following ordered criteria:
  
  a. If the port has no untagged VLAN memberships, the switch drops the packet.
  
  b. If the port has an untagged VLAN membership in a protocol VLAN that matches the protocol type of the incoming packet, then the switch forwards the packet on that VLAN.
  
  c. 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.
Static Virtual LANs (VLANs)
VLAN Operating Rules

Port “X” receives an inbound, untagged Packet.

Is the port an untagged member of any VLANs?

No
Drop the packet.

Yes

Does the packet’s protocol match the protocol of an untagged VLAN membership on the port?

Yes
Forward the packet on that protocol VLAN.

No

Is the port a member of an untagged, port-based VLAN?

No
Drop the packet.

Yes
Forward the packet on the port-based VLAN.

Figure 2-7. 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.)

![Flowchart of Tagged VLAN Operation]

**Figure 2-8. Tagged VLAN Operation**

See also “Multiple VLAN Considerations” on page 2-18.

---

### General Steps for Using VLANs

1. Plan your VLAN strategy and create a map of the logical topology that will result from configuring VLANs. Include consideration for the interaction between VLANs and other features such as Spanning Tree Protocol, port trunking, and IGMP. (Refer to “Effect of VLANs on Other Switch Features” on page 2-53.) If you plan on using dynamic VLANs, include the port configuration planning necessary to support this feature. (Refer to chapter 3, “GVRP”.)

   By default, VLAN support is enabled and the switch is configured for eight VLANs.

2. Configure at least one VLAN in addition to the default VLAN.
3. Assign the desired switch ports to the new VLAN(s).  

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. Refer to the chapter titled “Configuring IP Addressing”, in the Management and Configuration Guide for your switch.

---

### 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 means they allow 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. Table 2-5 illustrates the functional difference between the two database types.

#### Table 2-5. Example of Forwarding Database Content

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Destination VLAN ID</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0004ea-84d9f4</td>
<td>1</td>
<td>A5</td>
</tr>
<tr>
<td>0004ea-84d9f4</td>
<td>22</td>
<td>A12</td>
</tr>
<tr>
<td>0004ea-84d9f4</td>
<td>44</td>
<td>A20</td>
</tr>
<tr>
<td>0060b0-880a81</td>
<td>33</td>
<td>A20</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Destination VLAN ID</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0004ea-84d9f4</td>
<td>100</td>
<td>A9</td>
</tr>
<tr>
<td>0060b0-880af9</td>
<td>105</td>
<td>A10</td>
</tr>
<tr>
<td>0060b0-880a81</td>
<td>107</td>
<td>A17</td>
</tr>
</tbody>
</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.

Table 2-6 lists the database structure of current ProCurve switch models.
Table 2-6. Forwarding Database Structure for Managed ProCurve Switches

<table>
<thead>
<tr>
<th>Multiple Forwarding Databases*</th>
<th>Single Forwarding Database*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Series 6400cl switches</td>
<td>Series 2810 switches</td>
</tr>
<tr>
<td>Switch 6200yl</td>
<td>Series 2800 switches</td>
</tr>
<tr>
<td>Switch 6108</td>
<td>Series 2600 switches</td>
</tr>
<tr>
<td>Series 5400zl switches</td>
<td>Switch 1600M/2400M/2424M</td>
</tr>
<tr>
<td>Series 5300xl switches</td>
<td>Switch 4000M/8000M</td>
</tr>
<tr>
<td>Series 4200vl switches</td>
<td>Series 2500 switches</td>
</tr>
<tr>
<td>Series 4100gl switches</td>
<td>Switch 800T</td>
</tr>
<tr>
<td>Series 3500yl switches</td>
<td>Switch 2000</td>
</tr>
<tr>
<td>Series 3400cl switches</td>
<td></td>
</tr>
<tr>
<td>Switch 2900</td>
<td></td>
</tr>
</tbody>
</table>

*To determine whether other vendors’ devices use single-forwarding or multiple-forwarding database architectures, refer to the documentation provided for those devices.

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 (refer to table 2-6, above) 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. If (1) you connect the two types of switches through multiple ports or trunks belonging to different VLANs, and (2) enable routing on the switch having the multiple forwarding database; then, on the switch having the single forwarding database, the port and VLAN record it maintains for the connected multiple-forwarding-database switch can frequently change. This causes poor performance and the appearance of an intermittent or broken connection.
Example of an Unsupported Configuration and How To Correct It

The Problem. In figure 2-9, 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):

![Diagram of network setup](image)

Figure 2-9. Example of Invalid Configuration for Single-Forwarding to Multiple-Forwarding Database Devices in a Multiple VLAN Environment

In figure 2-9, PC “A” sends an IP packet to PC “B”.

1. The packet enters VLAN 1 in the Switch 8000 with the 2900 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 2900 switch. The 2900 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 2900 switch on VLAN 2 (port “B1”), the 8000M’s single forwarding database records the 2900 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 2900 switch’s MAC address in the destination field. However, this time the Switch 8000M’s single forwarding database indicates that the 2900 switch is on port B1 (VLAN 2), and the 8000M drops the packet instead of forwarding it.

3. Later, the 2900 switch transmits a packet to the 8000M through the VLAN 1 link, and the 8000M updates its address table to indicate that the 2900 switch is on port A1 (VLAN 1) instead of port B1 (VLAN 2). Thus, the 8000M’s information on the location of the 2900 switch changes over
time. For this reason, the 8000M discards some packets directed through it for the 2900 switch, resulting in poor performance and the appearance of an intermittent or broken link.

**The Solution.** To avoid the preceding problem, use only one cable or port trunk between the single-forwarding and multiple-forwarding database devices, and configure the link with multiple, tagged VLANs.

![Diagram of network connection](image)

**Figure 2-10. Example of a Solution for Single-Forwarding to Multiple-Forwarding Database Devices in a Multiple VLAN Environment**

Now, the 8000M forwarding database always lists the Switch 2900 MAC address on port A1, and the 8000M will send traffic to either VLAN on the Switch 2900.

To increase the network bandwidth of the connection between the devices, you can use a trunk of multiple physical links rather than a single physical link.

**Multiple Forwarding Database Operation**

If you want to connect one of the switches covered by this guide to another switch that has a multiple forwarding database, you can use either 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 2-5.) 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:

![Diagram of a topology with two switches, VLAN 1 and VLAN 2, connected through a 4108gl Switch and a Switch 2900. Both switches have multiple forwarding databases.]

Figure 2-11. Example of a Valid Topology for Devices Having Multiple Forwarding Databases in a Multiple VLAN Environment

### Configuring VLANs

#### Menu: Configuring Port-Based VLAN Parameters

The Menu interface enables you to configure and view port-based VLANs.

**Note**

The Menu interface configures and displays only port-based VLANs. The CLI configures and displays port-based *and* protocol-based VLANs (page 2-28).

In the factory default state, support is enabled for up to eight VLANs. (You can reconfigure the switch to support up to 256 VLANs.) Also, in the default configuration, all ports on the switch belong to the default VLAN and are in the same broadcast/multicast domain. (The default VLAN is also the default Primary VLAN—refer to “The Primary VLAN” on page 2-45.) In addition to the default VLAN, you can configure additional static VLANs by adding new VLAN names and VIDs, and then assigning one or more ports to each VLAN. (The maximum of 256 VLANs includes the default VLAN, all additional static VLANs you configure, and any dynamic VLANs the switch creates if you enable GVRP—page 3-1.) Note that each port can be assigned to multiple VLANs by using VLAN tagging. (See “802.1Q VLAN Tagging” on page 2-40.)
To Change VLAN Support Settings

This section describes:
- Changing the maximum number of VLANs to support
- Changing the Primary VLAN selection (See “Changing the Primary VLAN” on page 2-34.)
- Enabling or disabling dynamic VLANs (Refer to chapter 3, “GVRP”.)

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

   You will then see the following screen:

   ![The Default VLAN Support Screen](image)

   **Figure 2-12. The Default VLAN Support Screen**

2. Press [E] (for **Edit**), then do one or more of the following:
   - To change the maximum number of VLANs, type the new number (1 - 256 allowed; default 8).
   - 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. (Note that 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, refer to chapter 3, “GVRP”.)

   **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**, you will see an asterisk next to the **VLAN Support** option (see below).

![Figure 2-13. VLAN Menu Screen Indicating the Need To Reboot the Switch](image)

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

4. Press [0] to return to the Main Menu.

Adding or Editing VLAN Names

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 2-14:
2. Press [A] (for Add). You will then be prompted for a new VLAN name and VLAN ID:

```
802.1Q VLAN ID : 1
Name : _
```

3. Type in 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.)

Remember that 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. Refer to chapter 3, “GVRP”.)

4. Press [1] to move the cursor to the Name line and type the VLAN name (up to 12 characters, with no spaces) of a new VLAN that you want to add, then press [Enter].

(Avoid these characters in VLAN names: 2, #, $, ^, &, *, (, and ).)

5. Press [S] (for Save). You will then see the VLAN Names screen with the new VLAN listed.
Configuring VLANs

Example of a New VLAN and ID

Figure 2-15. Example of VLAN Names Screen with a New VLAN Added

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

Remember that you can add VLANs until you reach the number specified in the Maximum VLANs to support field on the VLAN Support screen (see figure 2-12 on page 2-23). This includes any VLANs added dynamically due to GVRP operation.

7. Return to the VLAN Menu to assign ports to the new VLAN(s) as described in the next section, “Adding or Changing a VLAN Port Assignment”.

Adding or Changing a VLAN Port Assignment

Use this procedure to add ports to a VLAN or to change the VLAN assignment(s) for any port. (Ports not specifically assigned to a VLAN are automatically in the default VLAN.)

1. From the Main Menu select:
   2. Switch Configuration
   8. VLAN Menu …
   3. VLAN Port Assignment

You will then see a VLAN Port Assignment screen similar to the following:

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 CLI command `show vlans [VID | ports <port-list>]` to list data on VLANs having VIDs numbered sequentially higher than the first 32.
A port can be assigned to several VLANs, but only one of those assignments can be “Untagged”.

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”.

Figure 2-16. Example of the Port-Based VLAN Port Assignment Screen in the Menu Interface

2. To change a port’s VLAN assignment(s):
   b. Use the arrow keys to select a VLAN assignment you want to change.
   c. Press the Space bar to make your assignment selection (No, Tagged, Untagged, or Forbid).

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. See “Per-Port Options for Dynamic VLAN Advertising and Joining” on page 3-9.

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 example, if you want ports A4 and A5 to belong to both DEFAULT_VLAN and VLAN-22, and ports A6 and A7 to belong only to VLAN-22, you would use the settings in figure page 2-28. (This example assumes the default GVRP setting—disabled—and that you do not plan to enable GVRP later.)
Static Virtual LANs (VLANs)
Configuring VLANs

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.

Figure 2-17. Example of Port-Based VLAN Assignments for Specific Ports

For information on VLAN tags ("Untagged" and "Tagged"), refer to "802.1Q VLAN Tagging" on page 2-40.

d. If you are finished assigning ports to VLANs, press [Enter] and then [S] (for Save) to activate the changes you've made and to return to the Configuration menu. (The console then returns to the VLAN menu.)

3. Return to the Main menu.

CLI: Configuring Port-Based and Protocol-Based VLAN Parameters

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. For more on this topic, refer to “The Primary VLAN” on page 2-45.) 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 256 VLANs, including the default VLAN and any dynamic VLANs the switch creates if you enable GVRP. Refer to chapter 3, “GVRP”.) Note that each port can be assigned to multiple VLANs by using VLAN tagging. (See “802.1Q VLAN Tagging” on page 2-40.)
### VLAN Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlans</td>
<td>below</td>
</tr>
<tr>
<td>show vlans &lt; vid &gt;</td>
<td>2-31</td>
</tr>
<tr>
<td>show vlans ports &lt;port-list&gt;</td>
<td>2-33</td>
</tr>
<tr>
<td>max-vlans &lt;1-256&gt;</td>
<td>2-33</td>
</tr>
<tr>
<td>primary-vlan &lt; vid &gt;</td>
<td>2-34</td>
</tr>
<tr>
<td>[no] vlan &lt; vid &gt;</td>
<td>2-35</td>
</tr>
<tr>
<td>auto &lt; port-list &gt;</td>
<td>2-37 (Available if GVRP enabled.)</td>
</tr>
<tr>
<td>forbid</td>
<td>2-37</td>
</tr>
<tr>
<td>name &lt; vlan-name &gt;</td>
<td>2-37</td>
</tr>
<tr>
<td>protocol &lt; protocol-list&gt;</td>
<td>2-35</td>
</tr>
<tr>
<td>tagged &lt; port-list &gt;</td>
<td>2-37</td>
</tr>
<tr>
<td>untagged &lt; port-list &gt;</td>
<td>2-37</td>
</tr>
<tr>
<td>voice</td>
<td>2-51</td>
</tr>
<tr>
<td>static-vlan &lt; vlan-id &gt;</td>
<td>2-37 (Available if GVRP enabled.)</td>
</tr>
</tbody>
</table>

### Displaying the Switch’s VLAN Configuration.

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. (Refer to chapter 3, “GVRP”.)

**Syntax:** show vlans

- **Maximum VLANs to support:** Shows the number of VLANs the switch can currently support. (Default: 8; Maximum: 256)

- **Primary VLAN:** Refer to “The Primary VLAN” on page 2-45.

- **Management VLAN:** Refer to “The Secure Management VLAN” on page 2-46.

- **802.1Q VLAN ID:** The VLAN identification number, or VID. Refer to “Terminology” on page 2-6.

- **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.
Static Virtual LANs (VLANs)
Configuring VLANs

Status:

**Port-Based:** Port-Based, static VLAN

**Protocol:** Protocol-Based, static VLAN

**Dynamic:** Port-Based, temporary VLAN learned through GVRP (Refer to chapter 3, “GVRP”.)

**Voice:** Indicates whether a (port-based) VLAN is configured as a voice VLAN. Refer to “Voice VLANs” on page 2-51.

**Jumbo:** Indicates whether a VLAN is configured for Jumbo packets. For more on jumbos, refer to the chapter titled “Port Traffic Controls” in the Management and Configuration Guide for your switch.

For example:

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

  802.1Q 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            | GVRP_33     | Dynamic No | No |
```

**Figure 2-18. Example of “Show VLAN” Listing (GVRP Enabled)**

**Displaying the VLAN Membership of One or More Ports.**

This command shows to which VLAN a port belongs.
**Syntax**  

`show vlan ports <port-list>`

**802.1Q VLAN ID:** The VLAN identification number, or VID. Refer to “Terminology” on page 2-6.

**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 (Refer to chapter 3, “GVRP”.)

**Voice:** Indicates whether a (port-based) VLAN is configured as a voice VLAN. Refer to “Voice VLANs” on page 2-51.

**Jumbo:** Indicates whether a VLAN is configured for Jumbo packets. For more on jumbos, refer to the chapter titled “Port Traffic Controls” in the Management and Configuration Guide for your switch.

For example:

```
ProCurve# show vlan ports a1-a33

Status and Counters - VLAN Information - for ports a1-a33

<table>
<thead>
<tr>
<th>802.1Q VLAN ID</th>
<th>Name</th>
<th>Status</th>
<th>Voice</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>Port-based</td>
<td>No</td>
</tr>
<tr>
<td>10</td>
<td>VLAN_10</td>
<td>Port-based</td>
<td>Yes</td>
</tr>
<tr>
<td>15</td>
<td>VLAN_15</td>
<td>Port-based</td>
<td>No</td>
</tr>
<tr>
<td>20</td>
<td>VLAN_20</td>
<td>Protocol</td>
<td>No</td>
</tr>
<tr>
<td>33</td>
<td>GVRP_33</td>
<td>Dynamic</td>
<td>No</td>
</tr>
</tbody>
</table>
```

**Figure 2-19. Example of “Show VLAN Ports” listing**

**Displaying the Configuration for a Particular VLAN.** This command uses the VID to identify and display the data for a specific static or dynamic VLAN.
Syntax: show vlans < vlan-id >

802.1Q VLAN ID: The VLAN identification number, or VID. Refer to “Terminology” on page 2-6.

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 (Refer to chapter 3, “GVRP” in this guide.)

Voice: Indicates whether a (port-based) VLAN is configured as a voice VLAN. Refer to “Voice VLANs” on page 2-51.

Jumbo: Indicates whether a VLAN is configured for Jumbo packets. For more on jumbos, refer to the chapter titled “Port Traffic Controls” in the Management and Configuration Guide 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. Refer to table 3-1 on page 3-8.

Status: Shows whether the port is participating in an active link.
Static Virtual LANs (VLANs)

Configuring VLANs

Figure 2-20. Example of “Show VLAN” for a Specific Static VLAN

```
ProCurve(config)# show vlans 22
Status and Counters - VLAN Information - Ports - VLAN 22
  802.1Q VLAN ID : 22
  Name : VLAN22
  Status : Port-based
  Voice : Yes
  Jumbo : No

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Unknown VLAN</th>
<th>Status</th>
</tr>
</thead>
</table>
| A12   | Un
tagged | Learn | Up     |
| A13   | Un
tagged | Learn | Up     |
| A14   | Un
tagged | Learn | Up     |
| A15   | Un
tagged | Learn | Down   |
| A16   | Un
tagged | Learn | Up     |
| A17   | Un
tagged | Learn | Up     |
| A18   | Un
tagged | Learn | Up     |
```

Figure 2-21. Example of “Show VLAN” for a Specific Dynamic VLAN

```
ProCurve# show vlans 33
Status and Counters - VLAN Information - Ports - VLAN 33
  802.1Q VLAN ID : 33
  Name : GVRP_33
  Status : Dynamic
  Voice : No
  Jumbo : No

<table>
<thead>
<tr>
<th>Port</th>
<th>DEFAULT</th>
<th>Unknown VLAN</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A6</td>
<td>Auto</td>
<td>Learn</td>
<td>Up</td>
</tr>
</tbody>
</table>
```

Changing the Number of VLANs Allowed on the Switch. In the default VLAN configuration, the switch allows a maximum of 8 VLANs. You can specify any value from 1 to 256.

**Syntax:** max-vlans < 1-256 >

Specifies the maximum number of VLANs to allow. (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.
For example, to reconfigure the switch to allow 10 VLANs:

```
ProCurve(config)# max-vlans 10
Command will take effect after saving configuration and reboot.
ProCurve(config)# write memory
ProCurve(config)# boot
Device will be rebooted, do you want to continue [y/n]? y
```

**Figure 2-22. Example of Command Sequence for Changing the Number of VLANs**

**Changing the Primary VLAN.** In the default VLAN configuration, the port-based default VLAN (*DEFAULT_VLAN*) is the Primary VLAN. However, you can reassign the Primary VLAN to any port-based, static VLAN on the switch. (For more on the Primary VLAN, refer to “The Primary VLAN” on page 2-45.) To identify the current Primary VLAN and list the available VLANs and their respective VIDs, use `show vlans`.

**Syntax:** `primary-vlan < vid | ascii-name-string >`

Reassigns the Primary VLAN function. Re-assignment must be to an existing, port-based, static VLAN. (The switch will not reassign the Primary VLAN function to a protocol VLAN.) If you re-assign the Primary VLAN to a non-default VLAN, you cannot later delete that VLAN from the switch until you again re-assign the Primary VLAN to another port-based, static VLAN.

For example, if you wanted to reassign the Primary VLAN to VLAN 22 and rename the VLAN with “22-Primary” and display the result:

```
ProCurve(config)# primary-vlan 22
ProCurve(config)# vlan 22 name 22-Primary
ProCurve(config)# show vlans
```

**Figure 2-23. Example of Reassigning Primary VLAN and Changing the VLAN Name**

<table>
<thead>
<tr>
<th>802.1Q VLAN ID</th>
<th>Name</th>
<th>Status</th>
<th>Voice</th>
<th>Jumbo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>Static</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>22</td>
<td>22-Primary</td>
<td>Static</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Creating a New Static VLAN (Port-Based or Protocol-Based)
Changing the VLAN Context Level. The `vlan <vid>` command operates in the global configuration context to either configure a static VLAN and/or take the CLI to the 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 you do not specify an optional name, the switch assigns a name in the default format: `VLANn` 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, then the `[no]` form removes the specified protocol from the VLAN. 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 also assign the ARP protocol option to the VLAN to provide IP address resolution. Otherwise, IP packets are not deliverable. A “Caution” message appears in the CLI if you configure IPv4 in 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 for creating a new static VLAN, specifies a non-default VLAN name. Also used to change the current name of an existing VLAN. (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 (‘...’ or “…”).

[ voice ]

Designates a VLAN for VoIP use. For more on this topic, refer to “Voice VLANs” on page 2-51.

For example, to create a new, port-based, static VLAN with a VID of 100:

```plaintext
ProCurve(config)# vlan 100
ProCurve(vlan-100)# show vlans
```

Status and Counters – VLAN Information

- Maximum VLANs to support: 8
- Primary VLAN: DEFAULT_VLAN
- Management VLAN:

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
<th>Port-based</th>
<th>Voice</th>
<th>Jumbo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>VLAN100</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

If this field is empty, a Secure Management VLAN is not configured in the switch. Refer to “The Secure Management VLAN” on page 2-46

Figure 2-24. Example of Creating a New, Port-Based, Static VLAN

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

```plaintext
ProCurve(vlan-100)# vlan default_vlan
ProCurve(vlan-1) _
```

Deleting a VLAN. If ports B1-B5 belong to both VLAN 2 and VLAN 3, and ports B6-B10 belong to VLAN 3 only, then 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.)

```plaintext
ProCurve(config)# no vlan 3
The following ports will be moved to the default VLAN: B6-B10
Do you want to continue? [y/n] y
ProCurve(config)#
```
Converting a Dynamic VLAN to a Static VLAN. Use this feature if you want to convert a dynamic, port-based VLAN membership to a static, port-based VLAN membership. This is necessary if you want to make the VLAN permanent on the switch.

**Syntax:** static-vlan < vlan-id >

Converts a dynamic, port-based VLAN membership to a 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 you need to use.) 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, refer to chapter 3, “GVRP”.)

For example, 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.

ProCurve(config)# static-vlan 125

**Configuring Static VLAN Per-Port Settings.** The `vlan < vlan-id >` command, used with the options listed below, changes the name of an existing static VLAN and changes the per-port VLAN membership settings.

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 typing the command option.

**Syntax:** [no] vlan < vid >

tagged < port-list >

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

untagged < port-list >

Configures the indicated port(s) as Untagged for the specified VLAN. The “no” version sets the port(s) to either No or (if GVRP is enabled) to Auto.
forbid < port-list>

*Used in port-based VLANs to configure < port-list> as “forbidden” to become a member of the specified VLAN, as well as other actions. Does not operate with protocol VLANs. The “no” version sets the port(s) to either No or (if GVRP is enabled) to Auto. Refer to chapter 3, “GVRP”, in this guide.*

auto < port-list>

*Available if GVRP is enabled on the switch. Returns the per-port settings for the specified VLAN to Auto operation. Note that 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, refer to chapter 3, “GVRP”, in this guide.)*

For example, suppose you have 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, you would use these commands:

```plaintext
ProCurve(config)# vlan 100 name Blue_Team
ProCurve(config)# vlan 100 tagged a1-a5
```

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

```plaintext
ProCurve(config)# vlan 100
ProCurve(vlan-100)# name Blue_Team
ProCurve(vlan-100)# tagged a1-a5
```

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

At the global config level, use:

```plaintext
ProCurve(config)# no vlan 100 tagged a1-a5
```

-  or -

At the VLAN 100 context level, use:

```plaintext
ProCurve(vlan-100)# no tagged a1-a5
```

**Note**

You cannot use these commands with dynamic VLANs. Attempting to do so results in the message “VLAN already exists.” and no change occurs.
Web: Viewing and Configuring VLAN Parameters

In the web browser interface you can do the following:
- Add VLANs
- Rename VLANs
- Remove VLANs
- Configure VLAN tagging mode per-port
- Configure GVRP mode
- Select a new Primary VLAN

To configure other static VLAN port parameters, you will need to use either the CLI or the menu interface (available by Telnet from the web browser interface).

1. Click on the Configuration tab.
2. Click on [Vlan Configuration].
3. Click on [Add/Remove VLANS].

For web-based Help on how to use the web browser interface screen, click on the [?] button provided on the web browser screen.
802.1Q VLAN Tagging

General Applications:

- 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. (If multiple, non-routable VLANs exist in the switch—such as NETbeui protocol VLANs—then they cannot receive traffic from each other under any circumstances.)

- 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.

For example, 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 2-25 shows this concept:
Static Virtual LANs (VLANs)

802.1Q VLAN Tagging

Figure 2-25. Example of Tagged and Untagged VLAN Port Assignments

- In switch X:
  - VLANs assigned to ports X1 - X6 can all 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 all 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 figure 2-25 (above), 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.
Each 802.1Q-compliant VLAN must have its own unique VID number, and that VLAN *must* be given the same VID in every device in which it is configured. That is, if the Red VLAN has a VID of 10 in switch X, then 10 must also be used for the Red VID in switch Y.

Figure 2-26. Example of VLAN ID Numbers Assigned in the VLAN Names Screen

VLAN tagging gives you several options:

- 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:
  
<table>
<thead>
<tr>
<th>Port-Based VLANs</th>
<th>Protocol VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged.</td>
<td>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.</td>
</tr>
<tr>
<td>A port can be a tagged member of any port-based VLAN. See above.</td>
<td>A port can be a tagged member of any protocol-based VLAN. See above.</td>
</tr>
</tbody>
</table>

*Note:* 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.
If all end nodes on a port comply with the 802.1Q standard and are configured to use the correct VID, then, 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, refer to the following under “VLAN Operating Rules” on pages 2-14 through 2-17:

- “Inbound Tagged Packets”
- “Untagged Packet Forwarding” and figure 2-7
- “Tagged Packet Forwarding” and figure 2-8

**Example.** 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.

![Network Diagram](image)

*Figure 2-27. Example of Networked 802.1Q-Compliant Devices with Multiple VLANs on Some Ports*
The VLANs assigned to ports X4 - X6, 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.

<table>
<thead>
<tr>
<th>Port</th>
<th>AT-1 VLAN</th>
<th>AT-2 VLAN</th>
<th>Red VLAN</th>
<th>Green VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>X1</td>
<td>Untagged</td>
<td>Tagged</td>
<td>No*</td>
<td>No*</td>
</tr>
<tr>
<td>X2</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
<td>Tagged</td>
</tr>
<tr>
<td>X3</td>
<td>No*</td>
<td>Untagged</td>
<td>Untagged</td>
<td>Tagged</td>
</tr>
<tr>
<td>X4</td>
<td>No*</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
</tr>
<tr>
<td>X5</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
<td>No*</td>
</tr>
<tr>
<td>X6</td>
<td>Untagged</td>
<td>No*</td>
<td>No*</td>
<td>No*</td>
</tr>
<tr>
<td>Y1</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
<td>Tagged</td>
</tr>
<tr>
<td>Y2</td>
<td>No*</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
</tr>
<tr>
<td>Y3</td>
<td>No*</td>
<td>Untagged</td>
<td>No*</td>
<td>No*</td>
</tr>
<tr>
<td>Y4</td>
<td>No*</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
</tr>
<tr>
<td>Y5</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
<td>No*</td>
</tr>
<tr>
<td>Y6</td>
<td>No</td>
<td>Untagged</td>
<td>Untagged</td>
<td>Tagged</td>
</tr>
</tbody>
</table>

**“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; that is, both ports configure the Red VLAN as “Untagged” and the Green VLAN as “Tagged”.

---

2-44
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 256 static and dynamic VLANs.) You can change the name of the default VLAN, but you cannot change the default VLAN’s VID (which is always “1”). Although you can remove all ports from the default VLAN (by placing them in another port-based VLAN), this VLAN is always present; that is, you cannot delete it from the switch.

For details on port VLAN settings, refer to “Configuring Static VLAN Per-Port Settings” on page 2-37

The Primary VLAN

Because 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, to provide more control in your network, 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 (except, as noted above, you cannot delete it or change its VID).

■ Any ports not specifically assigned to another VLAN will remain assigned to the Default VLAN, regardless of whether 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, refer to “Changing the Primary VLAN” on page 2-34.

### The Secure Management VLAN

Configuring a secure Management VLAN creates an isolated network for managing the ProCurve switches that support this feature. (As of August, 2006, the Secure Management VLAN feature is available on these ProCurve switches:

- Series 6400cl switches
- Switch 6200yl
- Switch 6108
- Series 5400zl switches
- Series 5300xl switches
- Series 4200vl switches
- Series 4100gl switches
- Series 3500yl switches
- Series 3400cl switches
- Switch 2900
- Series 2800 switches
- Series 2600 switches

If you configure a Secure Management VLAN, access to the VLAN and to the switch’s management functions (Menu, CLI, and web browser interface) 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 you want to have access to the Management VLAN, while at the same time 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.
Figure 2-28 illustrates use of the Management VLAN feature to support management access by a group of management workstations.

**Note**

The Secure Management VLAN must be a static, port-based VLAN with a manually configured IP address and subnet mask. (The switch does not allow the Management VLAN to acquire IP addressing through DHCP/Bootp.)

- Switches “A”, “B”, and “C” are connected by ports belonging to the management VLAN.
- Hub “X” is connected to a switch port that belongs to the management VLAN. As a result, the devices connected to Hub X are included in the management VLAN.
- Other devices connected to the switches through ports that are not in the management VLAN are excluded from management traffic.

**Figure 2-28. Example of Potential Security Breaches**

In figure 2-29, 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.
Preparation

1. Determine a VID and VLAN name suitable for your Management VLAN.

   (You must manually configure the IP addressing for the Management VLAN. The switch does not allow the Management VLAN to acquire an IP address through DHCP/Bootp.)

2. Plan your Management VLAN topology to use ProCurve switches that support this feature. (Refer to page 2-46.) The ports belonging to the Management VLAN should be only the following:
   
   - Ports to which you will connect authorized management stations (such as Port A7 in figure 2-29.)
   - Ports on one switch that you will use to extend the Management VLAN to ports on other ProCurve switches (such as ports A1 and B2 or B4 and C2 in figure 2-29 on page 2-48.).
Hubs dedicated to connecting management stations to the Management VLAN can also be included in the above topology. Note that any device connected to a hub in the Management VLAN will also have Management VLAN access.

3. Configure the Management VLAN on the selected switch ports.

4. Test the management VLAN from all of the management stations authorized to use the Management VLAN, including any SNMP-based network management stations. Ensure that you include testing any Management VLAN links between switches.

**Note**

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

**Configuration**

**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.

For example, suppose you have already configured a VLAN named **My_VLAN** with a VID of 100. Now you 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 ProCurve switch that supports the Management VLAN feature.

![Figure 2-30. Illustration of Configuration Example](image)

ProCurve(config)# management-vlan 100
ProCurve(config)# vlan 100 tagged a1
ProCurve(config)# vlan 100 tagged a2
Deleting the Management VLAN

You can disable the Secure Management feature without deleting the VLAN itself. For example, either of the following commands disables the Secure Management feature in the above example:

ProCurve(config)# no management-vlan 100
ProCurve(config)# no management-vlan my_vlan

Operating Notes for Management VLANs

- Use only a static, port-based VLAN for the Management VLAN.
- 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.
- During a web browser 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 close the browser session or rebooting the switch.

Note

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

- Enabling Spanning Tree where there are multiple links using separate VLANs, including the Management VLAN, between a pair of switches, Spanning Tree 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, refer to the appendix titled “Monitoring Resources” in the Management and Configuration Guide for your switch.

Voice VLANs
Configuring voice VLANs separates voice traffic from data traffic and shields your voice traffic from broadcast storms. This section describes how to configure the switch for voice VLAN operation.

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(s):** 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 QoS Prioritizing (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, then 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. To set a priority on a voice VLAN, use the following command:

**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.*
For example, if you configured a voice VLAN with a VID of 10, and wanted the highest priority for all traffic on this VLAN, you would execute the following command:

```
ProCurve(config) # vlan 10 qos priority 7
ProCurve(config) # write memory
```

Note that you also have the option of resetting the DSCP (DiffServ Code-point) on tagged voice VLAN traffic moving through the switch. For more on this and other QoS topics, refer to the chapter titled “Quality of Service (QoS): Managing Bandwidth More Effectively” in this guide.

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. Refer to 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.

Effect 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) or multiple instance on a per-VLAN basis. For single-instance operation, this means that if redundant physical links exist between the switch and another 802.1Q device, all but one link will be blocked, regardless of whether 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. Refer to chapter 4, “Multiple Instance Spanning-Tree Operation”. 
Note that Spanning Tree operates differently in different devices. For example, in the (obsolete, non-802.1Q) ProCurve Switch 2000 and the ProCurve Switch 800T, Spanning Tree operates on a per-VLAN basis, allowing redundant physical links as long as they are in separate VLANs.

**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 covered by this guide 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. Likewise, you can assign an IP address to the VLAN interface, and 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, refer to “Multiple VLAN Considerations” on page 2-18.

**Port Trunks**

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

**Port Monitoring**

If you designate a port on the switch for network monitoring, this port will appear in the Port VLAN 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, refer to 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, refer to 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 the same type, 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.

- Prior to deleting a static VLAN, you must 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, refer to “Creating a New Static VLAN (Port-Based or Protocol-Based) Changing the VLAN Context Level” on page 2-35.
—This page is intentionally unused—
Contents

Overview ................................................................. 3-2
Introduction ............................................................... 3-3
General Operation ......................................................... 3-4
Per-Port Options for Handling GVRP “Unknown VLANs” ........ 3-7
Per-Port Options for Dynamic VLAN Advertising and Joining ... 3-9
GVRP and VLAN Access Control ..................................... 3-11
  Advertisements and Dynamic Joins ............................. 3-11
  Port-Leave From a Dynamic VLAN ............................. 3-11
Planning for GVRP Operation .......................................... 3-12
Configuring GVRP On a Switch ...................................... 3-13
  Menu: Viewing and Configuring GVRP .......................... 3-13
  CLI: Viewing and Configuring GVRP ............................ 3-14
  Web: Viewing and Configuring GVRP ........................... 3-18
GVRP Operating Notes .................................................. 3-18
Overview

This chapter describes GVRP and how to configure it with the switch’s built-in interfaces, and assumes an understanding of VLANs, which are described in chapter 2, “Static Virtual LANs (VLANs)”.

For general information on how to use the switch’s built-in interfaces, refer to these chapters in the Management and Configuration Guide for your switch:

- Chapter 3, “Using the Menu Interface”
- Chapter 4, “Using the Command Line Interface (CLI)”
- Chapter 5, “Using the Web Browser Interface”
- Chapter 6, “Switch Memory and Configuration”
Introduction

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>view GVRP configuration</td>
<td>n/a</td>
<td>page 3-13</td>
<td>page 3-14</td>
<td>page 3-18</td>
</tr>
<tr>
<td>list static and dynamic VLANs</td>
<td>n/a</td>
<td>—</td>
<td>page 3-16</td>
<td>page 3-18</td>
</tr>
<tr>
<td>on a GVRP-enabled switch</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>enable or disable GVRP</td>
<td>disabled</td>
<td>page 3-13</td>
<td>page 3-15</td>
<td>page 3-18</td>
</tr>
<tr>
<td>enable or disable GVRP on individual ports</td>
<td>enabled</td>
<td>page 3-13</td>
<td>page 3-15</td>
<td>—</td>
</tr>
<tr>
<td>control how individual ports</td>
<td>Learn</td>
<td>page 3-13</td>
<td>page 3-15</td>
<td>page 3-18</td>
</tr>
<tr>
<td>handle advertisements for new VLANs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>convert a dynamic VLAN to a static VLAN</td>
<td>n/a</td>
<td>—</td>
<td>page 3-17</td>
<td>—</td>
</tr>
<tr>
<td>configure static VLANs</td>
<td>DEFAULT_VLAN (VID = 1)</td>
<td>page 2-22</td>
<td>page 2-28</td>
<td>page 2-39</td>
</tr>
</tbody>
</table>

GVRP—GARP VLAN Registration Protocol—is an application of the Generic Attribute Registration Protocol—GARP. GVRP is defined in the IEEE 802.1Q standard, and GARP is defined in the IEEE 802.1D-1998 standard.

**Note**

To understand and use GVRP you must have a working knowledge of 802.1Q VLAN tagging. (Refer to chapter 2, “Static Virtual LANs (VLANs)”.)

GVRP uses “GVRP Bridge Protocol Data Units” (“GVRP BPDUs”) to “advertise” static VLANs. In this manual, a GVRP BPDU is termed an advertisement. Advertisements are sent outbound from ports on a switch to the devices directly connected to those ports.

While GVRP is enabled on the switch, you cannot apply any ACLs to VLANs configured on the same switch.

GVRP enables the switch to dynamically create 802.1Q-compliant VLANs on links with other devices running GVRP. This enables the switch to automatically create VLAN links between GVRP-aware devices. (A GVRP link can include intermediate devices that are not GVRP-aware.) This operation reduces the chances for errors in VLAN configuration by automatically providing VLAN ID (VID) consistency across the network. That is, you can use GVRP to propagate VLANs to other GVRP-aware devices instead of manually
having to set up VLANs across your network. After the switch creates a
dynamic VLAN, you can optionally use the CLI `static <vlan-id>` command to
convert it to a static VLAN or allow it to continue as a dynamic VLAN for as
long as needed. You can also use GVRP to dynamically enable port membership in static VLANs configured on a switch.

---

**General Operation**

When GVRP is enabled on a switch, the VID for any static VLANs 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 advertise-
ment 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 adver-
tisement for that VLAN is received through a link from another device (exter-
nal source) on that specific port.
Operating Note: When a GVRP-aware port on a switch learns a VID through GVRP from another device, the switch begins advertising that VID out all of its ports except the port on which the VID was learned.

Core switch with static VLANs (VID= 1, 2, & 3). Port 2 is a member of VIDs 1, 2, & 3.

1. Port 2 advertises VIDs 1, 2, & 3.

2. Port 1 receives advertisement of VIDs 1, 2, & 3 AND becomes a member of VIDs 1, 2, & 3.

3. Port 3 advertises VIDs 1, 2, & 3, but port 3 is NOT a member of VIDs 1, 2, & 3 at this point.

4. Port 4 receives advertisement of VIDs 1, 2, & 3 AND becomes a member of VIDs 1, 2, & 3.

5. Port 5 advertises VIDs 1, 2, & 3, but port 5 is NOT a member of VIDs 1, 2, & 3 at this point.

Port 6 is statically configured to be a member of VID 3.

11. Port 2 receives advertisement of VID 3. (Port 2 is already statically configured for VID 3.)

9. Port 3 receives advertisement of VID 3 AND becomes a member of VID 3. (Still not a member of VIDs 1 & 2.)

10. Port 1 advertises VID 3.

7. Port 5 receives advertisement of VID 3 AND becomes a member of VID 3. (Still not a member of VIDs 1 & 2.)

8. Port 4 advertises VID 3.

6. Port 6 advertises VID 3.

Figure 3-1. Example of Forwarding Advertisements and Dynamic Joining

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

For example, in the following figure, 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.
A port can learn of a dynamic VLAN through devices that are not aware of GVRP (Switch “B”, above). VLANs must be disabled in GVRP-unaware devices to allow tagged packets to pass through.

A GVRP-aware port receiving advertisements has these options:

- If there is not already a static VLAN with the advertised VID on the receiving port, then 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” on page 3-9.)

- Ignore the advertisement for that VID.

- Don’t participate in that VLAN.
Note also that a port belonging to a Tagged or Untagged static VLAN has these configurable options:

- Send VLAN advertisements, and also 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 that you 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 (manually created) VLAN.
**Table 3-1. Options for Handling “Unknown VLAN” Advertisements:**

<table>
<thead>
<tr>
<th>Unknown VLAN Mode</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn (the Default)</td>
<td>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.</td>
</tr>
<tr>
<td>Block</td>
<td>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.</td>
</tr>
<tr>
<td>Disable</td>
<td>Causes the port to ignore and drop all GVRP advertisements it receives and also prevents the port from sending any GVRP advertisements.</td>
</tr>
</tbody>
</table>

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

```plaintext
ProCurve# show gvrp

GVVPN support
Maximum VLANs to support : 8
GVVPN Enabled : Yes

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Unknown VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>10/100TX</td>
</tr>
<tr>
<td>A2</td>
<td>10/100TX</td>
</tr>
<tr>
<td>A3</td>
<td>10/100TX</td>
</tr>
<tr>
<td>A4</td>
<td>10/100TX</td>
</tr>
<tr>
<td>A5</td>
<td>10/100TX</td>
</tr>
<tr>
<td>A6</td>
<td>10/100TX</td>
</tr>
<tr>
<td>A7</td>
<td>10/100TX</td>
</tr>
<tr>
<td>A8</td>
<td>10/100TX</td>
</tr>
</tbody>
</table>

GVVPN Enabled
(Required for Unknown VLAN operation.)

Unknown VLAN Settings
Default: Learn
```

**Figure 3-3. Example of GVRP Unknown VLAN Settings**
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 then 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 3-2, on the next page.

**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 the following table:
## Table 3-2. Controlling VLAN Behavior on Ports with Static VLANs

<table>
<thead>
<tr>
<th>Per-Port &quot;Unknown VLAN&quot; (GVRP) Configuration</th>
<th>Static VLAN Options—Per VLAN Specified on Each Port (^1)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Learn</strong> (the Default)</td>
<td>The port:</td>
</tr>
<tr>
<td></td>
<td>• Belongs to specified VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Advertises specified VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Can become a member of dynamic VLANs for which it receives advertisements.</td>
</tr>
<tr>
<td></td>
<td>• Advertises dynamic VLANs that have at least one other port (on the same switch) as a member.</td>
</tr>
<tr>
<td></td>
<td>The port:</td>
</tr>
<tr>
<td></td>
<td>• Will become a member of specified VLAN if it receives advertisements for specified VLAN from another device.</td>
</tr>
<tr>
<td></td>
<td>• Will advertise specified VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Can become a member of other, dynamic VLANs for which it receives advertisements.</td>
</tr>
<tr>
<td></td>
<td>• Will advertise a dynamic VLAN that has at least one other port (on the same switch) as a member.</td>
</tr>
<tr>
<td></td>
<td>The port:</td>
</tr>
<tr>
<td></td>
<td>1. Will not become a member of the specified VLAN.</td>
</tr>
<tr>
<td></td>
<td>2. Will not advertise specified VLAN.</td>
</tr>
<tr>
<td></td>
<td>3. Can become a member of other dynamic VLANs for which it receives advertisements.</td>
</tr>
<tr>
<td></td>
<td>4. Will advertise a dynamic VLAN that has at least one other port on the same switch as a member.</td>
</tr>
<tr>
<td><strong>Block</strong></td>
<td>The port:</td>
</tr>
<tr>
<td></td>
<td>• Belongs to the specified VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Advertises this VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Will not become a member of new dynamic VLANs for which it receives advertisements.</td>
</tr>
<tr>
<td></td>
<td>• Will advertise dynamic VLANs that have at least one other port as a member.</td>
</tr>
<tr>
<td></td>
<td>The port:</td>
</tr>
<tr>
<td></td>
<td>• Will become a member of specified VLAN if it receives advertisements for this VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Will advertise this VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Will not become a member of new dynamic VLANs for which it receives advertisements.</td>
</tr>
<tr>
<td></td>
<td>• Will advertise dynamic VLANs that have at least one other port (on the same switch) as a member.</td>
</tr>
<tr>
<td></td>
<td>The port:</td>
</tr>
<tr>
<td></td>
<td>• Will not become a member of the specified VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Will not advertise this VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Will not become a member of dynamic VLANs for which it receives advertisements.</td>
</tr>
<tr>
<td></td>
<td>• Will advertise dynamic VLANs that have at least one other port (on the same switch) as a member.</td>
</tr>
<tr>
<td><strong>Disable</strong></td>
<td>The port:</td>
</tr>
<tr>
<td></td>
<td>• Is a member of the specified VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Will ignore GVRP PDUs.</td>
</tr>
<tr>
<td></td>
<td>• Will not join any advertised VLANs.</td>
</tr>
<tr>
<td></td>
<td>• Will not advertise VLANs.</td>
</tr>
<tr>
<td></td>
<td>The port:</td>
</tr>
<tr>
<td></td>
<td>• Will not become a member of the specified VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Will ignore GVRP PDUs.</td>
</tr>
<tr>
<td></td>
<td>• Will not join any dynamic VLANs.</td>
</tr>
<tr>
<td></td>
<td>• Will not advertise VLANs.</td>
</tr>
<tr>
<td></td>
<td>The port:</td>
</tr>
<tr>
<td></td>
<td>• Will not become a member of this VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Will ignore GVRP PDUs.</td>
</tr>
<tr>
<td></td>
<td>• Will not join any dynamic VLANs.</td>
</tr>
<tr>
<td></td>
<td>• Will not advertise VLANs.</td>
</tr>
</tbody>
</table>

\(^1\) 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.

\(^2\) To configure tagging, **Auto**, or **Forbid**, see “Configuring Static VLAN Per-Port Settings” on page 2-37 (for the CLI) or “Adding or Changing a VLAN Port Assignment” on page 2-26 (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 3-2, above, 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, ProCurve 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. The two preceding sections describe the per-port features you can use to control and limit VLAN propagation. To summarize, you can:

- Allow a port to advertise and/or join dynamic VLANs (Learn mode—the default).
- Allow 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).
- Prevent 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 continues to receive advertisements of that VLAN from another device connected to that port or until you:

- Convert the VLAN to a static VLAN (See “Converting a Dynamic VLAN to a Static VLAN” on page 3-17.)
- Reconfigure the port to **Block** or **Disable**
disable gvrp

reboot the switch

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

---

planning for gvrp operation

these steps outline the procedure for setting up dynamic vlans for a segment.

1. determine the vlan topology you want for each segment (broadcast domain) on your network.

2. determine the vlans that must be static and the vlans that can be dynamically propagated.

3. determine the device or devices on which you must manually create static vlans in order to propagate vlans throughout the segment.

4. determine security boundaries and how the individual ports in the segment will handle dynamic vlan advertisements. (see table 3-1 on page 3-8 and table 3-2 on page 3-10.)

5. enable gvrp on all devices you want to use with dynamic vlans and configure the appropriate “unknown vlan” parameter (learn, block, or disable) for each port.

6. configure the static vlans on the switch(es) where they are needed, along with the per-vlan parameters (tagged, untagged, auto, and forbid—see table 3-2 on page 3-10) on each port.

7. dynamic vlans will then appear automatically, according to the configuration options you have chosen.

8. convert dynamic vlans to static vlans where you want dynamic vlans to become permanent.
Configuring GVRP On a Switch

The procedures in this section describe how to:

- View the GVRP configuration on a switch
- Enable and disable GVRP on a switch
- Specify how individual ports will handle advertisements

To view or configure static VLANs for GVRP operation, refer to “Per-Port Static VLAN Configuration Options” on page 2-12.

Menu: Viewing and Configuring GVRP

1. From the Main Menu, select:

   2. Switch Configuration …
   8. VLAN Menu …
   1. VLAN Support

   ![](image)

   Figure 3-4. The VLAN Support Screen (Default Configuration)

2. Do the following to enable GVRP and display the Unknown VLAN fields:
   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.
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.

Figure 3-5. Example Showing Default Settings for Handling Advertisements

3. Use the arrow keys to select the port you want, and the Space bar to select 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.

CLI: Viewing and Configuring GVRP

GVRP Commands Used in This Section

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show gvrp</td>
<td></td>
</tr>
<tr>
<td>gvrp</td>
<td>3-15</td>
</tr>
<tr>
<td>unknown-vlans</td>
<td>3-15</td>
</tr>
</tbody>
</table>

Displaying the Switch’s Current GVRP Configuration. This command shows whether GVRP is disabled, along with the current settings for the maximum number of VLANs and the current Primary VLAN. (For more on the last two parameters, see chapter 2, “Static Virtual LANs (VLANs)”.)

Syntax: show gvrp  Shows the current settings.
Enabling and Disabling GVRP on the Switch. This command enables GVRP on the switch.

**Syntax:**  
gvrp

This example enables GVRP:

ProCurve(config)# gvrp

This example disables GVRP operation on the switch:

ProCurve(config)# no gvrp

Enabling and Disabling GVRP On Individual Ports. When GVRP is enabled on the switch, use the *unknown-vlans* command to change the Unknown VLAN field for one or more ports. You can use this command at either the Manager level or the interface context level for the desired port(s).
Configuring GVRP On a Switch

**Syntax:**

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

*Changes the Unknown VLAN field setting for the specified port(s).*

For example, to change and view the configuration for ports A1-A2 to **Block**:

```
ProCurve(config)#interface a1-a2 unknown-vlans block
```

```
HP4108(config)#show gvrp
GVRP support
  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled : Yes

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Unknown VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/100TX</td>
<td>Block</td>
</tr>
<tr>
<td>10/100TX</td>
<td>Block</td>
</tr>
<tr>
<td>10/100TX</td>
<td>Learn</td>
</tr>
<tr>
<td>10/100TX</td>
<td>Learn</td>
</tr>
</tbody>
</table>
```

**Figure 3-8. Displaying the Static and Dynamic VLANs Active on the Switch**

**Syntax:**

```
show vlans
```

*The `show vlans` command lists all VLANs present in the switch.*

For example, 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:
Configuring GVRP On a Switch

Switch “A”
GVRP enabled.
3 Static VLANs:
- DEFAULT_VLAN
- VLAN-222
- VLAN-333

Switch “B”
GVRP enabled.
1 Static VLANs:
- DEFAULT_VLAN

Port 1: Set to “Learn” Mode

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

Dynamic VLANs Learned from Switch “A” through Port 1
```

**Figure 3-9. Example of Listing Showing Dynamic VLANs**

**Converting a Dynamic VLAN to a Static VLAN.** 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:

**Syntax:**
```
static < dynamic-vlan-id >
```

*Converts the a dynamic VLAN to a static VLAN.*

For example, to convert dynamic VLAN 333 (from the previous example) to a static VLAN:

```
ProCurve(config)# static 333
```

When you convert a dynamic VLAN to a static VLAN, all ports on the switch are assigned to the VLAN in Auto mode.
Web: Viewing and Configuring GVRP

To view, enable, disable, or reconfigure GVRP:

1. Click on the Configuration tab.

2. Click on [VLAN Configuration] and do the following:
   - To enable or disable GVRP, click on GVRP Enabled.
   - To change the Unknown VLAN field for any port:
     i. Click on [GVRP Security] and make the desired changes.
     ii. Click on [Apply] to save and implement your changes to the Unknown VLAN fields.

For web-based Help on how to use the web browser interface screen, click on the [?] button provided on the web browser screen.

GVRP Operating Notes

- 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 eight VLANs. Thus, in a case where four static VLANs are configured on the switch, the switch can accept up to four additional VLANs in any combination of static and dynamic. 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 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, you must first convert it to a static VLAN.
■ Rebooting a switch on which a dynamic VLAN exists deletes that VLAN. However, the dynamic VLAN re-appears 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 port(s) on which it originally learned of those VLANs.

■ While GVRP is enabled on the switch, you cannot apply any ACLs to VLANs configured on the same switch.

■ 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.
— This page intentionally unused. —
# Multiple Instance Spanning-Tree Operation

## Contents

**Overview** ......................................................... 4-2

**802.1s Multiple Spanning Tree Protocol (MSTP)** ............. 4-5

- MSTP Structure ............................................... 4-6
- How MSTP Operates ............................................ 4-9
- MST Regions ..................................................... 4-9
- Regions, Legacy STP and RSTP Switches, and the
  Common Spanning Tree (CST) ................................. 4-11
- MSTP Operation with 802.1Q VLANs ........................... 4-11

**Terminology** .................................................. 4-13

**Operating Rules** .............................................. 4-14

**Transitioning from STP or RSTP to MSTP** ..................... 4-15

**Tips for Planning an MSTP Application** ....................... 4-16

**Steps for Configuring MSTP** ................................ 4-17

**Configuring MSTP Operation Mode and Global Parameters** ... 4-19

**Configuring Basic Port Connectivity Parameters** .............. 4-22

**Configuring MST Instance Parameters** ........................ 4-25

**Configuring MST Instance Per-Port Parameters** ............... 4-28

**Enabling or Disabling Spanning Tree Operation** ............... 4-31

**Enabling an Entire MST Region at Once or**
**Exchanging One Region Configuration for Another** ............ 4-31

**Displaying MSTP Statistics and Configuration** ............... 4-33

- **Displaying MSTP Statistics** ............................... 4-33
- **Displaying the MSTP Configuration** ......................... 4-36

**Operating Notes** .............................................. 4-40

**Troubleshooting** .............................................. 4-40
Multiple Instance Spanning-Tree Operation
Overview

### Overview

**MSTP Features**

<table>
<thead>
<tr>
<th>802.1s Spanning Tree Protocol</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing the MSTP Status and Configuration</td>
<td>n/a</td>
<td>—</td>
<td>page 4-33</td>
<td>—</td>
</tr>
<tr>
<td>Enable/Disable MSTP and Configure Global Parameters</td>
<td>Disabled</td>
<td>—</td>
<td>page 4-19</td>
<td>—</td>
</tr>
<tr>
<td>Configuring Basic Port Connectivity Parameters</td>
<td>edge-port: No, mcheck: Yes, hello-time: 2, path-cost: auto, point-to-point MAC: Force-True, priority: 128 (multiplier: 8)</td>
<td>—</td>
<td>page 4-22 and following</td>
<td>—</td>
</tr>
<tr>
<td>Configuring MSTP Instance Parameters</td>
<td>instance (MSTPI): none, priority: 32768 (multiplier: 8)</td>
<td>—</td>
<td>page 4-25</td>
<td>—</td>
</tr>
<tr>
<td>Configuring MSTP Instance Per-Port Parameters</td>
<td>Auto</td>
<td>—</td>
<td>page 4-28</td>
<td>—</td>
</tr>
<tr>
<td>Enabling/Disabling MSTP Spanning Tree Operation</td>
<td>Disabled</td>
<td>—</td>
<td>page 4-31</td>
<td>—</td>
</tr>
<tr>
<td>Enabling an Entire MST Region at Once</td>
<td>n/a</td>
<td>—</td>
<td>page 4-31</td>
<td>—</td>
</tr>
</tbody>
</table>

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.

*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. For example, suppose you have three switches in a region...
configured with VLANs grouped into two instances, as follows:

<table>
<thead>
<tr>
<th>VLANs</th>
<th>Instance 1</th>
<th>Instance 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>10, 11, 12</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>20, 21, 22</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The logical and physical topologies resulting from these VLAN/Instance groupings result in blocking on different links for different VLANs:

Figure 4-1. Example of a Multiple Spanning-Tree Application
RSTP and MSTP implements a greater range of path costs and new default path cost values to account for higher network speeds. These values are different than the values defined by 802.1D STP as shown below.

<table>
<thead>
<tr>
<th>Port Type</th>
<th>802.1D STP Path Cost</th>
<th>RSTP and MSTP Path Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps</td>
<td>100</td>
<td>2000000</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>10</td>
<td>200000</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>5</td>
<td>20000</td>
</tr>
</tbody>
</table>

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/or MSTP, you should reconfigure the devices so the path costs match for ports with the same network speeds.
802.1s Multiple Spanning Tree Protocol (MSTP)

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. Also, because incorrect MSTP settings can adversely affect network performance, you should 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, refer to the IEEE 802.1s standard.

MSTP Structure

MSTP maps active, separate paths through separate spanning tree instances and between MST regions. Each MST region comprises one or more MSTP switches. Note that MSTP recognizes an STP or RSTP LAN as a distinct spanning-tree region.
Common and Internal Spanning Tree (CIST): The CIST identifies the regions in a network and administers the CIST root bridge for the network, the root bridge for each region, and the root bridge for each spanning-tree instance in each region.

Common Spanning Tree (CST): The CST administers the connectivity among the MST regions, STP LANs, and RSTP LANs in a bridged network.

MST Region: An MST region comprises the VLANs configured on physically connected MSTP switches. All switches in a given region must be configured with the same VLANs and Multiple Spanning Tree Instances (MSTIs).

Internal Spanning Tree (IST): The IST administers the topology within a given MST region. When you configure a switch for MSTP operation, the switch automatically includes all of the static VLANs configured on the switch.
in a single, active spanning tree topology (instance) within the IST. This is termed the “IST instance”. Any VLANs you subsequently configure on the switch are added to this IST instance. To create separate forwarding paths within a region, group specific VLANs into different Multiple Spanning Tree Instances (MSTIs). (Refer to “Multiple Spanning Tree Instance”, below.)

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). All VLANs in the IST instance of a region are part of the same, single spanning tree topology, which allows only one forwarding path between any two nodes belonging to any of the VLANs included in the IST instance. All switches in the region must belong to the set of VLANs that comprise 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).

- **MSTI (Multiple Spanning Tree Instance):** This type of configurable spanning tree instance comprises all static VLANs you specifically assign to it, and must include at least one VLAN. The VLAN(s) 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.)
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. Note that inappropriate changes to these settings can result in severely degraded network performance. For this reason, *ProCurve 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.*

**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. (Refer to “Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another” on page 4-31.)

*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, *ProCurve 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.*

**MST Regions**

All MSTP switches in a given region must be configured with the same VLANs. Also, each MSTP switch within the same region must have the same VLAN-to-instance assignments. (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 Operation. Assigning different groups of VLANs to different instances ensures that those VLAN groups use independent forwarding paths. For example, in figure 4-3 each instance has a different forwarding path.

**Figure 4-3. 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. (Refer to figure 4-2 on page 4-7.)

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. This means that 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
Multiple Instance Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

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.

Problem:
An MST instance with two separate (non-trunked) links blocks a VLAN link.

Solution:
Configure one trunked link for the two VLAN memberships.

Nodes 1 and 2 cannot communicate because MSTP is blocking the link.

Nodes 1 and 2 can communicate because the MST instance sees the trunk as a single link and 802.1Q (tagged) VLANs enable the use of one (trunked) link for both VLANs.

Figure 4-4. Example of 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.
Terminology

**Bridge:** See “MSTP Bridge”.

**Common and Internal Spanning Tree (CIST):** Comprises all LANs, STP, and RSTP bridges and MSTP regions in a network. The CIST automatically determines the MST regions in a network and defines the root bridge (switch) and designated port for each region. The CIST includes the Common Spanning Tree (CST), the Internal Spanning Tree (IST) within each region, and any multiple spanning-tree instances (MSTIs) in a region.

**Common Spanning Tree (CST):** Refers to the single forwarding path the switch calculates for STP (802.1D) and RSTP (802.1w) topologies, and for inter-regional paths in MSTP (802.1s) topologies. Note that all three types of spanning tree can interoperate in the same network. Also, the MSTP switch interprets a device running 802.1D STP or 802.1w RSTP as a separate region. (Refer to figure 4-2 on page 4-7.)

**Internal Spanning Tree (IST):** Comprises all VLANs within a region that are not assigned to a multiple spanning-tree instance configured within the region. All MST switches in a region should belong to the IST. In a given region “X”, the IST root switch is the regional root switch and provides information on region “X” to other regions.

**MSTP (Multiple Spanning Tree Protocol):** A network supporting MSTP allows multiple spanning tree instances within configured regions, and a single spanning tree among regions, STP bridges, and RSTP bridges.

**MSTP BPDU (MSTP Bridge Protocol Data Unit):** These BPDUs carry region-specific information, such as the region identifier (region name and revision number). If a switch receives an MSTP BPDU with a region identifier that differs from its own, then the port on which that BPDU was received is on the boundary of the region in which the switch resides.

**MSTP Bridge:** In this manual, an MSTP bridge is a switch (or another 802.1s-compatible device) configured for MSTP operation.

**MST Region:** An MST region forms a multiple spanning tree domain and is a component of a single spanning-tree domain within a network. For switches internal to the MST region:
- All switches have identical MST configuration identifiers (region name and revision number).
- All switches have identical VLAN assignments to the region’s IST and (optional) MST instances.
Multiple Instance Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

- One switch functions as the designated bridge (IST root) for the region.
- No switch has a point-to-point connection to a bridging device that cannot process RSTP BPDUs.

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 and VID-to-IST instance assignments.
- There is one root MST switch per configured MST instance.
- Within any region, the root switch for the IST instance is also the root switch for the region. 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). Note that the per-port hello-time parameter assignments on the CIST root switch propagate to the ports on downstream switches in the network and override the hello-time configured on the downstream switch ports.
- 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 spanning tree (one physical, communication path) between any two nodes. That is, within an MSTI, there is one instance of spanning tree, 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.
- Communication between MST regions uses a single spanning tree.
Multiple Instance Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

- 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.

- A dynamic VLAN learned by GVRP will always be placed in the IST instance and cannot be moved to any configured MST instance.

Transitioning from STP or RSTP to MSTP

IEEE 802.1s MSTP includes RSTP functionality and is designed to be compatible with both IEEE 802.1D and 802.1w spanning-tree protocols. Even if all the other devices in your network are using STP, you can enable MSTP on the switches covered in this guide. Also, using the default configuration values, your switches will interoperate effectively with STP and RSTP 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.

Because MSTP is so efficient at establishing the network path, ProCurve highly recommends that you update all of the switches covered in this guide to support 802.1s/MSTP. (For switches that do not support 802.1s/MSTP, ProCurve recommends that you update to RSTP to benefit from the convergence times of less than one second under optimal circumstances.) To make the best use of MSTP and achieve the fastest possible convergence times, there are some changes that you should make to the MSTP default configuration.

Note

Under some circumstances, it is possible for the rapid state transitions employed by MSTP and RSTP to result in an increase in the rates of frame duplication and misordering in the switched LAN. In order to allow MSTP and RSTP switches to support applications and protocols that may be sensitive to frame duplication and misordering, setting the Force Protocol Version param-
eter to **STP-compatible** allows MSTP and RSTP to operate with the rapid transitions disabled. The value of this parameter applies to all ports on the switch. See information on **force version** on page 4-21.

As indicated above, one of the benefits of MSTP and RSTP is the implementation of a larger range of port path costs, which accommodates higher network speeds. New default values have also been implemented for the path costs associated with the different network speeds. This can create some incompatibility between devices running the older 802.1D STP and your switch running MSTP or RSTP. Please see the “Note on Path Cost” on page 4-4 for more information on adjusting to this incompatibility.

### Tips for Planning an MSTP Application

- 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.

- All ports or trunks connecting one switch to another within a region should be configured 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.)

- There is one logical spanning-tree path through the following:
  - Any inter-regional links
  - Any IST 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 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. (Refer to “MSTP Operation with 802.1Q VLANs” on page 4-11.)

Identify the edge ports connected to end nodes and enable the edge-port setting for these ports. Leave the edge-port setting disabled for ports connected to another switch, a bridge, or a hub.

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. See the information on force-version on page 4-21.

Steps for Configuring MSTP

This section outlines the general steps for configuring MSTP operation in your network, and assumes you have already planned and configured the VLANs you want MSTP to use. The actual MSTP parameter descriptions are in the following sections.

The switch supports MSTP configuration through the CLI.

1. Configure MSTP global parameters. This step involves configuring the following:
   - Required parameters for MST region identity:
     - Region Name: `spanning-tree config-name`
     - Region Revision Number: `spanning-tree config-revision`
   - Optional MSTP parameter changes for region settings:
     - ProCurve recommends that you leave these parameters at their default settings for most networks. Refer to the “Caution” on page 4-9.
     - The maximum number of hops before the MSTP BPDU is discarded (default: 20)
       - `spanning-tree max-hops`
Multiple Instance Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

- Force-Version operation
  spanning-tree force-version

- Forward Delay
  spanning-tree forward-delay

- Hello Time (used if the switch operates as 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

2. 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.
     spanning-tree instance

     To move a VLAN from one instance to another, first use no spanning-
     tree instance < n > vlan < vid > to unmapping 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.)

     • Configure the priority for each instance.
       spanning-tree instance

3. Configure MST instance port parameters. Enable edge-port for ports
   connected to end nodes (page 4-22), but leave it disabled (the default) for
   connections to another switch, a bridge, or a hub. Set the path cost value
   for the port(s) used by a specific MST instance. Leaving this setting at the
   default auto allows the switch to calculate the path-cost from the link
   speed.
   spanning-tree instance

4. Enable spanning-tree operation on the switch.
   spanning-tree
Configuring MSTP Operation Mode and Global Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree config-name &lt; ascii-string &gt;</td>
<td>4-19</td>
</tr>
<tr>
<td>spanning-tree config-revision &lt; revision-number &gt;</td>
<td>4-20</td>
</tr>
<tr>
<td>spanning-tree max-hops &lt; hop-count &gt;</td>
<td>4-20</td>
</tr>
<tr>
<td>spanning-tree force-version</td>
<td>4-21</td>
</tr>
<tr>
<td>span-t-compatible</td>
<td>rstp-operation</td>
</tr>
<tr>
<td>spanning-tree hello-time &lt; 1..10 &gt;</td>
<td>4-21</td>
</tr>
<tr>
<td>spanning-tree legacy-mode</td>
<td>4-21</td>
</tr>
<tr>
<td>spanning-tree legacy-path-cost</td>
<td>4-21</td>
</tr>
</tbody>
</table>

The commands in this section apply on the switch level, and do not affect individual port configurations.

**Syntax:** [no] spanning-tree config-name < ascii-string >

This command 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. Thus, if you want more than one MSTP switch in the same MST region, you must configure the identical region name on all such switches. If you retain the default configuration name on a switch, it cannot exist in the same MST region with another switch. (Default Name: 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. Also, there is no defined limit on the number of regions you can configure.
**Syntax:** spanning-tree config-revision < revision-number >

This command configures the revision number you designate 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.

Note that 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.

**Syntax:** spanning-tree max-hops < hop-count >

This command 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. Note that 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)
**Syntax:** spanning-tree force-version < stp-compatible | rstp-operation | mstp-operation >

Sets the spanning-tree compatibility mode. When the switch is configured with MSTP 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.

**stp-compatible:** The switch applies 802.1D STP operation on all ports.

**rstp-operation:** The switch applies 802.1w operation on all ports except those ports where it detects a system using 802.1D Spanning Tree.

**mstp-operation:** The switch applies 802.1s MSTP operation on all ports where compatibility with 802.1D or 802.1w spanning tree protocols is not required.

This command is available when the protocol version is set to mstp (see 'protocol-version' above).

Note that 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 the “Note on MSTP Rapid State Transitions” on page 4-17, 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.

**Syntax:** spanning-tree hello-time < 1..10 >

If MSTP is running and the switch is operating as the CIST 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 > (page 4-22). (Default: 2.)

**Syntax** spanning-tree legacy-mode

Set spanning tree protocol to operate either in 802.1d legacy mode or in 802.1s native mode.

**Syntax** spanning-tree legacy-path-cost

Set 802.1d (legacy) or 802.1t (not legacy) default pathcost values.
Configuring Basic Port Connectivity Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree &lt; port-list &gt;</td>
<td></td>
</tr>
<tr>
<td>edge-port</td>
<td>below</td>
</tr>
<tr>
<td>mcheck</td>
<td>below</td>
</tr>
<tr>
<td>hello-time &lt; global</td>
<td>1..10 &gt;</td>
</tr>
<tr>
<td>spanning-tree path-cost &lt; auto</td>
<td>200000000 &gt;</td>
</tr>
<tr>
<td>spanning-tree point-to-point-mac &lt; force-true</td>
<td>force-false</td>
</tr>
<tr>
<td>spanning-tree priority &lt;priority-multiplier&gt;</td>
<td></td>
</tr>
</tbody>
</table>

The basic port connectivity parameters affect spanning-tree links at the global level. In most cases, ProCurve 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.

**Syntax:** [no] spanning-tree < port-list > < edge-port | mcheck >

[ edge-port ]

*Enable edge-port on ports connected to end nodes. During spanning tree establishment, ports with edge-port enabled transition immediately to the forwarding state. Disable this feature on any switch port that is connected to another switch, bridge, or hub. (Default: No - disabled)*

The no spanning-tree < port-list > edge-port command disables edge-port operation on the specified ports.

[ mcheck ]

*Forces a port to send RSTP BPDUs for 3 seconds. This allows for another switch connected to the port and running RSTP to establish its connection quickly and for identifying switches running 802.1D STP. If the whole-switch force-version parameter is set to stp-compatible, the switch ignores the mcheck setting and sends 802.1D STP BPDUs out all ports. Disable this feature on all ports that are known to be connected to devices that are running 802.1D STP. (Default: Yes - enabled)*

The no spanning-tree < port-list > mcheck command disables mcheck.
Multiple Instance Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

Syntax: spanning-tree < port-list > < hello-time | path-cost | point-to-point-mac | priority >

[ 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 (page 4-21). 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. (That is, 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.)

[ 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

Refer to “Note on Path Cost” on page 4-4 for information on compatibility with devices running 802.1D STP for the path cost values (Default: Auto.).

[point-to-point-mac < force-true | force-false | auto >]

This parameter informs the switch of the type of device to which a specific port connects.

Force-True (default): Indicates a point-to-point link to a device such as a switch, bridge, or end-node.

Force-False: Indicates a connection to a hub (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. (Connections to hubs are half-duplex.)
Multiple Instance Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

[priority < priority-multiplier>]

MSTP uses this parameter to determine the port(s) to use for forwarding. The port with the lowest priority number has the highest priority. The range is 0 to 240, and is configured by specifying a multiplier in the range of 0 - 15. That is, when you specify a priority multiplier of 0 - 15, the actual priority assigned to the switch is:

\[(\text{priority-multiplier}) \times 16\]

For example, if you configure “2” as the priority multiplier on a given port, then the actual Priority setting is 32. Thus, after you specify 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 this line in the show running output:

spanning-tree A2 priority 3
Configuring MST Instance Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] spanning-tree instance &lt; 1..16 &gt; vlan &lt; vid&gt; [ vid..vid ]</td>
<td>4-22</td>
</tr>
<tr>
<td>no spanning-tree instance &lt; 1..16 &gt;</td>
<td></td>
</tr>
<tr>
<td>spanning-tree instance &lt; 1..16 &gt; priority &lt; 0..15 &gt;</td>
<td>4-25</td>
</tr>
<tr>
<td>spanning-tree priority &lt; 0..15 &gt;</td>
<td>4-26</td>
</tr>
</tbody>
</table>

**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 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. At least one VLAN must be mapped to a MSTI when you create it. (A VLAN cannot be mapped to more than one instance at a time.) You can create up to 16 MSTIs in a region. The no form of the command deletes the specified VLAN or if no VLANs are specified, the no form of the command deletes the specified MSTI. (Removing a VLAN from an MSTI returns the VLAN to the IST instance, where it can either remain or be re-assigned to another MSTI configured in the region.) The no form of the command deletes the specified VLAN, or if no VLANs are specified, the no form of the command deletes the specified MSTI.
**Syntax:** spanning-tree instance < 1..16 > priority < priority-multiplier >

This command 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 for the instance. 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 root bridge in a given instance provides the path to connected instances in other regions that share one or more of the same VLAN(s). (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 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, then 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, then the switch with the lowest MAC address becomes the root switch for that instance.
**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, if you configure “2” as the priority-multiplier on a given MSTP switch, then 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.
Configuring MST Instance Per-Port Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree instance &lt; 1..16 &gt; &lt; port-list &gt; path-cost &lt; auto</td>
<td>1..200000000 &gt;</td>
</tr>
<tr>
<td>spanning-tree instance &lt; 1..16 &gt; &lt; port-list &gt; priority &lt; priority-multiplier &gt;</td>
<td>4-29</td>
</tr>
<tr>
<td>spanning-tree &lt; port-list &gt; priority &lt; priority-multiplier &gt;</td>
<td>4-30</td>
</tr>
</tbody>
</table>

**Syntax:** spanning-tree instance < 1..16 > < port-list > path-cost < auto | 1..200000000 >

This command assigns an individual port cost 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)
Multiple Instance Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

**Syntax:** spanning-tree instance < 1..16 >< port-list > priority <priority-multiplier>

This command sets the priority for the specified port(s) 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. That is, when you specify a priority multiplier of 0 - 15, the actual priority assigned to the switch is:

\[(priority-multiplier) \times 16\]

For example, if you configure “2” as the priority multiplier on a given port in an MST instance, then the actual priority setting is 32. Thus, 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 this 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
```
Multiple Instance Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

**Syntax:** spanning-tree < port-list > priority < priority-multiplier >

This command sets the priority for the specified port(s) for the IST (that is, 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. That is, when you specify a priority multiplier of 0 - 15, the actual priority assigned to the switch is:

\[(\text{priority-multiplier}) \times 16\]

For example, configuring “5” as the priority multiplier on a given port in the IST instance for a region creates an actual Priority setting of 80. Thus, after you specify the port priority multiplier for the IST instance, the switch displays the actual port priority (and 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 >

For example, 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 this command to enable spanning tree, ensure that the version you want to use is active on the switch.

**Syntax:** [no] 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.

Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree pending &lt; apply</td>
<td>config-name</td>
</tr>
</tbody>
</table>

This operation exchanges the currently active MSTP configuration with the currently pending MSTP configuration. It enables you to implement a new MSTP configuration with minimal network disruption or to exchange MSTP configurations for testing or troubleshooting purposes.

When you configure or reconfigure MSTP, the switch re-calculates 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 RSTP 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.

**To Create a Pending MSTP Configuration.** This procedure creates a pending MSTP configuration and exchanges it with the active MSTP configuration.
1. Configure the VLANs you want included in any instances in the new region. When you create the pending region, all VLANs configured on the switch will be assigned to the pending IST instance unless assigned to other, pending MST instances.

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 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). (The `pending` command creates the region's IST instance automatically.)

6. Repeat step 5 for each additional MST instance you want to configure.

7. Use the `show spanning-tree pending` command to review your pending configuration (page 4-39).

8. Use the `spanning-tree pending apply` command to exchange the currently active MSTP configuration with the pending MSTP configuration.

**Syntax:** spanning-tree pending < apply | config-name | config-revision | instance | reset >

- **apply**
  
  Exchanges the currently active MSTP configuration with the pending MSTP configuration.

- **config-name**
  
  Specifies the pending MST region name. Must be the same for all MSTP switches in the region. (Default: The switch's MAC address.)

- **config-revision**
  
  Specifies the pending MST region configuration revision number. Must be the same for all MSTP switches in the region. (Default: 0).

- **instance < 1..16 > vlan [< vid | vid-range >**
  
  Creates the pending instance and assigns one or more VLANs to the instance.

- **reset**
  
  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.
To view the current pending MSTP configuration, use the `show spanning-tree pending` command (page 4-39).

### Displaying MSTP Statistics and Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSTP Statistics:</td>
<td></td>
</tr>
<tr>
<td><code>show spanning-tree [&lt;port-list&gt;]</code></td>
<td>below</td>
</tr>
<tr>
<td>`show spanning-tree instance &lt;ist</td>
<td>1..16&gt;`</td>
</tr>
<tr>
<td>MSTP Configuration</td>
<td></td>
</tr>
<tr>
<td><code>show spanning-tree [&lt;port-list&gt;] config</code></td>
<td>4-36</td>
</tr>
<tr>
<td>`show spanning-tree [&lt;port-list&gt;] config instance &lt;ist</td>
<td>1..16&gt;`</td>
</tr>
<tr>
<td><code>show spanning-tree mst-config</code></td>
<td>4-38</td>
</tr>
<tr>
<td>`show spanning-tree pending &lt; &lt;instance</td>
<td>ist &gt;</td>
</tr>
</tbody>
</table>

### Displaying MSTP Statistics

#### Displaying Switch Statistics for the Common Spanning Tree.
This command displays the MSTP statistics for the connections between MST regions in a network.

**Syntax:** `show spanning-tree`

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

**Syntax:** `show spanning-tree <port-list>`

> This command displays the spanning-tree status for the designated port(s). 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-a42,trk1`
Multiple Instance Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Cost</th>
<th>Priority</th>
<th>State</th>
<th>Designated Bridge</th>
<th>Hello Time</th>
<th>PtP Edge</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Forwarding</td>
<td>000883-028300</td>
<td>9</td>
<td>Yes No</td>
</tr>
<tr>
<td>A2 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Blocking</td>
<td>0001e7-948300</td>
<td>9</td>
<td>Yes No</td>
</tr>
<tr>
<td>A3 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Forwarding</td>
<td>000883-02a700</td>
<td>2</td>
<td>Yes No</td>
</tr>
<tr>
<td>A4 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A5 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4-5. Example of Common Spanning Tree Status on an MSTP Switch
Displaying Switch Statistics for a Specific MST Instance.

**Syntax:** show spanning-tree instance < ist | 1..16 >

*This command displays the MSTP statistics for either the IST instance or a numbered MST instance running on the switch.*

```
Switch-1(config)# show spanning-tree instance 1

MST Instance Information

  Instance ID : 1
  Mapped VLANs : 11,22

  Switch Priority : 32768
  Topology Change Count : 4
  Time Since Last Change : 6 secs

  Regional Root MAC Address : 0001e7-948300
  Regional Root Priority : 32768
  Regional Root Path Cost : 400000
  Regional Root Port : A1
  Remaining Hops : 18

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Cost</th>
<th>Priority</th>
<th>Role</th>
<th>State</th>
<th>Bridge</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>200000</td>
<td>128</td>
<td>Root</td>
<td>Forwarding</td>
<td>00883-028300</td>
</tr>
<tr>
<td>A2</td>
<td>200000</td>
<td>128</td>
<td>Designated</td>
<td>Forwarding</td>
<td>00883-02a700</td>
</tr>
<tr>
<td>A3</td>
<td>200000</td>
<td>112</td>
<td>Designated</td>
<td>Forwarding</td>
<td>00883-02a700</td>
</tr>
<tr>
<td>A4</td>
<td>Auto</td>
<td>128</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>
```

Figure 4-6. Example of MSTP Statistics for a Specific Instance on an MSTP Switch
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, refer to “Configuring Basic Port Connectivity Parameters” on page 4-22.

**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(s) and/or trunk(s). 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, use this command: `show spanning-tree a20-a24,trk1 config`

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Cost</th>
<th>Priority</th>
<th>Edge</th>
<th>Point-to-Point</th>
<th>MCheck</th>
<th>Hello Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>A4</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A20</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>A21</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>A22</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>A23</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>A24</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>Trk1</td>
<td>Auto</td>
<td>128</td>
<td></td>
<td></td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
</tbody>
</table>

Figure 4-7. Example of Displaying the Switch’s Global Spanning-Tree Configuration
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 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 above command, but lists the spanning-tree port parameter settings for only the specified port(s) and/or trunk(s). 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, use this command:

```
show spanning-tree a20-a24,trk1 config instance 1
```

```
Switch-2(config)# show spanning-tree config instance 1

MST Instance Configuration Information
[---------------------------]
|Instance ID : 1
|Switch Priority : 32768
|Mapped VLANs : 11,22
[---------------------------]
<table>
<thead>
<tr>
<th>Port Type</th>
<th>Cost</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3 10/100TX</td>
<td>Auto</td>
<td>128</td>
</tr>
<tr>
<td>A4 10/100TX</td>
<td>Auto</td>
<td>128</td>
</tr>
<tr>
<td>A5 10/100TX</td>
<td>Auto</td>
<td>128</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>A23 10/100TX</td>
<td>Auto</td>
<td>128</td>
</tr>
<tr>
<td>A24 10/100TX</td>
<td>Auto</td>
<td>128</td>
</tr>
<tr>
<td>Trk1</td>
<td>100000</td>
<td>128</td>
</tr>
</tbody>
</table>
[---------------------------]
```

Figure 4-8. Example of the Configuration Listing for a Specific Instance
Displaying the Region-Level Configuration in Brief. This command output 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

*This command displays the switch’s regional configuration.*

**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, then they cannot be members of the same region.

```
Switch-2(config)# show spanning-tree mst-config

MST Configuration Identifier Information

MST Configuration Name: REGION_1
MST Configuration Revision: 1
MST Configuration Digest: 0xDAD6A13EC5141980B7EBDA71D8991E7C

IST Mapped VLANs: 1.66

<table>
<thead>
<tr>
<th>Instance ID</th>
<th>Mapped VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11.22</td>
</tr>
<tr>
<td>2</td>
<td>33.44,55</td>
</tr>
</tbody>
</table>
```

Figure 4-9. Example of a Region-Level Configuration Display
Displaying the Pending MSTP Configuration. This command displays the MSTP configuration the switch will implement if you execute the spanning-tree pending apply command (Refer to “Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another” on page 4-31.)

**Syntax:** `show spanning-tree pending < instance | mst-config >`

- **instance < 1..16 | ist >**
  - Lists region, instance I.D. and VLAN information for the specified, pending instance.

- **mst-config**
  - Lists region, IST instance VLAN(s), numbered instances, and assigned VLAN information for the pending MSTP configuration.

```
ProCurve# show spanning-tree pending instance 1

Pending MST Instance Configuration Information

  MST Configuration Name : New-Version_01
  MST Configuration Revision : 10
  Instance ID : 1
  Mapped VLANs : 1.22

Switch-1(config)# show spanning-tree pending mst-config

Pending MST Configuration Identifier Information

  MST Configuration Name : New-Version_01
  MST Configuration Revision : 10
  IST Mapped VLANs : 11.33
  Instance ID Mapped VLANs

  ----------------------------------
  1  1.22
  -----------------
```

**Figure 4-10. Example of Displaying a Pending Configuration**
Operating Notes

**SNMP MIB Support for MSTP.** MSTP is a superset of the STP/802.1D and RSTP/802.1w protocols and uses the MIB objects defined for these two protocols.

Troubleshooting

**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 Within 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 and MSTP Configuration Revision number must be identical on all MSTP switches intended for the same region. Another possibility is that the set of VLANs configured on the switch may not match the set of VLANs configured on other switches in the intended region.
Quality of Service (QoS): Managing Bandwidth More Effectively

Contents

Introduction ................................................................. 5-3
Terminology .............................................................. 5-6
Overview ................................................................. 5-7
Classifiers for Prioritizing Outbound Packets .................. 5-10
Packet Classifiers and Evaluation Order ...................... 5-10
Preparation for Configuring QoS ........................................ 5-11
  Preserving 802.1p Priority ....................................... 5-11
  Steps for Configuring QoS on the Switch ................... 5-11
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic ........ 5-13
  Viewing the QoS Configuration .................................. 5-14
  No Override ....................................................... 5-14
  QoS UDP/TCP Priority ........................................... 5-15
    Assigning an 802.1p Priority Based on TCP or UDP Port Number ..................... 5-16
    Assigning a DSCP Policy Based on TCP or UDP Port Number ....................... 5-18
  QoS IP-Device Priority .......................................... 5-21
    Assigning a Priority Based on IP Address .................................. 5-22
    Assigning a DSCP Policy Based on IP Address ................................ 5-23
  QoS IP Type-of-Service (ToS) Policy and Priority ........... 5-27
    Assigning an 802.1p Priority to IPv4 Packets on the Basis of the ToS Precedence Bits .......... 5-28
    Assigning an 802.1p Priority to IPv4 Packets on the Basis of Incoming DSCP ............ 5-29
    Assigning a DSCP Policy on the Basis of the DSCP in IPv4 Packets Received from Upstream Devices .......... 5-33
    Details of QoS IP Type-of-Service ................................ 5-36
Quality of Service (QoS): Managing Bandwidth More Effectively

Contents

Assigning a Priority Based on Layer-3 Protocol ....................... 5-39
QoS VLAN-ID (VID) Priority ........................................... 5-41
  Assigning a Priority Based on VLAN-ID .......................... 5-41
  Assigning a DSCP Policy Based on VLAN-ID (VID) .............. 5-43
QoS Source-Port Priority .............................................. 5-47
  Assigning a Priority Based on Source-Port ....................... 5-47
  Assigning a DSCP Policy Based on the Source-Port .......... 5-49
Differentiated Services Codepoint (DSCP) Mapping ................. 5-52
  Default Priority Settings for Selected Codepoints .......... 5-54
  Quickly Listing Non-Default Codepoint Settings ............. 5-54
Note On Changing a Priority Setting ............................... 5-55
  Example of Changing the Priority Setting on a Policy
  When One or More Classifiers Are Currently Using the Policy . 5-56

IP Multicast (IGMP) Interaction with QoS ......................... 5-59

QoS Messages in the CLI ............................................. 5-60

QoS Operating Notes and Restrictions .............................. 5-61
Introduction

<table>
<thead>
<tr>
<th>QoS Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP/TCP Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-15</td>
<td>Refer to the Online Help.</td>
</tr>
<tr>
<td>IP-Device Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-21</td>
<td>&quot;</td>
</tr>
<tr>
<td>IP Type-of-Service Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-27</td>
<td>&quot;</td>
</tr>
<tr>
<td>LAN Protocol Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-39</td>
<td>&quot;</td>
</tr>
<tr>
<td>VLAN-ID Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-41</td>
<td>&quot;</td>
</tr>
<tr>
<td>Source-Port Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-47</td>
<td>&quot;</td>
</tr>
<tr>
<td>DSCP Policy Table</td>
<td>Various</td>
<td>—</td>
<td>page 5-52</td>
<td>&quot;</td>
</tr>
</tbody>
</table>

As the term suggests, network policy refers to the network-wide controls you can implement to:

- Ensure uniform and efficient traffic handling throughout your network, 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 is often a good idea, but it is not always feasible and does not completely eliminate the potential for network congestion. There will always be points in the network where multiple traffic streams merge or where network links will change speed and capacity. The impact and number of these congestion points will increase over time as more applications and devices are added to the network.

When (not if) network congestion occurs, it is important to move traffic on the basis of relative importance. However, without Quality of Service (QoS) prioritization, less important traffic can consume network bandwidth and slow down or halt the delivery of more important traffic. That is, 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.

This section gives an overview of QoS operation and benefits, and describes how to configure QoS in the console interface.
Quality of Service (QoS): Managing Bandwidth More Effectively

Introduction

Quality of Service is a general term for classifying and prioritizing traffic throughout a network. That is, QoS enables you to establish an end-to-end traffic priority policy to improve control and throughput of important data. You can manage available bandwidth so that the most important traffic goes first. 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 5-1. Example of 802.1p Priority Based on CoS (Class-of-Service) Types and Use of VLAN Tags](image1)

![Figure 5-2. Example Application of Differentiated Services Codepoint (DSCP) Policies](image2)

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.
Quality of Service (QoS): Managing Bandwidth More Effectively

Introduction

QoS is implemented in the form of rules or policies that are configured on the switch. While you can use QoS to prioritize only the outbound traffic while it is moving 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) where QoS can set priorities that downstream devices can support without re-classifying the traffic.

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. That is, 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.
- Avoid or delay the need to add higher-cost NICs (network interface cards) to implement prioritizing. (Instead, control priority through network policy.)

QoS on the switches covered in this guide support these types of traffic marking:

- **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 the downstream devices.
- **IP Type-of-Service (ToS)**: Enables the switch to set, change, and honor prioritization policies by using the Differentiated Services (difserv) bits in the ToS byte of IPv4 packet headers.
## Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Use in This Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1p priority</td>
<td>A traffic priority setting carried by a VLAN-tagged packet moving from one device to another through ports that are tagged members of the VLAN to which the packet belongs. This setting can be from 0 - 7. The switch handles an outbound packet on the basis of its 802.1p priority. However, if the packet leaves the switch through a VLAN on which the port is an untagged member, this priority is dropped, and the packet arrives at the next, downstream device without an 802.1p priority assignment.</td>
</tr>
<tr>
<td>802.1Q field</td>
<td>A four-byte field that is present in the header of Ethernet packets entering or leaving the switch through a port that is a tagged member of a VLAN. This field includes an 802.1p priority setting, a VLAN tag, or ID number (VID), and other data. A packet entering or leaving the switch through a port that is an untagged member of the outbound VLAN does not have this field in its header and thus does not carry a VID or an 802.1p priority. See also “802.1p priority”.</td>
</tr>
<tr>
<td>codepoint</td>
<td>Refer to DSCP, below.</td>
</tr>
<tr>
<td>downstream device</td>
<td>A device linked directly or indirectly to an outbound switch port. That is, the switch sends traffic to downstream devices.</td>
</tr>
<tr>
<td>DSCP</td>
<td><strong>Differentiated Services Codepoint.</strong> (Also termed codepoint.) A DSCP is comprised of the upper six bits of the ToS (Type-of-Service) byte in IP packets. There are 64 possible codepoints. In the default QoS configuration for the switches covered in this guide, some codepoints are configured with default 802.1p priority settings for Assured-Forwarding and Expedited Forwarding. All other codepoints are unused (and listed with <strong>No-override</strong> for a priority).</td>
</tr>
<tr>
<td>DSCP policy</td>
<td>A DSCP configured with a specific 802.1p priority (0-7). (Default: <strong>No-override</strong>). Using a DSCP policy, you can configure the switch to assign priority to IP packets. That is, for an IP packet identified by the specified classifier, you can assign a new DSCP and an 802.1p priority (0-7). For more on DSCP, refer to “Details of QoS IP Type-of-Service” on page 5-36. For the DSCP map, see figure 5-19 on page 5-37.</td>
</tr>
<tr>
<td>edge switch</td>
<td>In the QoS context, this is a switch that receives traffic from the edge of the LAN or from outside the LAN and forwards it to devices within the LAN. Typically, an edge switch is used with QoS to recognize packets based on classifiers such as TCP/UDP application type, IP-device (address), Protocol (LAN), VLAN-ID (VID), and Source-Port (although it can also be used to recognize packets on the basis of ToS bits). Using this packet recognition, the edge switch can be used to set 802.1p priorities or DSCP policies that downstream devices will honor.</td>
</tr>
<tr>
<td>inbound port</td>
<td>Any port on the switch through which traffic enters the switch.</td>
</tr>
<tr>
<td>IP Options</td>
<td>In an IPv4 packet, optional, these are extra fields in the packet header.</td>
</tr>
<tr>
<td>IP-precedence bits</td>
<td>The upper three bits in the Type of Service (ToS) field of an IP packet.</td>
</tr>
<tr>
<td>IPv4</td>
<td>Version 4 of the IP protocol.</td>
</tr>
<tr>
<td>outbound packet</td>
<td>A packet leaving the switch through any LAN port.</td>
</tr>
<tr>
<td>outbound port</td>
<td>Any port on the switch through which traffic leaves the switch.</td>
</tr>
</tbody>
</table>
Quality of Service (QoS): Managing Bandwidth More Effectively

Introduction

<table>
<thead>
<tr>
<th>Term</th>
<th>Use in This Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>outbound port queue</td>
<td>For any port, a buffer that holds outbound traffic until it can leave the switch through that port. There are four outbound queues for each port in the switch. Queue 8 is the highest priority queue; queue 1 is the lowest priority queue. Traffic in a port’s high priority queue leaves the switch before any traffic in the port’s medium or low priority queues.</td>
</tr>
<tr>
<td>re-marking (DSCP re-marking)</td>
<td>Assigns a new QoS policy to an outbound packet by changing the DSCP bit settings in the ToS byte.</td>
</tr>
<tr>
<td>tagged port membership</td>
<td>Identifies a port as belonging to a specific VLAN and enables VLAN-tagged packets belonging to that VLAN to carry an 802.1p priority setting when outbound from that port. Where a port is an untagged member of a VLAN, outbound packets belonging to that VLAN do not carry an 802.1p priority setting.</td>
</tr>
<tr>
<td>Type-of-Service (ToS) byte</td>
<td>Comprised of a three-bit (high-order) precedence field and a five-bit (low-order) Type-of-Service field. Later implementations may use this byte as a six-bit (high-order) Differentiated Services field and a two-bit (low-order) reserved field. See also “IP-precedence bits” and DSCP elsewhere in this table.</td>
</tr>
<tr>
<td>upstream device</td>
<td>A device linked directly or indirectly to an inbound switch port. That is, the switch receives traffic from upstream devices.</td>
</tr>
</tbody>
</table>

Overview

QoS settings operate on two levels:

- **Controlling the priority of outbound packets moving through the switch:** Each switch port has four outbound traffic queues; queue one has the lowest priority and queue four has the highest priority. Packets leave the switch port on the basis of their queue assignment and whether any higher queues are empty:

<table>
<thead>
<tr>
<th>Port Queue and 802.1p Priority Values</th>
<th>Priority for Exiting From the Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low (1)</td>
<td>Fourth</td>
</tr>
<tr>
<td>Normal (0, 3)</td>
<td>Third</td>
</tr>
<tr>
<td>Medium (4 - 5)</td>
<td>Second</td>
</tr>
<tr>
<td>High (6 - 7)</td>
<td>First</td>
</tr>
</tbody>
</table>

A QoS configuration enables you to set the outbound priority queue to which a packet is sent. (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 forwarding queues in the switch.)
Configuring a priority for outbound packets and a service (priority) policy for use by downstream devices:

- **DSCP Policy:** This feature enables you to set a priority policy in outbound IP packets. (You can configure downstream devices to read and use this policy.) This method is not dependent on VLAN-tagged ports to carry priority policy to downstream devices, and can:
  - Change the codepoint (the upper six bits) in the ToS byte.
  - Set a new 802.1p priority for the packet.

  (Setting DSCP policies requires IPv4 inbound packets. Refer to the “IPv4” entry under “Terminology” on page 5-6.)

- **802.1p Priority Rules:** An outbound, VLAN-tagged packet carries an 802.1p priority setting that was configured (or preserved) in the switch. This priority setting ranges from 0 to 7, and can be used by downstream devices having up to eight outbound port queues. Thus, while packets within the switch move at the four priority levels shown in Table 5-1, above, they still can carry an 802.1p priority that can be used by downstream devices having more or less than the four priority levels in the switches covered in this guide. Also, if the packet enters the switch with an 802.1p priority setting, QoS can override this setting if configured with an 802.1p priority rule to do so.

**Notes**

If your network uses only one VLAN (and therefore does not require VLAN-tagged ports) you can still preserve 802.1p priority settings in your traffic by configuring the ports as tagged VLAN members on the links between devices you want to honor traffic priorities.

**Rule and Policy Limits:** The switches covered in this guide allow up to **400** 802.1p priority rules and/or DSCP policies in any combination. For more information, refer to “Maximum QoS Configuration Entries” under “QoS Operating Notes and Restrictions” on page 5-61.

You can configure a QoS priority of 0 through 3 for an outbound packet. When the packet is then sent to a port, the QoS priority determines which outbound queue the packet uses:
Table 5-2. QoS Priority Settings and Operation

<table>
<thead>
<tr>
<th>QoS Priority Setting</th>
<th>Outbound Port Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 2</td>
<td>low priority</td>
</tr>
<tr>
<td>0 - 3</td>
<td>normal priority</td>
</tr>
<tr>
<td>4 - 5</td>
<td>medium priority</td>
</tr>
<tr>
<td>6 - 7</td>
<td>high priority</td>
</tr>
</tbody>
</table>

If a packet is not in a VLAN-tagged port environment, then the QoS settings in table 5-2 control only to which outbound queue the packet goes. Without VLAN tagging, no 802.1p priority is added to the packet for downstream device use. But if the packet is in a VLAN-tagged environment, then the above setting is also added to the packet as an 802.1p priority for use by downstream devices and applications (shown in table 5-3). In either case, an IP packet can also carry a priority policy to downstream devices by using DSCP-marking in the ToS byte.

5-3. Mapping Switch QoS Priority Settings to Device Queues

<table>
<thead>
<tr>
<th>Priority Setting</th>
<th>Outbound Port Queues in the Switch</th>
<th>802.1p Priority Setting Added to Tagged VLAN Packets Leaving the Switch</th>
<th>Queue Assignment in Downstream Devices With:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Queue 1</td>
<td>1 (low priority)</td>
<td>Queue 1</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>2</td>
<td>Queue 2</td>
</tr>
<tr>
<td>0</td>
<td>Queue 2</td>
<td>0 (normal priority)</td>
<td>Queue 3</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>3</td>
<td>Queue 4</td>
</tr>
<tr>
<td>4</td>
<td>Queue 3</td>
<td>4 (medium priority)</td>
<td>Queue 5</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>5</td>
<td>Queue 6</td>
</tr>
<tr>
<td>6</td>
<td>Queue 4</td>
<td>6 (high priority)</td>
<td>Queue 7</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>7</td>
<td>Queue 8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Classifiers for Prioritizing Outbound Packets

ProCurve recommends that you configure a minimum number of the available QoS classifiers for prioritizing any given packet type. Increasing the number of active classifier options for a packet type increases the complexity of the possible outcomes and consumes switch resources.

Packet Classifiers and Evaluation Order

The switches covered in this guide provide six QoS classifiers (packet criteria) you can use to configure QoS priority.

Table 5-4. Classifier Search Order and Precedence

<table>
<thead>
<tr>
<th>Search Order</th>
<th>Precedence</th>
<th>QoS Classifier Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 (highest)</td>
<td>UDP/TCP Application Type (port)</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Device Priority (destination or source IP address)</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>IP Type of Service (ToS) field (IP packets only)</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>Protocol Priority (IP, IPX, ARP, AppleTalk, SNA, and NetBeui)</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>VLAN Priority</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>Incoming source-port on the switch</td>
</tr>
<tr>
<td>7</td>
<td>7 (lowest)</td>
<td>Incoming 802.1p priority (present in tagged VLAN environments)</td>
</tr>
</tbody>
</table>

Where multiple classifier types are configured, a switch uses the highest-to-lowest search order shown in table 5-4 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 that classifier and the packet is handled accordingly.

Note that on the switches covered in this guide, if the switch is configured with multiple classifiers that address the same packet, the switch uses only the QoS configuration for the QoS classifier that has the highest precedence. In this case, the QoS configuration for another, lower-precedence classifier that may apply is ignored. For example, if QoS assigns high priority to packets belonging to VLAN 100, but normal priority to all IP protocol packets, since protocol priority (4) has precedence over VLAN priority (5), IP protocol packets on VLAN 100 will be set to normal priority.
Preparation for Configuring QoS

Preserving 802.1p Priority

QoS operates in VLAN-tagged and VLAN-untagged environments. If your network does not use multiple VLANs, you can still implement the 802.1Q VLAN capability for packets to carry their 802.1p priority to the next downstream device. To do so, configure ports as VLAN-tagged members on the links between switches and routers in your network infrastructure.

Table 5-5. Summary of QoS Capabilities

<table>
<thead>
<tr>
<th>Outbound Packet Options</th>
<th>Port Membership in VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Tagged</td>
</tr>
<tr>
<td>Control Port Queue Priority for Packet Types</td>
<td>Yes</td>
</tr>
<tr>
<td>Carry 802.1p Priority Assignment to Next Downstream Device</td>
<td>Yes</td>
</tr>
<tr>
<td>Carry DSCP Policy to Downstream Devices. The policy includes:</td>
<td>Yes ¹</td>
</tr>
<tr>
<td>Assigning a ToS Codepoint</td>
<td></td>
</tr>
<tr>
<td>Assigning an 802.1p Priority ² to the Codepoint</td>
<td></td>
</tr>
</tbody>
</table>

¹ Except for non-IPv4 packets or packets processed using either the Layer 3 Protocol or QoS IP-Precedence methods, which do not include the DSCP policy option. Also, to use a service policy in this manner, the downstream devices must be configured to interpret and use the DSCP carried in the IP packets.

² This priority corresponds to the 802.1p priority scheme and is used to determine the packet’s port queue priority. When used in a VLAN-tagged environment, this priority is also assigned as the 802.1p priority carried outbound in packets having an 802.1Q field in the header.

Steps for Configuring QoS on the Switch

1. Determine the QoS policy you want to implement. This includes analyzing the types of traffic flowing through your network and identifying one or more traffic types to prioritize. In order of QoS precedence, these are:
   a. UDP/TCP applications
   b. Device Priority—destination or source IP address (Note that destination has precedence over source. See Table 5-6.)
   c. IP Type-of-Service Precedence Bits (Leftmost three bits in the ToS field of IP packets)
   d. IP Type-of-Service Differentiated Service bits (Leftmost six bits in the ToS field of IP packets)
   e. Protocol Priority
Quality of Service (QoS): Managing Bandwidth More Effectively

Preparation for Configuring QoS

f. VLAN Priority (requires at least one tagged VLAN on the network)
g. Source-Port
h. Incoming 802.1p Priority (requires at least one tagged VLAN on the network)

2. Select the QoS option you want to use. Table 5-6 lists the traffic types (QoS classifiers) and the QoS options you can use for prioritizing or setting a policy on these traffic types:

Table 5-6. Applying QoS Options to Traffic Types Defined by QoS Classifiers

<table>
<thead>
<tr>
<th>QoS Options for Prioritizing Outbound Traffic</th>
<th>QoS Classifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UDP/ TCP</td>
</tr>
<tr>
<td>Option 1: Configure 802.1p Priority Rules Only</td>
<td>Prioritize traffic by sending specific packet types (determined by QoS classifier) to different outbound port queues on the switch.</td>
</tr>
<tr>
<td></td>
<td>Rely on VLAN-tagged ports to carry packet priority as an 802.1p value to downstream devices.</td>
</tr>
<tr>
<td>Option 2: Configure ToS DSCP Policies with 802.1p Priorities</td>
<td>Prioritize traffic by sending specific packet types (determined by QoS classifier) to different outbound port queues on the switch.</td>
</tr>
<tr>
<td></td>
<td>Propagate a service policy by reconfiguring the DSCP in outbound IP packets according to packet type. The packet is placed in an outbound port queue according to the 802.1p priority configured for that DSCP policy. (The policy assumes that downstream devices can be configured to recognize the DSCP in IP packets and implement the service policy it indicates.)</td>
</tr>
<tr>
<td></td>
<td>Use VLAN-tagged ports to include packet priority as an 802.1p value to downstream devices.</td>
</tr>
</tbody>
</table>

1 In this mode the configuration is fixed. You cannot change the automatic priority assignment when using IP-ToS Precedence as a QoS classifier.

3. If you want 802.1p priority settings to be included in outbound packets, ensure that tagged VLANs are configured on the appropriate downstream links.
4. Determine the actual QoS configuration changes you will need to make on each QoS-capable device in your network in order to implement the desired policy. Also, if you want downstream devices to read and use DSCPs in IP packets from the switch, configure them to do so by enabling ToS Differentiated Service mode and making sure the same DSCP policies are configured.

**Demonstrating How the Switch Uses Resources in DSCP Configurations.** In the default configuration, the DSCP map is configured with one DSCP policy (Expedited Forwarding; 101110 with a “7” priority) but, because no ToS Diff-Services options are configured, no rules are used. If ToS Diff-Services mode is enabled, then one rule is immediately used for this codepoint. Adding a new DSCP policy (for example, 001111 with a “5” priority) and then configuring ToS Diff-Services to assign inbound packets with a codepoint of 001010 to the 001111 policy implements all policies configured in the DSCP map and, in this case, uses three rules; one for each codepoint invoked in the switch’s current DSCP configuration (101110-the default, 001111, and 001010). Adding another Diff-Services assignment, such as assigning inbound packets with a codepoint of 000111 to the Expedited Forwarding policy (101110), would use one more rule on all ports.

**Using QoS Classifiers To Configure Quality of Service for Outbound Traffic**

<table>
<thead>
<tr>
<th>QoS Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP/TCP Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-15</td>
<td>Refer to Online Help.</td>
</tr>
<tr>
<td>IP-Device Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-21</td>
<td>&quot;</td>
</tr>
<tr>
<td>IP Type-of-Service Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-27</td>
<td>&quot;</td>
</tr>
<tr>
<td>Protocol Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-39</td>
<td>&quot;</td>
</tr>
<tr>
<td>VLAN-ID Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-41</td>
<td>&quot;</td>
</tr>
<tr>
<td>Source-Port Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 5-47</td>
<td>&quot;</td>
</tr>
</tbody>
</table>

**Note**

In addition to the information in this section on the various QoS classifiers, refer to “QoS Operating Notes and Restrictions” on page 5-61.
Viewing the QoS Configuration

All of these commands are available on the switches covered in this guide. Examples of the `show qos` output are included with the example for each priority type.

**Syntax:** `show qos < priority-classifier >`

- **tcp-udp-port-priority**
  
  Displays the current TCP/UDP port priority configuration. Refer to figure 5-7 on page 5-21.

- **device-priority**
  
  Displays the current device (IP address) priority configuration. Refer to figure 5-8 on page 5-23.

- **type-of-service**
  
  Displays the current type-of-service priority configuration. The display output differs according to the ToS option used:

  - **IP Precedence:** Refer to figure 5-12 on page 5-28.
  - **Diffserve:** Refer to figure 5-14 on page 5-32.

- **protocol-priority**
  
  Displays the current protocol priority configuration.

- **vlan-priority**
  
  Displays the current VLAN priority configuration. Refer to figure 5-22 on page 5-43.

- **port-priority**
  
  Displays the current source-port priority configuration. Refer to figure 5-27 on page 5-48.

- **dscp-map**
  
  Displays mappings between DSCP policy and 802.1p priority.

No Override

By default, the IP ToS, Protocol, VLAN-ID, and (source) port `show` outputs automatically list **No-override** for priority options that have not been configured. This means that if you do not configure a priority for a specific option, QoS does not prioritize packets to which that option applies, resulting in the **No override** state. In this case, IP packets received through a VLAN-tagged port
receive whatever 802.1p priority they carry in the 802.1Q tag in the packet’s header. VLAN-Tagged packets received through an untagged port are handled in the switch with “normal” priority.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No-override</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>22</td>
<td>Priority</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>33</td>
<td>DSCP</td>
<td>00010</td>
<td>6</td>
</tr>
</tbody>
</table>

This output shows that VLAN 1 is in the default state, while VLANs 22 and 33 have been configured for 802.1p and DSCP Policy priorities respectively.

Figure 5-3. Example of the Show QoS Output for VLAN Priority

**QoS UDP/TCP Priority**

**QoS Classifier Precedence:** 1

When you use UDP or TCP and a layer 4 Application port number as a QoS classifier, traffic carrying the specified UDP/TCP port number(s) is marked with the UDP/TCP classifier’s configured priority level, without regard for any other QoS classifiers in the switch.

**Note**

UDP/TCP QoS applications are supported only for IPv4 packets only. For more information on packet-type restrictions, refer to “Details of Packet Criteria and Restrictions for QoS Support”, on page 5-61.

**Options for Assigning Priority.** Priority control options for TCP or UDP packets carrying a specified TCP or UDP port number include:

- 802.1p priority
- DSCP policy (Assigning a new DSCP and an associated 802.1p priority; inbound packets must be IPv4.)

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. You can have up to 30 rules maximum for all TCP or UDP ports with assigned priorities.
TCP/UDP Port Number Ranges. There are three ranges:

- Well-Known Ports: 0 - 1023
- Registered Ports: 1024 - 49151
- Dynamic and/or 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

Then click on:

Protocol Number Assignment Services

P (Under “Directory of General Assigned Numbers” heading)

Port Numbers

Assigning an 802.1p Priority Based on TCP or UDP Port Number

This option assigns an 802.1p priority to (IPv4) TCP or UDP packets as described below.

**Syntax:** qos < udp-port | tcp-port > < tcp or udp port number > priority < 0 - 7 >

Configures an 802.1p priority for outbound packets having the specified TCP or UDP application port number. 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.

(Default: Disabled)

no qos < udp-port | tcp-port > < tcp-udp port number >

Deletes the specified UDP or TCP port number as a QoS classifier.

show qos tcp-udp-port-priority

Displays a listing of all TCP and UDP QoS classifiers currently in the running-config file.
For example, configure and list 802.1p priority for the following UDP and TCP port prioritization:

<table>
<thead>
<tr>
<th>TCP/UDP Port</th>
<th>802.1p Priority for TCP</th>
<th>802.1p Priority for UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port 23 (Telnet)</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>UDP Port 23 (Telnet)</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>TCP Port 80 (World Wide Web HTTP)</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>UDP Port 80 (World Wide Web HTTP)</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

```sh
ProCurve(config)# qos tcp-port 23 priority 7
ProCurve(config)# qos udp-port 23 priority 7
ProCurve(config)# qos tcp-port 80 priority 2
ProCurve(config)# qos udp-port 80 priority 1
ProCurve(config)# show qos tcp-udp-port-priority
```

TCP/UDP port based priorities

<table>
<thead>
<tr>
<th>Application</th>
<th>Protocol</th>
<th>port</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP</td>
<td>TCP</td>
<td>23</td>
<td>Priority</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>UDP</td>
<td>23</td>
<td>Priority</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>TCP</td>
<td>80</td>
<td>Priority</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>UDP</td>
<td>80</td>
<td>Priority</td>
<td>7</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 5-4. Example of Configuring and Listing 802.1p Priority Assignments on TCP/UDP Ports
Assigning a DSCP Policy Based on TCP or UDP Port Number

The switches covered in this guide do not support DSCP policies on IPv4 packets with IP options. For more information on packet-type restrictions, refer to “Details of Packet Criteria and Restrictions for QoS Support”, on page 5-61.

This option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to (IPv4) TCP or UDP packets having the specified port number. That is, the switch:

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 5-4, above).
2. Overwrites (re-marks) the packet’s DSCP with the DSCP configured in the switch for such packets.
3. Assigns the 802.1p priority configured in the switch for the new DSCP. (Refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.)
4. Forwards the packet through the appropriate outbound port queue.

For more on DSCP, refer to “Terminology” on page 5-6.

**Steps for Creating a DSCP Policy Based on TCP/UDP Port Number Classifiers.** This procedure creates a DSCP policy for IPv4 packets carrying the selected UDP or TCP 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.
   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. Configure the DSCP policy by using `qos dscp-map` to configure the priority to the codepoint you selected in step 2a. (For details, refer to the example later in this section, and to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.)
A codepoint must have an 802.1p priority assignment (0 - 7) before you can configure a policy for prioritizing packets by TCP or UDP port numbers. If a codepoint you want to use shows No-override in the Priority column of the DSCP map (show qos dscp-map), then you must assign a 0 - 7 priority before proceeding.

4. Configure the switch to assign the DSCP policy to packets with the specified TCP or UDP port number.

**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 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 IPv4 packets, the DSCP will be replaced by the codepoint specified in this command. (Default: No-override for most codepoints. See table 5-9 on page 5-53.)

**Syntax:** qos < udp-port | tcp-port > < tcp or udp port number > dscp < codepoint >

Assigns a DSCP policy to outbound packets having the specified TCP or UDP application port number and overwrites the DSCP in these packets with the assigned <codepoint> value. This policy includes an 802.1p priority and determines the packet's queue in the outbound port to which it is sent. (The <codepoint> must be configured with an 802.1p setting. See step 3 on page 5-18.) 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)

no qos < udp-port | tcp-port > < tcp-udp port number >

Deletes the specified UDP or TCP port number as a QoS classifier.

show qos tcp-udp-port-priority

Displays a listing of all TCP and UDP QoS classifiers currently in the running-config file.
For example, suppose you wanted to assign these DSCP policies to the packets identified by the indicated UDP and TDP port applications:

<table>
<thead>
<tr>
<th>Port Applications</th>
<th>DSCP Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DSCP</td>
</tr>
<tr>
<td>23-UDP</td>
<td>000111</td>
</tr>
<tr>
<td>80-TCP</td>
<td>000101</td>
</tr>
<tr>
<td>914-TCP</td>
<td>000010</td>
</tr>
<tr>
<td>1001-UDP</td>
<td>000010</td>
</tr>
</tbody>
</table>

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. (Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

```
ProCurve(config)# show qos dscp-map
DSCP --> 802.1p priority mappings
DSCP policy 802.1p tag  Policy name
------------ -------------- ---------------
000000  No-override
000001  No-override
000010  No-override
000011  No-override
000100  No-override
000101  No-override
000110  No-override
000111  No-override
.
.
The DSCPs for this example have not yet been assigned an 802.1p priority level.
```

**Figure 5-5. Display the Current DSCP-Map Configuration**

2. Configure the DSCP policies for the codepoints you want to use.

```
ProCurve(config)# qos dscp-map 000111 priority 7
ProCurve(config)# qos dscp-map 000101 priority 5
ProCurve(config)# qos dscp-map 000010 priority 1
ProCurve(config)# show qos dscp-map
DSCP --> 802.1p priority mappings
DSCP policy 802.1p tag  Policy name
------------ -------------- ---------------
000000  No-override
000001  No-override
000010  1
000011  No-override
000100  No-override
000101  5
000110  No-override
000111  7
001000  No-override
.
```

**Figure 5-6. Assign Priorities to the Selected DSCPs**
3. Assign the DSCP policies to the selected UDP/TCP port applications and display the result.

```yaml
ProCurve(config)# qos udp-port 23 dscp 000111
ProCurve(config)# qos tcp-port 80 dscp 000101
ProCurve(config)# qos tcp-port 914 dscp 000010
ProCurve(config)# qos udp-port 1001 dscp 000010
ProCurve(config)# show qos tcp-udp-port-priority
```

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>23</td>
<td>DSCP</td>
<td>000111</td>
<td>7</td>
</tr>
<tr>
<td>TCP</td>
<td>80</td>
<td>DSCP</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>TCP</td>
<td>914</td>
<td>DSCP</td>
<td>000010</td>
<td>1</td>
</tr>
<tr>
<td>UDP</td>
<td>1001</td>
<td>DSCP</td>
<td>(000010)</td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure 5-7. The Completed DSCP Policy Configuration for the Specified UDP/TCP Port Applications**

The switch will now apply the DSCP policies in figure 5-7 to IPV4 packets received in the switch with the specified UDP/TCP port applications. 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 selected packets.

**QoS IP-Device Priority**

**QoS Classifier Precedence: 2**

The IP device option, which applies only to IPv4 packets, enables you to use up to 256 IP addresses (source or destination) as QoS classifiers.

Where a particular device-IP address classifier has the highest precedence in the switch for traffic addressed to or from that device, then traffic received on the switch with that address is marked with the IP address classifier’s configured priority level. Different IP device classifiers can have differing priority levels.
The switch does not allow a QoS IP-device priority for the Management VLAN IP address, if configured. If there is no Management VLAN configured, then the switch does not allow configuring a QoS IP-device priority for the Default VLAN IP address.

IP address QoS does not support layer-2 SAP encapsulation. For more information on packet-type restrictions, refer to table 5-10, “Details of Packet Criteria and Restrictions for QoS Support”, on page 5-61.

**Options for Assigning Priority.** Priority control options for packets carrying a specified IP address include:

- 802.1p priority
- DSCP policy (Assigning a new DSCP and an 802.1p priority; inbound packets must be IPv4.)

(For operation when other QoS classifiers apply to the same traffic, refer to “Classifiers for Prioritizing Outbound Packets” on page 5-10.)

For a given IP address, you can use only one of the above options at a time. However, for different IP addresses, you can use different options.

**Assigning a Priority Based on IP Address**

This option assigns an 802.1p priority to all IPv4 packets having the specified IP address as either a source or destination. (If both match, the priority for the IP destination address has precedence.)

**Syntax:** `qos device-priority < ip-address > priority < 0 - 7 >`

`Configure an 802.1p priority for outbound packets having the specified IP address. 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. (Default: Disabled)`

`no qos device-priority < ip-address >`

`Removes the specified IP device-priority QoS classifier and resets the priority for that VLAN to No-override.`

`show qos device-priority`

`Displays a listing of all IP device-priority QoS classifiers currently in the running-config file.`
For example, configure and list the 802.1p priority for packets carrying the following IP addresses:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>802.1p Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.28.31.1</td>
<td>7</td>
</tr>
<tr>
<td>10.28.31.130</td>
<td>5</td>
</tr>
<tr>
<td>10.28.31.100</td>
<td>1</td>
</tr>
<tr>
<td>10.28.31.101</td>
<td>1</td>
</tr>
</tbody>
</table>

![Figure 5-8. Example of Configuring and Listing 802.1p Priority Assignments for Packets Carrying Specific IP Addresses](image)

Assigning a DSCP Policy Based on IP Address

**Note**

On the switches covered in this guide, DSCP policies cannot be applied to IPv4 packets having IP options. For more information on packet criteria and restrictions, refer to table 5-10 on page 5-61.

This option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to outbound IP packets having the specified IP address (either source or destination). That is, the switch:

1. Selects an incoming IPv4 packet on the basis of the source or destination IP address it carries.
2. Overwrites the packet’s DSCP with the DSCP configured in the switch for such packets, and assigns the 802.1p priority configured in the switch for the new DSCP. (Refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.)
3. Forwards the packet through the appropriate outbound port queue.
Steps for Creating a Policy Based on IP Address. This procedure creates a DSCP policy for IPv4 packets carrying the selected IP address (source or destination).

1. Identify the IP 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. Configure the DSCP policy by using **dscp-map** to configure the priority to the codepoint you selected in step 2a. (For details, refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.)

**Notes**

A codepoint must have an 802.1p priority assignment (0 - 7) before you can configure a policy for prioritizing packets by IP address. If a codepoint you want to use shows **No-override** in the **Priority** column of the DSCP map (**show qos dscp-map**), then you must assign a 0 - 7 priority before proceeding.

On the switches covered in this guide, DSCP policies cannot be applied to IPv4 packets having IP options. For more information on packet criteria and restrictions, refer to 5-10 on page 5-61.

4. Configure the switch to assign the DSCP policy to packets with the specified IP address.

**Syntax:**  
```
qos dscp-map < codepoint > priority < 0 - 7 >
```

This command is optional if a priority is already 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 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. If the packet is IPv4, the packet’s DSCP will be replaced by the codepoint specified in this command. (Default: For most codepoints, **No-override**. See figure 5-9 on page 5-53.)
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

Syntax:  qos device-priority < ip-address > dscp < codepoint>

Assigns a DSCP policy to packets carrying the specified IP address, and overwrites the DSCP in these packets with the assigned < codepoint > value. This 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)

no qos device-priority < ip-address >

Deletes the specified IP address as a QoS classifier.

show qos device-priority

Displays a listing of all QoS Device Priority classifiers currently in the running-config file.

For example, suppose you wanted to assign these DSCP policies to the packets identified by the indicated IP addresses:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>DSCP Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DSCP</td>
</tr>
<tr>
<td>10.28.31.1</td>
<td>000111</td>
</tr>
<tr>
<td>10.28.31.130</td>
<td>000101</td>
</tr>
<tr>
<td>10.28.31.100</td>
<td>000010</td>
</tr>
<tr>
<td>10.28.31.101</td>
<td>000010</td>
</tr>
</tbody>
</table>

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. This is not a problem if the configured priorities are acceptable for all applications using the same DSCP. (Refer to the “Note On Changing a Priority Setting” on page 5-55. Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

```
ProCurve(config)# show qos dscp-map
DSCP -> 802.p priority mappings
DSCP policy 802.1p tag  Policy name
--------------------  --------  ------------------------------
0000000  No-override
0000001  No-override
      000010  No-override
      000011  No-override
      000100  No-override
      000101  No-override
      000110  No-override
      000111  No-override

The DSCPs for this example have not yet been assigned an 802.1p priority level.
```

Figure 5-9. Display the Current DSCP-Map Configuration
2. Configure the priorities for the DSCPs you want to use.

```
ProCurve(config)# qos dscp-map 000111 priority 7
ProCurve(config)# qos dscp-map 000101 priority 5
ProCurve(config)# qos dscp-map 000010 priority 1
ProCurve(config)# show qos dscp-map
DSCP -> 802.1p priority mappings
DSCP policy 802.1p tag Policy name
----------------- ---------------
000000  No-override
000001  No-override
000010  1
000011  No-override
000100  No-override
000101  5
000110  No-override
000111  7
001000  No-override
```

![DSCP Policies Configured in this step.](image)

**Figure 5-10. Assigning 802.1p Priorities to the Selected DSCPs**

3. Assign the DSCP policies to the selected device IP addresses and display the result.

```
ProCurve(config)# qos device-priority 10.28.31.1 dscp 000111
ProCurve(config)# qos device-priority 10.28.31.130 dscp 000101
ProCurve(config)# qos device-priority 10.28.31.100 dscp 000010
ProCurve(config)# qos device-priority 10.28.31.101 dscp 000010
ProCurve(config)# show qos device-priority
Device priorities
<table>
<thead>
<tr>
<th>Device Address</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.28.31.1</td>
<td>DSCP</td>
<td>000111</td>
<td>7</td>
</tr>
<tr>
<td>10.28.31.130</td>
<td>DSCP</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>10.28.31.100</td>
<td>DSCP</td>
<td>000010</td>
<td>1</td>
</tr>
<tr>
<td>10.28.31.101</td>
<td>DSCP</td>
<td>000010</td>
<td>1</td>
</tr>
</tbody>
</table>
```

**Figure 5-11. The Completed Device-Priority/Codepoint Configuration**

The switch will now apply the DSCP policies in figure 5-10 to IPv4 packets received on the switch with the specified IP addresses (source or destination). 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.
QoS IP Type-of-Service (ToS) Policy and Priority

QoS Classifier Precedence: 3

You can assign a maximum of 64 ToS rules. This feature applies only to IPv4 traffic and performs either of the following:

- **ToS IP-Precedence Mode**: All IP packets generated by upstream devices and applications include precedence bits in the ToS byte. Using this mode, the switch uses these bits to compute and assign the corresponding 802.1p priority.

- **ToS Differentiated Services (Diffserv) Mode**: This mode requires knowledge of the codepoints set in IP packets by the upstream devices and applications. It uses the ToS codepoint in IP packets coming from upstream devices and applications to assign 802.1p priorities to the packets. You can use this option to do both of the following:
  
  - **Assign a New Prioritization Policy**: A “policy” includes both a codepoint and a corresponding 802.1p priority. This option selects an incoming IPv4 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—page 5-52.)
  
  - **Assign an 802.1p Priority**: This option reads the DSCP of an incoming IPv4 packet and, without changing this codepoint, assigns the 802.1p priority to the packet, as configured in the DSCP Policy Table (page 5-52). This means that a priority value of 0 - 7 must be configured for a DSCP before the switch will attempt to perform a QoS match on the packet’s DSCP bits.

Before configuring the ToS Diffserv mode, you must use the `dscp-map` command to configure the desired 802.1p priorities for the codepoints you want to use for either option. This command is illustrated in the following examples and is described under “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.

Unless IP-Precedence mode and Diffserv mode are both disabled (the default setting), enabling one automatically disables the other. For more on ToS operation, refer to “Details of QoS IP Type-of-Service” on page 5-36.
Assigning an 802.1p Priority to IPv4 Packets on the Basis of the ToS Precedence Bits

If a device or application upstream of the switch sets the precedence bits in the ToS byte of IPv4 packets, you can use this feature to apply that setting for prioritizing 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 IPv4 packets by computing each 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 ip-precedence is enabled (or if neither ToS option is configured), shows the ToS configuration status. If diff-services is enabled, lists codepoint data as described under “Assigning a DSCP Policy on the Basis of the DSCP in IPv4 Packets Received from Upstream Devices” on page 5-33.*

With this option, 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:

```
ProCurve(config)# qos type-of-service ip-precedence
ProCurve(config)# show qos type-of-service
    Type of Service [Disabled] : IP Precedence
```

![Figure 5-12. Example of Enabling ToS IP-Precedence Prioritization](image)
To replace this option with the ToS diff-services option, just configure `diff-services` as described below, which automatically disables IP-Precedence. To disable IP-Precedence without enabling the diff-services option, use this command:

```
ProCurve(config)# no qos type-of-service
```

**Assigning an 802.1p Priority to IPv4 Packets on the Basis of Incoming DSCP**

One of the best uses for this option is on an interior switch where you want to honor (continue) a policy set on an edge switch. That is, it enables you to select incoming packets having a specific DSCP and forward 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 5-13. Interior Switch “B” Honors the Policy Established in Edge Switch “A”](image)

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 IPv4 packet carrying one of these codepoints, it assigns the configured priority to the packet and sends it out the appropriate priority 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 (described later in this section), as long as the DSCPs specified in the two options do not match.
Operating Notes

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 packets you want 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 criteria:

- 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.

To use this option:

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. Use qos dscp-map < codepoint > priority < 0 - 7 > to assign the 802.1p priority you want to the specified DSCP. (For more on this topic, refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.)
4. Enable diff-services
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

**Syntax:** qos type-of-service diff-services < codepoint >

*Causes the switch to read the < codepoint > (DSCP) of an incoming IPv4 packet and, when a match occurs, assign a corresponding 802.1p priority, as configured in the switch’s DSCP table (page 5-53).*

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 5-14 you cannot change the priority for the 000000 codepoint until you redirect the DSCP policy for 000001 away from using 000000 as a policy. (Refer to “Note On Changing a Priority Setting” on page 5-55. Refer also to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.)*

show qos type-of-service

*Displays current Type-of-Service configuration. In diffserv mode it also shows the current direct 802.1p assignments and the current DSCP assignments covered later in this section.*

For example, 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`.

```
ProCurve(config)# show qos type-of-service
Type of Service [Disabled] : Disabled

<table>
<thead>
<tr>
<th>Codepoint</th>
<th>DSCP Policy</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td>000000</td>
<td>1</td>
</tr>
<tr>
<td>000001</td>
<td>No-override</td>
<td>1</td>
</tr>
<tr>
<td>000010</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>000011</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>000100</td>
<td>001001</td>
<td>5</td>
</tr>
<tr>
<td>000101</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>000110</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>001000</td>
<td>No-override</td>
<td>5</td>
</tr>
<tr>
<td>001001</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>001010</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>001011</td>
<td>No-override</td>
<td></td>
</tr>
</tbody>
</table>

Executing this command displays the current ToS configuration and shows that the selected DSCP is not currently in use.

The 000110 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 5-14. Example Showing Codepoints Available for Direct 802.1p Priority Assignments
```

```
ProCurve(config)# qos dscp-map 000110 priority 7
ProCurve(config)# qos type-of-service diff-services
ProCurve(config)# show qos type-of-service
Type of Service [Disabled] : Differentiated Services

<table>
<thead>
<tr>
<th>Codepoint</th>
<th>DSCP Policy</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td>000000</td>
<td>1</td>
</tr>
<tr>
<td>000001</td>
<td>No-override</td>
<td>1</td>
</tr>
<tr>
<td>000010</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>000011</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>000100</td>
<td>001001</td>
<td>5</td>
</tr>
<tr>
<td>000101</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>000110</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>001011</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>001000</td>
<td>No-override</td>
<td>5</td>
</tr>
<tr>
<td>001001</td>
<td>No-override</td>
<td></td>
</tr>
</tbody>
</table>

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 000110 respectively). This means they are not available for changing to a different 802.1p priority.

Figure 5-15. Example of a Type-of-Service Configuration Enabling Both Direct 802.1p Priority Assignment and DSCP Policy Assignment
Assigning a DSCP Policy on the Basis of the DSCP in IPv4 Packets Received from Upstream Devices

The preceding section describes how to forward a policy set by an edge (or upstream) switch. This option changes a DSCP policy in an IPv4 packet by changing its IP ToS codepoint and applying the priority associated with the new codepoint. (A DSCP policy consists of a differentiated services codepoint and an associated 802.1p priority.) You can use this option concurrently with the diffserv 802.1p priority option (above), as long as the DSCPs specified in the two options do not match.

To use this option to configure a change in policy:

1. Identify a DSCP used to set a policy in packets received from an upstream or edge switch.
2. Create a new policy by using `qos dscp-map < codepoint > priority < 0 - 7 >` to configure an 802.1p priority for the codepoint you will use to overwrite the DSCP the packet carries from upstream. (For more on this topic, refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.)
3. Use `qos type-of-service diff-services < incoming-DSCP > dscp < outgoing-DSCP >` to change the policy on packets coming from the edge or upstream switch with the specified incoming DSCP.

   (Figure 5-13 on page 5-29 illustrates this scenario.)

**Note**

On the switches covered in this guide, DSCP policies (codepoint re-marking) cannot be applied to outbound IPv4 packets having IP options. (The 802.1p priority in the VLAN tag is applied.) For more information on packet criteria and restrictions, refer to 5-10 on page 5-61.
**Quality of Service (QoS): Managing Bandwidth More Effectively**

Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

**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. (Use the qos dscp-map command to define the priority for the DSCPs—page 5-52.)

**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. (This will be 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 re-assignments for outbound packets. Also lists the (802.1p) priority for each codepoint that does not have a DSCP policy assigned to it.

For example, suppose you want to configure the following two DSCP policies for packets received with the indicated DSCPs.

<table>
<thead>
<tr>
<th>Received DSCP</th>
<th>Policy DSCP</th>
<th>802.1p Priority</th>
<th>Policy Name (Optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>001100</td>
<td>000010</td>
<td>6</td>
<td>Level 6</td>
</tr>
<tr>
<td>001101</td>
<td>000101</td>
<td>4</td>
<td>Level 4</td>
</tr>
</tbody>
</table>

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. This is not a problem as long as the configured priorities are acceptable for all applications using the
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

same DSCP. (Refer to the “Note On Changing a Priority Setting” on page 5-55. Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

```
ProCurve(config)# show qos dscp-map
DSCP -> 802.1p priority mappings
DSCP policy 802.1p tag Policy name

The DSCPs for this example have not yet been assigned an 802.1p priority level.
```

Figure 5-16. Display the Current DSCP-Map Configuration

2. Configure the policies in the DSCP table:

```
ProCurve(config)# qos dscp-map 000010 priority 6 name 'Level 6'
ProCurve(config)# qos dscp-map 000101 priority 4 name 'Level 4'
```

```
ProCurve(config)# show qos dscp-map
DSCP -> 802.1p priority mappings
DSCP policy 802.1p tag Policy name

The DSCPs for this example have not yet been assigned an 802.1p priority level.
```

Figure 5-17. Example of Policies Configured (with Optional Names) in the DSCP Table
3. Assign the policies to the codepoints in the selected packet types.

```
ProCurve(config)# qos type-of-service diff-services 001100 dscp 000010
ProCurve(config)# qos type-of-service diff-services 001101 dscp 000101
ProCurve(config)# show qos type-of-service
Type of Service [Disabled] : Differentiated Services

<table>
<thead>
<tr>
<th>Codepoint</th>
<th>DSCP Policy</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td></td>
<td>No-override</td>
</tr>
<tr>
<td>000001</td>
<td></td>
<td>No-override</td>
</tr>
<tr>
<td>000010</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>000011</td>
<td></td>
<td>No-override</td>
</tr>
<tr>
<td>000100</td>
<td></td>
<td>No-override</td>
</tr>
<tr>
<td>000101</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>000110</td>
<td></td>
<td>No-override</td>
</tr>
<tr>
<td>000111</td>
<td></td>
<td>No-override</td>
</tr>
<tr>
<td>001000</td>
<td></td>
<td>No-override</td>
</tr>
<tr>
<td>001010</td>
<td></td>
<td>No-override</td>
</tr>
<tr>
<td>001011</td>
<td></td>
<td>No-override</td>
</tr>
<tr>
<td>001100</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>
| 001101    | 000010      | 6
| 001110    |             | No-override          |
| 001111    |             | No-override          |
| 010000    |             | No-override          |
| 010001    |             | No-override          |

-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

Figure 5-18. Example of Policy Assignment to Outbound Packets on the Basis of the DSCP in the Packets Received from Upstream Devices

**Details of QoS IP Type-of-Service**

IP packets include a Type of Service (ToS) byte. The ToS byte includes:

- **A Differentiated Services Codepoint (DSCP):** This element is comprised of the upper six bits of the ToS byte. There are 64 possible codepoints.
  - In the switches covered in this guide, the default qos configuration includes some codepoints with 802.1p priority settings for Assured-Forwarding and Expedited Forwarding (codepoint 101110), while others are unused (and listed with No-override for a Priority).

Refer to figure 5-9 on page 5-53 for an illustration of the default DSCP policy table.

Using the `qos dscp map` command, you can configure the switch to assign different prioritization policies to IPv4 packets having different codepoints. As an alternative, you can configure the switch to assign a new codepoint to an IPv4 packet, along with a corresponding 802.1p priority (0-7). To use this option in the simplest case, you would:

a. Configure a specific DSCP with a specific priority in an edge switch.
b. Configure the switch to mark a specific type of inbound traffic with that DSCP (and thus create a policy for that traffic type).

c. 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, refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.

■ Precedence Bits: This element is a subset of the DSCP and is comprised of the upper three bits of the ToS byte. When configured to do so, the switch uses the precedence bits to determine a priority for handling the associated packet. (The switch does not change the setting of the precedence bits.) Using the ToS Precedence bits to prioritize IPv4 packets relies on priorities set in upstream devices and applications.

Figure 5-19 shows an example of the ToS byte in the header for an IPv4 packet, and illustrates the diffserv bits and precedence bits in the ToS byte. (Note that the Precedence bits are a subset of the Differentiated Services bits.)

<table>
<thead>
<tr>
<th>Field: Destination MAC Address</th>
<th>Source MAC Address</th>
<th>802.1Q Field</th>
<th>Type &amp; Version</th>
<th>ToS Byte</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet: FF FF FF FF FF FF</td>
<td>08 00 09 00 00 16</td>
<td>08 00</td>
<td>45</td>
<td>E 0</td>
<td>...</td>
</tr>
</tbody>
</table>

Figure 5-19. The ToS Codepoint and Precedence Bits
5-7. How the Switch Uses the ToS Configuration

<table>
<thead>
<tr>
<th>Outbound Port</th>
<th>ToS Option:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>802.1p (Value = 0 - 7)</td>
</tr>
</tbody>
</table>

IP Packet Sent Out an Untagged Port in a VLAN

- Depending on the value of the IP Precedence bits in the packet’s ToS field, the packet will go to one of four outbound port queues in the switch:
  - 1 - 2 = low priority
  - 0 - 3 = normal priority
  - 4 - 5 = medium priority
  - 6 - 7 = high priority

  For a given packet carrying a ToS codepoint that the switch has been configured to detect:
  - Change the codepoint according to the configured policy and assign the 802.1p priority specified for the new codepoint in the DSCP Policy Table (page 5-52).
  - Do not change the codepoint, but assign the 802.1p priority specified for the existing codepoint in the DSCP Policy Table (page 5-52).

  Depending on the 802.1p priority used, the packet will leave the switch through one of the following queues:
  - 1 - 2 = low priority
  - 0 - 3 = normal priority
  - 4 - 5 = medium priority
  - 6 - 7 = high priority

  If No-override (the default) has been configured for a specified codepoint, then the packet is not prioritized by ToS and, by default, is sent to the “normal priority” queue.

Table 5-8. ToS IP-Precedence Bit Mappings to 802.1p Priorities

<table>
<thead>
<tr>
<th>ToS Byte IP Precedence Bits</th>
<th>Corresponding 802.1p Priority</th>
<th>Service Priority Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>1</td>
<td>Lowest</td>
</tr>
<tr>
<td>001</td>
<td>2</td>
<td>Low</td>
</tr>
<tr>
<td>002</td>
<td>0</td>
<td>Normal</td>
</tr>
<tr>
<td>003</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>004</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>005</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>006</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>007</td>
<td>7</td>
<td>Highest</td>
</tr>
</tbody>
</table>
Assigning a Priority Based on Layer-3 Protocol

When QoS on the switch is configured with a Layer-3 protocol as the highest-precedence classifier and the switch receives traffic carrying that protocol, then this traffic is assigned the priority configured for this classifier. (For operation when other QoS classifiers apply to the same traffic, refer to “Classifiers for Prioritizing Outbound Packets” on page 5-10.)

**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 >
```

*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.*

For example:

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.
Figure 5-20 shows the command sequence and displays for the above steps.

```
ProCurve(config)# qos protocol ip priority 0
ProCurve(config)# qos protocol appletalk priority 7
ProCurve(config)# qos protocol arp priority 5

ProCurve(config)# show qos protocol
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>0</td>
</tr>
<tr>
<td>IPX</td>
<td>No-override</td>
</tr>
<tr>
<td>ARP</td>
<td>5</td>
</tr>
<tr>
<td>DEC_LAT</td>
<td>No-override</td>
</tr>
<tr>
<td>AppleTalk</td>
<td>7</td>
</tr>
<tr>
<td>SNA</td>
<td>No-override</td>
</tr>
<tr>
<td>NetBEUI</td>
<td>No-override</td>
</tr>
</tbody>
</table>

ProCurve(config)# no qos protocol ip
ProCurve(config)# qos protocol arp priority 4

ProCurve(config)# show qos protocol
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>No-override</td>
</tr>
<tr>
<td>IPX</td>
<td>No-override</td>
</tr>
<tr>
<td>ARP</td>
<td>4</td>
</tr>
<tr>
<td>DEC_LAT</td>
<td>No-override</td>
</tr>
<tr>
<td>AppleTalk</td>
<td>7</td>
</tr>
<tr>
<td>SNA</td>
<td>No-override</td>
</tr>
<tr>
<td>NetBEUI</td>
<td>No-override</td>
</tr>
</tbody>
</table>
```

Figure 5-20. Adding, Displaying, Removing, and Changing QoS Protocol Classifiers
QoS VLAN-ID (VID) Priority

QoS Classifier Precedence: 5

The QoS protocol precedence option enables you to use up to 256 VIDs as QoS classifiers. Where a particular VLAN-ID classifier has the highest precedence in the switch for traffic in that VLAN, then traffic received in that VLAN is marked with the VID classifier's configured priority level. Different VLAN-ID classifiers can have differing priority levels.

Options for Assigning Priority. Priority control options for packets carrying 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 operation when other QoS classifiers apply to the same traffic, refer to “Classifiers for Prioritizing Outbound Packets” on page 5-10.)

Note

QoS with VID priority applies to static VLANs only, and applying QoS to dynamic VLANs created by GVRP operation is not supported. A VLAN must exist while a subject of a QoS configuration, and eliminating a VLAN from the switch causes the switch to clear any QoS features configured for that VID.

Assigning a Priority Based on VLAN-ID

This 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)

**Syntax**: no vlan <vid> qos

Removes the specified VLAN-ID as a QoS classifier and resets the priority for that VLAN to No-override.

**Syntax**: show qos vlan-priority

Displays a listing of the QoS VLAN-ID classifiers currently in the running-config file, with their priority data.

1. For example, suppose that you have the following VLANs configured on the switch and want to prioritize them as shown:

```
ProCurve(config)# show vlan
Status and Counters - VLAN Information
Maximum VLANs to support : 8
Primary VLAN : DEFAULT_VLAN

<table>
<thead>
<tr>
<th>Set Priority To 2</th>
<th>802.1Q VLAN ID</th>
<th>Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>DEFAULT_VLAN</td>
<td>Static</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>VLAN_20</td>
<td>Static</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>VLAN_30</td>
<td>Static</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>VLAN_40</td>
<td>Static</td>
</tr>
</tbody>
</table>
```

*Figure 5-21. Example of a List of VLANs Available for QoS Prioritization*
2. You would then execute the following commands to prioritize the VLANs by VID:

```
ProCurve(config)# vlan 1 qos priority 2
ProCurve(config)# vlan 20 qos priority 5
ProCurve(config)# vlan 30 qos priority 5
ProCurve(config)# vlan 40 qos priority 7

ProCurve(config)# show qos vlan
```

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Priority</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Priority</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Priority</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Priority</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 5-22. Configuring and Displaying QoS Priorities on VLANs**

If you then decided to remove VLAN_20 from QoS prioritization:

```
ProCurve(config)# no vlan 20 qos
ProCurve(config)# show qos vlan
```

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Priority</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>No-override</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Priority</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Priority</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 5-23. Returning a QoS-Prioritized VLAN to “No-override” Status**

**Assigning a DSCP Policy Based on VLAN-ID (VID)**

This option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to outbound IP packets having the specified VLAN-ID (VID). That is, 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 in the switch for such packets.
3. Assigns the 802.1p priority configured in the switch for the new DSCP. (Refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.)
4. Forwards the packet through the appropriate outbound port queue.

For more on DSCP, refer to “Terminology” on page 5-6.
Steps for Creating a Policy Based on 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. Configure the DSCP policy by using `qos dscp-map` to configure the priority for each codepoint. (For details, see the example later in this section, and to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.)

   **Note**

   A codepoint must have an 802.1p priority (0 - 7) before you can configure the codepoint for use in prioritizing packets by VLAN-ID. If a codepoint you want to use shows No-override in the Priority column of the DSCP Policy table (`show qos dscp-map`), then assign a priority before proceeding.

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. If the packet is IPv4, the packet's DSCP will be replaced by the codepoint specified in this command. (Default: For most codepoints, No-override. See figure 5-9 on page 5-53 on page 5-53.)*
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

Syntax: vlan < vid > qos dscp < codepoint>

Assigns a DSCP policy to packets carrying the specified VLAN-ID, and overwrites the DSCP in these packets with the assigned < codepoint > value. This 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 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.

For example, suppose you wanted to assign this set of priorities:

<table>
<thead>
<tr>
<th>VLAN-ID</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>000111</td>
<td>7</td>
</tr>
<tr>
<td>30</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>20</td>
<td>000010</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>000010</td>
<td>1</td>
</tr>
</tbody>
</table>

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. This is not a problem as long as the configured priorities are acceptable for all applications using the same DSCP. (Refer to the "Note On Changing a Priority Setting" on page 5-55. Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

The DSCPs for this example have not yet been assigned an 802.1p priority level.

Figure 5-24. Display the Current Configuration in the DSCP Policy Table
2. Configure the priorities for the DSCPs you want to use.

![Figure 5-25. Assign Priorities to the Selected DSCPs]

3. Assign the DSCP policies to the selected VIDs and display the result.

![Figure 5-26. The Completed VID-DSCP Priority Configuration]

The switch will now apply the DSCP policies in figure 5-26 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.
QoS Source-Port Priority

QoS Classifier Precedence: 6

The QoS source-port option enables you to use a packet’s source-port on the switch as a QoS classifier. Where a particular source-port classifier has the highest precedence in the switch for traffic entering through that port, then traffic received from the port is marked with the source-port classifier’s configured priority level. Different source-port classifiers can have different priority levels.

Options for Assigning Priority on the Switch. Priority control options for packets from a specified source-port include:

- 802.1p priority
- DSCP policy (Assigning a new DSCP and an associated 802.1p priority; inbound packets must be IPv4.)

(For operation when other QoS classifiers apply to the same traffic, refer to “Classifiers for Prioritizing Outbound Packets” on page 5-10.)

Options for Assigning Priority From a RADIUS Server. You can use a RADIUS server to impose a QoS source-port priority during an 802.1X port-access authentication session. Refer to the RADIUS chapter in the Access Security Guide for your switch (August 2006 or later).

Assigning a Priority Based on Source-Port

This option assigns a priority to all outbound packets having the specified source-port. You can configure this option 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. (If you are configuring multiple source-ports with the same priority, you may find it 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 port(s) 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> qos

Disables use of the specified source-port(s) for QoS classifier(s) and resets the priority for the specified source-port(s) to No-override.

Syntax: show qos port-priority

Lists the QoS port-priority classifiers with their priority data.

For example, suppose that you want to prioritize inbound traffic on the following source-ports:

<table>
<thead>
<tr>
<th>Source-Port</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 - A3</td>
<td>2</td>
</tr>
<tr>
<td>A4</td>
<td>3</td>
</tr>
<tr>
<td>B1, B4</td>
<td>5</td>
</tr>
<tr>
<td>C1-C3</td>
<td>6</td>
</tr>
</tbody>
</table>

You would then execute the following commands to prioritize traffic received on the above ports:

ProCurve(config)# interface e c1-c3 qos priority 6
ProCurve(config)# interface e b1,b4 qos priority 5
ProCurve(config)# interface e a4 qos priority 3
ProCurve(config)# interface e a1-a3 qos priority 2
ProCurve(config)# show qos port-priority

Figure 5-27. Configuring and Displaying Source-Port QoS Priorities
If you then decided to remove port A1 from QoS prioritization:

```
ProCurve(config)# no interface e a1 qos
ProCurve(config)# show qos port-priority

<table>
<thead>
<tr>
<th>Port</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
<th>Radius Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>No-override</td>
<td>None</td>
<td>No-override</td>
<td>No-override</td>
</tr>
<tr>
<td>A2</td>
<td>Priority</td>
<td>2</td>
<td>No-override</td>
<td>No-override</td>
</tr>
<tr>
<td>A3</td>
<td>Priority</td>
<td>2</td>
<td>No-override</td>
<td>No-override</td>
</tr>
<tr>
<td>A4</td>
<td>Priority</td>
<td>3</td>
<td>No-override</td>
<td>No-override</td>
</tr>
</tbody>
</table>
```

Figure 5-28. Returning a QoS-Prioritized VLAN to “No-override” Status

Assigning a DSCP Policy Based on the Source-Port

This option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to outbound IP packets (received from the specified source-ports). That is, the switch:

1. Selects an incoming IP packet on the basis of its source-port on the switch.
2. Overwrites the packet’s DSCP with the DSCP configured in the switch for such packets.
3. Assigns the 802.1p priority configured in the switch for the new DSCP. (Refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.)
4. Forwards the packet through the appropriate outbound port queue.

For more on DSCP, refer to “Terminology” on page 5-6.

**Steps for Creating a Policy Based on Source-Port Classifiers.**

**Note**

You can select one DSCP per source-port. Also, configuring a new DSCP for a source-port automatically overwrites (replaces) any previous DSCP or 802.1p priority configuration for that port.)

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. Configure the DSCP policy by using `qos dscp-map` to configure the priority for each codepoint. (For details, refer to the example later in this section and to “Differentiated Services Codepoint (DSCP) Mapping” on page 5-52.)

**Note**

A codepoint must have an 802.1p priority assignment (0 - 7) before you can configure that codepoint as a criteria for prioritizing packets by source-port. If a codepoint shows **No-override** in the **Priority** column of the DSCP Policy Table (show qos dscp-map), then you must assign a 0 - 7 priority before proceeding.

4. Configure the switch to assign the DSCP policy to packets from the specified source-port.

**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. (Default: For most codepoints, **No-override**. See figure 5-9 on page 5-53 on page 5-53.)*

**Syntax:** `interface < port-list > qos dscp < codepoint >`

*Assigns a DSCP policy to packets from the specified source-port(s), and overwrites the DSCP in these packets with the assigned `< codepoint >` value. This 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 QoS classifier for the specified source-port(s).*

**Syntax:** `show qos source-port`

*Displays a listing of all source-port QoS classifiers currently in the running-config file.*
For example, suppose you wanted to assign this set of priorities:

<table>
<thead>
<tr>
<th>Source-Port</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2</td>
<td>000111</td>
<td>7</td>
</tr>
<tr>
<td>B1-B3</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>B4, C2</td>
<td>000010</td>
<td>1</td>
</tr>
</tbody>
</table>

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. This is not a problem as long as the configured priorities are acceptable for all applications using the same DSCP. (Refer to the “Note On Changing a Priority Setting” on page 5-55. Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

The DSCPs for this example have not yet been assigned an 802.1p priority level.

2. Configure the priorities for the DSCPs you want to use.
3. Assign the DSCP policies to the selected source-ports and display the result.

```
ProCurve(eth-A2)# int e b4,c2
ProCurve(eth-B4,C2)# qos dscp 000010
ProCurve(eth-B4,C2)# int e b1-b3
ProCurve(eth-B1-B3)# qos dscp 000101
ProCurve(eth-B1-B3)# int e a2
ProCurve(eth-A2)# qos dscp 000111
ProCurve(eth-A2)# show qos port-priority
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
<th>Radius Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>No-override</td>
<td></td>
<td>No-override</td>
<td>No-override</td>
</tr>
<tr>
<td>A2</td>
<td>DSCP</td>
<td>000111</td>
<td>7</td>
<td>No-override</td>
</tr>
<tr>
<td>A3</td>
<td>No-override</td>
<td></td>
<td>No-override</td>
<td>No-override</td>
</tr>
<tr>
<td>A4</td>
<td>No-override</td>
<td></td>
<td>No-override</td>
<td>No-override</td>
</tr>
<tr>
<td>B1</td>
<td>DSCP</td>
<td>000101</td>
<td>5</td>
<td>No-override</td>
</tr>
<tr>
<td>B2</td>
<td>DSCP</td>
<td>000101</td>
<td>5</td>
<td>No-override</td>
</tr>
<tr>
<td>B3</td>
<td>DSCP</td>
<td>000101</td>
<td>5</td>
<td>No-override</td>
</tr>
<tr>
<td>B4</td>
<td>DSCP</td>
<td>000010</td>
<td>1</td>
<td>No-override</td>
</tr>
<tr>
<td>C1</td>
<td>No-override</td>
<td></td>
<td>No-override</td>
<td>No-override</td>
</tr>
<tr>
<td>C2</td>
<td>DSCP</td>
<td>000010</td>
<td>1</td>
<td>No-override</td>
</tr>
<tr>
<td>C3</td>
<td>No-override</td>
<td></td>
<td>No-override</td>
<td>No-override</td>
</tr>
<tr>
<td>C4</td>
<td>No-override</td>
<td></td>
<td>No-override</td>
<td>No-override</td>
</tr>
</tbody>
</table>

Figure 5-31. The Completed Source-Port DSCP-Priority Configuration

**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. Refer to the RADIUS chapter in the Access Security Guide for your switch (August 2006 or later).

**Differentiated Services Codepoint (DSCP) Mapping**

The DSCP Policy Table associates an 802.1p priority with a specific ToS byte codepoint in an IPv4 packet. This enables you to 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 5-9 on page 5-53.

You can use the following command to list the current DSCP Policy table, change 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, optionally, an identifying (policy) name.*

no qos dscp-map <codepoint>

*Reconfigures the 802.1p priority for <codepoint> to No-override. Also deletes the codepoint policy name, if configured.*

no qos dscp-map <codepoint> name

*Deletes only the policy name, if configured, for <codepoint>.*

---

**Table 5-9. The Default DSCP Policy Table**

<table>
<thead>
<tr>
<th>DSCP Policy</th>
<th>802.1p Priority</th>
<th>DSCP Policy</th>
<th>802.1p Priority</th>
<th>DSCP Policy</th>
<th>802.1p Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td>No-override</td>
<td>010110</td>
<td>3*</td>
<td>101011</td>
<td>No-override</td>
</tr>
<tr>
<td>000001</td>
<td>No-override</td>
<td>010111</td>
<td>No-override</td>
<td>101100</td>
<td>No-override</td>
</tr>
<tr>
<td>000010</td>
<td>No-override</td>
<td>011000</td>
<td>No-override</td>
<td>101101</td>
<td>No-override</td>
</tr>
<tr>
<td>000011</td>
<td>No-override</td>
<td>011001</td>
<td>No-override</td>
<td>101110</td>
<td>7**</td>
</tr>
<tr>
<td>000100</td>
<td>No-override</td>
<td>011010</td>
<td>4*</td>
<td>101111</td>
<td>No-override</td>
</tr>
<tr>
<td>000101</td>
<td>No-override</td>
<td>011101</td>
<td>No-override</td>
<td>110000</td>
<td>No-override</td>
</tr>
<tr>
<td>000110</td>
<td>No-override</td>
<td>011100</td>
<td>4*</td>
<td>110001</td>
<td>No-override</td>
</tr>
<tr>
<td>000111</td>
<td>No-override</td>
<td>011101</td>
<td>No-override</td>
<td>110010</td>
<td>No-override</td>
</tr>
<tr>
<td>001000</td>
<td>No-override</td>
<td>011110</td>
<td>5*</td>
<td>110011</td>
<td>No-override</td>
</tr>
<tr>
<td>001001</td>
<td>No-override</td>
<td>011111</td>
<td>No-override</td>
<td>110100</td>
<td>No-override</td>
</tr>
<tr>
<td>001010</td>
<td>1*</td>
<td>100000</td>
<td>No-override</td>
<td>110101</td>
<td>No-override</td>
</tr>
<tr>
<td>001011</td>
<td>No-override</td>
<td>100001</td>
<td>No-override</td>
<td>110110</td>
<td>No-override</td>
</tr>
<tr>
<td>001100</td>
<td>1*</td>
<td>100010</td>
<td>6*</td>
<td>110111</td>
<td>No-override</td>
</tr>
<tr>
<td>001101</td>
<td>No-override</td>
<td>100011</td>
<td>No-override</td>
<td>111000</td>
<td>No-override</td>
</tr>
<tr>
<td>001110</td>
<td>2*</td>
<td>100100</td>
<td>6*</td>
<td>111001</td>
<td>No-override</td>
</tr>
<tr>
<td>001111</td>
<td>No-override</td>
<td>100101</td>
<td>No-override</td>
<td>111010</td>
<td>No-override</td>
</tr>
<tr>
<td>010000</td>
<td>No-override</td>
<td>100110</td>
<td>7*</td>
<td>111011</td>
<td>No-override</td>
</tr>
<tr>
<td>010001</td>
<td>No-override</td>
<td>100111</td>
<td>No-override</td>
<td>111100</td>
<td>No-override</td>
</tr>
<tr>
<td>010010</td>
<td>0*</td>
<td>101000</td>
<td>No-override</td>
<td>111101</td>
<td>No-override</td>
</tr>
<tr>
<td>010011</td>
<td>No-override</td>
<td>101001</td>
<td>No-override</td>
<td>111110</td>
<td>No-override</td>
</tr>
<tr>
<td>010100</td>
<td>0*</td>
<td>101010</td>
<td>No-override</td>
<td>111111</td>
<td>No-override</td>
</tr>
<tr>
<td>010101</td>
<td>No-override</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

<table>
<thead>
<tr>
<th>DSCP Policy</th>
<th>802.1p Priority</th>
<th>DSCP Policy</th>
<th>802.1p Priority</th>
<th>DSCP Policy</th>
<th>802.1p Priority</th>
</tr>
</thead>
</table>
| *Assured Forwarding codepoints; configured by default on the switches covered in this guide. These codepoints are configured as "No-override" in the Series 3400cl, Series 6400cl and Series 2600/2800 switches. **Expedited Forwarding codepoint configured by default.

Default Priority Settings for Selected Codepoints

In a few cases, such as 001010 and 001100, a default 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 `qos dscp-map < codepoint > priority < 0 - 7 >`. (These policies are not in effect unless you have either applied the policies to a QoS classifier or configured QoS Type-of-Service to be in `diff-services` mode.)

Quickly Listing Non-Default Codepoint Settings

Table 5-9 lists the switch's default codepoint/priority settings. If you change the priority of any codepoint setting to a non-default value and then execute `write memory`, the switch will list the non-default setting in the show config display. For example, in the default configuration, the following codepoint settings are true:

<table>
<thead>
<tr>
<th>Codepoint</th>
<th>Default Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>001100</td>
<td>1</td>
</tr>
<tr>
<td>001101</td>
<td>No-override</td>
</tr>
<tr>
<td>001110</td>
<td>2</td>
</tr>
</tbody>
</table>

If you change all three settings to a priority of 3, and then execute `write memory`, the switch will reflect these changes in the show config listing:
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

Configure these three codepoints with non-default priorities.

Show config lists the non default codepoint settings.

Figure 5-32. Example of Show Config Listing with Non-Default Priority Settings in the DSCP Table

Effect of “No-override”. In the QoS Type-of-Service differentiated services mode, a No-override assignment for the codepoint of an outbound packet means that QoS is effectively disabled for such packets. That is, QoS does not affect the packet queuing priority or VLAN tagging. In this case, the packets are handled as follows (as long as no other QoS feature creates priority assignments for them):

<table>
<thead>
<tr>
<th>802.1Q Status</th>
<th>Outbound 802.1p Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received and Forwarded on a tagged port member of a VLAN.</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Received on an Untagged port member of a VLAN; Forwarded on a tagged port member of a VLAN.</td>
<td>0 (zero)—&quot;normal&quot;</td>
</tr>
<tr>
<td>Forwarded on an Untagged port member of a VLAN.</td>
<td>None</td>
</tr>
</tbody>
</table>

Note On Changing a Priority Setting

If a QoS classifier is using a policy (codepoint and associated priority) in the DSCP Policy table, you must delete or change this usage before you can change the priority setting on the codepoint. Otherwise the switch blocks the change and displays this message:

Cannot modify DSCP Policy < codepoint > - in use by other qos rules.

In this case, use show qos < classifier> to identify the specific classifiers using the policy you want to change; that is:
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

```
show qos device-priority
show qos port-priority
show qos tcp-udp-port-priority
show qos vlan-priority
show qos type-of-service
```

For example, suppose that the 000001 codepoint has a priority of 6, and several classifiers use the 000001 codepoint to assign a priority to their respective types of traffic. If you wanted to change the priority of codepoint 000001 you would do the following:

1. Identify which QoS classifiers use the codepoint.
2. Change the classifier configurations by assigning them to a different DSCP policy, or to an 802.1p priority, or to **No-override**.
3. Reconfigure the desired priority for the 000001 codepoint.
4. Either reassign the classifiers to the 00001 codepoint policy or leave them as they were after step 2, above.

**Example of Changing the Priority Setting on a Policy When One or More Classifiers Are Currently Using the Policy**

Suppose that codepoint 000001 is in use by one or more classifiers. If you try to change its priority, you see a result similar to the following:

```
ProCurve(config)# qos dscp-map 000001 priority 2
Cannot modify DSCP Policy 000001 — in use by other qos rules.
```

**Figure 5-33. Example of Trying To Change the Priority on a Policy In Use by a Classifier**

In this case, you would use steps similar to the following to change the priority.

1. Identify which classifiers use the codepoint you want to change.
Three classifiers use the codepoint that is to be changed.

Figure 5-34. Example of a Search to Identify Classifiers Using a Codepoint You Want To Change
2. Change the classifier configurations by assigning them to a different DSCP policy, or to an 802.1p priority, or to **No-override**. For example:
   a. Delete the policy assignment for the **device-priority** classifier. (That is, assign it to **No-override**.)
   b. Create a new DSCP policy to use for re-assigning the remaining classifiers.
   c. Assign the **port-priority** classifier to the new DSCP policy.
   d. Assign the **udp-port 1260** classifier to an 802.1p priority.

   ```
   (a) ProCurve(config)# no qos device-priority 10.26.50.104
   (b) ProCurve(config)# qos dscp-map 000100 priority 6
   (c) ProCurve(config)# int e a3 qos dscp 000100
   (d) ProCurve(config)# qos udp-port 1260 priority 2
   ```

3. Reconfigure the desired priority for the 000001 codepoint.
   ```
   ProCurve(config)# qos dscp-map 000001 priority 4
   ```

4. You could now re-assign the classifiers to the original policy codepoint or leave them as currently configured.
IP Multicast (IGMP) Interaction with QoS

IGMP high-priority-forward causes the switch to service the subscribed IP multicast group traffic at high priority, even if QoS on the switch has relegated the traffic to a lower priority. This does not affect any QoS priority settings, so the QoS priority is honored by downstream devices. However, QoS does take precedence over IGMP normal-priority traffic.

The switch’s ability to prioritize IGMP traffic for either a normal or high priority outbound queue overrides any QoS criteria, and does not affect any 802.1p priority settings the switch may assign. For a given packet, if both IGMP high priority and QoS are configured, the QoS classification occurs and the switch marks the packet for downstream devices, but the packet is serviced by the high-priority queue when leaving the switch.

<table>
<thead>
<tr>
<th>IGMP High Priority</th>
<th>QoS Configuration Affects Packet</th>
<th>Switch Port Output Queue</th>
<th>Outbound 802.1p Setting (Requires Tagged VLAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Enabled</td>
<td>Yes</td>
<td>Determined by QoS</td>
<td>Determined by QoS</td>
</tr>
<tr>
<td>Enabled</td>
<td>See above paragraph.</td>
<td>High</td>
<td>As determined by QoS if QoS is active.</td>
</tr>
</tbody>
</table>
# QoS Messages in the CLI

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP Policy <code>&lt; decimal-codepoint &gt;</code> not configured</td>
<td>You have attempted to map a QoS classifier to a codepoint for which there is no configured priority (<strong>No-override</strong>). Use the <code>qos dscp-map</code> command to configure a priority for the codepoint, then map the classifier to the codepoint.</td>
</tr>
<tr>
<td>Cannot modify DSCP Policy <code>&lt; codepoint &gt;</code> - in use by other qos rules.</td>
<td>You have attempted to map a QoS classifier to a codepoint that is already in use by other QoS classifiers. Before remapping the codepoint to a new priority, you must reconfigure the other QoS classifiers so that they do not use this codepoint. You can have multiple QoS classifiers use this same codepoint as long as it is acceptable for all such classifiers to use the same priority.</td>
</tr>
</tbody>
</table>
QoS Operating Notes and Restrictions

5-10. Details of Packet Criteria and Restrictions for QoS Support

<table>
<thead>
<tr>
<th>Packet Criteria or Restriction</th>
<th>UDP/TCP</th>
<th>Device Priority (IP Address)</th>
<th>IP Type-of-Service</th>
<th>Layer 3 Protocol</th>
<th>VLAN</th>
<th>Source Port</th>
<th>Incoming 802.1p</th>
<th>DSCP Overwrite (Re-Marking)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted to IPv4 Packets Only</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow Packets with IP Options¹</td>
<td>Yes</td>
<td>Yes²</td>
<td>Yes²</td>
<td>Yes²</td>
<td>Ye²³</td>
<td>Yes²</td>
<td>Yes²</td>
<td>No</td>
</tr>
<tr>
<td>Support IPv6 Packets¹</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Support Layer-2 SAP Encapsulation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

¹For explicit QoS support of IPv6 packets, force IPv6 traffic into its own set of VLANs and then configure VLAN-based classifiers for those VLANs.

²On IPv4 packets with IP options, the switches covered in this guide support QoS for 802.1p priority policies, but does not do any DSCP re-marking for DSCP policies.

- **All Switches:** For explicit QoS support of IP subnets, ProCurve 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, refer to chapter 2, “Static Virtual LANs (VLANs)”.

**Maximum QoS Configuration Entries:** The switches covered in this guide accept the maximum outbound priority and/or DSCP policy configuration entries shown in table 5-11.
Table 5-11. Maximum QoS Entries.

<table>
<thead>
<tr>
<th>Switch</th>
<th>Software Version</th>
<th>Maximum QoS Entries</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 2900</td>
<td>T.11.XX</td>
<td>400*</td>
<td>• Each device (IP address) QoS configuration uses two entries.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Each TCP/UDP port QoS configuration uses four entries.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• All other classifier configurations use one entry each.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*Configuring device (IP address) or TCP/UDP QoS entries reduces this maximum. See the “Notes” column.</td>
</tr>
</tbody>
</table>

Attempting to exceed the above limits generates the following message in the CLI:

Unable to add this QoS rule.

- **Non-Supported IP Packets:** The DSCP policy codepoint-remarking operation is not supported in any QoS classifier for packets carrying IP options in the packet header.

- **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.

- **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, refer to the appendix titled “Monitoring Resources” in the *Management and Configuration Guide* for your switch.
# Stack Management

## Contents

### Introduction to Stack Management

- Stacking Support on ProCurve Switches ........................................ 6-3
- Components of ProCurve Stack Management .................................. 6-5
- General Stacking Operation ......................................................... 6-5
- Operating Rules for Stacking ...................................................... 6-7
  - General Rules ........................................................................... 6-7
  - Specific Rules ........................................................................... 6-8

### Configuring Stack Management .................................................. 6-9

- Overview of Configuring and Bringing Up a Stack ......................... 6-9
  - General Steps for Creating a Stack ............................................. 6-11
- Using the Menu Interface To View Stack Status and Configure Stacking .................................................. 6-13
  - Using the Menu Interface To View and Configure a Commander Switch ............................................. 6-13
  - Using the Menu To Manage a Candidate Switch ......................... 6-15
- Using the Commander To Manage The Stack ................................ 6-17
  - Using the Commander To Access Member Switches for Configuration Changes and Monitoring Traffic ............................................. 6-23
  - Converting a Commander or Member to a Member of Another Stack .................................................. 6-25
- Monitoring Stack Status .............................................................. 6-25
- Using the CLI To View Stack Status and Configure Stacking ............ 6-30
  - Using the CLI To View Stack Status ............................................. 6-32
  - Using the CLI To Configure a Commander Switch ...................... 6-34
  - Adding to a Stack or Moving Switches Between Stacks ............... 6-36
  - Using the CLI To Remove a Member from a Stack ....................... 6-41
  - Using the CLI To Access Member Switches for Configuration Changes and Traffic Monitoring .................. 6-43
SNMP Community Operation in a Stack .......................... 6-44
Using the CLI To Disable or Re-Enable Stacking .................. 6-45
Transmission Interval .............................................. 6-45
Stacking Operation with Multiple VLANs Configured ............... 6-45
Status Messages .................................................... 6-46
Introduction to Stack Management

ProCurve Stack Management (stacking) enables you to use a single IP address and standard network cabling to manage a group of up to 16 total switches in the same IP subnet (broadcast domain). Using stacking, you can:

■ Reduce the number of IP addresses needed in your network.
■ Simplify management of small workgroups or wiring closets while scaling your network to handle increased bandwidth demand.
■ Eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technologies.
■ Add switches to your network without having to first perform IP addressing tasks.

Stacking Support on ProCurve Switches

As of August 2006, the following ProCurve switches include stacking:

■ ProCurve Series 6400cl
■ ProCurve Series 6200yl
■ ProCurve Series 6108
■ ProCurve Series 4200vl
■ ProCurve Series 4100gl
■ ProCurve Series 3500yl
■ ProCurve Series 3400cl
■ ProCurve Switch 2900
■ ProCurve Series 2810
■ ProCurve Series 2800
■ ProCurve Series 2600
■ ProCurve Series 2500
■ ProCurve Switch 8000M\(^1,2\)
■ ProCurve Switch 4000M\(^1,2\)
■ ProCurve Switch 2424M1\(^1,2\)
■ ProCurve Switch 2400M\(^1,2\)
■ ProCurve Switch 1600M\(^1,2\)

\(^1\)Requires software release C.08.03 or later, which is included with the 8000M, 4000M, 2424M, and 1600M models as of July, 2000. Release C.08.03 or a later version is also available on the ProCurve Networking web site at [www.procurve.com](http://www.procurve.com). (Click on Software updates.)

\(^2\)Discontinued product.
## Summary of Stacking Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>view stack status</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>view status of a single switch</td>
<td>n/a</td>
<td>page 6-26 thru page 6-29</td>
<td>page 6-32</td>
<td>Refer to Online Help</td>
</tr>
<tr>
<td>view candidate status</td>
<td>n/a</td>
<td></td>
<td>page 6-32</td>
<td></td>
</tr>
<tr>
<td>view status of commander and its stack</td>
<td>n/a</td>
<td></td>
<td>page 6-33</td>
<td></td>
</tr>
<tr>
<td>view status of all stacking-enabled switches in the ip subnet</td>
<td>n/a</td>
<td></td>
<td>page 6-33</td>
<td></td>
</tr>
<tr>
<td><strong>configure stacking</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>enable/disable candidate Auto-Join</td>
<td>enabled/Yes</td>
<td>page 6-15</td>
<td>page 6-38</td>
<td></td>
</tr>
<tr>
<td>“push” a candidate into a stack</td>
<td>n/a</td>
<td>page 6-15</td>
<td>page 6-39</td>
<td></td>
</tr>
<tr>
<td>configure a switch to be a commander</td>
<td>n/a</td>
<td>page 6-13</td>
<td>page 6-34</td>
<td></td>
</tr>
<tr>
<td>“push” a member into another stack</td>
<td>n/a</td>
<td>page 6-25</td>
<td>page 6-40</td>
<td></td>
</tr>
<tr>
<td>remove a member from a stack</td>
<td>n/a</td>
<td>page 6-21</td>
<td>page 6-41 or page 6-42</td>
<td></td>
</tr>
<tr>
<td>“pull” a candidate into a stack</td>
<td>n/a</td>
<td>page 6-17</td>
<td>page 6-37</td>
<td></td>
</tr>
<tr>
<td>“pull” a member from another stack</td>
<td>n/a</td>
<td>page 6-19</td>
<td>page 6-39</td>
<td></td>
</tr>
<tr>
<td>convert a commander or member to a member of another stack</td>
<td>n/a</td>
<td>page 6-25</td>
<td>page 6-40</td>
<td></td>
</tr>
<tr>
<td>access member switches for configuration and traffic monitoring</td>
<td>n/a</td>
<td>page 6-23</td>
<td>page 6-43</td>
<td></td>
</tr>
<tr>
<td>disable stacking</td>
<td>enabled</td>
<td>page 6-15</td>
<td>page 6-45</td>
<td></td>
</tr>
<tr>
<td>transmission interval</td>
<td>60 seconds</td>
<td>page 6-13</td>
<td>page 6-45</td>
<td></td>
</tr>
</tbody>
</table>
Components of ProCurve Stack Management

Table 6-1. Stacking Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack</td>
<td>Consists of a Commander switch and any Member switches belonging to that Commander’s stack.</td>
</tr>
<tr>
<td>Commander</td>
<td>A switch that has been manually configured as the controlling device for a stack. When this occurs, the switch’s stacking configuration appears as <strong>Commander</strong>.</td>
</tr>
<tr>
<td>Candidate</td>
<td>A switch that is ready to join (become a Member of) a stack through either automatic or manual methods. A switch configured as a Candidate is not in a stack.</td>
</tr>
<tr>
<td>Member</td>
<td>A switch that has joined a stack and is accessible from the stack Commander.</td>
</tr>
</tbody>
</table>

![Figure 6-1. Illustration of a Switch Moving from Candidate to Member](image)

**General Stacking Operation**

After you configure one switch to operate as the Commander of a stack, additional switches can join the stack by either automatic or manual methods. After a switch becomes a Member, you can work through the Commander switch to further configure the Member switch as necessary for all of the additional software features available in the switch.

The Commander switch serves as the in-band entry point for access to the Member switches. For example, the Commander's IP address becomes the path to all stack Members and the Commander's Manager password controls access to all stack Members.
Use the Commander’s console or web browser interface to access the user interface on any Member switch in the same stack.

**Network Backbone**

**Commander Switch 0**
IP Address: 10.28.227.100
Manager Password: leader

**Member Switch 1**
IP Address: None Assigned
Manager Password: leader

**Candidate Switch**
IP Address: None Assigned
Manager Password: francois

**Non-Member Switch**
IP Address: 10.28.227.105
Manager Password: donald

**Member Switch 2**
IP Address: None Assigned
Manager Password: leader

Figure 6-2. Example of Stacking with One Commander Controlling Access to Wiring Closet Switches

**Interface Options.** You can configure stacking through the switch’s menu interface, CLI, or the web browser interface. For information on how to use the web browser interface to configure stacking, see the online Help for the web browser interface.

**Web Browser Interface Window for Commander Switches.** The web browser interface window for a Commander switch differs in appearance from the same window for non-commander switches.
Operating Rules for Stacking

General Rules

- Stacking is an optional feature (enabled in the default configuration) and can easily be disabled. Stacking has no effect on the normal operation of the switch in your network.

- A stack requires one Commander switch. (Only one Commander allowed per stack.)

- All switches in a particular stack must be in the same IP subnet (broadcast domain). A stack cannot cross a router.

- A stack accepts up to 16 switches (numbered 0-15), including the Commander (always numbered 0).

- The stacking feature supports up to 100 switches in the same IP subnet (broadcast domain), however, a switch can belong to only one stack.

- If multiple VLANs are configured, stacking uses only the primary VLAN on any switch. In the factory-default configuration, the DEFAULT_VLAN is the primary VLAN. (See “Stacking Operation with Multiple VLANs Configured” on page 6-45 and “The Primary VLAN” on page 2-45.)

- Stacking allows intermediate devices that do not support stacking. This enables you to include switches that are distant from the Commander.

---

![Diagram](image-url)

**Figure 6-3. Example of a Non-Stacking Device Used in a Stacking Environment**
Specific Rules

Table 6-2. Specific Rules for Commander, Candidate, and Member Switch

<table>
<thead>
<tr>
<th>Commander</th>
<th>IP Addr: Requires an assigned IP address and mask for access via the network.</th>
<th>Stack Name: Required</th>
<th>Number Allowed Per Stack</th>
<th>Passwords</th>
<th>SNMP Communities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Only one Commander switch is allowed per stack.</td>
<td></td>
<td>The Commander’s Manager and Operator passwords are assigned to any switch becoming a Member of the stack. If you change the Commander’s passwords, the Commander propagates the new passwords to all stack Members.</td>
<td>Standard SNMP community operation. The Commander also operates as an SNMP proxy to Members for all SNMP communities configured in the Commander.</td>
<td></td>
</tr>
<tr>
<td>Candidate</td>
<td>IP Addr: Optional. Configuring an IP address allows access via Telnet or web browser interface while the switch is not a stack member. In the factory default configuration the switch automatically acquires an IP address if your network includes DHCP service. Stack Name: N/A</td>
<td>n/a</td>
<td>Passwords optional. If the Candidate becomes a stack Member, it assumes the Commander’s Manager and Operator passwords. If a candidate has a password, it cannot be automatically added to a stack. In this case, if you want the Candidate in a stack, you must manually add it to the stack.</td>
<td>Uses standard SNMP community operation if the Candidate has its own IP addressing.</td>
<td></td>
</tr>
<tr>
<td>Member</td>
<td>IP Addr: Optional. Configuring an IP address allows access via Telnet or web browser interface without going through the Commander switch. This is useful, for example, if the stack Commander fails and you need to convert a Member switch to operate as a replacement Commander. Stack Name: N/A</td>
<td>Up to 15 Members per stack.</td>
<td>When the switch joins the stack, it automatically assumes the Commander’s Manager and Operator passwords and discards any passwords it may have had while a Candidate. Note: If a Member leaves a stack for any reason, it retains the passwords assigned to the stack Commander at the time of departure from the stack.</td>
<td>Belongs to the same SNMP communities as the Commander (which serves as an SNMP proxy to the Member for communities to which the Commander belongs). To join other communities that exclude the Commander, the Member must have its own IP address. Loss of stack membership means loss of membership in any community that is configured only in the Commander. See “SNMP Community Operation in a Stack” on page 6-44.</td>
<td></td>
</tr>
</tbody>
</table>
In the default stack configuration, the Candidate **Auto Join** parameter is enabled, but the Commander **Auto Grab** parameter is disabled. This prevents Candidates from automatically joining a stack prematurely or joining the wrong stack (if more than one stack Commander is configured in a subnet or broadcast domain). If you plan to install more than one stack in a subnet, ProCurve recommends that you leave **Auto Grab** disabled on all Commander switches and manually add Members to their stacks. Similarly, if you plan to install a stack in a subnet (broadcast domain) where stacking-capable switches are not intended for stack membership, you should set the **Stack State** parameter (in the Stack Configuration screen) to **Disabled** on those particular switches.

---

**Configuring Stack Management**

**Overview of Configuring and Bringing Up a Stack**

This process assumes that:

- All switches you want to include in a stack are connected to the same subnet (broadcast domain).

- If VLANs are enabled on the switches you want to include in the stack, then the ports linking the stacked switches must be on the primary VLAN in each switch (which, in the default configuration, is the default VLAN). If the primary VLAN is tagged, then each switch in the stack must use the same VLAN ID (VID) for the primary VLAN. (Refer to “The Primary VLAN” on page 2-45, and “Stacking Operation with Multiple VLANs Configured” on page 6-45.)

- *If you are including a ProCurve Switch 8000M, 4000M, 2424M, 2400M, or 1600M in a stack, you must first update all such devices to software version C.08.03 or later.* (You can get a copy of the latest software version from the ProCurve Networking web site and/or copy it from one switch to another. For downloading instructions, see appendix A, “File Transfers”, in the *Management and Configuration Guide* for your switch.)
Options for Configuring a Commander and Candidates. Depending on how Commander and Candidate switches are configured, Candidates can join a stack either automatically or by a Commander manually adding (“pulling”) them into the stack. In the default configuration, a Candidate joins only when *manually* pulled by a Commander. You can reconfigure a Commander to *automatically* pull in Candidates that are in the default stacking configuration. You can also reconfigure a Candidate switch to either “push” itself into a particular Commander’s stack, convert the Candidate to a Commander (for a stack that does not already have a Commander), or to operate as a standalone switch without stacking. The following table shows your control options for adding Members to a stack.

**Table 6-3. Stacking Configuration Guide**

<table>
<thead>
<tr>
<th>Join Method1</th>
<th>Commander (IP Addressing Required)</th>
<th>Candidate (IP Addressing Optional)</th>
<th>Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Auto Grab</td>
<td>Auto Join</td>
<td></td>
</tr>
<tr>
<td>Automatically add Candidate to Stack (Causes the first 15 eligible, discovered switches in the subnet to automatically join a stack.)</td>
<td>Yes</td>
<td>Yes <em>(default)</em></td>
<td>No <em>(default)</em>*</td>
</tr>
<tr>
<td>Manually add Candidate to Stack (Prevent automatic joining of switches you don’t want in the stack)</td>
<td>No <em>(default)</em></td>
<td>Yes <em>(default)</em></td>
<td>Optional*</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Optional*</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes <em>(default) or No</em></td>
<td>Configured</td>
</tr>
<tr>
<td>Prevent a switch from being a Candidate</td>
<td>N/A</td>
<td>Disabled</td>
<td>Optional</td>
</tr>
</tbody>
</table>

*The Commander’s Manager and Operator passwords propagate to the candidate when it joins the stack.

The easiest way to *automatically* create a stack is to:

1. Configure a switch as a Commander.
2. Configure IP addressing and a stack name on the Commander.
3. Set the Commander’s Auto Grab parameter to Yes.
4. Connect Candidate switches (in their factory default configuration) to the network.

This approach automatically creates a stack of up to 16 switches (including the Commander). However this replaces manual control with an automatic process that may bring switches into the stack that you did not intend to include. With the Commander’s Auto Grab parameter set to Yes, any switch conforming to all four of the following factors automatically becomes a stack Member:
- Default stacking configuration (Stack State set to Candidate, and Auto Join set to Yes)
- Same subnet (broadcast domain) and default VLAN as the Commander (If VLANs are used in the stack environment, see “Stacking Operation with a Tagged VLAN” on page 6-45.)
- No Manager password
- 14 or fewer stack members at the moment

**General Steps for Creating a Stack**

This section describes the general stack creation process. For the detailed configuration processes, see pages 6-13 through 6-37 for the menu interface and pages 6-30 through 6-42 for the CLI.

1. Determine the naming conventions for the stack. You will need a stack name. Also, to help distinguish one switch from another in the stack, you can configure a unique system name for each switch. Otherwise, the system name for a switch appearing in the Stacking Status screen appears as the stack name plus an automatically assigned switch number. For example:

   ![Stacking Status Screen]

   **Figure 6-4. Using the System Name to Help Identify Individual Switches**
2. Configure the Commander switch. Doing this first helps to establish consistency in your stack configuration, which can help prevent startup problems.
   - A stack requires one Commander switch. If you plan to implement more than one stack in a subnet (broadcast domain), the easiest way to avoid unintentionally adding a Candidate to the wrong stack is to manually control the joining process by leaving the Commander’s **Auto Grab** parameter set to **No** (the default).
   - The Commander assigns its Manager and Operator passwords to any Candidate switch that joins the stack.
   - The Commander’s SNMP community names apply to members.

3. For automatically or manually pulling Candidate switches into a stack, you can leave such switches in their default stacking configuration. If you need to access Candidate switches through your network before they join the stack, assign IP addresses to these devices. Otherwise, IP addressing is optional for Candidates and Members. (Note that once a Candidate becomes a member, you can access it through the Commander to assign IP addressing or make other configuration changes.)

4. Make a record of any Manager passwords assigned to the switches (intended for your stack) that are not currently members. (You will use these passwords to enable the protected switches to join the stack.)

5. If you are using VLANs in the stacking environment, you must use the default VLAN for stacking links. For more information, see “Stacking Operation with a Tagged VLAN” on page 6-45.

6. Ensure that all switches intended for the stack are connected to the same subnet (broadcast domain). As soon as you connect the Commander, it will begin discovering the available Candidates in the subnet.
   - If you configured the Commander to automatically add Members (**Auto Grab = Yes**), the first fifteen discovered Candidates meeting both of the following criteria will automatically join the stack:
     - **Auto Join** parameter set to **Yes** (the default)
     - Manager password not configured
   - If you configured the Commander to manually add Members (**Auto Grab** set to **No**—the default), you can begin the process of selecting and adding the desired Candidates.

7. Ensure that all switches intended for the stack have joined.

8. If you need to do specific configuration or monitoring tasks on a Member, use the console interface on the Commander to access the Member.
Using the Menu Interface To View Stack Status and Configure Stacking

Using the Menu Interface To View and Configure a Commander Switch

1. Configure an IP address and subnet mask on the Commander switch. (Refer to the Management and Configuration Guide for your switch.)

2. Display the Stacking Menu by selecting **Stacking** in the Main Menu.

3. Display the Stack Configuration menu by pressing [3] to select **Stack Configuration**.

![Figure 6-5. The Default Stacking Menu](image)

![Figure 6-6. The Default Stack Configuration Screen](image)
4. Move the cursor to the Stack State field by pressing **[E]** (for **Edit**). Then use the Space bar to select the **Commander** option.

5. Press the downarrow key to display the Commander configuration fields in the Stack Configuration screen.

![DEFAULT_CONFIG](image)

Figure 6-7. The Default Commander Configuration in the Stack Configuration Screen

6. Enter a unique stack name (up to 15 characters; no spaces) and press the downarrow key.

7. Ensure that the Commander has the desired **Auto Grab** setting, then press the downarrow key:

   - **No** (the default) prevents automatic joining of Candidates that have their **Auto Join** set to **Yes**.
   - **Yes** enables the Commander to automatically take a Candidate into the stack as a Member if the Candidate has **Auto Join** set to **Yes** (the default Candidate setting) and does not have a previously configured password.

8. Accept or change the transmission interval (default: 60 seconds), then press **[Enter]** to return the cursor to the **Actions** line.

9. Press **[S]** (for **Save**) to save your configuration changes and return to the Stacking menu.

Your Commander switch should now be ready to automatically or manually acquire Member switches from the list of discovered Candidates, depending on your configuration choices.
Using the Menu To Manage a Candidate Switch

Using the menu interface, you can perform these actions on a Candidate switch:

- Add ("push") the Candidate into an existing stack
- Modify the Candidate’s stacking configuration (Auto Join and Transmission Interval)
- Convert the Candidate to a Commander
- Disable stacking on the Candidate so that it operates as a standalone switch

In its default stacking configuration, a Candidate switch can either automatically join a stack or be manually added ("pulled") into a stack by a Commander, depending on the Commander’s Auto Grab setting. The following table lists the Candidate’s configuration options:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Setting</th>
<th>Other Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack State</td>
<td>Candidate</td>
<td>Commander, Member, or Disabled</td>
</tr>
<tr>
<td>Auto Join</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Transmission Interval</td>
<td>60 Seconds</td>
<td>Range: 1 to 300 seconds</td>
</tr>
</tbody>
</table>

Using the Menu To “Push” a Switch Into a Stack, Modify the Switch’s Configuration, or Disable Stacking on the Switch. Use Telnet or the web browser interface to access the Candidate if it has an IP address. Otherwise, use a direct connection from a terminal device to the switch’s console port. (For information on how to use the web browser interface, see the online Help provided for the browser.)

1. Display the Stacking Menu by selecting Stacking in the console Main Menu.
Figure 6-8. The Default Stack Configuration Screen

3. Move the cursor to the Stack State field by pressing [E] (for Edit).

4. Do one of the following:
   - To disable stacking on the Candidate, use the Space bar to select the Disabled option, then go to step 5.
     
     **Note:** Using the menu interface to disable stacking on a Candidate removes the Candidate from all stacking menus.

   - To insert the Candidate into a specific Commander’s stack:
     i. Use the space bar to select Member.
     ii. Press [Tab] once to display the Commander MAC Address parameter, then enter the MAC address of the desired Commander.

   - To change Auto Join or Transmission Interval, use [Tab] to select the desired parameter, and:
     - To change Auto Join, use the Space bar.
     - To change Transmission Interval, type in the new value in the range of 1 to 300 seconds.
     
     **Note:** All switches in the stack must be set to the same transmission interval to help ensure proper stacking operation. ProCurve recommends that you leave this parameter set to the default 60 seconds.

     Then go to step 5.
5. Press [Enter] to return the cursor to the Actions line.

6. Press [S] (for Save) to save your configuration changes and return to the Stacking menu.

Using the Commander To Manage The Stack

The Commander normally operates as your stack manager and point of entry into other switches in the stack. This typically includes:

- Adding new stack members
- Moving members between stacks
- Removing members from a stack
- Accessing stack members for individual configuration changes and traffic monitoring

The Commander also imposes its passwords on all stack members and provides SNMP community membership to the stack. (See “SNMP Community Operation in a Stack” on page 6-44.)

Using the Commander’s Menu To Manually Add a Candidate to a Stack. In the default configuration, you must manually add stack Members from the Candidate pool. Reasons for a switch remaining a Candidate instead of becoming a Member include any of the following:

- **Auto Grab** in the Commander is set to No (the default).
- **Auto Join** in the Candidate is set to No.
  
  **Note:** When a switch leaves a stack and returns to Candidate status, its Auto Join parameter resets to No so that it will not immediately rejoin a stack from which it has just departed.

- A Manager password is set in the Candidate.

- The stack is full.

Unless the stack is already full, you can use the Stack Management screen to manually convert a Candidate to a Member. If the Candidate has a Manager password, you will need to use it to make the Candidate a Member of the stack.

1. To add a Member, start at the Main Menu and select:
   
   **9. Stacking...**
   
   **4. Stack Management**

   You will then see the Stack Management screen:
2. Press [A] (for Add) to add a Candidate. You will then see this screen listing the available Candidates:

<table>
<thead>
<tr>
<th>SN</th>
<th>MAC Address</th>
<th>System Name</th>
<th>Device Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>006000-4E4300</td>
<td>Coral Sea</td>
<td>3500EI-19G</td>
<td>Member Up</td>
</tr>
<tr>
<td>2</td>
<td>080009-8E5D30</td>
<td>North Atlantic</td>
<td>3500y1</td>
<td>Member Up</td>
</tr>
</tbody>
</table>

For status descriptions, see the table on page 6-46.

3. Either accept the displayed switch number or enter another available number. (The range is 0 - 15, with 0 reserved for the Commander.)

4. Use the downarrow key to move the cursor to the MAC Address field, then type the MAC address of the desired Candidate from the Candidate list in the lower part of the screen.
5. Do one of the following:
   - If the desired Candidate has a Manager password, press the downarrow key to move the cursor to the Candidate Password field, then type the password.
   - If the desired Candidate does not have a password, go to step 6.

6. Press [Enter] to return to the Actions line, then press [S] (for Save) to complete the Add process for the selected Candidate. You will then see a screen similar to the one in figure 6-11, below, with the newly added Member listed.

   **Note**: If the message **Unable to add stack member: Invalid Password** appears in the console menu's Help line, then you either omitted the Candidate's Manager password or incorrectly entered the Manager password.

   ![Figure 6-11. Example of Stack Management Screen After New Member Added](image)

   For status descriptions, see the table on page 6-46.

Using the Commander’s Menu To Move a Member From One Stack to Another. Where two or more stacks exist in the same subnet (broadcast domain), you can easily move a Member of one stack to another stack if the destination stack is not full. (If you are using VLANs in your stack environment, see “Stacking Operation with a Tagged VLAN” on page 6-45.) This procedure is nearly identical to manually adding a Candidate to a stack (page 6-17). (If the stack from which you want to move the Member has a Manager password, you will need to know the password to make the move.)

1. To move a Member from one stack to another, go to the Main Menu of the Commander in the destination stack and display the Stacking Menu by selecting

   9. Stacking...
2. To learn or verify the MAC address of the Member you want to move, display a listing of all Commanders, Members, and Candidates in the subnet by selecting:

**2. Stacking Status (All)**

You will then see the Stacking Status (All) screen:

![Stacking Status (All) Screen](image)

- **Big Water**: 00:00:00-88:15:00, Pacific Ocean, Commander, Up
- **Newstack**: 00:10:03-89:30:00, Newstack-0, Commander, Up
- **Newstack**: 08:00:00-89:30:00, Newstack-1, Member, Up
- **Newstack**: 00:00:00-89:30:00, Newstack-2, Member, Up
- **Others**: 00:00:00-89:30:00, DEFAULT CONFIG, Candidate

This column lists the MAC Addresses for switches discovered (in the local subnet) that are configured for Stacking.

Using the MAC addresses for these Members, you can move them between stacks in the same subnet.

**Figure 6-12. Example of How the Stacking Status (All) Screen Helps You Find Member MAC Addresses**

3. In the Stacking Status (All) screen, find the Member switch that you want to move and note its MAC address, then press [B] (for Back) to return to the Stacking Menu.

4. Display the Commander’s Stack Management screen by selecting

**4. Stack Management**

(For an example of this screen, see figure 6-9 on page 6-18.)

5. Press [A] (for Add) to add the Member. You will then see a screen listing any available candidates. (See figure 6-10 on page 6-18.) Note that you will not see the switch you want to add because it is a Member of another stack and not a Candidate.)
6. Either accept the displayed switch number or enter another available number. (The range is 0 - 15, with 0 reserved for the Commander.)

7. Use the downarrow key to move the cursor to the MAC Address field, then type the MAC address of the desired Member you want to move from another stack.

8. Do one of the following:
   - If the stack containing the Member you are moving has a Manager password, press the downarrow key to select the Candidate Password field, then type the password.
   - If the stack containing the Member you want to move does not have a password, go to step 9.

9. Press [Enter] to return to the Actions line, then press [S] (for Save) to complete the Add process for the selected Member. You will then see a screen similar to the one in figure 6-9 on page 6-18, with the newly added Member listed.

---

**Note**

If the message **Unable to add stack member: Invalid Password** appears in the console menu's Help line, then you either omitted the Manager password for the stack containing the Member or incorrectly entered the Manager password.

You can “push” a Member from one stack to another by going to the Member’s interface and entering the MAC address of the destination stack Commander in the Member’s **Commander MAC Address** field. Using this method moves the Member to another stack without a need for knowing the Manager password in that stack, but also blocks access to the Member from the original Commander.

**Using the Commander’s Menu To Remove a Stack Member.** These rules affect removals from a stack:

- When a Candidate becomes a Member, its **Auto Join** parameter is automatically set to **No**. This prevents the switch from automatically rejoining a stack as soon as you remove it from the stack.

- When you use the Commander to remove a switch from a stack, the switch rejoins the Candidate pool for your IP subnet (broadcast domain), with **Auto Join** set to **No**.

- When you remove a Member from a stack, it frees the previously assigned switch number (**SN**), which then becomes available for assignment to another switch that you may subsequently add to the
Stack Management
Configuring Stack Management

stack. The default switch number used for an add is the lowest unassigned number in the Member range (1 - 15; 0 is reserved for the Commander).

To remove a Member from a stack, use the Stack Management screen.

1. From the Main Menu, select:

   9. Stacking...

   4. Stack Management

You will then see the Stack Management screen:

![Stack Member List](image)

**Figure 6-13. Example of Stack Management Screen with Stack Members Listed**

2. Use the downarrow key to select the Member you want to remove from the stack.

![Stack Member List](image)

**Figure 6-14. Example of Selecting a Member for Removal from the Stack**
3. Type [D] (for Delete) to remove the selected Member from the stack. You will then see the following prompt:

```
Continue Deletion of record ? Yes
```

Figure 6-15. The Prompt for Completing the Deletion of a Member from the Stack

4. To continue deleting the selected Member, press the Space bar once to select Yes for the prompt, then press [Enter] to complete the deletion. The Stack Management screen updates to show the new stack Member list.

Using the Commander To Access Member Switches for Configuration Changes and Monitoring Traffic

After a Candidate becomes a stack Member, you can use that stack's Commander to access the Member's console interface for the same configuration and monitoring that you would do through a Telnet or direct-connect access.

1. From the Main Menu, select:
   
   **9. Stacking...**
   
   **5. Stack Access**
   
   You will then see the Stack Access screen:

   ![Stack Access Screen](image)
   
   For status descriptions, see the table on page 6-46.

Figure 6-16. Example of the Stack Access Screen
Use the down arrow key to select the stack Member you want to access, then press [X] (for eXecute) to display the console interface for the selected Member. For example, if you selected switch number 1 (system name: Coral Sea) in figure 6-16 and then pressed [X], you would see the Main Menu for the switch named Coral Sea.

![Coral Sea Main Menu](image)

**Coral Sea**

---

**Main Menu**

1. Status and Counters...
2. Switch Configuration...
3. Console Passwords...
4. Event Log
5. Command Line (CLI)
6. Reboot Switch
7. Download OS
8. Run Setup
9. Stacking...
10. Logout

---

Figure 6-17. The eXecute Command Displays the Console Main Menu for the Selected Stack Member

2. You can now make configuration changes and/or view status data for the selected Member in the same way that you would if you were directly connected or telnetted into the switch.

3. When you are finished accessing the selected Member, do the following to return to the Commander's Stack Access screen:
   a. Return to the Member's Main Menu.
   b. Press [0] (for Logout), then [Y] (for Yes).
   c. Press [Return].

You should now see the Commander's Stack Access screen. (For an example, see figure 6-16 on page 6-23.)
Converting a Commander or Member to a Member of Another Stack

When moving a commander, the following procedure returns the stack members to Candidate status (with Auto-Join set to “No”) and converts the stack Commander to a Member of another stack. When moving a member, the procedure simply pulls a Member out of one stack and pushes it into another.

1. From the Main Menu of the switch you want to move, select

   9. Stacking

2. To determine the MAC address of the destination Commander, select

   2. Stacking Status (All)

3. Press [B] (for Back) to return to the Stacking Menu.

4. To display Stack Configuration menu for the switch you are moving, select

   3. Stack Configuration

5. Press [E] (for Edit) to select the Stack State parameter.

6. Use the Space bar to select Member, then press ↓ to move to the Commander MAC Address field.

7. Enter the MAC address of the destination Commander and press [Enter].


Monitoring Stack Status

Using the stacking options in the menu interface for any switch in a stack, you can view stacking data for that switch or for all stacks in the subnet (broadcast domain). (If you are using VLANs in your stack environment, see “Stacking Operation with a Tagged VLAN” on page 6-45.) This can help you in such ways as determining the stacking configuration for individual switches, identifying stack Members and Candidates, and determining the status of individual switches in a stack. See table 6-5 on page 6-26.
Table 6-5. Stack Status Environments

<table>
<thead>
<tr>
<th>Screen Name</th>
<th>Commander</th>
<th>Member</th>
<th>Candidate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack Status (This Switch)</td>
<td>• Commander’s stacking configuration</td>
<td>• Member’s stacking configuration</td>
<td>Candidate’s stacking configuration</td>
</tr>
<tr>
<td></td>
<td>• Data on stack Members:</td>
<td>• Data identifying Member’s Commander:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Switch Number</td>
<td>- Commander Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- MAC Address</td>
<td>- Commander IP Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- System Name</td>
<td>- Commander MAC Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Device Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stack Status (All)</td>
<td>Lists devices by stack name or Candidate status (if device is not a stack Member). Includes:</td>
<td>Same as for Commander.</td>
<td>Same as for Commander.</td>
</tr>
<tr>
<td></td>
<td>• Stack Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• System Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Status</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Using Any Stacked Switch To View the Status for All Switches with Stacking Enabled. This procedure displays the general status of all switches in the IP subnet (broadcast domain) that have stacking enabled.

1. Go to the console Main Menu for any switch configured for stacking and select:

   **9. Stacking ...**

   2. **Stacking Status (All)**

   You will then see a Stacking Status screen similar to the following:
Stack Management
Configuring Stack Management

For status descriptions, see the table on page 6-46.

Figure 6-18. Example of Stacking Status for All Detected Switches Configured for Stacking

Viewing Commander Status. This procedure displays the Commander and stack configuration, plus information identifying each stack member.

To display the status for a Commander, go to the console Main Menu for the switch and select:

9. Stacking ...
1. Stacking Status (This Switch)

You will then see the Commander’s Stacking Status screen:
Configuring Stack Management

Figure 6-19. Example of the Commander’s Stacking Status Screen

Viewing Member Status. This procedure displays the Member’s stacking information plus the Commander’s status, IP address, and MAC address.

To display the status for a Member:

1. Go to the console Main Menu of the Commander switch and select

   9. Stacking ...

   5. Stack Access

2. Use the downarrow key to select the Member switch whose status you want to view, then press [X] (for eXecute). You will then see the Main Menu for the selected Member switch.

3. In the Member’s Main Menu screen, select

   9. Stacking ...

   1. Stacking Status (This Switch)

   You will then see the Member’s Stacking Status screen:
Stack Management
Configuring Stack Management

---

**Figure 6-20. Example of a Member’s Stacking Status Screen**

**Viewing Candidate Status.** This procedure displays the Candidate’s stacking configuration.

To display the status for a Candidate:

1. Use Telnet (if the Candidate has a valid IP address for your network) or a direct serial port connection to access the menu interface Main Menu for the Candidate switch and select

   9. **Stacking ...**

   1. **Stacking Status (This Switch)**

   You will then see the Candidate’s Stacking Status screen:

---

**Figure 6-21. Example of a Candidate’s Stacking Screen**
Using the CLI To View Stack Status and Configure Stacking

The CLI enables you to do all of the stacking tasks available through the menu interface.

Table 6-6. CLI Commands for Configuring Stacking on a Switch

<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>show stack</td>
<td><strong>Commander:</strong> Shows Commander’s stacking configuration and lists the stack members and their individual status. <strong>Member:</strong> Lists Member’s stacking configuration and status, and the status and the IP address and subnet mask of the stack Commander.</td>
</tr>
<tr>
<td></td>
<td>Options:</td>
</tr>
<tr>
<td></td>
<td>candidates: (Commander only) Lists stack Candidates.</td>
</tr>
<tr>
<td></td>
<td>view: (Commander only) Lists current stack Members and their individual status.</td>
</tr>
<tr>
<td></td>
<td>all: Lists all stack Commanders, Members and Candidates, with their individual status.</td>
</tr>
<tr>
<td>[no] stack</td>
<td><strong>Any Stacking-Capable Switch:</strong> Enables or disables stacking on the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Stacking Enabled</td>
</tr>
</tbody>
</table>
| [no] stack commander <stack name> | **Candidate or Commander:** Converts a Candidate to a Commander or changes the stack name of an existing commander.  
|                             | “No” form eliminates named stack and returns Commander and stack Members to Candidate status with **Auto Join** set to **No**.  
|                             | “No” form prevents the switch from being discovered as a stacking-capable switch.  
|                             | **Default:** Switch Configured as a Candidate                             |
| [no] stack auto-grab         | **Commander:** Causes Commander to automatically add to its stack any discovered Candidate in the subnet that does not have a Manager password and has **Auto-Join** set to **Yes**.  
<p>|                             | <strong>Default:</strong> Disabled                                                      |
|                             | <strong>Note:</strong> If the Commander’s stack already has 15 members, the Candidate cannot join until an existing member leaves the stack.  |</p>
<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] stack member &lt;switch-num&gt; mac-address &lt;mac-addr&gt; [password &lt;password-str&gt;]</td>
<td><strong>Commander:</strong> Adds a Candidate to stack membership. “No” form removes a Member from stack membership. To easily determine the MAC address of a Candidate, use the <code>show stack candidates</code> command. To determine the MAC address of a Member you want to remove, use the <code>show stack view</code> command. The password (<code>password-str</code>) is required only when adding a Candidate that has a Manager password.</td>
</tr>
<tr>
<td>telnet &lt;1..15&gt;</td>
<td><strong>Commander:</strong> Uses the SN (switch number—assigned by the stack Commander) to access the console interface (menu interface or CLI) of a stack member. To view the list of SN assignments for a stack, execute the <code>show stack</code> command in the Commander’s CLI.</td>
</tr>
<tr>
<td>[no] stack join &lt;mac-addr&gt;</td>
<td><strong>Candidate:</strong> Causes the Candidate to join the stack whose Commander has the indicated MAC address. “No” form is used in a Member to remove it from the stack of the Commander having the specified address. <strong>Member:</strong> “Pushes” the member to another stack whose Commander has the indicated MAC address.</td>
</tr>
<tr>
<td>[no] stack auto-join</td>
<td><strong>Candidate:</strong> Enables Candidate to automatically join the stack of any Commander in the IP subnet that has Auto Grab enabled, or disables Auto-Join in the candidate. <strong>Default:</strong> Auto Join enabled. <strong>Note:</strong> If the Candidate has a Manager password or if the available stack(s) already have the maximum of 15 Members, the automatic join will not occur.</td>
</tr>
<tr>
<td>stack transmission-interval</td>
<td><strong>All Stack Members:</strong> specifies the interval in seconds for transmitting stacking discovery packets. <strong>Default:</strong> 60 seconds</td>
</tr>
</tbody>
</table>
Using the CLI To View Stack Status

You can list the stack status for an individual switch and for other switches that have been discovered in the same subnet.

**Syntax:** show stack [candidates | view | all]

**Viewing the Status of an Individual Switch.** The following example illustrates how to use the CLI in a to display the stack status for that switch. In this case, the switch is in the default stacking configuration.

**Syntax:** show stack

| ProCurve(config)# show stack | Stack Management Configuration
|------------------------------|-----------------------------------
| **Stacking - Stacking Status (This Switch)** |-----------------------------------
| Stack State : Commander |-----------------------------------
| Transmission Interval : 60 |-----------------------------------
| Stack Name : Big_Waters | Number of members : 1 |-----------------------------------
| Auto Grab : Yes | Members unreachable : 0 |-----------------------------------
| SN MAC Address | System Name | Device Type | Status
| 0 0030c1-7fcc40 | 3500yl | Commander Up |-----------------------------------
| 1 0030c1-7fed40 | piles-1 | 3500yl | Member Up |

**Figure 6-22. Example of Using the Show Stack Command To List the Stacking Configuration for an Individual Switch**

**Viewing the Status of Candidates the Commander Has Detected.**

This example illustrates how to list stack candidates the Commander has discovered in the ip subnet (broadcast domain).

**Syntax:** show stack candidates

| ProCurve (config)# show stack candidates | Stack Management Configuration
|----------------------------------------|-----------------------------------
| **Stack Candidates** |-----------------------------------
| Candidate MAC | System Name | Device Type
| 0060b0-889e00 | DEFAULT_CONFIG | 3500yl |

**Figure 6-23. Example of Using the Show Stack Candidates Command To List Candidates**
Viewing the Status of all Stack-Enabled Switches Discovered in the IP Subnet. The next example lists all the stack-configured switches discovered in the IP subnet. Because the switch on which the `show stack all` command was executed is a candidate, it is included in the “Others” category.

**Syntax:**  
show stack all

```
ProCurve (config)# show stack all

Stacking - Stacking Status (All)

<table>
<thead>
<tr>
<th>Stack Name</th>
<th>MAC Address</th>
<th>System Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Big_Waters</td>
<td>0030c1-7fcc40 3500yl</td>
<td></td>
<td>Commander Up</td>
</tr>
<tr>
<td></td>
<td>0030c1-7fec40 Big_Waters-1</td>
<td></td>
<td>Member Up</td>
</tr>
<tr>
<td>Others:</td>
<td>0060b0-889e00 DEFAULT_CONFIG</td>
<td></td>
<td>Candidate</td>
</tr>
</tbody>
</table>
```

**Figure 6-24. Result of Using the Show Stack All Command To List Discovered Switches in the IP Subnet**

Viewing the Status of the Commander and Current Members of the Commander’s Stack. The next example lists all switches in the stack of the selected switch.

**Syntax:**  
show stack view

```
ProCurve(config)# show stack view

Stack Members

<table>
<thead>
<tr>
<th>SN</th>
<th>MAC Address</th>
<th>System Name</th>
<th>Device Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0030c1-7fcc40 3500yl</td>
<td></td>
<td>3500yl</td>
<td>Commander Up</td>
</tr>
<tr>
<td>1</td>
<td>0030c1-7fec40 Big_Waters-1</td>
<td>3500yl</td>
<td>Member Up</td>
<td></td>
</tr>
</tbody>
</table>
```

**Figure 6-25. Example of the Show Stack View Command To List the Stack Assigned to the Selected Commander**
Using the CLI To Configure a Commander Switch

You can configure any stacking-enabled switch to be a Commander as long as the intended stack name does not already exist on the broadcast domain. (When you configure a Commander, you automatically create a corresponding stack.)

Before you begin configuring stacking parameters:

1. Configure IP addressing on the switch intended for stack commander and, if not already configured, on the primary VLAN. (For more on configuring IP addressing, refer to the Management and Configuration Guide for your switch.)

   **Note**
   The primary VLAN must have an IP address in order for stacking to operate properly. For more on the primary VLAN, see “The Primary VLAN” on page 2-45.

2. Configure a Manager password on the switch intended for commander. (The Commander’s Manager password controls access to stack Members.) For more on passwords, see the local manager and operator password information in the Access Security Guide for your switch.

**Configure the Stack Commander.** Assigning a stack name to a switch makes it a Commander and automatically creates a stack.

**Syntax:** stack commander < name-str >

This example creates a Commander switch with a stack name of Big_Waters. (Note that if stacking was previously disabled on the switch, this command also enables stacking.)

ProCurve(config)# stack commander Big_Waters

As the following show stack display shows, the Commander switch is now ready to add members to the stack.
Stack Management
Configuring Stack Management

The stack commander command configures the Commander and names the stack.

The Commander appears in the stack as Switch Number (SN) 0.

Figure 6-26. Example of the Commander's Show Stack Screen with Only the Commander Discovered

Using a Member's CLI to Convert the Member to the Commander of a New Stack. This procedure requires that you first remove the Member from its current stack, then create the new stack. If you do not know the MAC address for the Commander of the current stack, use show stack to list it.

Syntax: no stack
         stack commander < stack name >

Suppose, for example, that a ProCurve switch named “Bering Sea” is a Member of a stack named “Big_Waters”. To use the switch’s CLI to convert it from a stack Member to the Commander of a new stack named “Lakes”, you would use the following commands:

ProCurve(config)# show stack
Stacking - Stacking Status (This Switch)
Stack State : Commander
Transmission Interval : 60
Stack Name : Big_Waters Number of members : 0
Auto Grab : No Members unreachable : 0

<table>
<thead>
<tr>
<th>SN</th>
<th>MAC Address</th>
<th>System Name</th>
<th>Device Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0030c1-b24ac0</td>
<td>3500yl</td>
<td>3500yl</td>
<td>Commander Up</td>
</tr>
</tbody>
</table>

The stack commander command configures the Commander and names the stack.
Adding to a Stack or Moving Switches Between Stacks

You can add switches to a stack by adding discovered Candidates or by moving switches from other stacks that may exist in the same subnet. (You cannot add a Candidate that the Commander has not discovered.)

In its default configuration, the Commander’s Auto-Grab parameter is set to No to give you manual control over which switches join the stack and when they join. This prevents the Commander from automatically trying to add every Candidate it finds that has Auto Join set to Yes (the default for the Candidate).

(If you want any eligible Candidate to automatically join the stack when the Commander discovers it, configure Auto Grab in the Commander to Yes. When you do so, any Candidate discovered with Auto Join set to Yes (the default) and no Manager password will join the stack, up to the limit of 15 Members.)
Using the Commander’s CLI To Manually Add a Candidate to the Stack. To manually add a candidate, you will use:

- A switch number (SN) to assign to the new member. Member SNs range from 1 to 15. To see which SNs are already assigned to Members, use show stack view. You can use any SN not included in the listing. (SNs are viewable only on a Commander switch.)

- The MAC address of the discovered Candidate you are adding to the stack. To see this data, use the show stack candidates listing.

For example:

```
ProCurve(config)# show stack view
Stack Members
--- ----------------- ---------------------- ----------------------
SN MAC Address System Name Device Type Status
0  0030c1-7fe4c0  3500y1  3500y1  Commander Up
1  0060b0-880a80  Indian Ocean  3500y1  Member Up
```

Note: When manually adding a switch, you must assign an SN. However, if the Commander automatically adds a new Member, it assigns an SN from the available pool of unused SNs.

In this stack, the only SNs in use are 0 and 1, so you can use any SN number from 2 through 15 for new Members. (The SN of "0" is always reserved for the stack Commander.)

To display all discovered Candidates with their MAC addresses, execute show stack candidates from the Commander’s CLI. For example, to list the discovered candidates for the above Commander:

```
ProCurve(config)# show stack candidates
Stack Candidates
--- ----------------- ----------------------
Candidate MAC System Name Device Type
0030c1-b24ac0  North Sea  3500y1
0060b0-df1a00  DEFAULT_CONFIG  3500y1
```

Knowing the available switch numbers (SNs) and Candidate MAC addresses, you can proceed to manually assign a Candidate to be a Member of the stack:

**Syntax:**  
```
stack member < switch-number > mac-address < mac-addr >  
[ password < password-str > ]
```
For example, if the switch in the above listing did not have a Manager password and you wanted to make it a stack Member with an SN of 2, you would execute the following command:

ProCurve(config)# stack member 2 mac-address 0060b0-dfla00

The `show stack view` command then lists the Member added by the above command:

```
ProCurve(config)# show stack view
Stack Members
SN   MAC Address  System Name  Device Type  Status
---   -----------  ------------  -----------  --------
 0    0030c1-7fec40 3500yl     3500yl      Commander Up
 1    0060b0-880a80 Indian Ocean 3500yl    Member Up
 2    0060b0-dfla00 Big_Waters-2 3500yl    Member Up
```

Figure 6-30. Example Showing the Stack After Adding a New Member

**Using Auto Join on a Candidate.** In the default configuration, a Candidate’s Auto Join parameter is set to “Yes”, meaning that it will automatically join a stack if the stack’s Commander detects the Candidate and the Commander’s Auto Grab parameter is set to “Yes”. You can disable Auto Join on a Candidate if you want to prevent automatic joining in this case. There is also the instance where a Candidate’s Auto Join is disabled, for example, when a Commander leaves a stack and its members automatically return to Candidate status, or if you manually remove a Member from a stack. In this case, you may want to reset Auto Join to “Yes”.

**Status:** 

- [no] stack auto-join

ProCurve(config)# no stack auto-join

*Disables Auto Join on a Candidate.*

ProCurve(config)# stack auto-join

*Enables Auto Join on a Candidate.*
Using a Candidate CLI To Manually “Push” the Candidate Into a Stack. Use this method if any of the following apply:

- The Candidate’s **Auto Join** is set to **Yes** (and you do not want to enable **Auto Grab** on the Commander) or the Candidate’s **Auto Join** is set to **No**.
- Either you know the MAC address of the Commander for the stack into which you want to insert the Candidate, or the Candidate has a valid IP address and is operating in your network.

**Syntax:**

```
stack join < mac-addr >
```

where: `<mac-addr>` is the MAC address of the Commander in the destination stack.

Use Telnet (if the Candidate has an IP address valid for your network) or a direct serial port connection to access the CLI for the Candidate switch. For example, suppose that a Candidate named “North Sea” with **Auto Join** off and a valid IP address of 10.28.227.104 is running on a network. You could Telnet to the Candidate, use `show stack all` to determine the Commander’s MAC address, and then “push” the Candidate into the desired stack.

1. Telnet to the Candidate named “North Sea”.
2. Use `show stack all` to display the Commander’s MAC address.
3. Set the Candidate CLI to Config mode.
4. Execute `stack join` with the Commander’s MAC address to “push” the Candidate into the stack.

To verify that the Candidate successfully joined the stack, execute `show stack all` again to view the stacking status.

**Using the Destination Commander CLI To “Pull” a Member from Another Stack.** This method uses the Commander in the destination stack to “pull” the Member from the source stack.
Stack Management
Configuring Stack Management

**Syntax:**

```
stack member <switch-number>
mac-address <mac-addr>
[password <password-str>]
```

In the destination Commander, use `show stack all` to find the MAC address of the Member you want to pull into the destination stack. For example, suppose you created a new Commander with a stack name of “Cold_Waters” and you wanted to move a switch named “Bering Sea” into the new stack:

```
ProCurve(config)# show stack all
Stacking - Stacking Status (All)
Stack Name       MAC Address       System Name    Status
-----------------------------------------------------------------
Big_Waters       0030c1-7fec40    3500y1           Commander Up
                 0060b0-880a80    Indian Ocean      Member Up
                 0060b0-df1a00    Bering Sea        Member Up
Cold_Waters      0030c1-7fc700    3500y1           Commander Up
```

**Figure 6-32. Example of Stack Listing with Two Stacks in the Subnet**

You would then execute the following command to pull the desired switch into the new stack:

```
ProCurve(config)# stack member 1 mac-address 0060b0-df1a00
```

*Where* 1 is an unused switch number (SN).

Since a password is not set on the Candidate, a password is not needed in this example.

You could then use `show stack all` again to verify that the move took place.

**Using a Member CLI To “Push” the Member into Another Stack.** You can use the Member’s CLI to “push” a stack Member into a destination stack if you know the MAC address of the destination Commander.

**Syntax:**

```
stack join <mac-addr>
```

*where:* `<mac-addr>` is the MAC address of the Commander for the destination stack.

**Converting a Commander to a Member of Another Stack.** Removing the Commander from a stack eliminates the stack and returns its Members to the Candidate pool with Auto Join disabled.
**Stack Management**

**Configuring Stack Management**

**Syntax:**

```
no stack name <stack name>
stack join <mac-address>
```

If you don't know the MAC address of the destination Commander, you can use `show stack all` to identify it.

For example, suppose you have a switch operating as the Commander for a temporary stack named “Test”. When it is time to eliminate the temporary “Test” stack and convert the switch into a member of an existing stack named “Big_Waters”, you would execute the following commands in the switch’s CLI:

```
ProCurve(config)# no stack name Test
ProCurve(config)# show stack all
Stacking - Stacking Status (All)

<table>
<thead>
<tr>
<th>Stack Commander</th>
<th>MAC Address</th>
<th>System Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Big_Waters</td>
<td>0030c1-7fc700</td>
<td>3500yl</td>
<td>Commander Up</td>
</tr>
<tr>
<td></td>
<td>0060b0-889e00</td>
<td>Big_Waters-1</td>
<td>Member Up</td>
</tr>
<tr>
<td>Others:</td>
<td>0030c1-7fe40</td>
<td>3500yl</td>
<td>Candidate</td>
</tr>
</tbody>
</table>

ProCurve(config)# stack join 0030c1-7fc700
```

**Figure 6-33. Example of Command Sequence for Converting a Commander to a Member**

Using the CLI To Remove a Member from a Stack

You can remove a Member from a stack using the CLI of either the Commander or the Member.

**Note**

When you remove a Member from a stack, the Member’s **Auto Join** parameter is set to **No**.

**Using the Commander CLI To Remove a Stack Member.** This option requires the switch number (SN) and the MAC address of the switch to remove. (Because the Commander propagates its Manager password to all stack members, knowing the Manager password is necessary only for gaining access to the Commander.)

**Syntax:**

```
[no] stack member <switch-num> mac-address <mac-addr>
```
Use `show stack view` to list the stack Members. For example, suppose that you wanted to use the Commander to remove the “North Sea” Member from the following stack:

<table>
<thead>
<tr>
<th>SN</th>
<th>MAC Address</th>
<th>System Name</th>
<th>Device Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0030c1-7fc40</td>
<td>3500yl</td>
<td>3500yl</td>
<td>Commander Up</td>
</tr>
<tr>
<td>1</td>
<td>0060b0-880a80</td>
<td>Indian Ocean</td>
<td>3500yl</td>
<td>Member Up</td>
</tr>
<tr>
<td>2</td>
<td>0060b0-dfla00</td>
<td>Bering Sea</td>
<td>3500yl</td>
<td>Member Up</td>
</tr>
<tr>
<td>3</td>
<td>0030c1-7fc700</td>
<td>North Sea</td>
<td>3500yl</td>
<td>Member Up</td>
</tr>
</tbody>
</table>

You would then execute this command to remove the “North Sea” switch from the stack:

```
ProCurve(config)# no stack member 3 mac-address 0030c1-7fc700
```

*where:*

- 3 is the “North Sea” Member's switch number (SN)
- 0030c1-7fc700 is the “North Sea” Member's MAC address

### Using the Member’s CLI To Remove the Member from a Stack.

**Syntax:** `no stack join <mac-addr>`

To use this method, you need the Commander's MAC address, which is available using the show stack command in the Member's CLI. For example:
You would then execute this command in the “North Sea” switch’s CLI to remove the switch from the stack:

North Sea(config)# no stack join 0030c1-7fec40

Using the CLI To Access Member Switches for Configuration Changes and Traffic Monitoring

After a Candidate becomes a Member, you can use the telnet command from the Commander to access the Member’s CLI or console interface for the same configuration and monitoring that you would do through a Telnet or direct-connect access from a terminal.

**Syntax:** telnet <switch-number>

*where:* unsigned integer is the switch number (SN) assigned by the Commander to each member (range: 1 - 15).

To find the switch number for the Member you want to access, execute the show stack view command in the Commander’s CLI. For example, suppose that you wanted to configure a port trunk on the switch named “North Sea” in the stack named “Big_Waters”. Do do so you would go to the CLI for the “Big_Waters” Commander and execute show stack view to find the switch number for the “North Sea” switch:

![Figure 6-36. Example of a Stack Showing Switch Number (SN) Assignments](image)

The switch number (SN) for the “North Sea” switch is “3”.

To access the “North Sea” console, you would then execute the following telnet command:

ProCurve(config)# telnet 3

You would then see the CLI prompt for the “North Sea” switch, allowing you to configure or monitor the switch as if you were directly connected to the console.
SNMP Community Operation in a Stack

Community Membership

In the default stacking configuration, when a Candidate joins a stack, it automatically becomes a Member of any SNMP community to which the Commander belongs, even though any community names configured in the Commander are not propagated to the Member’s SNMP Communities listing. However, if a Member has its own (optional) IP addressing, it can belong to SNMP communities to which other switches in the stack, including the Commander, do not belong. For example:

<table>
<thead>
<tr>
<th>Commander Switch</th>
<th>Member Switch 1</th>
<th>Member Switch 2</th>
<th>Member Switch 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Addr: 10.31.29.100</td>
<td>IP Addr: 10.31.29.18</td>
<td>IP Addr: None</td>
<td>IP Addr: 10.31.29.15</td>
</tr>
<tr>
<td>Community Names:</td>
<td>Community Names:</td>
<td>Community Names:</td>
<td>Community Names:</td>
</tr>
<tr>
<td>– blue</td>
<td>– public (the default)</td>
<td>– red</td>
<td></td>
</tr>
<tr>
<td>– red</td>
<td>– public (the default)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Commander and all Members of the stack belong to the blue and red communities. Only switch 3 belongs to the gray community. Switches 1, 2, and 3 belong to the public community.

If Member Switch 1 ceases to be a stack Member, it still belongs to the public SNMP community because it has IP addressing of its own. But, with the loss of stack Membership, Switch 1 loses membership in the blue and red communities because they are not specifically configured in the switch.

If Member Switch 2 ceases to be a stack Member, it loses membership in all SNMP communities.

If Member Switch 3 ceases to be a stack Member, it loses membership in the blue and red communities, but—because it has its own IP addressing—retains membership in the public and gray communities.

Figure 6-37. Example of SNMP Community Operation with Stacking

SNMP Management Station Access to Members Via the Commander.

To use a management station for SNMP Get or Set access through the Commander’s IP address to a Member, you must append @sw<switch number> to the community name. For example, in figure 6-37, you would use the following command in your management station to access Switch 1’s MIB using the blue community:

```
snmpget <MIB variable> 10.31.29.100 blue@sw1
```

Note that because the gray community is only on switch 3, you could not use the Commander IP address for gray community access from the management station. Instead, you would access switch 3 directly using the switch’s own IP address. For example:

```
snmpget <MIB variable> 10.31.29.15 gray
```
Stack Management
Configuring Stack Management

Note that in the above example (figure 6-37) you cannot use the public community through the Commander to access any of the Member switches. For example, you can use the public community to access the MIB in switches 1 and 3 by using their unique IP addresses. However, you must use the red or blue community to access the MIB for switch 2.

```bash
snmpget <MIB variable> 10.31.29.100 blue@sw2
```

Using the CLI To Disable or Re-Enable Stacking

In the default configuration, stacking is enabled on the switch. You can use the CLI to disable stacking on the switch at any time. Disabling stacking has the following effects:

- **Disabling a Commander:** Eliminates the stack, returns the stack Members to Candidates with **Auto Join** disabled, and changes the Commander to a stand-alone (nonstacking) switch. You must re-enable stacking on the switch before it can become a Candidate, Member, or Commander.

- **Disabling a Member:** Removes the Member from the stack and changes it to a stand-alone (nonstacking) switch. You must re-enable stacking on the switch before it can become a Candidate, Member, or Commander.

- **Disabling a Candidate:** Changes the Candidate to a stand-alone (nonstacking) switch.

**Syntax:**

- `no stack` *(Disables stacking on the switch.)*
- `stack` *(Enables stacking on the switch.)*

Transmission Interval

All switches in the stack must be set to the same transmission interval to help ensure proper stacking operation. ProCurve recommends that you leave this parameter set to the default 60 seconds.

**Syntax:**

- `stack transmission-interval <seconds>`

Stacking Operation with Multiple VLANs Configured

Stacking uses the primary VLAN in a switch. In the factory-default configuration, the DEFAULT_VLAN is the primary VLAN. However, you can designate any VLAN configured in the switch as the primary VLAN. (See “The Primary VLAN” on page 2-45.)
When using stacking in a multiple-VLAN environment, the following criteria applies:

- Stacking uses only the primary VLAN on each switch in a stack.
- The primary VLAN can be tagged or untagged as needed in the stacking path from switch to switch.
- The same VLAN ID (VID) must be assigned to the primary VLAN in each stacked switch.

### Status Messages

Stacking screens and listings display these status messages:

<table>
<thead>
<tr>
<th>Message</th>
<th>Condition</th>
<th>Action or Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Candidate Auto-join</td>
<td>Indicates a switch configured with Stack State set to Candidate, Auto Join set to Yes (the default), and no Manager password.</td>
<td>None required</td>
</tr>
</tbody>
</table>
| Candidate      | Candidate cannot automatically join the stack because one or both of the following conditions apply:  
  • Candidate has Auto Join set to No.  
  • Candidate has a Manager password. | Manually add the candidate to the stack.                                         |
| Commander Down | Member has lost connectivity to its Commander. | Check connectivity between the Commander and the Member. |
| Commander Up   | The Member has stacking connectivity with the Commander. | None required.                                                                   |
| Mismatch       | This may be a temporary condition while a Candidate is trying to join a stack. If the Candidate does not join, then stack configuration is inconsistent. | Initially, wait for an update. If condition persists, reconfigure the Commander or the Member. |
| Member Down    | A Member has become detached from the stack. A possible cause is an interruption to the link between the Member and the Commander. | Check the connectivity between the Commander and the Member.                     |
| Member Up      | The Commander has stacking connectivity to the Member. | None required.                                                                   |
| Rejected       | The Candidate has failed to be added to the stack. | The candidate may have a password. In this case, manually add the candidate. Otherwise, the stack may already be full. A stack can hold up to 15 Members (plus the Commander). |
Index

Numerics
802.1p priority (QoS)
  definition … 5-6
802.1w as a region … 4-15

A
advertisement, GVRP
  definition … 3-3

B
bandwidth
  effect of QoS … 5-1
  bandwidth loss, spanning tree … 4-11
blocked link from STP operation … 4-12
blocked port
  from STP operation … 4-10
Bootp
  gateway ignored … 2-46
BPDU … 3-3
bridge protocol data unit … 3-3
broadcast domain … 2-4
broadcast storm … 4-2

C
configuration … 4-10
  Class of Service … 5-11
  factory default … 2-22, 2-28, 4-9
  spanning tree protocol … 4-10
CoS
  See Class of Service.

D
dedicated management VLAN … 2-45
DHCP
  gateway ignored … 2-46
domain … 2-22, 2-28
downstream device (QoS)
  definition … 5-6
  effect of priority settings … 5-9
DSCP
  Policy Table … 5-53
  policy, defined … 5-6
  See also priority.

F
forbid option
  See GVRP.
  forwarding database
  See VLAN.

G
GARP
  See GVRP
gateway, manual config … 2-46
GVRP … 4-8
  ACLs, restriction … 3-19
  advertisement … 3-19
  advertisement, defined … 3-3
  advertisement, responses to … 3-6
  advertisements, generating … 3-11
  auto option … 3-10
  benefit … 3-3
  block … 3-8
  CLI, configuring … 3-14
  configurable port options … 3-7
  configuring learn, block, disable … 3-8
  convert dynamic to static … 3-7
  converting to static VLAN … 3-4
  disable … 3-8
  dynamic VLAN and reboots … 3-19
  dynamic VLANs always tagged … 3-4
  forbid option … 3-10
  GARP … 3-3
  general operation … 3-4
  IP addressing … 3-7
  jumbo packets … 3-19
  learn … 3-8
  learn, block, disable … 3-10
  menu, configuring … 3-13
  non-GVRP aware … 3-18
  non-GVRP device … 3-18
  operating notes … 3-18
  port control options … 3-11
  port-leave from dynamic … 3-11
  reboot, switch … 3-12
  recommended tagging … 3-11
standard ... 3-3
  tagged, dynamic VLAN ... 3-4
unknown VLAN ... 3-11
unknown VLAN, options ... 3-7
VLAN behavior ... 2-12
VLAN, dynamic adds ... 2-26
VLAN, maximum ... 3-18
with QoS ... 5-41

I
inbound port (QoS)
  definition ... 5-6
IP
  gateway ... 2-46
  traffic priority based on ToS field ... 5-27
IP, type of service
  configuring priority ... 5-27

J
jumbo packets
  GVRP ... 3-19

L
legacy VLAN ... 2-11
loop, network ... 4-10

M
MAC address
  duplicate ... 2-18
  same for all VLANs ... 2-54
  single forwarding database ... 2-18
MAC address, per switch ... 2-18
MAC address, per VLAN ... 2-18
management VLAN ... 2-46
maximum VLANs, GVRP ... 3-18
mesh
  management VLAN ... 2-50
  spanning tree ... 4-15
message
  VLAN already exists ... 2-38
MSTI, configuration ... 4-25
MSTP
  See spanning-tree, 802.1s.
multiple ... 2-18
multiple forwarding database ... 2-18

N
non-routable VLAN ... 2-50

O
outbound port (QoS)
  definition ... 5-6
outbound port queue (QoS)
  definition ... 5-7

P
port
  blocked by STP operation ... 4-10
  loop ... 4-10
  monitoring ... 2-54
  redundant path ... 4-10
port trunk
  VLAN ... 2-54
precedence bits (QoS)
  definition ... 5-6
primary VLAN
  See VLAN
priority
  802.1p priority, defined ... 5-6
  codepoint, defined ... 5-6
  downstream device, defined ... 5-6
  DSCP policy, defined ... 5-6
  DSCP, defined ... 5-6
  inbound port, defined ... 5-6
  outbound port, defined ... 5-6
  upstream device, defined ... 5-7
priority (QoS)
  criteria for prioritizing packets ... 5-10
  type of service screen ... 5-27
VID, effect of eliminating ... 5-41
VLAN ID priority ... 5-41, 5-47
priority QoS)
  device priority screen ... 5-21
  IP address, source and destination match ... 5-22

Q
Quality of Service
  basic operation ... 5-7
configuring … 5-11, 5-13
configuring IP type of service … 5-27
criteria for prioritizing outbound packets … 5-10
definitions of terms … 5-6
device priority screen … 5-21
DSCP Policy Table … 5-53
GVRP not supported … 5-41
maximum entry limit … 5-61
no override definition … 5-14
No override, effect of … 5-55
overview … 5-1
prioritizing traffic based on IP ToS field … 5-27
priority settings map to outbound queues … 5-9
priority settings mapped to downstream
  devices … 5-9
type of service screen … 5-27
VLAN ID priority … 5-41, 5-47
quick start … 1-8

R
reboot … 3-12
redundant path … 4-10
region … 4-9
  See spanning-tree, 802.1s.
revision number … 4-13
routing
  non-routable VLAN … 2-50

S
secure management VLAN … 2-46
setup screen … 1-8
single forwarding database … 2-18
spanning tree
  802.1s
    See spanning tree, 802.1s.
  blocked link … 4-12
  blocked port … 4-10
  broadcast storm … 4-2
  enabling MSTP … 4-31
  MSTP
    See spanning-tree, 802.1s
  VLAN effect on … 2-53
spanning-tree, 802.1s … 4-2, 4-5
  802.1D and 802.1w connections … 4-15
  802.1D as a region … 4-13, 4-15
  802.1D connection requirement … 4-22
  802.1Q VLANs … 4-11
  802.1s standard-compliant … 4-5
  802.1w as a region … 4-13
  active path … 4-10
  active paths … 4-14
  bandwidth loss … 4-11
  benefit … 4-5
  blocked traffic … 4-11
  boundary port, region … 4-13, 4-14
  boundary port, VLAN membership … 4-11
  BPDU … 4-11, 4-17, 4-20, 4-21, 4-22
  BPDU requirement … 4-14
  BPDU, function … 4-13
  bridge … 4-13
  bridge, designated for region … 4-14
  caution … 4-5, 4-9
  CIST … 4-7, 4-13, 4-14
  CIST per-port hello time … 4-14
  CIST root … 4-23
  common and internal spanning tree
    See CIST.
  common spanning tree
    See CST.
  compatibility … 4-15
  compatibility mode … 4-21
  configuration … 4-19, 4-31
  configuration identifier … 4-13
  configuration steps … 4-17
  configuration, exchanging … 4-31
  configuration, MST instance … 4-25
  configuration, MSTI per-port … 4-28
  configuration, port … 4-22
  CST … 4-7, 4-11, 4-13
  CST and legacy devices … 4-11
  CST, view status … 4-33, 4-34
  default configuration … 4-9
  designated bridge … 4-11, 4-14
  designated port … 4-11
  disabling MSTP … 4-31
  display statistics and configuration … 4-33
  dynamic VLANs, disallowed … 4-8
  edge port … 4-22
  enabling a region … 4-31
  enabling MSTP … 4-31
  example of multiple topologies … 4-10
  fault tolerance … 4-5
  force protocol version … 4-15
  force-version … 4-22
forwarding paths ... 4-15
forwarding state ... 4-22
frame duplication and misordering ... 4-15
general operation ... 4-2, 4-5
GVRP ... 4-8, 4-15
hello-time, CIST root, propagated ... 4-14, 4-21
hello-time, override ... 4-14
hello-time, propagated ... 4-14
hop-count decremented ... 4-20
instance ... 4-2, 4-14, 4-18
instance, forwarding topology ... 4-15
instance, IST ... 4-8
instance, type ... 4-8
internal spanning tree
See IST.
interoperating with 802.1D and 802.1w ... 4-13
IST ... 4-7
IST instance ... 4-8, 4-25
IST root ... 4-8, 4-10, 4-14
IST, defined ... 4-13
IST, dynamic VLAN ... 4-15
IST, root switch ... 4-13
IST, switch membership ... 4-13
IST, VLAN membership ... 4-8
legacy devices and the CST ... 4-11
legacy STP and RSTP ... 4-11
legacy-mode ... 4-21
legacy-path-cost ... 4-21
mesh environment ... 4-5, 4-15
MIB ... 4-40
MST region
See region.
MSTI ... 4-8, 4-14
MSTI root ... 4-10
MSTI, view status ... 4-35
MSTP ... 4-9
MSTP operation ... 4-9
MSTP, view global configuration ... 4-36
multiple spanning tree instance
See MSTI
override hello-time ... 4-14
path cost, effect on 802.1D ... 4-16
pending configuration ... 4-39
pending option ... 4-9, 4-20, 4-31, 4-32
per-VLAN STP ... 4-5
planning ... 4-16
port connectivity ... 4-22
port states ... 4-10, 4-15
priority resolution ... 4-26
priority, device ... 4-18, 4-27
priority, IST port ... 4-30
priority, MSTI port ... 4-29
rapid state transitions ... 4-15
redundant links ... 4-11
region ... 4-2, 4-6, 4-7, 4-8
region name ... 4-13, 4-19
region root switch ... 4-8
region, configuration name ... 4-40
region, Configuration Revision number ... 4-40
region, defined ... 4-13
region, enabling ... 4-31
region, root bridge ... 4-13
region, RSTP bridge ... 4-14
region, switch configuration ... 4-14
region, switch excluded ... 4-40
region, view configuration ... 4-38
region, VLAN assignments ... 4-13
regional boundary port ... 4-13
regional root bridge per-instance ... 4-11
regional root switch ... 4-13
regional root switch, configuration ... 4-14
regions, communication between ... 4-14
root bridge ... 4-7
root bridge per-instance ... 4-11
root bridge per-region ... 4-13
root port per-instance ... 4-11
root switch, instance ... 4-26
root switch, IST instance ... 4-8, 4-13
root switch, MST instance ... 4-14
root switch, regional ... 4-13, 4-14
root, CIST ... 4-21
root, IST ... 4-14
root, MSTI ... 4-10
routed traffic in a region ... 4-11
RSTP as a region ... 4-6
RSTP BPDU requirement ... 4-14
RSTP bridge ... 4-14
rules for operation ... 4-14
separate forwarding paths ... 4-8
show commands ... 4-33
SNMP MIB ... 4-40
STP as a region ... 4-6
switch excluded from region ... 4-40
topology between regions ... 4-9
trunk, root, per-instance ... 4-11
trunked link ... 4-36
Index – 5

trunked link example ... 4-12
types of MST instances ... 4-8
VLAN assignments, region ... 4-13, 4-14
VLAN membership, region ... 4-12
VLAN, change instance ... 4-18
VLAN, configuration error ... 4-40
VLAN, connectivity between regions ... 4-14
VLAN, duplicate or missing packets ... 4-40
VLAN, dynamic ... 4-8
VLAN, instance assigned ... 4-10, 4-14, 4-25
with legacy STP and RSTP ... 4-7
stacking
benefits ... 6-3
minimum software version, other ProCurve switches ... 6-9
primary ... 6-46
See also virtual stacking.
static VLAN, convert to ... 3-4
subnet ... 2-4
subnet address ... 2-7

T
ToS
See Class of Service.
trunk, spanning-tree example ... 4-12
Type of Service
using to prioritize IP traffic ... 5-27
Type of Service field (IP)
configuring packet priority ... 5-27
how the switch uses it ... 5-38

U
upstream device QoS)
definition ... 5-7

V
VID
See VLAN.
virtual stacking
transmission interval range ... 6-16
VLAN ... 2-54
broadcast domain ... 2-4
CLI, commands ... 2-29
CLI, configuring parameters ... 2-28
convert dynamic to static ... 2-37, 3-4
dedicated management ... 2-45
default VLAN VID ... 2-45
default VLAN, name change ... 2-45
DEFAULT_VLAN ... 2-45
deleting ... 2-14, 2-35, 2-55
deleting, with member ports ... 2-14, 2-35, 2-36
DHCP, primary VLAN ... 2-45
duplicate MAC address ... 2-18
dynamic ... 2-4, 2-17, 2-22, 2-28, 2-37
effect on spanning tree ... 2-53
gateway, IP ... 2-46
GVRP, auto ... 2-13
layer-2 broadcast domain ... 2-5
layer-3 broadcast domain ... 2-5
limit ... 2-8, 2-22, 2-28
MAC address assignment ... 2-54
maximum per-switch ... 2-4
maximum, GVRP ... 3-18
menu, configuring parameters ... 2-22
menu, maximum capacity ... 2-26
menu, missing VLAN ... 2-26
multiple forwarding database ... 2-18, 2-21
multiple VLANs on port ... 2-42
non-routable ... 2-50
number allowed, including dynamic ... 2-26
per port configuration options ... 2-13
port assignment ... 2-26
port configuration ... 2-44
port monitoring ... 2-54
port restriction ... 2-55
port trunk ... 2-54
port-based ... 2-5
primary ... 2-34, 2-45, 6-9, 6-34, 6-46
primary, CLI command ... 2-29, 2-34
primary, select in menu ... 2-23
primary, web configure ... 2-39
primary, with DHCP ... 2-14
prioritizing traffic from with QoS ... 5-41, 5-47
protocol ... 2-5, 2-6, 2-10, 2-14, 2-16, 2-54
    ARP requirement ... 2-14, 2-35
capacity per VLAN ... 2-14
CLI only ... 2-22
commands ... 2-29
compared to port-based ... 2-7
configuration ... 2-28, 2-35
example ... 2-43
forbid option not allowed ... 2-38
IP addressing ... 2-7
VLAN already exists, message ... 2-38
VLAN, dynamic ... 4-15
VLANs
  static, 802.1s spanning tree ... 4-7
  voice VLAN

See VLAN.

VoIP
  See VLAN, voice.

W
  warranty ... 1-ii
  write memory ... 3-18