Port-Based Virtual LANs (VLANs) and GVRP

Contents

Overview ................................................................. 11-2

Port-Based Virtual LANs (Static VLANs) ......................... 11-3
  Overview of Using VLANs ........................................... 11-6
  Multiple VLAN Considerations ................................. 11-10
  Menu: Configuring VLAN Parameters ............................... 11-14
  CLI: Configuring VLAN Parameters ................................. 11-19
  Web: Viewing and Configuring VLAN Parameters .................. 11-25
  VLAN Tagging Information ........................................... 11-26
  The Secure Management VLAN ...................................................... 11-31
  Effect of VLANs on Other Switch Features .................. 11-35
  VLAN Restrictions .................................................. 11-36

GVRP ................................................................. 11-37
  General Operation .................................................. 11-38
  Per-Port Options for Handling GVRP “Unknown VLANs” .......... 11-40
  Per-Port Options for Dynamic VLAN Advertising and Joining ..... 11-42
  GVRP and VLAN Access Control ........................................ 11-44
  Planning for GVRP Operation ........................................... 11-45
  Configuring GVRP On a Switch .................................. 11-45
  GVRP Operating Notes .............................................. 11-50
Overview

This chapter describes the following features and how to configure them with the switch's built-in interfaces:

■ Port-Based VLANs — Page 11-3:
■ GVRP — Page 11-37:

For general information on how to use the switch's built-in interfaces, see:

■ Chapter 2, “Using the Menu Interface”
■ Chapter 3, “Using the Command Line Interface (CLI)”
■ Chapter 4, “Using the HP Web Browser Interface
■ Chapter 5, “Switch Memory and Configuration”
Port-Based Virtual LANs (Static VLANs)

<table>
<thead>
<tr>
<th>VLAN Features</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>view existing VLANs</td>
<td>n/a</td>
<td>page 11-14</td>
<td>page 11-20</td>
<td>page 11-25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>thru 11-19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>configuring static</td>
<td>default VLAN with</td>
<td>page 11-14</td>
<td>page 11-19</td>
<td>page 11-25</td>
</tr>
<tr>
<td>VLANs</td>
<td>VID = 1</td>
<td>thru 11-19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>configuring dynamic</td>
<td>disabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLANs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A VLAN is a group of ports designated by the switch as belonging to the same broadcast domain. (That is, all ports carrying traffic for a particular subnet address would normally belong to the same VLAN.)

**Note**

This section describes static VLANs, which are VLANs you manually configure with a name, VLAN ID (VID), and port assignments. (For information on dynamic VLANs, see “GVRP” on page 11-37.)

Using a VLAN, you can group users by logical function instead of physical location. This helps to control bandwidth usage 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.

By default, the Series 5300XL switch is 802.1Q VLAN enabled and allow up to 256 port-based VLANs (default: 8). For information on GVRP, see “GVRP” on page 11-37. (The 802.1Q compatibility enables you to assign each switch port to multiple VLANs, if needed, and the port-based nature of the configuration allows interoperation with older switches that require a separate port for each VLAN.)

**General Use and Operation.** Port-based VLANs are typically used to enable broadcast traffic reduction and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs that may be configured on a switch. On a given switch, packets are forwarded only between ports that are designated for the same VLAN. Thus, all ports carrying traffic for a particular subnet address should be configured to the same VLAN. Cross-domain broadcast traffic in the switch is
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

eliminated and bandwidth is saved by not allowing packets to flood out all ports. An external router is required to enable separate VLANs on a switch to communicate with each other.

For example, referring to figure 11-1, if ports A1 through A4 belong to VLAN_1 and ports A5 through A8 belong to VLAN_2, traffic from end-node stations on ports A2 through A4 is restricted to only VLAN_1, while traffic from ports A5 through A7 is restricted to only VLAN_2. For nodes on VLAN_1 to communicate with VLAN_2, their traffic must go through an external router via ports A1 and A8.

![Figure 11-1. Example of Routing Between VLANs via an External Router](image)

**Overlapping (Tagged) VLANs.** A port on the Series 5300XL switches can be a member of more than one VLAN if the device to which they are connected 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 to distinguish between traffic from different VLANs.
Similarly, using 802.1Q-compliant switches, you can connect multiple VLANs through a single switch-to-switch link.

Introducing Tagged VLAN Technology into Networks Running Legacy (Untagged) VLANs. You can introduce 802.1Q-compliant devices into networks that have built untagged VLANs based on earlier VLAN technology. The fundamental rule is that legacy/untagged VLANs require a separate link for each VLAN, while 802.1Q, or tagged VLANs can combine several VLANs in one link. This means that on the 802.1Q-compliant device, separate ports (configured as untagged) must be used to connect separate VLANs to non-802.1Q devices.
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

Overview of Using VLANs

VLAN Support and the Default VLAN

In the factory default configuration, VLAN support is enabled and all ports on the switch belong to the 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 the primary VLAN.

You can partition the switch into multiple virtual broadcast domains by adding one or more additional VLANs and moving ports from the default VLAN to the new VLANs. (The switch supports up to 256 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, this VLAN is always present; that is, you cannot delete it from the switch.

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) as the primary VLAN. However, to provide more control in your network, you can designate another 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 VLAN currently configured on the switch. (A dynamic—GVRP-learned—VLAN that has 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 act as primary.

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

**Per-Port Static VLAN Configuration Options**

The following figure and table show the options you have for assigning 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 11-1 briefly describes these options.
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

Example of Per-Port VLAN Configuration with GVRP Disabled (the default)

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

Example of Per-Port VLAN Configuration with GVRP Enabled

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

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

Figure 11-5. Comparing Per-Port VLAN Options With and Without GVRP

Table 14-1. Per-Port VLAN Configuration Options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Effect on Port Participation in Designated VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tagged</td>
<td>Allows the port to join multiple VLANs.</td>
</tr>
<tr>
<td>Untagged</td>
<td>Allows VLAN connection to a device that is configured for an untagged VLAN instead of a tagged VLAN. The switch allows no more than one untagged VLAN assignment per port.</td>
</tr>
<tr>
<td>No</td>
<td>No: Appears when the switch is not GVRP-enabled; prevents the port from joining that VLAN.</td>
</tr>
<tr>
<td>- or -</td>
<td>Auto: Appears when GVRP is enabled on the switch; allows the port to dynamically join any advertised VLAN that has the same VID</td>
</tr>
<tr>
<td>Forbid</td>
<td>Prevents the port from joining the VLAN, regardless of whether GVRP is enabled on the switch.</td>
</tr>
</tbody>
</table>
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, load balancing, and IGMP. (Refer to “Effect of VLANs on Other Switch Features” on page 11-35.) If you plan on using dynamic VLANs, include the port configuration planning necessary to support this feature. (See “GVRP” on page 11-37.)

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, each VLAN must have an IP address. Refer to “IP Configuration” on page 7-3.

VLAN Operating Notes

- **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 assigned to another VLAN will remain assigned to the DEFAULT_VLAN.

- **Deleting VLANs**: To delete a VLAN from the switch, you must first remove from that VLAN any ports assigned to it.

- **Adding or Deleting VLANs**: Changing the number of VLANs supported on the switch requires a reboot. Other VLAN configuration changes are dynamic.

See also “Multiple VLAN Considerations” on page 11-10.
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 Series 5300XL family, 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 an HP Procurve series 5300XL switch use the same MAC address. Thus, connecting a Series 5300XL (multiple forwarding database) switch to a single forwarding database switch where multiple VLANs exist imposes some cabling and port VLAN assignment restrictions. Table 11-2 illustrates the functional difference between the two database types.

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

This database allows multiple destinations for the same MAC address. If the switch detects a new destination for an existing MAC entry, it just adds a new instance of that MAC to the table.

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Destination VLAN ID</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0004ea-84d9f4</td>
<td>100</td>
<td>A9</td>
</tr>
<tr>
<td>0060b0-880a9</td>
<td>105</td>
<td>A10</td>
</tr>
<tr>
<td>0060b0-880a81</td>
<td>107</td>
<td>A17</td>
</tr>
</tbody>
</table>

This database allows only one destination for a MAC address. If the switch detects a new destination for an existing MAC entry, it replaces the existing MAC instance with a new instance showing the new destination.

Table 11-3 lists the database structure of current HP Procurve switch models.

### Table 11-3. Forwarding Database Structure for HP Procurve Switches

<table>
<thead>
<tr>
<th>Multiple Forwarding Databases*</th>
<th>Single Forwarding Database*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Series 5300XL switches</td>
<td>Switch 1600M/2400M/2424M</td>
</tr>
<tr>
<td>Series 4100GL switches</td>
<td>Switch 4000M/8000M</td>
</tr>
<tr>
<td>Switch 2650</td>
<td>Switch 800T</td>
</tr>
<tr>
<td>Switch 6108</td>
<td>Switch 2000</td>
</tr>
</tbody>
</table>

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

When a packet arrives with a destination MAC address that matches a MAC address in the switch's forwarding table, the switch tries to send the packet to the port listed for that MAC address. But, if the destination port is in a different VLAN than the VLAN on which the packet was received, the switch drops the packet. This is not a problem for a switch with a multiple forwarding database, because the switch allows multiple instances of a given MAC address; one for each valid destination. However, as shown above, a switch with a single forwarding database allows only one instance of a given MAC address. If you connect the two types of switches through multiple ports or trunks belonging to different VLANs, and enable routing on the Series 5300XL switch, then the other switch's record of the port and VLAN on which the 5300XL exists 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 11-6, the MAC address table for Switch 8000M will sometimes record the 5308XL as accessed on port A1 (VLAN 1), and other times as accessed on port B1 (VLAN 2):

![Diagram](https://example.com/diagram.png)

Figure 11-6. Example of Invalid Configuration for Single-Forwarding to Multiple-Forwarding Database Devices in a Multiple VLAN Environment

In figure 11-6, PC “A” sends an IP packet to PC “B”.

1. The packet enters VLAN 1 in the Switch 8000 with the 5308XLs 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 5308XL. The 5308XL 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 5308XL on VLAN 2 (port “B1”), the 8000M’s single forwarding database records the 5308XL 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 5308XL’s MAC address in the destination field. However, this time the Switch 8000M’s single forwarding database indicates that the 5308XL is on port B1 (VLAN 2), and the 8000M drops the packet instead of forwarding it.

3. Later, the 5308XL transmits a packet to the 8000M through the VLAN 1 link, and the 8000M updates its address table to indicate that the 5308XL is on port A1 (VLAN 1) instead of port B1 (VLAN 2). Thus, the 8000M’s information on the location of the 5308XL changes over time. For this reason, the 8000M discards some packets directed through it for the 5308XL, 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 11-7. Example of a Solution for Single-Forwarding to Multiple-Forwarding Database Devices in a Multiple VLAN Environment](image)

Now, the 8000M forwarding database always lists the 5308XL MAC address on port A1, and the 8000M will send traffic to either VLAN on the 5308X.

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 a Series 5300XL switch 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 11-2.) The fact that the Series 5300XL Switch uses the same MAC address on all VLAN interfaces causes no problems.

- The same port or port trunk interface for multiple (tagged) VLANs. This results in a forwarding database having multiple instances of the same MAC address with different VLAN IDs, but the same port number.

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

![Diagram of a valid topology for devices having multiple forwarding databases in a multiple VLAN environment.](image)

Figure 11-8. Example of a Valid Topology for Devices Having Multiple Forwarding Databases in a Multiple VLAN Environment
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

Menu: Configuring VLAN Parameters

In the factory default state, support is enabled for up to eight VLANs. (You can change the switch VLAN configuration to support up to 256 VLANs.) Also, all ports on the switch belong to the default VLAN (DEFAULT_VLAN) and are in the same broadcast/multicast domain. (The default VLAN is also the default primary VLAN—see “The Primary VLAN” on page 11-6.) In addition to the default VLAN, you can configure up to 255 other static VLANs by changing the “Maximum VLANs” parameter, adding new VLAN names and VIDs, and then assigning one or more ports to each VLAN. (The switch accepts a maximum of 256 VLANs, including the default VLAN and any dynamic VLANs the switch creates if you enable GVRP—page 11-37.) Note that each port can be assigned to multiple VLANs by using VLAN tagging. (See “VLAN Tagging Information” on page 11-26.)

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 11-22.)
- Enabling or disabling dynamic VLANs (See “GVRP” on page 11-37.)

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

   You will then see the following screen:

   Figure 11-9. The Default VLAN Support Screen

2. Press [E] (for Edit), then do one or more of the following:
To change the maximum number of VLANs, type the new number (1 - 256 allowed; default 8).

To designate a different VLAN as the primary VLAN, select the **Primary VLAN** field and use the space bar to select from the existing options.

To enable or disable dynamic VLANs, select the **GVRP Enabled** field and use the Space bar to toggle between options. (For GVRP information, see “GVRP” on page 11-37.)

**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.

---

**Figure 11-10. 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 11-11:

   
   DEFAULT_VLAN

   Figure 11-11. 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. See “GVRP” on page 11-37.)

4. Press [1] to move the cursor to the Name line and type the VLAN name (up to 12 characters, with no spaces) of a new VLAN that you want to add, then press [Enter].
   (Avoid these characters in VLAN names: 2, #, $, ^, &, *, {, and }.)

5. Press [S] (for Save). You will then see the VLAN Names screen with the new VLAN listed.
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

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 11-9 on page 11-14). 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:
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

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”.

<table>
<thead>
<tr>
<th>Port</th>
<th>DEFAULT_VLAN</th>
<th>VLAN-22</th>
<th>Port</th>
<th>DEFAULT_VLAN</th>
<th>VLAN-22</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Untagged</td>
<td>No</td>
<td>A9</td>
<td>Untagged</td>
<td>No</td>
</tr>
<tr>
<td>A2</td>
<td>Tagged</td>
<td>No</td>
<td>A10</td>
<td>Untagged</td>
<td>No</td>
</tr>
<tr>
<td>A3</td>
<td>Untagged</td>
<td>No</td>
<td>A11</td>
<td>Untagged</td>
<td>No</td>
</tr>
<tr>
<td>A4</td>
<td>Untagged</td>
<td>No</td>
<td>A12</td>
<td>Untagged</td>
<td>No</td>
</tr>
<tr>
<td>A5</td>
<td>Untagged</td>
<td>No</td>
<td>A13</td>
<td>Untagged</td>
<td>No</td>
</tr>
<tr>
<td>A6</td>
<td>Untagged</td>
<td>No</td>
<td>A14</td>
<td>Untagged</td>
<td>No</td>
</tr>
</tbody>
</table>

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 11-13. Example of VLAN Port Assignment Screen

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

Note

For GVRP Operation: If you enable GVRP on the switch, “No” converts to “Auto”, which allows the VLAN to dynamically join an advertised VLAN that has the same VID. See “Per-Port Options for Dynamic VLAN Advertising and Joining” on page 11-42.

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 11-19. (This example assumes the default GVRP setting—disabled—and that you do not plan to enable GVRP later.)
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

Ports A4 and A5 are assigned to both VLANs.
Ports A6 and A7 are assigned only to VLAN-22.
All other ports are assigned only to the Default VLAN.

---

For information on VLAN tags ("Untagged" and "Tagged"), refer to "VLAN Tagging Information" on page 11-26.

Figure 11-14. Example of VLAN Assignments for Specific Ports

For information on VLAN tags ("Untagged" and "Tagged"), refer to "VLAN Tagging Information" on page 11-26.

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 VLAN Parameters

In the factory default state, all ports on the switch belong to the default VLAN (DEFAULT_VLAN) and are in the same broadcast/multicast domain. (The default VLAN is also the default primary VLAN—see “The Primary VLAN” on page 11-6.) You can configure up to 29 additional static VLANs by adding new VLAN names, and then assigning one or more ports to each VLAN. (The switch accepts a maximum of 256 VLANs, including the default VLAN and any dynamic VLANs the switch creates if you enable GVRP—page 11-37.) Note that each port can be assigned to multiple VLANs by using VLAN tagging. (See “VLAN Tagging Information” on page 11-26.)
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

VLAN Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlans</td>
<td>below</td>
</tr>
<tr>
<td>show vlan &lt;vlan-id&gt;</td>
<td>11-21</td>
</tr>
<tr>
<td>max-vlans 1-256</td>
<td>11-22</td>
</tr>
<tr>
<td>primary-vlan &lt;vlan-id&gt;</td>
<td>11-22</td>
</tr>
<tr>
<td>[no] vlan &lt;vlan-id&gt;</td>
<td>11-23</td>
</tr>
<tr>
<td>name &lt;vlan-name&gt;</td>
<td>11-24</td>
</tr>
<tr>
<td>[no] tagged &lt;port-list&gt;</td>
<td>11-24</td>
</tr>
<tr>
<td>[no] untagged &lt;port-list&gt;</td>
<td>11-24</td>
</tr>
<tr>
<td>[no] forbid</td>
<td>11-24</td>
</tr>
<tr>
<td>auto &lt;port-list&gt;</td>
<td>11-24 (Available if GVRP enabled.)</td>
</tr>
<tr>
<td>static-vlan &lt;vlan-id&gt;</td>
<td>11-24 (Available if GVRP enabled.)</td>
</tr>
</tbody>
</table>

Displaying the Switch’s VLAN Configuration. The next 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. (See “GVRP” on page 11-37.)

Syntax:  show vlan

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

  802.1Q VLAN ID Name            Status
  ---------------------------------------
    1   DEFAULT_VLAN            Static
    22  VLAN-22                  Static
    33  GVRP_33                  Dynamic
```

Figure 11-15. Example of “Show VLAN” Listing (GVRP Enabled)
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 vlan <vlan-id>

<table>
<thead>
<tr>
<th>Port Information</th>
<th>Mode</th>
<th>Unknown VLAN Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Tagged</td>
<td>Learn</td>
</tr>
<tr>
<td>A2</td>
<td>Tagged</td>
<td>Learn</td>
</tr>
<tr>
<td>A5</td>
<td>Untagged</td>
<td>Learn</td>
</tr>
<tr>
<td>A6</td>
<td>Untagged</td>
<td>Learn</td>
</tr>
<tr>
<td>A7</td>
<td>Untagged</td>
<td>Learn</td>
</tr>
</tbody>
</table>

**Figure 11-16. Example of “Show VLAN” for a Specific Static VLAN**

**Figure 11-17. Example of “Show VLAN” for a Specific Dynamic VLAN**
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

Changing the Number of VLANs Allowed on the Switch. By default, the switch allows a maximum of 8 VLANs. You can specify any value from 1 to 256. (If GVRP is enabled, this setting includes any dynamic VLANs on the switch.) As part of implementing a new value, you must execute a write memory command (to save the new value to the startup-config file) and then reboot the switch.

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

For example, to reconfigure the switch to allow 10 VLANs:

```
HPswitch(config)# max-vlans 10
Command will take effect after saving configuration and reboot.
HP4108(config)# write memory
HP4108(config)# boot
Device will be rebooted, do you want to continue [y/n]? y
```

Figure 11-18. Example of Command Sequence for Changing the Number of VLANs

Changing the Primary VLAN. In the factory-default configuration, the default VLAN (DEFAULT_VLAN) is the primary VLAN. However, you can designate any static VLAN on the switch as the primary VLAN. (For more on the primary VLAN, see “The Primary VLAN” on page 11-6.) To view the available VLANs and their respective VIDs, use **show vlan**.

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

For example, to make VLAN 22 the primary VLAN:

```
HPswitch(config)# primary-vlan 22
```
Creating a New Static VLAN
Changing the VLAN Context Level.

With this command, entering a new VID creates a new static VLAN. Entering the VID or name of an existing static VLAN places you in the context level for that VLAN.

**Syntax:** `vlan <vlan-id> [name <name-str>]` Creates a new static VLAN if a VLAN with that VID does not already exist, and places you in that VLAN’s context level. If you do not use the name option, the switch uses “VLAN” and the new VID to automatically name the VLAN.

If the VLAN already exists, the switch places you in the context level for that VLAN.

`vlan <vlan-name>` Places you in the context level for that static VLAN.

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

```
HPswitch(config)# vlan 100
100: VLAN added.
HP4108(vlan-100)# show vlan

Status and Counters - VLAN Information

VLAN support : Yes
Maximum VLANs to support : 10
Primary VLAN : DEFAULT_VLAN

802.1Q VLAN ID Name Status
------------------- -----------
1 DEFAULT_VLAN Static
100 VLAN100 Static
```

Figure 11-19. Example of Creating a New Static VLAN

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

```
HPswitch(vlan-100)# vlan default_vlan
HPswitch(vlan-1) 
```
**Port-Based Virtual LANs (VLANs) and GVRP**

**Port-Based Virtual LANs (Static VLANs)**

Converting a Dynamic VLAN to a Static VLAN. If GVRP is running on the switch and a port dynamically joins a VLAN, you can use the next command to convert the dynamic VLAN to a static VLAN. (For GVRP and dynamic VLAN operation, see “GVRP” on page 11-37.) This is necessary if you want to make the VLAN permanent. 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.

**Syntax:**
```
static-vlan <vlan-id>  
```
(Use `show vlan` to list current VIDs.)

For example, suppose a dynamic VLAN with a VID of 125 exists on the switch. The following command converts the VLAN to a static VLAN.

```
HPswitch(config)# static-vlan 125
```

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

You can use these options from the configuration level by beginning the command with `vlan <vlan-id>`, or from the context level of the specific VLAN.

**Syntax:**
```
name <vlan-name>  
[no] tagged <port-list>  
[no] untagged <port-list>  
[no] forbid <port-list>  
auto <port-list>
```

- **Changes the name of the existing static VLAN. (Avoid spaces and the following characters in the `<vlan-name>` entry: 2, #, $, ^, &, *, (, and ).)**
- **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.**
- **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.**
- **Configures the indicated port(s) as “forbidden” to participate in the designated VLAN. The “no” version sets the port(s) to either No or (if GVRP is enabled) to Auto.**
- **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, see “GVRP” on page 11-37.)
Port-Based Virtual LANs (VLANs) and GVRP

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 1-5 to Tagged, you could do so with these commands:

```
HPswitch(config)# vlan 100 name Blue_Team
HPswitch(config)# vlan 100 tagged 1-5
```

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

```
HPswitch(config)# vlan 100
HPswitch(vlan-100)# name Blue_Team
HPswitch(vlan-100)# tagged 1-5
```

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 config level, use:
```
HPswitch(config)# no vlan 100 tagged 1-5
```
- or -

At the VLAN 100 context level, use:
```
HPswitch(vlan-100)# no tagged 1-5
```

**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 GVRP mode
- Select a new Primary VLAN

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

1. Click on the Configuration tab.

Click on [Vlan Configuration].

2. 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.

**VLAN Tagging Information**

VLAN tagging enables traffic from more than one VLAN to use the same port. (Even when two or more VLANs use the same port they remain as separate domains and cannot receive traffic from each other without going through an external router.) As mentioned earlier, a “tag” is simply a unique VLAN identification number (VLAN ID, or VID) assigned to a VLAN at the time that you configure the VLAN name in the switch. In the Series 5300XL switches the tag can be any number from 1 to 4094 that is not already assigned to a VLAN. When you subsequently assign a port to a given VLAN, you must implement the VLAN tag (VID) if the port will carry traffic for more than one VLAN. Otherwise, the port VLAN assignment can remain “untagged” because the tag is not needed. On a given switch, this means you should use the “Untagged” designation for a port VLAN assignment where the port is connected to non 802.1Q-compliant device or is assigned to only one VLAN. Use the “Tagged” designation when the port is assigned to more than one VLAN or the port is connected to a device that does comply with the 802.1Q standard.

For example, if port A7 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 A7, then at least one of those VLAN assignments must be “tagged” so that Red VLAN traffic can be distinguished from Green VLAN traffic. The following illustration shows this concept:
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

Blue Server
White Server
Green Server
Red Server
Red VLAN
Green VLAN
Red VLAN: Untagged
Green VLAN: Tagged

Ports 1-6: Untagged
Port 7: Red VLAN Untagged
Green VLAN Tagged

Figure 11-20. 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 11-20 (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.
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

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.

![VID Numbers]

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).
- Any port that has two or more VLANs assigned to it can have one VLAN assignment for that port as “Untagged”. All other VLANs assigned to the same port must be configured as “Tagged”. (There can be no more than one Untagged VLAN on a port.)
- 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 makes it easier to manage your VLAN assignments, or for security reasons.

For example, in the following network, switches X and Y and servers S1 and S2 are 802.1Q-compliant. (Server S3 could also be 802.1Q-compliant, but it makes no difference for this example.)

![Figure 11-21. Example of VLAN ID Numbers Assigned in the VLAN Names Screen]
The VLANs assigned to ports X3, X4, Y2, Y3, and Y4 can all be untagged because there is only one VLAN assigned per port. Port X1 has multiple VLANs assigned, which means that one VLAN assigned to this port can be untagged and any others must be tagged. The same applies to ports X2, Y1, and Y5.

<table>
<thead>
<tr>
<th>Switch X</th>
<th>Port</th>
<th>Red VLAN</th>
<th>Green VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>X1</td>
<td>Untagged</td>
<td>Tagged</td>
<td></td>
</tr>
<tr>
<td>X2</td>
<td>Untagged</td>
<td>Tagged</td>
<td></td>
</tr>
<tr>
<td>X3</td>
<td>No*</td>
<td>Untagged</td>
<td></td>
</tr>
<tr>
<td>X4</td>
<td>Untagged</td>
<td>No*</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Switch Y</th>
<th>Port</th>
<th>Red VLAN</th>
<th>Green VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y1</td>
<td>Untagged</td>
<td>Tagged</td>
<td></td>
</tr>
<tr>
<td>Y2</td>
<td>No*</td>
<td>Untagged</td>
<td></td>
</tr>
<tr>
<td>Y3</td>
<td>No*</td>
<td>Untagged</td>
<td></td>
</tr>
<tr>
<td>Y4</td>
<td>Untagged</td>
<td>No*</td>
<td></td>
</tr>
<tr>
<td>Y5</td>
<td>Untagged</td>
<td>Tagged</td>
<td></td>
</tr>
</tbody>
</table>

*“No” means the port is not a member of that VLAN. For example, port X3 is not a member of the Red VLAN and does not carry Red VLAN traffic. Also, if GVRP were enabled, “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".
Port-Based Virtual LANs (VLANs) and GVRP
Port-Based Virtual LANs (Static VLANs)

To summarize:

<table>
<thead>
<tr>
<th>VLANs Per Port</th>
<th>Tagging Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Untagged or Tagged. If the device connected to the port is 802.1Q-compliant, then the recommended choice is “Tagged”.</td>
</tr>
<tr>
<td>2 or More</td>
<td>1 VLAN Untagged; all others Tagged or All VLANs Tagged</td>
</tr>
</tbody>
</table>

A given VLAN must have the same VID on any 802.1Q-compliant device in which the VLAN is configured. The ports connecting two 802.1Q devices should have identical VLAN configurations, as shown for ports X2 and Y5, above.
The Secure Management VLAN

Configures a secure Management VLAN by creating an isolated network for managing the HP Procurve switches that support this feature. (As of June 1, 2002, includes the HP Procurve Series 5300XL switches and Series 5300XL switches.) Access to this VLAN, and to the switch’s management functions (Menu, CLI, and web browser interface) is available only through ports configured as members.

- Multiple ports on the switch can belong to the Management VLAN. This allows connections for multiple management stations you want to have access to the Management VLAN, while at the same time allowing Management VLAN links between switches configured for the same Management VLAN.

- Only traffic from the Management VLAN can manage the switch, which means that only the workstations and PCs connected to ports belonging to the Management VLAN can manage and reconfigure the switch.

Figure 11-23 illustrates use of the Management VLAN feature to support management access by a group of management workstations.

![Figure 11-23. Example of Potential Security Breaches](image-url)
In figure 11-24, Workstation 1 has management access to all three switches through the Management VLAN, while the PCs do not. This is because configuring a switch to recognize a Management VLAN automatically excludes attempts to send management traffic from any other VLAN.

### Table 11-4. VLAN Membership in Figure 11-24

<table>
<thead>
<tr>
<th>Switch</th>
<th>A1</th>
<th>A3</th>
<th>A6</th>
<th>A7</th>
<th>B2</th>
<th>B4</th>
<th>B5</th>
<th>B9</th>
<th>C2</th>
<th>C3</th>
<th>C6</th>
<th>C8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management VLAN (VID = 7)</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Marketing VLAN (VID = 12)</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Shipping Dept. VLAN (VID = 20)</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>DEFAULT-VLAN (VID = 1)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

### Preparation

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

2. Determine the IP addressing for the Management VLAN (DHCP/Bootp or Manual).

3. Plan your Management VLAN topology to use HP Procurve switches that support this feature. (As of June 1, 2002, this includes the HP Procurve Series 5300XL and Series 4100GL switches.) 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 11-24.)
- Ports on one switch that you will use to extend the Management VLAN to ports on other HP ProCurve switches (such as ports A1 and B2 or B4 and C2 in figure 11-24 on page 11-32).

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.

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

5. 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:**

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

**Default:** Disabled

For example, suppose you have already configured a VLAN named `My_VLAN` with a VID of 100 in a Series 5300XL switch. 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 Series 5300XL switch.

![Figure 11-25. Illustration of Configuration Example](image-url)
Port-Based Virtual LANs (VLANs) and GVRP

Port-Based Virtual LANs (Static VLANs)

HPswitch (config)# management-vlan 100
HPswitch (config)# vlan 100 tagged a1
HPswitch (config)# vlan 100 tagged a2

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

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

Operating Notes for Management VLANs

- On Series 5300XL switches with routing enabled, 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. (HP Series 5300XL switches only.)
- If you implement a Management VLAN in a switch mesh environment, all meshed ports on Series 5300XL switches 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.

![Diagram of VLANs and Spanning Tree](image)

**Figure 11-26. Example of Inadvertently Blocking a Management VLAN Link by Implementing Spanning Tree**

**Effect of VLANs on Other Switch Features**

**Spanning Tree Operation with VLANs**

Because the Series 5300XL switches follows the 802.1Q VLAN recommendation to use single-instance spanning tree, Spanning Tree operates across all ports on the switch (regardless of VLAN assignments) instead of on a per-VLAN basis. 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. However, you can use port trunking to prevent Spanning Tree from unnecessarily blocking ports (and to improve overall network performance). Refer to “Spanning Tree Operation with 802.1Q VLANs” on page 13-4.

Note that Spanning Tree operates differently in different devices. For example, in the (obsolete, non-802.1Q) HP Switch 2000 and the HP Switch 800T, Spanning Tree operates 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 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 Series 5300XL switches have one unique MAC address for all of their VLAN interfaces. You can send an 802.2 test packet to this MAC address to verify connectivity to the switch. 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.

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, see “VLAN-Related Problems” on page C-23.

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 assigned to several VLANs, but only one of those assignments can be untagged. (The “Untagged” designation enables VLAN operation with non 802.1Q-compliant devices.)
- An external router must be used to communicate between tagged VLANs on the switch.
- Before you can delete a VLAN, you must first re-assign all ports in the VLAN to another VLAN.
GVRP

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>view GVRP configuration</td>
<td>n/a</td>
<td>page 11-45</td>
<td>page 11-47</td>
<td>page 11-50</td>
</tr>
<tr>
<td>list static and dynamic VLANs on a GVRP-enabled switch</td>
<td>n/a</td>
<td>—</td>
<td>page 11-49</td>
<td>page 11-50</td>
</tr>
<tr>
<td>enable or disable GVRP</td>
<td>disabled</td>
<td>page 11-45</td>
<td>page 11-48</td>
<td>page 11-50</td>
</tr>
<tr>
<td>enable or disable GVRP on individual ports</td>
<td>enabled</td>
<td>page 11-45</td>
<td>page 11-48</td>
<td>—</td>
</tr>
<tr>
<td>control how individual ports will handle advertisements for new VLANs</td>
<td>Learn</td>
<td>page 11-45</td>
<td>page 11-48</td>
<td>page 11-50</td>
</tr>
<tr>
<td>convert a dynamic VLAN to a static VLAN</td>
<td>n/a</td>
<td>—</td>
<td>page 11-50</td>
<td>—</td>
</tr>
<tr>
<td>configure static VLANs</td>
<td>DEFAULT_VLAN (VID = 1)</td>
<td>page 11-14</td>
<td>page 11-19</td>
<td>page 11-50</td>
</tr>
</tbody>
</table>

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

**Note**

To understand and use GVRP you must have a working knowledge of 802.1Q VLAN tagging. (See “Port-Based Virtual LANs (Static VLANs)” on page 11-3.)

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

GVRP enables the Series 5300XL switches to dynamically create 802.1Q-compliant VLANs on links with other devices running GVRP. This enables the switch to automatically create VLAN links between GVRP-aware devices. (A GVRP link can include intermediate devices that are not GVRP-aware.) This operation reduces the chances for errors in VLAN configuration by automatically providing VLAN ID (VID) consistency across the network. That is, you can use GVRP to propagate VLANs to other GVRP-aware devices instead of manually having to set up VLANs across your network. After the switch creates a dynamic VLAN, you can optionally use the CLI `static <vlan-id>` command to convert it to a static VLAN or allow it to continue as a dynamic VLAN for as long as needed. You can also use GVRP to dynamically enable port membership in static VLANs configured on a switch.
General Operation

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

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

**Operating Note:** When a GVRP-aware port on a switch learns a VID through GVRP from another device, the switch begins advertising that VID out all of its ports except the port on which the VID was learned.

<table>
<thead>
<tr>
<th>Core switch with static VLANs (VID= 1, 2, &amp; 3). Port 2 is a member of VIDs 1, 2, &amp; 3.</th>
<th>2. Port 1 receives advertisement of VIDs 1, 2, &amp; 3 AND becomes a member of VIDs 1, 2, &amp; 3.</th>
<th>4. Port 4 receives advertisement of VIDs 1, 2, &amp; 3 AND becomes a member of VIDs 1, 2, &amp; 3.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Port 2 advertises VIDs 1, 2, &amp; 3.</td>
<td>3. Port 3 advertises VIDs 1, 2, &amp; 3, but port 3 is NOT a member of VIDs 1, 2, &amp; 3 at this point.</td>
<td>5. Port 5 advertises VIDs 1, 2, &amp; 3, but port 5 is NOT a member of VIDs 1, 2, &amp; 3 at this point.</td>
</tr>
</tbody>
</table>

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

---

**Figure 11-27. Example of Forwarding Advertisements and Dynamic Joining**

Note that if a static VLAN is configured on at least one port of a switch, and that port has established a link with another device, then all other ports of that switch will send advertisements for that VLAN.
For example, in the following figure, Tagged VLAN ports on switch “A” and switch “C” advertise VLANs 22 and 33 to ports on other GVRP-enabled switches that can dynamically join the VLANs.

Figure 11-28. Example of GVRP Operation

Note

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

A GVRP-aware port receiving advertisements has these options:

- If there is not already a static VLAN with the advertised VID on the receiving port, then dynamically create the VLAN and become a member.
- If the switch already has a static VLAN assignment with the same VID as in the advertisement, and the port is configured to Auto for that VLAN, then the port will dynamically join the VLAN and begin moving that VLAN's traffic. (For more detail on Auto, see “Per-Port Options for Dynamic VLAN Advertising and Joining” on page 11-42.)
- Ignore the advertisement for that VID.
- Don’t participate in that VLAN.
Note also that a port belonging to a Tagged or Untagged static VLAN has these configurable options:

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

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

**Per-Port Options for Handling GVRP “Unknown VLANs”**

An “unknown VLAN” is a VLAN that the switch learns of by receiving an advertisement for that VLAN on a port that is not already a member of that VLAN. If the port is configured to learn unknown VLANs, then the VLAN is dynamically created and the port becomes a tagged member of the VLAN. For example, suppose that in figure 11-28 (page 11-39), port 1 on switch “A” is connected to port 5 on switch “C”. Because switch “A” has VLAN 22 statically configured, while switch “C” does not have this VLAN statically configured (and does not “Forbid” VLAN 22 on port 5), VLAN 22 is handled as an “Unknown VLAN” on port 5 in switch “C”. Conversely, if VLAN 22 was statically configured on switch C, but port 5 was not a member, port 5 would become a member when advertisements for VLAN 22 were received from switch “A”.

When you enable GVRP on a switch, you have the per-port join-request options listed in table 11-5:
Port-Based Virtual LANs (VLANs) and GVRP

Table 11-5. Options for Handling “Unknown VLAN” Advertisements:

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

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

![Figure 11-29. Example of GVRP Unknown VLAN Settings](image)

```
HPswitch# show gvrp

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

Port Type | Unknown VLAN
---------- | ---------------
A1 10/100TX | Learn
A2 10/100TX | Learn
A3 10/100TX | Block
A4 10/100TX | Block
A5 10/100TX | Learn
A6 10/100TX | Disable
A7 10/100TX | Learn
A8 10/100TX | Learn
```

Figure 11-29. Example of GVRP Unknown VLAN Settings
Per-Port Options for Dynamic VLAN Advertising and Joining

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

**Enabling a Port for Dynamic Joins.** You can configure a port to dynamically join a static VLAN. The join will then occur if that port subsequently receives an advertisement for the static VLAN. (This is done by using the Auto and Learn options described in table 11-6, below.

**Parameters for Controlling VLAN Propagation Behavior.** You can configure an individual port to actively or passively participate in dynamic VLAN propagation or to ignore dynamic VLAN (GVRP) operation. These options are controlled by the GVRP “Unknown VLAN” and the static VLAN configuration parameters, as described in the following table:
<table>
<thead>
<tr>
<th>Per-Port &quot;Unknown VLAN&quot; (GVRP) Configuration</th>
<th>Static VLAN Options—Per VLAN Specified on Each Port (^1)</th>
<th>Port Activity: Tagged or Untagged (Per VLAN) (^2)</th>
<th>Port Activity: Auto (^2) (Per VLAN)</th>
<th>Port Activity: Forbid (Per VLAN) (^2)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Learn</strong> (the Default)</td>
<td>The port:</td>
<td>The port:</td>
<td>The port:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Belongs to specified VLAN.</td>
<td>• Will become a member of</td>
<td>1. Will not become a member of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Advertises specified VLAN.</td>
<td>specified VLAN if it receives</td>
<td>the specified VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can become a member of</td>
<td>advertisements for specified</td>
<td>1. Will not advertise specified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dynamic VLANs for which it</td>
<td>VLAN from another device.</td>
<td>VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>receives advertisements.</td>
<td>• Will advertise specified</td>
<td>1. Can become a member of other dynamic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Advertises dynamic VLANs that have at least</td>
<td>VLAN.</td>
<td>VLANs for which it receives</td>
<td></td>
</tr>
<tr>
<td></td>
<td>one other port on the same switch as a member.</td>
<td>• Can become a member of other,</td>
<td>advertisements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>dynamic VLANs for which it</td>
<td>1. Will advertise a dynamic VLAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>receives advertisements.</td>
<td>that has at least one other port on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Will advertise a dynamic VLAN</td>
<td>same switch as a member.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>that has at least one other port</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(on the same switch) as a member.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Block</strong></td>
<td>The port:</td>
<td>The port:</td>
<td>The port:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Belongs to the specified VLAN.</td>
<td>• Will become a member of</td>
<td>1. Will not become a member of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Advertises this VLAN.</td>
<td>specified VLAN if it receives</td>
<td>the specified VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Will not become a member of new dynamic</td>
<td>advertisements for this VLAN.</td>
<td>1. Will not advertise this VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLANs for which it receives advertisements.</td>
<td>• Will advertise this VLAN.</td>
<td>1. Will not become a member of dynamic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Will advertise dynamic VLANs that have at</td>
<td>• Will not become a member of new</td>
<td>VLANs for which it receives advertisements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>least one other port on the same switch as a</td>
<td>dynamic VLANs for which it</td>
<td>• Will advertise dynamic VLANs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>member.</td>
<td>receives advertisements.</td>
<td>that have at least one other port on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Will advertise dynamic VLANs that</td>
<td>same switch as a member.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>have at least one other port (on the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>same switch) as a member.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Disable</strong></td>
<td>The port:</td>
<td>The port:</td>
<td>The port:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Is a member of the specified VLAN.</td>
<td>• Will not become a member of the</td>
<td>1. Will not become a member of this VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Will ignore GVRP PDUs.</td>
<td>specified VLAN.</td>
<td>• Will ignore GVRP PDUs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Will not join any advertised VLANs.</td>
<td>• Will not join any dynamic VLANs.</td>
<td>• Will not join any dynamic VLANs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Will not advertise VLANs.</td>
<td>• Will not advertise VLANs.</td>
<td>• Will not advertise VLANs.</td>
<td></td>
</tr>
</tbody>
</table>

\(^1\) Each port of a Series 5300XL switches must be a Tagged or Untagged member of at least one VLAN. Thus, any port configured for GVRP to Learn or Block will generate and forward advertisements for static VLAN(s) configured on the switch and also for dynamic VLANs the switch learns on other ports.

\(^2\) To configure tagging, Auto, or Forbid, see “Configuring Static VLAN Name and Per-Port Settings” on page 11-24 (for the CLI) or “Adding or Changing a VLAN Port Assignment” on page 11-17 (for the menu).
As the preceding table indicates, when you enable GVRP, a port that has a Tagged or Untagged static VLAN has the option for both generating advertisements and dynamically joining other VLANs.

**Note**

In table 11-6, above, the Unknown VLAN parameters are configured on a per-port basis using the CLI. The Tagged, Untagged, Auto, and Forbid options are configured per static VLAN on every port, using either the menu interface or the CLI.

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

**GVRP and VLAN Access Control**

When you enable GVRP on a switch, the default GVRP parameter settings allow all of the switch’s ports to transmit and receive dynamic VLAN advertisements (GVRP advertisements) and to dynamically join VLANs. The two preceding sections describe the per-port features you can use to control and limit VLAN propagation. To summarize, you can:

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

**Port-Leave From a Dynamic VLAN**

A dynamic VLAN continues to exist on a port for as long as the port continues to receive advertisements of that VLAN from another device connected to that port or until you:

- Convert the VLAN to a static VLAN (See “Converting a Dynamic VLAN to a Static VLAN” on page 11-24.)
- Reconfigure the port to **Block** or **Disable**
- Disable GVRP
- Reboot the switch

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

These steps outline the procedure for setting up dynamic VLANs for a segment.

1. Determine the VLAN topology you want for each segment (broadcast domain) on your network.
2. Determine the VLANs that must be static and the VLANs that can be dynamically propagated.
3. Determine the device or devices on which you must manually create static VLANs in order to propagate VLANs throughout the segment.
4. Determine security boundaries and how the individual ports in the segment will handle dynamic VLAN advertisements. (See table 11-5 on page 11-41 and table 11-6 on page 11-43.)
5. Enable GVRP on all devices you want to use with dynamic VLANs and configure the appropriate “Unknown VLAN” parameter (Learn, Block, or Disable) for each port.
6. Configure the static VLANs on the switch(es) where they are needed, along with the per-VLAN parameters (Tagged, Untagged, Auto, and Forbid—see table 11-6 on page 11-43) on each port.
7. Dynamic VLANs will then appear automatically, according to the configuration options you have chosen.
8. Convert dynamic VLANs to static VLANs where you want dynamic VLANs to become permanent.

Configuring GVRP On a Switch

The procedures in this section describe how to:

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

To view or configure static VLANs for GVRP operation, refer to “Per-Port Static VLAN Configuration Options” on page 11-7.

Menu: Viewing and Configuring GVRP

1. From the Main Menu, select:
Port-Based Virtual LANs (VLANs) and GVRP

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

The Unknown VLAN fields enable you to configure each port to:
- Learn - Dynamically join any advertised VLAN and advertise all VLANs learned through other ports.
- Block - Do not dynamically join any VLAN, but still advertise all VLANs learned through other ports.
- Disable - Ignore and drop all incoming advertisements and do not transmit any advertisements.

---

Figure 11-30. The VLAN Support Screen (Default Configuration)

2. Do the following to enable GVRP and display the Unknown VLAN fields:
   b. Use [v] to move the cursor to the GVRP Enabled field.
   c. Press the Space bar to select Yes.
   d. Press [v] again to display the Unknown VLAN fields.

---

Figure 11-31. Example Showing Default Settings for Handling Advertisements

3. Use the arrow keys to select the port you want, and the Space bar to select Unknown VLAN option for any ports you want to change.

4. When you finish making configuration changes, press [Enter], then [S] (for Save) to save your changes to the Startup-Config file.
Displaying the Switch’s Current GVRP Configuration. This command shows whether GVRP is disabled, along with the current settings for the maximum number of VLANs and the current Primary VLAN. (For more on the last two parameters, see “Port-Based Virtual LANs (Static VLANs)” on page 11-3.)

Syntax: show gvrp

Shows the current settings.

```
HPswitch> show gvrp
GVRP support
  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled : No
```

Figure 11-32. Example of “Show GVRP” Listing with GVRP Disabled

```
HPswitch> show gvrp
GVRP support
  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled : Yes

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

This example includes non-default settings for the Unknown VLAN field for some ports.
```

Figure 11-33. Example of Show GVRP Listing with GVRP Enabled
Enabling and Disabling GVRP on the Switch. This command enables GVRP on the switch.

**Syntax:** `gvrp`

This example enables GVRP:

```
HPswitch(config)# gvrp
```

This example disables GVRP operation on the switch:

```
HPswitch(config)# no gvrp
```

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

**Syntax:** `interface <port-list> unknown-vlans <learn | block | disable>`  Changes the Unknown VLAN field setting for the specified port(s).

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

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

```
HP4108(config)# show gvrp
GVRP support
  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled : Yes
Port Type | Unknown VLAN
----------+----------
  1 10/100TX | Block
  2 10/100TX | Block
  3 10/100TX | Learn
  4 10/100TX | Learn
            |          |          |          |          |          |
Displaying the Static and Dynamic VLANs Active on the Switch. The `show vlans` command lists all VLANs present in the switch.

**Syntax:**
```
show vlans
```

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

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

```
Switch-B> show vlans
Status and Counters - VLAN Information

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

802.1Q VLAN ID Name Status
----------------- -------------
1   DEFAULT_VLAN Static
222  GVRP_222    Dynamic
333  GVRP_333    Dynamic
```

Figure 11-34. Example of Listing Showing Dynamic VLANs
Converting a Dynamic VLAN to a Static VLAN. If a port on the switch has joined a dynamic VLAN, you can use the following command to convert that dynamic VLAN to a static VLAN:

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

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

```
HPswitch(config)# static 333
```

When you convert a dynamic VLAN to a static VLAN, all ports on the switch are assigned to the VLAN in Auto mode.

Web: Viewing and Configuring GVRP

To view, enable, disable, or reconfigure GVRP:

1. Click on the **Configuration** tab.

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

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

GVRP Operating Notes

- A dynamic VLAN must be converted to a static VLAN before it can have an IP address.

- The total number of VLANs on the switch (static and dynamic combined) cannot exceed the current Maximum VLANs setting. For example, in the factory default state, the switch supports eight VLANs. Thus, in a case where four static VLANs are configured on the switch, the switch can accept up to four additional VLANs in any combination of static and dynamic. Any additional VLANs advertised to the switch will not be added unless you first increase the Maximum VLANs setting. In the Menu interface, click on **2. Switch Configuration …** | **8. VLAN Menu** | **1. VLAN Support**. In the global config level of the CLI, use `max-vlans`.
■ Converting a dynamic VLAN to a static VLAN and then executing the **write memory** command saves the VLAN in the startup-config file and makes it a permanent part of the switch’s VLAN configuration.

■ Within the same broadcast domain, a dynamic VLAN can pass through a device that is not GVRP-aware. This is because a hub or a switch that is not GVRP-ware will flood the GVRP (multicast) advertisement packets out all ports.

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

■ Rebooting a switch on which a dynamic VLAN exists deletes that VLAN. However, the dynamic VLAN re-appears after the reboot if GVRP is enabled and the switch again receives advertisements for that VLAN through a port configured to add dynamic VLANs.

■ By receiving advertisements from other devices running GVRP, the switch learns of static VLANs on those other devices and dynamically (automatically) creates tagged VLANs on the links to the advertising devices. Similarly, the switch advertises its static VLANs to other GVRP-aware devices, as well as the dynamic VLANs the switch has learned.

■ A GVRP-enabled switch does not advertise any GVRP-learned VLANs out of the port(s) on which it originally learned of those VLANs.
Port-Based Virtual LANs (VLANs) and GVRP

GVRP

— This page intentionally unused. —