

# Static Virtual LANs (VLANs)

---

## Contents

<b>Overview</b> .....	2-3
<b>Introduction</b> .....	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
<b>Terminology</b> .....	2-6
<b>Static VLAN Operation</b> .....	2-7
VLAN Environments .....	2-8
VLAN Operation .....	2-9
Routing Options for VLANs .....	2-10
Overlapping (Tagged) VLANs .....	2-11
Per-Port Static VLAN Configuration Options .....	2-13
<b>VLAN Operating Rules</b> .....	2-14
<b>General Steps for Using VLANs</b> .....	2-17
<b>Multiple VLAN Considerations</b> .....	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
<b>Configuring VLANs</b> .....	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

Web: Viewing and Configuring VLAN Parameters .....	2-40
<b>802.1Q VLAN Tagging .....</b>	<b>2-41</b>
<b>Special VLAN Types .....</b>	<b>2-46</b>
VLAN Support and the Default VLAN .....	2-46
The Primary VLAN .....	2-46
The Secure Management VLAN .....	2-47
Preparation .....	2-49
Configuration .....	2-50
Using DHCP to Obtain an IP Address .....	2-51
Deleting the Management VLAN .....	2-54
Operating Notes for Management VLANs .....	2-54
Voice VLANs .....	2-55
Operating Rules for Voice VLANs .....	2-55
Components of Voice VLAN Operation .....	2-56
Voice VLAN QoS Prioritizing (Optional) .....	2-56
Voice VLAN Access Security .....	2-57
<b>Effect of VLANs on Other Switch Features .....</b>	<b>2-57</b>
Spanning Tree Operation with VLANs .....	2-57
IP Interfaces .....	2-58
VLAN MAC Address .....	2-58
Port Trunks .....	2-58
Port Monitoring .....	2-58
Jumbo Packet Support .....	2-58
<b>VLAN Restrictions .....</b>	<b>2-59</b>
<b>Migrating Layer 3 VLANs Using VLAN MAC Configuration .....</b>	<b>2-60</b>
VLAN MAC Address Reconfiguration .....	2-60
Handling Incoming and Outgoing VLAN Traffic .....	2-61
Sending Heartbeat Packets with a Configured MAC Address .....	2-62
Configuring a VLAN MAC Address with Heartbeat Interval .....	2-63
Operating Notes .....	2-63
Example .....	2-64
Verifying a VLAN MAC Address Configuration .....	2-64

## 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

Feature	Default	Menu	CLI	Web
view existing VLANs	n/a	page 2-23 thru 2-28	page 2-29	page 2-40
configuring static VLANs	default VLAN with VID = 1	page 2-23 thru 2-28	page 2-28	page 2-40

---

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 2048 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 2-46).
- **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 2-46).
- **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 2-47).
- **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 2-55).

---

**Note**

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

**Table 2-1. Comparative Operation of Port-Based and Protocol-Based VLANs**

	Port-Based VLANs	Protocol-Based VLANs
IP Addressing	<p>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 “Configuring IP Addressing” in the <i>Management and Configuration Guide</i> for the switch.)</p> <p>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 <i>Management and Configuration Guide</i> for the switch.)</p>	<p>You can configure IP addresses on all protocol VLANs. However, IP addressing is used only on IPv4 and IPv6 protocol VLANs.</p> <p><b>Restrictions:</b> When you configure an IP address on a VLAN interface, the following restrictions apply:</p> <ul style="list-style-type: none"> <li>Loopback interfaces share the same IP address space with VLAN configurations. The maximum number of IP addresses supported on a switch is 2048, which includes all IP addresses configured for both VLANs and loopback interfaces (except for the default loopback IP address 127.0.0.1).</li> <li>Each IP address that you configure on a VLAN interface must be unique in the switch. This means that the address cannot be used by a VLAN interface or another loopback interface.</li> </ul> <p>For more information, refer to the chapter on “Configuring IP Addressing” in the <i>Management and Configuration Guide</i>.</p>

## Static Virtual LANs (VLANs)

### Static VLAN Operation

	Port-Based VLANs	Protocol-Based VLANs
Untagged VLAN Membership	A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged.	<p>A port can be an untagged member of one protocol VLAN of a specific protocol type (such as IPX or IPv6). If the same protocol type is configured in multiple protocol VLANs, then a port can be an untagged member of only one of those 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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• Four single-protocol VLANs</li> <li>• Two protocol VLANs where one VLAN includes a single protocol and the other includes up to three protocols</li> <li>• One protocol VLAN where the VLAN includes four protocols</li> </ul>
Tagged VLAN Membership	A port can be a tagged member of any port-based VLAN. See above.	A port can be a tagged member of any protocol-based VLAN. See above.
Routing	<p>The switch can internally route IP (IPv4) traffic between port-based VLANs and between port-based and IPv4 protocol-based VLANs if the switch configuration enables IP routing.</p> <p>If the switch is not configured to route traffic internally between port-based VLANs, then an external router must be used to move traffic between VLANs.</p>	<p>If the switch configuration enables IP routing, the switch can internally route IPv4 traffic as follows:</p> <ul style="list-style-type: none"> <li>• Between multiple IPv4 protocol-based VLANs</li> <li>• Between IPv4 protocol-based VLANs and port-based VLANs.</li> </ul> <p>Other protocol-based VLANs require an external router for moving traffic between VLANs.</p> <p><b>Note:</b> NETbeui and SNA are non-routable protocols. End stations intended to receive traffic in these protocols must be attached to the same physical network.</p>
Commands for Configuring Static VLANs	<code>vlan &lt; VID &gt; [ tagged   untagged &lt; [e] port-list &gt; ]</code>	<code>vlan &lt; VID &gt; protocol &lt; ipx   ipv4   ipv6   arp   appletalk   sna   netbeui &gt;</code> <code>vlan &lt; VID &gt; [ tagged   untagged &lt; [e] port-list &gt; ]</code>

## 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 2-46.)

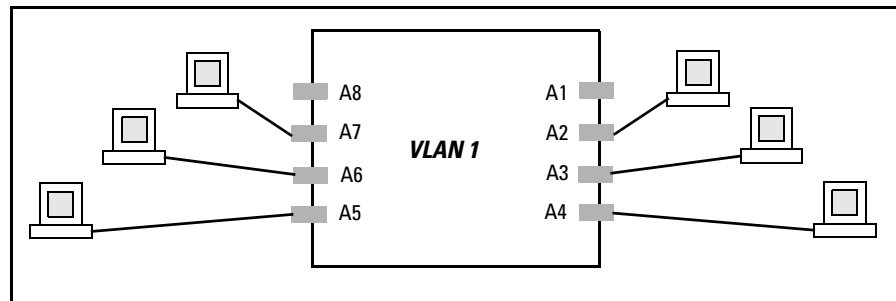


**Table 2-2. VLAN Environments**

VLAN Environment	Elements
The default VLAN (port-based; VID of "1") Only	In the default VLAN configuration, all ports belong to VLAN 1 as untagged members. VLAN 1 is a port-based VLAN, for IPv4 traffic.
Multiple VLAN Environment	In addition to the default VLAN, the configuration can include one or more other port-based VLANs and one or more protocol VLANs. (The switches covered in this guide allow up to 2048 (vids up to 4094) VLANs of all types.) Using VLAN tagging, ports can belong to multiple VLANs of all types. 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).

## VLAN Operation

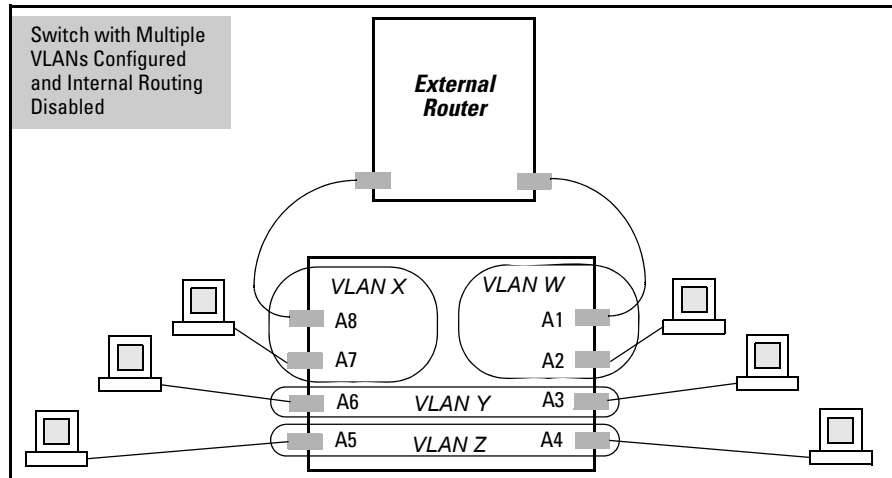
**The Default VLAN.** In figure 2-1, all ports belong to the default VLAN, and devices connected to these ports are in the same broadcast domain. Except for an IP address and subnet, no configuration steps are needed.



**Figure 2-1. Example of a Switch in the Default VLAN Configuration**

**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**

**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 2-3. Options for Routing Between VLAN Types in the Switch**

	Port-Based	IPX	IPv4	IPv6	ARP	Apple-Talk	SNA <sup>2</sup>	Netbeui <sup>2</sup>
Port-Based	Yes	—	Yes	—	—	—	—	—
Protocol								
IPX	—	Yes <sup>1</sup>	—	—	—	—	—	—
IPv4	Yes	—	Yes	—	—	—	—	—
IPv6	—	—	—	Yes <sup>1</sup>	—	—	—	—
ARP	—	—	—	—	Yes <sup>1</sup>	—	—	—
AppleTalk	—	—	—	—	—	Yes <sup>1</sup>	—	—

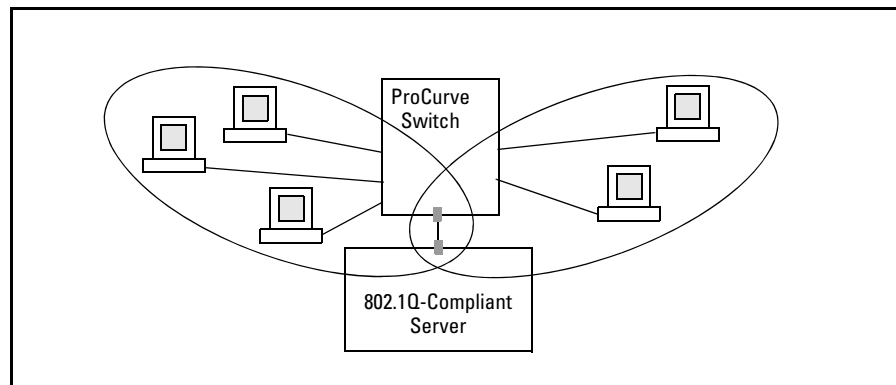
	Port- Based	IPX	IPv4	IPv6	ARP	Apple -Talk	SNA <sup>2</sup>	Netbeui <sup>2</sup>
SNA <sup>2</sup>	—	—	—	—	—	—	—	—
NETbeui <sup>2</sup>	—	—	—	—	—	—	—	—

<sup>1</sup>Requires an external router to route between VLANs.

<sup>2</sup>Not a routable protocol type. End stations intended to receive traffic in these protocols must be attached to the same physical network.

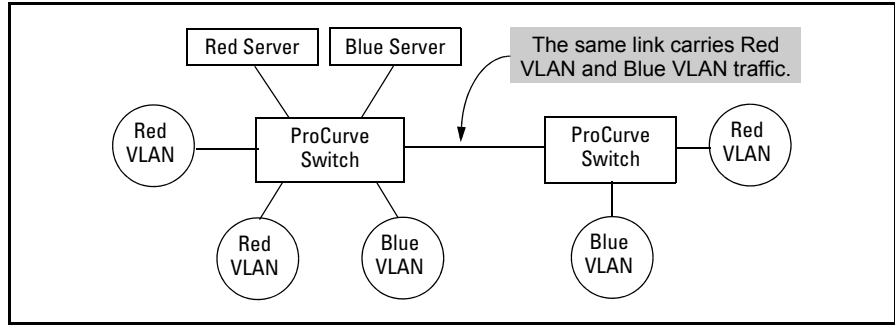
## Overlapping (Tagged) VLANs

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.



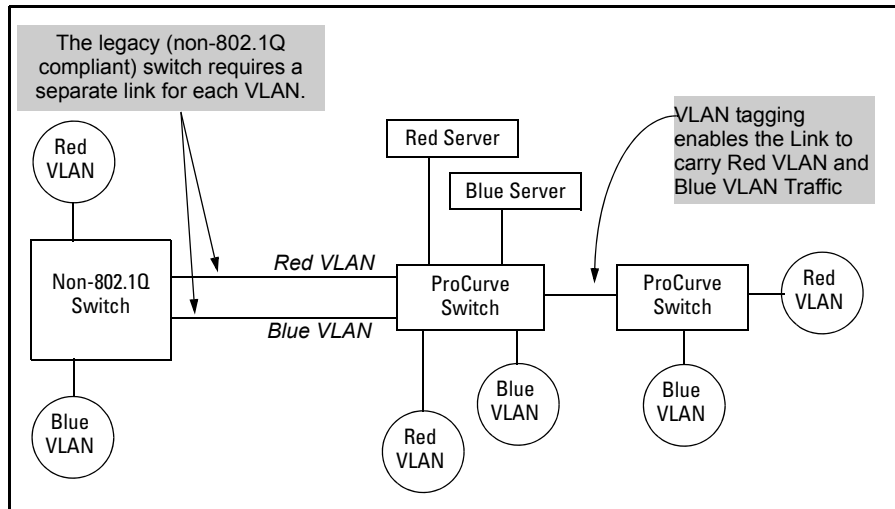
**Figure 2-3. Example of Overlapping VLANs Using the Same Server**

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



**Figure 2-4. Example of Connecting Multiple VLANs Through the Same 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.



**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 2-46)
- "Menu: Configuring VLAN Parameters (page 2-22)

- “CLI: Configuring VLAN Parameters” (page 2-22)
- “Web: Viewing and Configuring VLAN Parameters” (page 2-40)
- “VLAN Tagging Information” (page 2-41)
- “Effect of VLANs on Other Switch Features” (page 2-57)
- “VLAN Restrictions” (page 2-59)

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

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

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

**Table 2-4. Per-Port VLAN Configuration Options**

Parameter	Effect on Port Participation in Designated VLAN
<b>Tagged</b>	Allows the port to join multiple VLANs.
<b>Untagged</b>	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.

Parameter	Effect on Port Participation in Designated VLAN
<b>No</b> - or - <b>Auto</b>	<b>No:</b> Appears when the switch is not GVRP-enabled; prevents the port from joining that VLAN. <b>Auto:</b> Appears when GVRP is enabled on the switch; allows the port to dynamically join any advertised VLAN that has the same VID
<b>Forbid</b>	Prevents the port from joining the VLAN, even if GVRP is enabled on the switch.

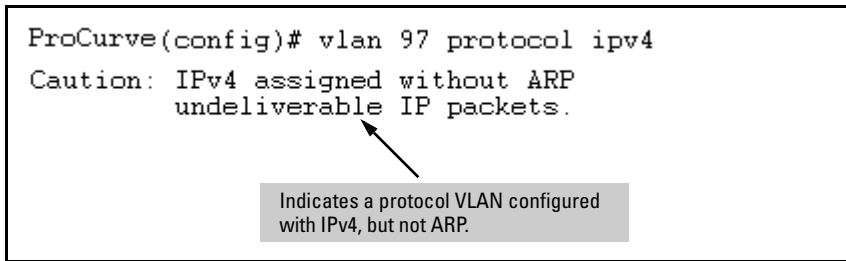
---

## 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

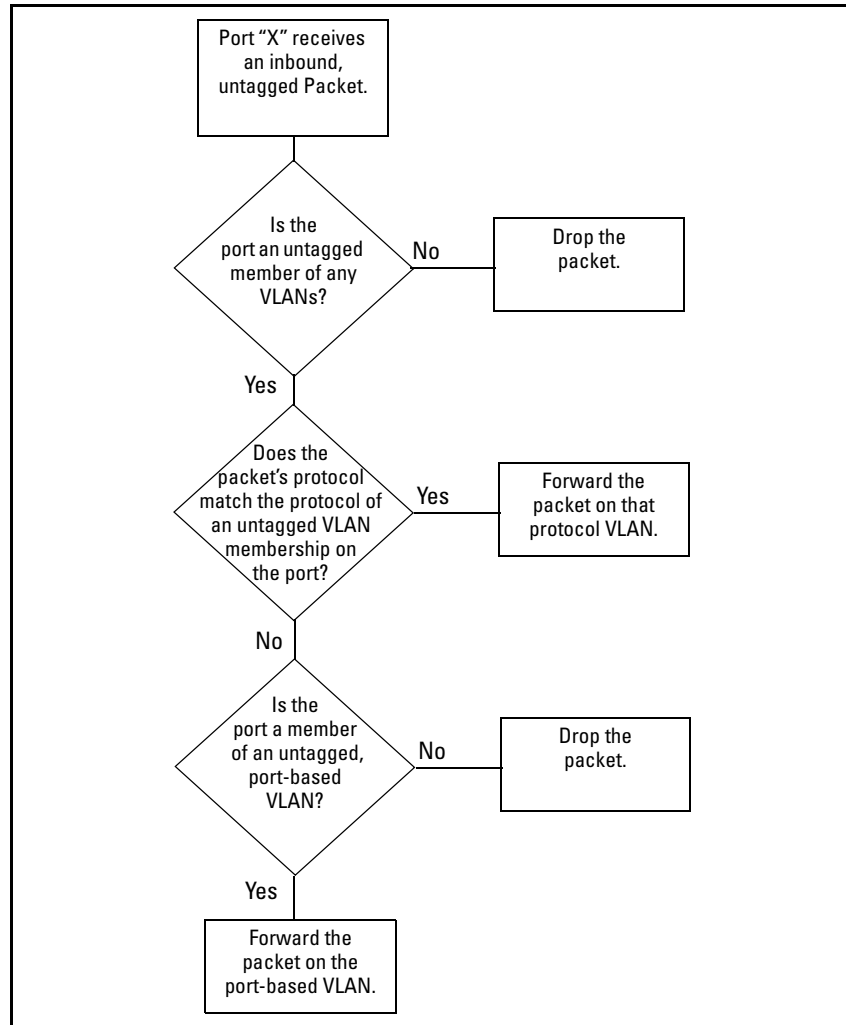
protocol VLAN that does not already include the ARP VLAN protocol, the switch displays this message:

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



Indicates a protocol VLAN configured with IPv4, but not ARP.

- **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.

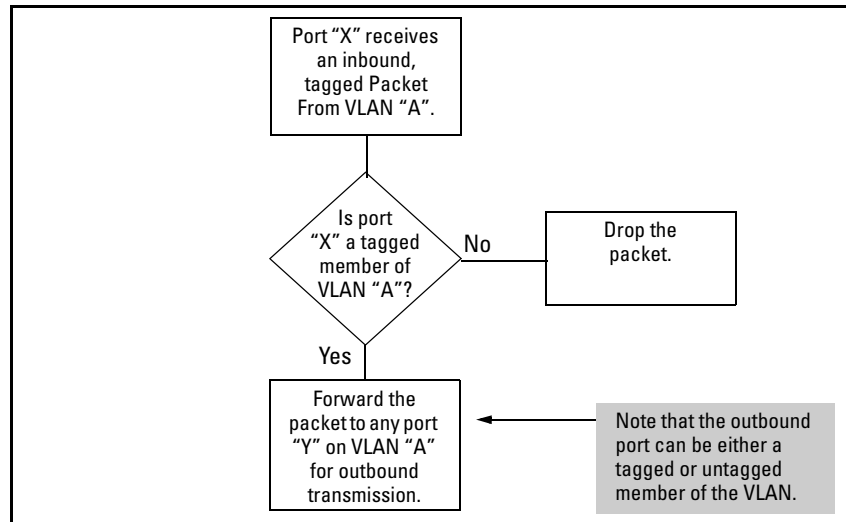


**Figure 2-7. Untagged VLAN Operation**

- **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.)



**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 2-57.) 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. For information on the procedure and restrictions when you configure an IP address on a VLAN interface, refer to Table 2-1 on page 2-7.

## 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**

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

Table 2-6 lists the database structure of current ProCurve switch models.

**Table 2-6. Forwarding Database Structure for Managed ProCurve Switches**

Multiple Forwarding Databases*	Single Forwarding Database*
Switch 8212zl	Switch 1600M/2400M/2424M
Series 6400cl switches	Switch 4000M/8000M
Switch 6200yl	Series 2500 switches
Switch 6108	Switch 2000
Series 5400zl switches	Switch 800T
Series 5300xl switches	
Series 4200vl switches	
Series 4100gl switches	
Series 3500yl switches	
Series 3400cl switches	
Switch 2810	
Series 2800 switches	
Series 2600/2600-PWR switches	
Series 2510 switches	

---

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

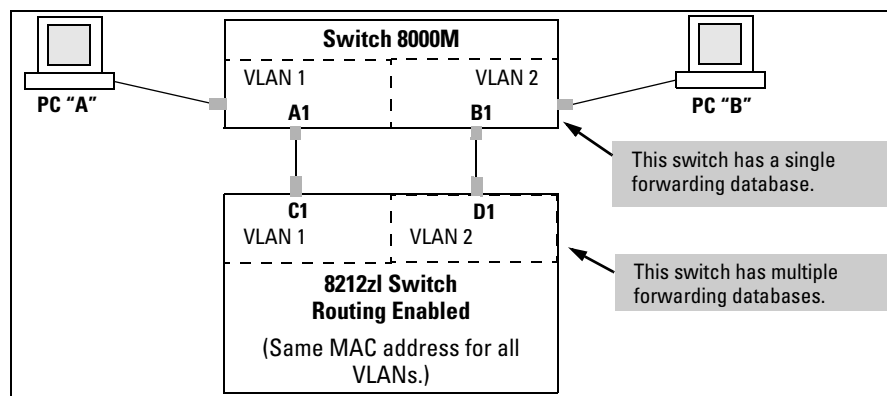
---

## 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):



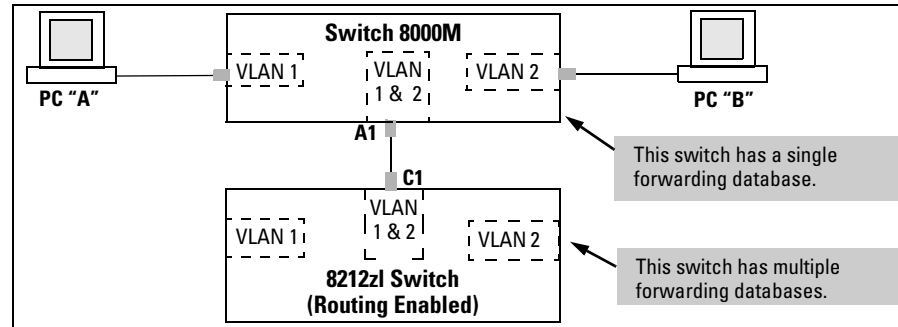
**Figure 2-9. Example of Invalid Configuration for Single-Forwarding to Multiple-Forwarding Database Devices in a Multiple VLAN Environment**

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

time. For this reason, the 8000M discards some packets directed through it for the 8212zl switch, 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.



**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 8212zl MAC address on port A1, and the 8000M will send traffic to either VLAN on the 8212zl.

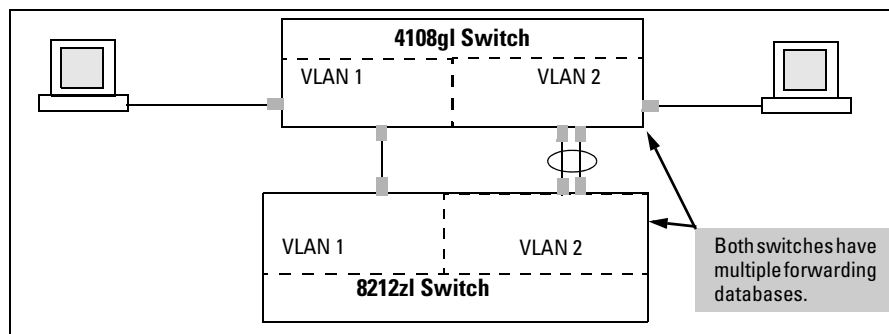
To increase the network bandwidth of the connection between the devices, you can use a trunk of multiple physical links rather than a single physical link.

## 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:



**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 256 VLANs. (You can reconfigure the switch to support up to 2048 (vids up to 4094) 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 2-46.) 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 2048 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 2-41.)

## 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 2-35.)
- 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:

```
----- CONSOLE - MANAGER MODE -----  
Switch Configuration - VLAN - VLAN Support  
  
Maximum VLANs to support [8] : 8  
Primary VLAN : DEFAULT_VLAN  
GVRP Enabled [No] : No  
  
Actions-> Cancel   Edit   Save   Help  
  
Cancel changes and return to previous screen.  
Use arrow keys to change action selection and <Enter> to execute action.
```

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

2. Press **[E]** (for **E**dit), then do one or more of the following:

- To change the maximum number of VLANs, type the new number (1 - 2048 allowed; default 256).
- 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).

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

```
----- CONSOLE - MANAGER MODE -----  
Switch Configuration - VLAN Menu  
  
*1. VLAN Support  
2. VLAN Names  
3. VLAN Port Assignment  
4. Return to Previous Menu...  
0. Return to Main Menu...  
  
Displays the menu to activate and configure, or deactivate VLAN support.  
To select menu item, press item number, or highlight item and press <Enter>.  
(*Needs reboot to activate changes.)
```

**Figure 2-13. VLAN Menu Screen Indicating the Need To Reboot the Switch**

- 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.

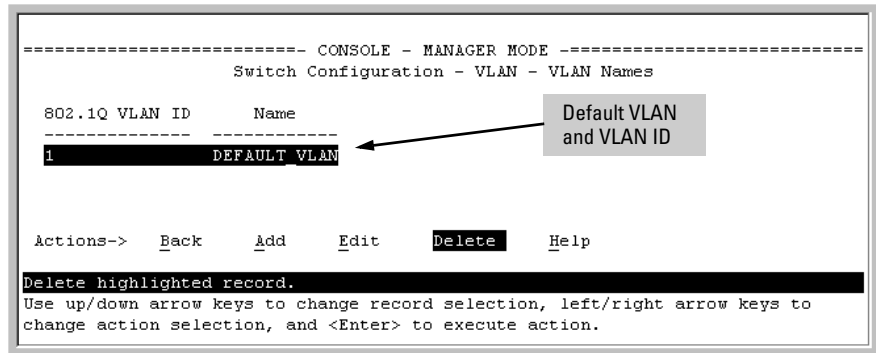
## Adding or Editing VLAN Names

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:





**Figure 2-14. The Default VLAN Names Screen**

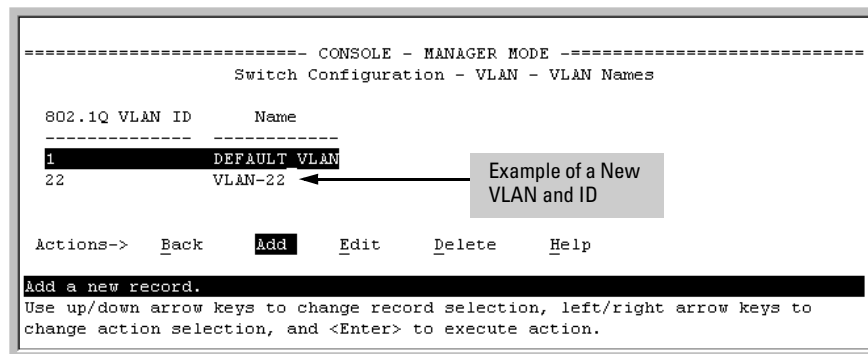
2. Press **[A]** (for **Add**). You will then be prompted for a new VLAN name and VLAN ID:

```
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 **[↓]** 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: @, #, \$, ^, &, \*, (, and ).)
5. Press **[S]** (for **Save**). You will then see the VLAN Names screen with the new VLAN listed.



**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 **show vlans [ VID | ports < port-list >]** command to list data on VLANs having VIDs numbered sequentially higher than the first 32.

---

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

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

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

```

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

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

Actions->  Cancel  Edit  Save  Help
Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
  
```

**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):
  - a. Press [E] (for **Edit**).
  - 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

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

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

Actions-> Cancel Edit Save Help

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

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 2-41.

- 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 2-46.) You can configure up to 255 additional static VLANs by adding new VLAN names, and then assigning one or more ports to each VLAN. (The switch accepts a maximum of 2048 (vids numbered up to 4094) 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 2-41.)

VLAN Commands	Page
show vlans	below
show vlans < vid >	2-33
show vlans ports <port-list>	
max-vlans <1-2048>	2-34
primary-vlan < vid >	2-35
[no] vlan < vid >	2-36
auto < port-list >	2-38 (Available if GVRP enabled.)
forbid	2-38
name < vlan-name >	2-38
protocol < protocol-list >	2-36
tagged < port-list >	2-38
untagged < port-list >	2-38
voice	2-55
static-vlan < vlan-id >	2-38 (Available if GVRP enabled.)

**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: 256 Maximum: 2048)

**Primary VLAN:** Refer to "The Primary VLAN" on page 2-46.

**Management VLAN:** Refer to "The Secure Management VLAN" on page 2-47.

**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 2-55.*

**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
    
```

When GVRP is disabled (the default), Dynamic VLANs do not exist on the switch and do not appear in this listing. (Refer to chapter 3, “GVRP” .)

**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 > [detail]

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

**port-list:** *Specify a single port number, a range of ports (for example, a1-a16), or all.*

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

Descriptions of items displayed by the command are provided below.

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

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

**Name:** The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of **VLAN-x** where “x” matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of **GVRP\_x** where “x” matches the applicable VID.

**Status:**

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

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

**Dynamic:** Port-Based, temporary VLAN learned through GVRP.

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

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

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

Figure 2-19 is an example of the output when the **detail** option is not used.

```
ProCurve# show vlan ports a1-a33

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

802.1Q	VLAN ID	Name	Status	Voice
1		DEFAULT_VLAN	Port-based	No
10		VLAN_10	Port-based	Yes
15		VLAN_15	Port-based	No
20		VLAN_20	Protocol	No
33		GVRP_33	Dynamic	No

Figure 2-19. Example of “Show VLAN Ports” Cumulative Listing

Figure 2-20 is an example of the output when the **detail** option is used.

```
ProCurve# show vlan ports a1-a4 detail

Status and Counters - VLAN Information - for ports A1

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

Status and Counters - VLAN Information - for ports A2

Port name: Uplink_Port
VLAN ID  Name                | Status      Voice Jumbo Mode
-----  -
1         DEFAULT_VLAN         | Port-based  No   No   Untagged
20        VLAN_20              | Protocol    No   No   Tagged
33        GVRP_33             | Dynamic     No   No   Tagged

Status and Counters - VLAN Information - for ports A3

VLAN ID  Name                | Status      Voice Jumbo Mode
-----  -
1         DEFAULT_VLAN         | Port-based  No   No   Untagged

Status and Counters - VLAN Information - for ports A4

VLAN ID  Name                | Status      Voice Jumbo Mode
-----  -
1         DEFAULT_VLAN         | Port-based  No   No   Untagged
```

**Figure 2-20. Example of “Show VLAN Ports” Detail 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 2-55.*

**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.*

```
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

Port Information Mode      Unknown VLAN Status
-----
A12              Untagged Learn      Up
A13              Untagged Learn      Up
A14              Untagged Learn      Up
A15              Untagged Learn      Down
A16              Untagged Learn      Up
A17              Untagged Learn      Up
A18              Untagged Learn      Up
```

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

**Show VLAN** lists this data when GVRP is enabled and at least one port on the switch has dynamically joined the designated 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

Port Information DEFAULT Unknown VLAN Status
-----
A6              Auto      Learn      Up
```

Figure 2-22. Example of “Show VLAN” for a Specific Dynamic VLAN

**Changing the Number of VLANs Allowed on the Switch.** In the default VLAN configuration, the switch allows a maximum of 256 VLANs. You can specify any value from 1 to 2048.

**Syntax:** max-vlans < 1-2048 >

*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:

Note that you can execute these three steps at another time.

```

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 2-23. 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 2-46.) 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
      
```

Status and Counters - VLAN Information

Maximum VLANs to support : 8  
 Primary VLAN : 22-Primary  
 Management VLAN :

802.1Q	VLAN ID	Name	Status	Voice	Jumbo
1		DEFAULT_VLAN	Static	No	No
22		22-Primary	Static	No	No

Reassigns the Primary VLAN to VLAN 22.

Renames VLAN 22 to "22-Primary".

**Figure 2-24. Example of Reassigning Primary VLAN and Changing the VLAN Name**

### 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 2-55.

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

```
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 :
```

802.1Q VLAN ID	Name	Status	Voice	Jumbo
1	DEFAULT_VLAN	Port-based	No	No
100	VLAN100	Port-based	No	No

If this field is empty, a Secure Management VLAN is not configured in the switch. Refer to "The Secure Management VLAN" on page 2-47

**Figure 2-25. Example of Creating a New, Port-Based, Static VLAN**

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

```
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.)

```
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.

---

**Note**

---

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

```
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:

```
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:

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

- or -

At the VLAN 100 context level, use:

```
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 2-26 shows this concept:

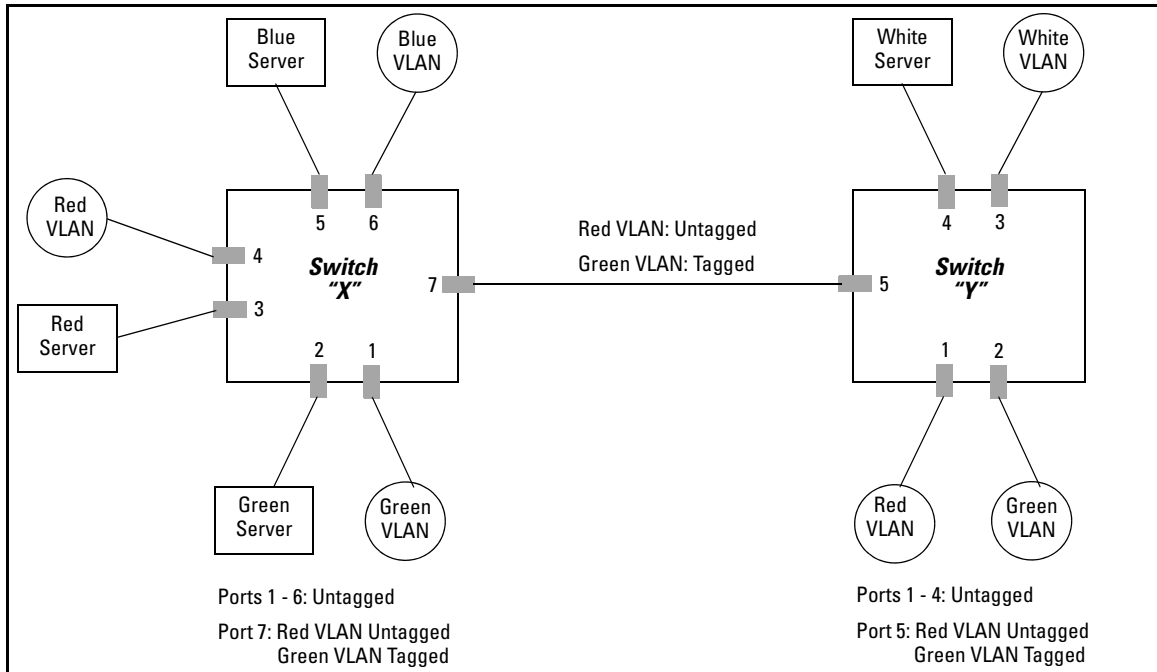
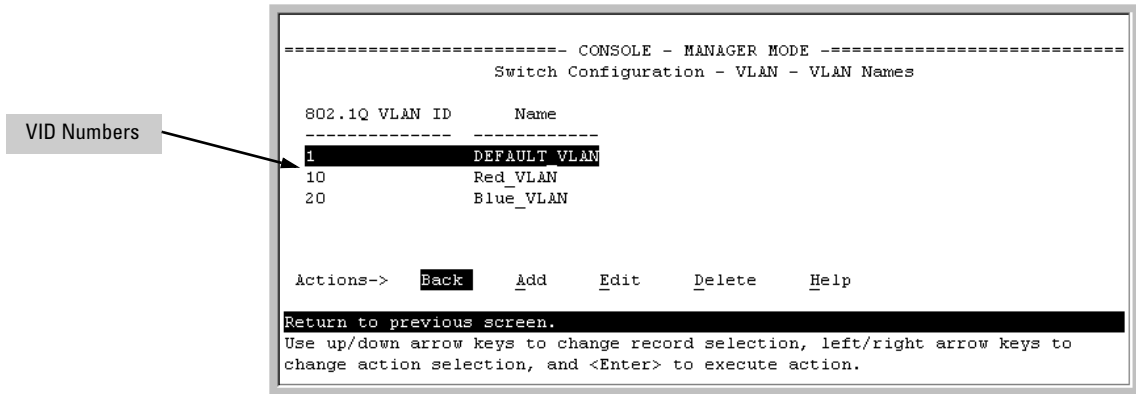


Figure 2-26. Example of Tagged and Untagged VLAN Port Assignments

- 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 2-26 (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.

**Note**

Each 802.1Q-compliant VLAN must have its own unique VID number, and that VLAN *must* be given the same VID in every device 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 2-27. 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:

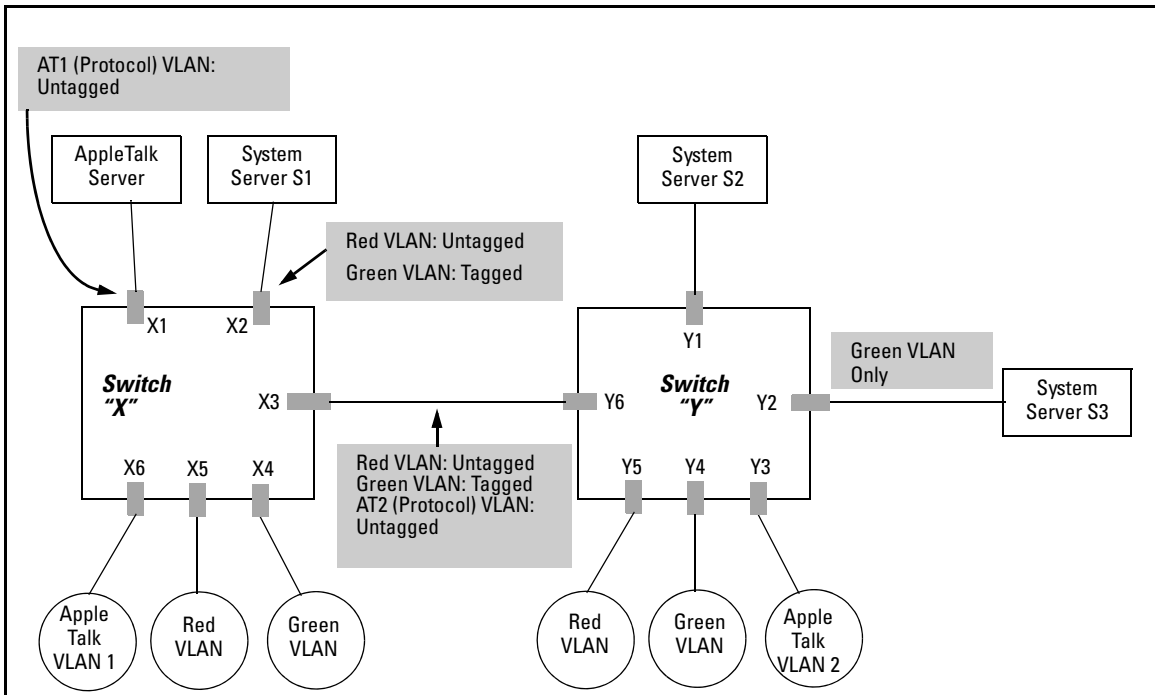
Port-Based VLANs	Protocol VLANs
A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged.	A port can be an untagged member of one protocol-based VLAN of each protocol type. When assigning a port to multiple, protocol-based VLANs sharing the same type, the port can be an untagged member of only one such VLAN.
A port can be a tagged member of any port-based VLAN. See above.	A port can be a tagged member of any protocol-based VLAN. See above.
<b>Note:</b> A given VLAN <i>must</i> 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.



**Figure 2-28. 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.

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

\*"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".

---

## Special VLAN Types

### VLAN Support and the Default VLAN

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

You can partition the switch into multiple virtual broadcast domains by configuring one or more additional VLANs and moving ports from the default VLAN to the new VLANs. (The switch supports up to 2048 (vids numbered up to 4094) 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 2-38

### 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 2-35.

## The Secure Management VLAN

Configuring a secure Management VLAN creates an isolated network for managing the ProCurve switches that support this feature. (As of December, 2005, the Secure Management VLAN feature is available on these ProCurve switches:

- Switch 8212zl
- 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
- Series 2800 switches
- Series 2600 switches

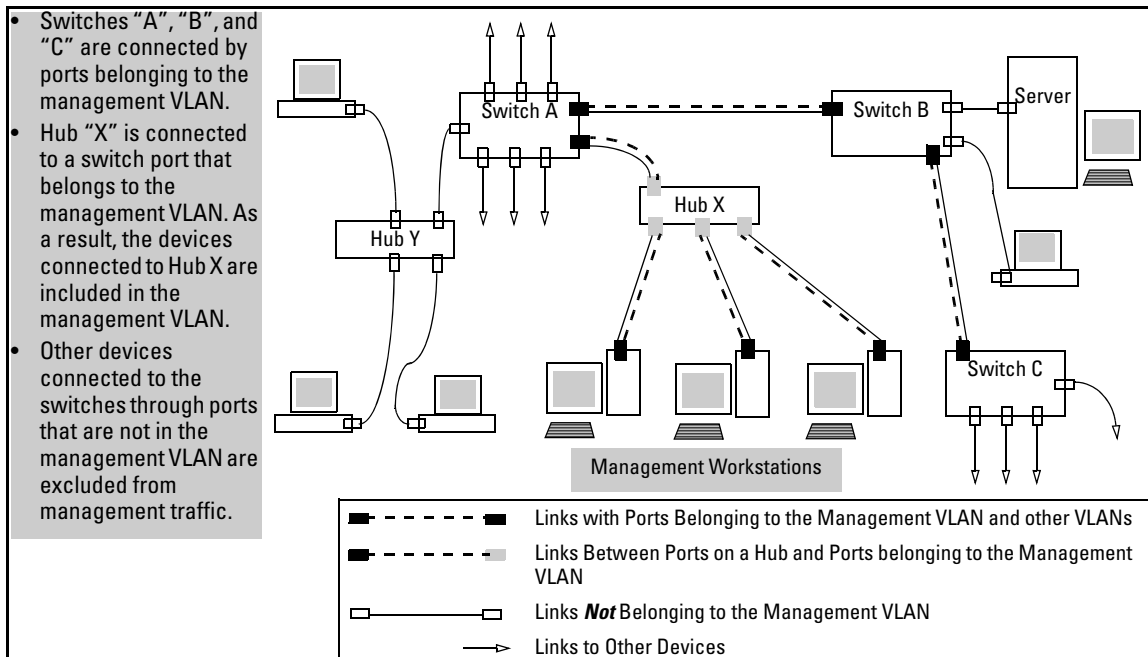
If you configure a Secure Management VLAN, access to the VLAN and to the switch’s management functions (Menu, CLI, and web browser interface) is available only through ports configured as members.

- 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.

**Static Virtual LANs (VLANs)**  
Special VLAN Types

- 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 2-29 illustrates use of the Management VLAN feature to support management access by a group of management workstations.



**Figure 2-29. Example of Potential Security Breaches**

In figure 2-30, 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.



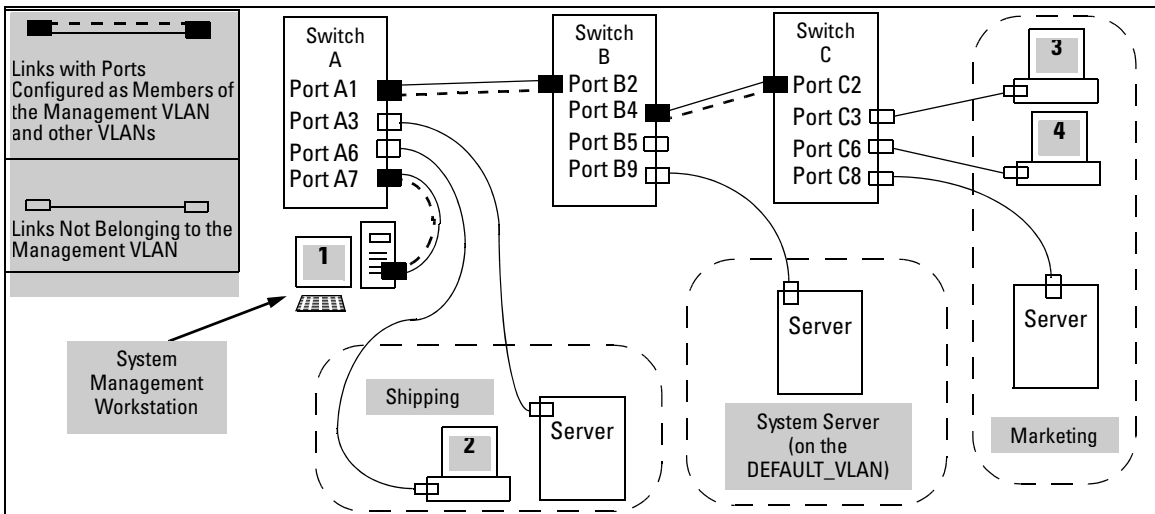


Figure 2-30. Example of Management VLAN Control in a LAN

Table 2-7. VLAN Membership in Figure 2-30

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

### Preparation

1. Determine a VID and VLAN name suitable for your Management VLAN.
2. Plan your Management VLAN topology to use ProCurve switches that support this feature. (Refer to page 2-47.) 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 2-30.)
  - 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 2-30 on page 2-49.).

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.

---

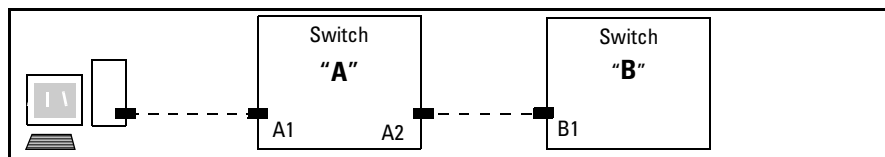
## Configuration

**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.



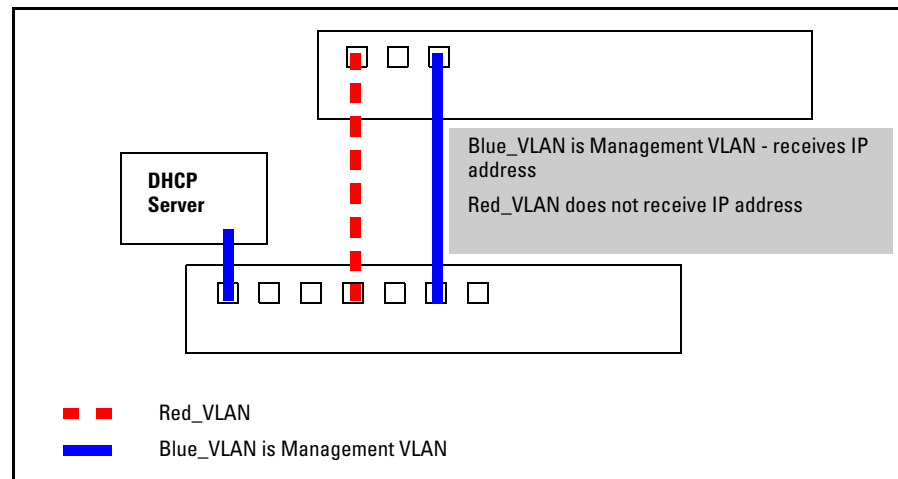
**Figure 2-31. Illustration of Configuration Example**

```
ProCurve (config)# management-vlan 100
ProCurve (config)# vlan 100 tagged a1
ProCurve (config)# vlan 100 tagged a2
```

## Using DHCP to Obtain an IP Address

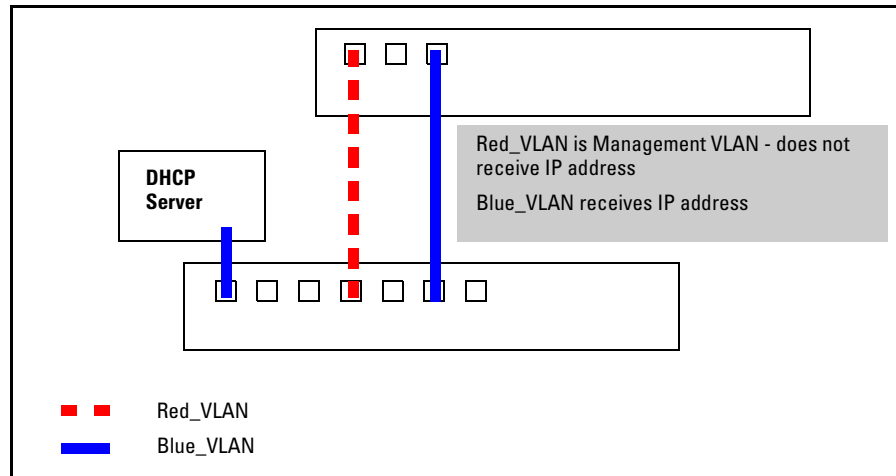
You can use DHCP to obtain an IPv4 address for your Management VLAN or a client on that VLAN. The following examples illustrate when an IP address will be received from the DHCP server.

1. If Blue\_VLAN is configured as the Management VLAN and the DHCP server is also on Blue\_VLAN, Blue\_VLAN receives an IP address. Because DHCP Relay does not forward onto or off of the Management VLAN, devices on Red\_VLAN cannot get an IP address from the DHCP server on Blue\_VLAN (Management VLAN) and Red\_VLAN does not receive an IP address. See figure 2-32.



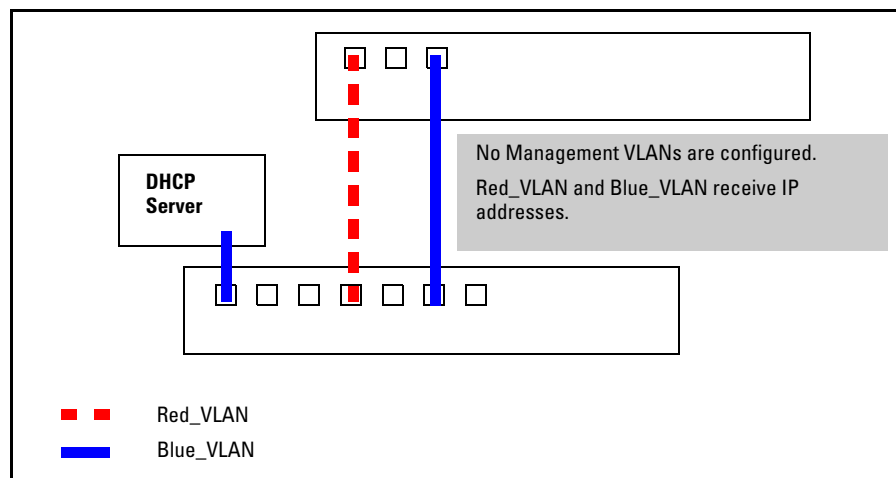
**Figure 2-32. Example of DHCP Server on Management VLAN**

2. If Red\_VLAN is configured as the Management VLAN and the DHCP server is on Blue\_VLAN, Blue\_VLAN receives an IP address but Red\_VLAN does not. See figure 2-33.



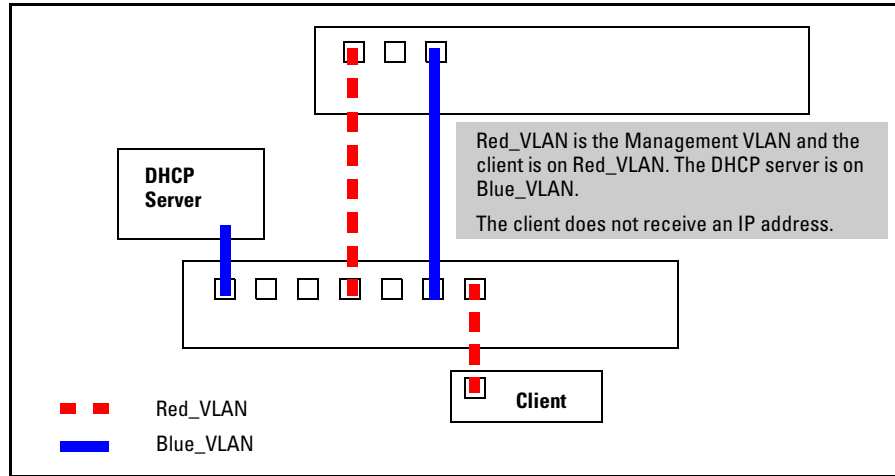
**Figure 2-33. Example of DHCP Server on Different VLAN from the Management VLAN**

3. If no Management VLAN is configured, both Blue\_VLAN and Red\_VLAN receive IP addresses. See figure 2-34.



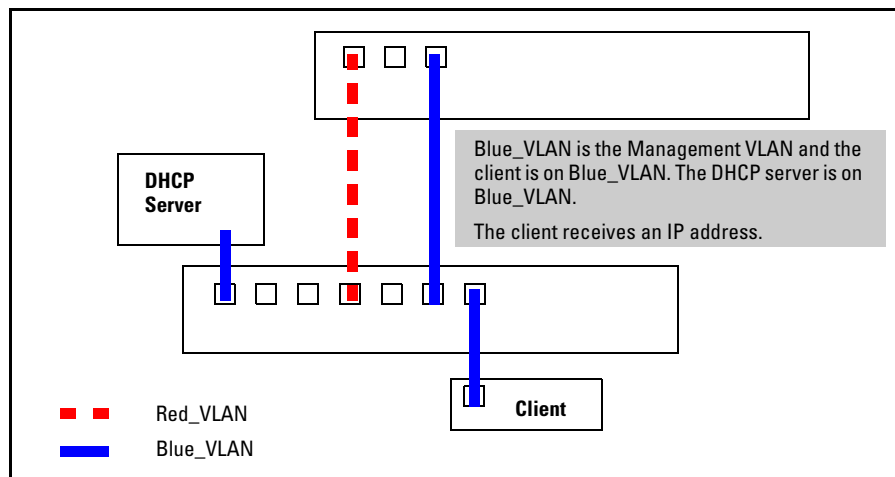
**Figure 2-34. Example of no Management VLANs Configured**

4. If Red\_VLAN is configured as the Management VLAN and the client is on Red\_VLAN, but the DHCP server is on Blue\_VLAN, the client will not receive an IP address. See figure 2-35.



**Figure 2-35. Example of Client on Different Management VLAN from DHCP Server**

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



**Figure 2-36. Example of DHCP Server and Client on the Management VLAN**

## 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.

---

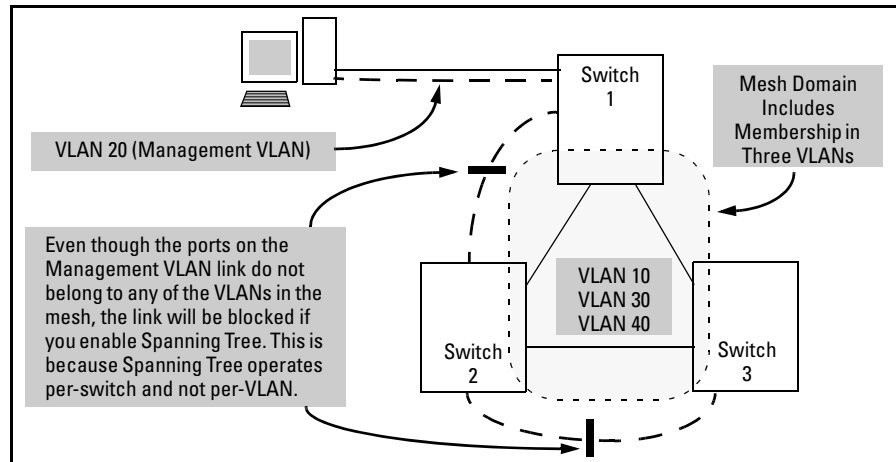
### Note

---

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.



**Figure 2-37. Example of Inadvertently Blocking a Management VLAN Link by Implementing Spanning Tree**

## Voice VLANs

Configuring voice VLANs separates voice traffic from data traffic and shields your voice traffic from broadcast storms. 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 (DiffServe 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 2-36.

## Migrating Layer 3 VLANs Using VLAN MAC Configuration

ProCurve routing switches provide an easy way to maintain Layer 3 VLAN configurations when you migrate distribution routers in a network configuration that is not centrally managed. By following the procedure described in this section, you can upgrade to ProCurve routing switches without stopping the operation of attached hosts that use existing routers as their default gateway to route traffic between VLANs. You can achieve seamless VLAN migration by configuring the MAC address of the previously installed router on the VLAN interfaces of a ProCurve routing switch.

### VLAN MAC Address Reconfiguration

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

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

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

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

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

When you reconfigure the MAC address on a VLAN interface, you may also specify a keepalive timeout to transmit heartbeat packets that advertise the new MAC address.

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

## Handling Incoming and Outgoing VLAN Traffic

Incoming VLAN data packets and ARP requests are received and processed on the routing switch according to the MAC address of the previously installed router that is configured for each VLAN interface.

Outgoing VLAN traffic uses the MAC address of the ProCurve switch as the source MAC address in packet headers. The MAC address configured on VLAN interfaces is not used on outbound VLAN traffic.

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

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

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

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

---

**Note**

---

The Virtual Router Redundancy Protocol (VRRP) is not supported on VLAN interfaces on which the MAC address for incoming traffic has been reconfigured

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

## Sending Heartbeat Packets with a Configured MAC Address

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

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

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

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

Heartbeat packets are sent at periodic intervals with a specific ProCurve unicast MAC address in destination field. This MAC address is assigned to ProCurve and is not used by other non-ProCurve routers. Because the heartbeat packet contains a unicast MAC address, it does not interrupt host operation. Even if you have multiple ProCurve switches connected to the network, there is no impact on network performance because each switch sends heartbeat packets with its configured MAC address as the destination address.

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

## Configuring a VLAN MAC Address with Heartbeat Interval

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

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

**Syntax:** [no] ip-recv-mac-address <mac-address> [interval <seconds>]

ip-recv-mac-address <mac-address>

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

interval <seconds>

*(Optional) Configures the time interval (in seconds) used between transmissions of heartbeat packets to all network devices configured on the VLAN. Valid values are from one to 255 seconds. The default is 60 seconds.*

### Operating Notes

- The **ip-recv-mac-address** command allows you to configure only one MAC address for a specified VLAN. If you re-enter the command to configure another MAC address, the previously configured MAC address is overwritten.
- Enter the **no** form of the command to remove a configured MAC address and restore the default MAC address of the ProCurve switch.
- When you configure a VLAN MAC address, you may also specify a heartbeat interval. The **interval <seconds>** parameter is optional.
- After you configure a VLAN MAC address:
  - IP router and MAC ARP replies to other VLAN devices contain the user-defined MAC address as the Ethernet sender hardware address.
  - Outbound VLAN traffic contains the ProCurve MAC address, not the configured MAC address, as the source MAC address in packet headers.

- Immediately after you configure a VLAN MAC address or remove a configured MAC address, a gratuitous ARP message is broadcast on the connected segment to announce the change of the IP-to-MAC address binding to all connected IP-based equipment.
- A configured VLAN MAC address supports proxy ARP and gracious ARP.
- A new MIB variable, **ifRcvAddressTable**, is introduced to support VLAN MAC configuration.
- You cannot configure a VLAN MAC address using the web browser or menu interface. You must use the CLI.
- VRRP is not supported on a VLAN interface with a user-configured MAC address.

### Example

The following example shows how to configure a MAC address on VLAN 101.

```
ProCurve# configure terminal
ProCurve(config)# vlan 101
ProCurve(vlan-101)# ip-recv-mac-address 0060b0-e9a200
interval 100
```

### Verifying a VLAN MAC Address Configuration

To verify the configuration of Layer 3 MAC addresses on the VLAN interfaces of a switch, enter the **show ip-recv-mac-address** command.

```
ProCurve# show ip-recv-mac-address

VLAN L3-Mac-Address Table

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