This chapter describes how to configure VLANs on HP routing switches using the CLI and the Web management interface.

A detailed summary of all CLI commands highlighted in this chapter, noting syntax and possible values, can be found in Appendix B.

Overview of Policy-Based VLANs

Policy-based VLANs allow users to assign VLANs on a protocol (IP, IPX, Decnet, AppleTalk, NetBIOS, Other), sub-net (IP Sub-net and IPX Network), port or 802.1Q tagged basis. VLANs are used to refer to a collection of devices that communicate as if they were on the same physical LAN.

HP routing switches can be configured with:

- No VLAN (system default)
- Port-based VLANs only (Layer 2 VLANs)
- Protocol-based VLANs only (Layer 3 VLANs)
- Port-based VLANs and protocol-based VLANs (Layer 2 and Layer 3 VLANs)

VLANs can overlay one another. A port or ports within a port-based VLAN can be further partitioned by assigning the ports to a protocol VLAN.

The following Layer 3 VLANs are supported:

- IP Protocol
- IPX Protocol
- IP Sub-net
- IPX Network Number
- AppleTalk
- Decnet
- NetBIOS
- Other
Port-based VLANs

Port-based VLANs allow the user to group specific port traffic into different broadcast domains. These domains can be used to isolate or consolidate certain types of traffic, such as all IP or IPX traffic in distinct VLANs. VLANs can also be used to separate corporate functions, such as finance or engineering and their broadcasts. Port-based VLANs should be used to maintain distinct spanning tree domains.

When port-based VLAN operation is first enabled, by default, all ports will be assigned to default VLAN 1. As other VLANs are created and ports are assigned to them, the ports will be removed from the default VLAN. All ports not assigned to another VLAN will remain members of default VLAN 1. This is to ensure that all ports are members of at least one VLAN.

HP routing switches support up to 4,096 port-based VLANs with a default of 8.

Protocol-based VLANs

By supporting the grouping of like protocols, protocol-based VLANs reduce the number of non-essential broadcasts on other ports by keeping all broadcasts for a given protocol within a defined VLAN.

It also allows a port to belong to multiple-protocol VLANs without VLAN tagging, easing design and administration burden.

Additionally, IP sub-net and IPX network VLANs allow devices within a common sub-net to be resident across multiple ports of HP routing switches. When sub-nets span multiple ports, a greater pool of bandwidth for all devices can increase performance.

Protocol VLAN Port Membership

There are three types of port membership within a protocol VLAN: static, dynamic and exclude. A VLAN can be made up of any combination of these port assignments.

Port Assignment

Ports are dynamically assigned when non-routable protocol VLANs such as Decnet and NetBIOS are created.

NOTE: When IP or IPX VLANs are created on routers or router modules, ports are not dynamically assigned to the VLANs. Only those ports explicitly configured to belong to an IP or IPX Protocol VLAN will be members of the VLAN.

Modifying Port Assignment

To modify dynamic port assignment, the user can specify a port as static or he or she can exclude the port from VLAN membership. When a port is assigned as static, it becomes a permanent member of the VLAN. Ports that are excluded are permanently removed from membership of a VLAN. In addition to using the static and exclude assignments for ports, the user can allow ports to age out automatically.

Aging of Dynamic Ports

Dynamic ports within any protocol VLAN will age out after 10 minutes, if no member protocol traffic is received on a port within the VLAN. The aged out port, however, remains as a candidate dynamic port for that VLAN. It will become active in the VLAN again, if member protocol traffic is received on that port.

Once re-activated, the aging out period for the port will be reset to 20 minutes. Each time a member protocol packet is received by a candidate dynamic port (aged out port) the port will become active again and the aging out period reset for 20 minutes.
Broadcast and Multicast Packets within VLANs
By default, all broadcast and multicast packets will be sent to all active dynamic ports. To discover protocol membership for those dynamic ports that have been aged out (candidate dynamic ports), one-eighth of the traffic from each source MAC address will be sent to candidate dynamic ports. Additionally, one-eighth of the ARP packets will be sent to candidate dynamic ports to aid in dynamic port discovery. Both of these actions are done so that the system software can determine if candidate dynamic ports should belong to the active dynamic ports.

Routing between VLANs using Virtual Interfaces
HP routing switches support routing between VLANs via virtual interfaces. These virtual interfaces are logical interfaces that provide VLANs access to the router functions.

For example, in Figure 14.1, the user wants to route IP traffic among the four ports that are running IP traffic. As an integrated switch-router, HP routing switches can support the assignment of VLANs, a switch capability, as well as route between VLANs. Given this, the user is able to configure IP sub-net VLANs and then assign virtual interfaces (v5 and v3) to route between the two IP sub-net VLANs.

Figure 14.1 Configuring IP sub-net VLANs and virtual interfaces to support routing of IP traffic across the ports without sacrificing physical ports (capacity)
Configuring Port-based VLANs

Port-based VLANs allow users to provide separate spanning tree domains or broadcast domains on a port-by-port basis.

A complete listing of all CLI commands described in this section can also be found in Appendix B.

The user can configure the following for port-based VLANs:

- Add a VLAN
- Delete a VLAN
- Modify a VLAN
  - Assign a higher priority to a VLAN
  - Change its priority
  - Enable or disable spanning tree on a VLAN

Configuration Notes and Rules

**VLAN Hierarchy**

A hierarchy of VLANs exists between the Layer 2 and Layer 3 protocol-based VLANs. Port-based VLANs are at the lowest level of the hierarchy. Layer 3 protocol-based VLANs, IP, IPX, AppleTalk, Decnet and NetBIOS are at the middle level of the hierarchy, with IP sub-net and IPX network at the top of the hierarchy.

As packets are received, the VLAN classification starts from the highest level VLAN first. Therefore, if an interface is configured with both a port-based VLAN and an IP protocol VLAN, IP packets coming into the interface will be classified as members of the IP protocol VLAN because that VLAN is higher in the VLAN hierarchy.

**Multiple VLAN Membership Rules**

A port can belong to multiple, overlapping Layer 3 protocol-based VLANs without VLAN tagging.

A port can belong to multiple, overlapping Layer 2 port-based VLANs only if the port is a tagged port. Packets sent out of a tagged port use a 802.1Q tagged frame.

When both port and protocol-based VLANs are configured in a given device, all protocol VLANs must be strictly contained in a port-based VLAN. A protocol VLAN cannot include ports from multiple port-based VLANs. This rule is required to ensure that port-based VLANs remain loop-free Layer 2 broadcast domains.

**Routing between VLANs**

Connection to an IP/IPX/AppleTalk router such as an HP9304M or HP9308M is required to support IP, IPX and AppleTalk routing between VLANs. All other routable protocol VLANs (e.g. DecNet) must be routed by another router capable of routing such a protocol.

**Virtual Interfaces**

Router interfaces must be defined at the highest level of the VLAN hierarchy. Therefore, if both an IP sub-net VLAN and a port-based VLAN are configured, the router interface should be defined at the IP sub-net level. The number of virtual interfaces supported on a routing switch corresponds directly to the number of ports supported on the module being configured.

**Assigning Trunk Group Ports**

When a “lead” trunk group port is assigned to a VLAN, all other members of the trunk group will automatically be added to that VLAN. A lead port is the first port of a trunk group port range; for example, “1” in 1-4 or “5” in 5-8.
EXAMPLE: A user wants to create two port-based VLANs. One will have ports 1-8 (VLAN 222) and the other ports 9-16 (VLAN 333). All ports within those VLANs will be untagged, as seen in Figure 14.2.

Figure 14.2 Port-based protocols, VLAN 222 and VLAN 333

To create the two port-based VLANs described above, the following commands should be entered, assuming ports are resident on module 2 of the routing switch:

USING THE CLI

HP9300 (config)# vlan 222 by port
HP9300 (config-vlan-222)# untag 2/1 to 2/8
HP9300 (config-vlan-333)# vlan 333 by port
HP9300 (config-vlan-333)# untag e 2/9 to 2/16

**syntax**: `vlan <vlan ID> by port`

**syntax**: `untagged ethernet <portnumber> [to <port number | ethernet <portnumber>]`
USING THE WEB MANAGEMENT INTERFACE

1. Verify that the **port-based VLANs** option is enabled on the System configuration sheet.
2. Select the **VLAN** link from the main menu. A VLAN summary panel will appear.
3. Select the **add port VLAN** link from the summary panel. The panel shown in **Figure 14.3** will display.
4. Enter 222 as the **VLAN ID**.
5. To assign port membership to the VLAN, click on the **select port members** button. The panel seen in **Figure 14.4** will appear.
6. Select ports 1 through 8.
7. Select the **apply** button to assign the ports to VLAN 222. The user will be returned to the port VLAN configuration panel.
8. Assign a **name** to the VLAN if desired, (optional).
9. Modify the **QoS** (priority) of the VLAN if desired. Possible values are 0 to 7. An assignment of 7 provides the highest priority. The default value is 0.
10. Enable or disable **STP** for the VLAN. The default value is disabled.
11. Assign a virtual **router interface** if routing between VLANs is desired. For this example no routing is desired, so the default value of none is left unchanged.
12. Select the **add** button to create the VLAN. The user is now ready to create VLAN 333.
13. Enter 333 as the **VLAN ID**.
14. Click on the **select port members** button. The panel seen in **Figure 14.4** will appear.
15. Select ports 9 through 16.
16. Select the **apply** button to assign the ports to VLAN 333.
17. Repeat steps 8 through 11 for VLAN 333.
18. Select the **add** button when all information for the VLAN is entered. The user will now have created two VLANs, 222 and 333 as seen in **Figure 14.5**.
Configuring VLANs

Figure 14.3 Creating port VLAN 222

Figure 14.4 Defining port membership for VLAN 222
NOTE: When port-based VLAN operation is first enabled via the System configuration sheet, by default, all ports will be assigned to the default VLAN 1. As ports are assigned to other VLANs, they will be removed from the default VLAN, as seen in Figure 14.5. All ports not assigned to another VLAN will remain members of default VLAN 1. This is to ensure that all ports are members of at least one VLAN.

Modifying a Port-based VLAN
The following modifications can be made to a port-based VLAN:
• Add or delete a VLAN port
• Change its priority
• Enable or disable the Spanning Tree Protocol (STP)

To remove a port-based VLAN, the user would do the following:
1. Select the delete button on the show port VLAN panel (Figure 14.5) next to the VLAN to be deleted.

To remove a port from a VLAN, the user would do the following:
1. Select the modify button next to the VLAN to be modified on the show port VLAN (Figure 14.5) panel.
2. Select enable or disable for the appropriate port(s) or parameter(s).
3. Select the modify button to apply the change(s).

To assign a higher priority to a VLAN:
1. Select the modify button.
2. Select a value between 0 and 7 from the QoS pull down menu.
3. Select the modify button to assign the changes.
To enable spanning tree on a VLAN:

1. Select the modify button next to the port VLAN entry that is to be modified. The user can find a summary listing of all existing VLANs by selecting the show VLAN link from the main menu.
2. Enable STP for the VLAN.
3. Select the modify button to assign the changes.

**NOTE:** To modify specific STP bridge or port parameters for a VLAN, the user will need to go to the STP configuration sheet.

**NOTE:** A tagged port cannot have STP enabled.
Configuring Protocol-based VLANs

A user wants to define separate broadcast domains for IP, IPX and AppleTalk traffic. To do so, the user would define protocol VLANs for each.

NOTE: When defining IP, IPX, IP sub-net and IPX network VLANs on an HP routing switch, there is no need to exclude ports, because ports are not dynamically assigned. Therefore, only those ports implicitly defined as members of an IP, IP sub-net, IPX or IPX network protocol VLAN will be members.

To assign IP, IPX and AppleTalk VLANs, the user would enter the following commands:

USING THE CLI

1. To assign ports 1, 2, 3, 6 and 8 (module 1) to an IP protocol VLAN, the user would enter the following:

   HP9300 (config)# ip-proto
   HP9300 (config-ip-proto)# static e 1/1 to 1/3 e 1/6 e 1/8
   HP9300 (config-ip-proto)# exit
2. To assign the IPX protocol VLAN with permanent ports 10 and 14, the user would enter the following:

   HP9300 (config)# ipx-proto
   HP9300 (config-ipx-proto)# static e 1/10 e 1/14
   HP9300 (config-ipx-proto)# exit

   **NOTE:** The IPX routing protocol must be active on the router to allow routing between IPX VLANs. To activate the IPX protocol, the user would enter the command, `router ipx` at the CONFIG level.

3. To assign the AppleTalk protocol VLAN with ports 9 and 13 (module 1), the user would enter the following:

   HP9300 (config)# atalk-proto
   HP9300 (config-atalk-proto)# static e 1/9 e 1/13
   HP9300 (config-atalk-proto)# no dynamic
   HP9300 (config-atalk-proto)# exit

   **NOTE:** In the case of the AppleTalk VLAN, no dynamic ports are desired for the VLAN, so the `no dynamic` command is used instead of the `exclude` command. This command will serve to remove all remaining ports other than 9 and 13 from membership in the AppleTalk VLAN.

**syntax:** `<ip-proto | ipx-proto | atalk-proto | decnet-proto | netbios-proto | other-proto> <static | exclude | dynamic> <ethernet> <number> [to <number>]`

**USING THE WEB MANAGEMENT INTERFACE**

To assign IP, IPX and AppleTalk protocol VLANs, the user would do the following:

1. Verify that the system is configured to operate with L3 Protocol VLANs on the System configuration sheet.
2. Select VLAN from the menu. A VLAN summary panel will appear.
3. Select the add protocol VLAN link from the summary panel. The panel shown in Figure 14.7 will appear.
4. Select IP as the protocol.
5. Click on the change static members button to assign ports to the VLAN.
6. Select ports 1, 2, 3, 6 and 8 as static ports on the appropriate module. For this example, the ports on module 1 are being configured.
7. Select the apply button when port assignment is complete. The user will be returned to the protocol VLAN configuration panel and port membership will be seen (Figure 14.8).
8. Select the add button to create the IP protocol VLAN. The user is now ready to define the IPX protocol VLAN.
9. Select IPX as the protocol.
10. Assign ports 10 and 14 as static ports on the appropriate module (module 1 for this example) by following steps 5-7 above.
11. Select the add button to create the IPX protocol VLAN. The user is now ready to define the AppleTalk protocol VLAN.
12. Select AppleTalk as the protocol.
13. Assign ports 9 and 13 as static ports by following steps 5-7 above.

   **NOTE:** Verify that the dynamic box is not checked. This will disable dynamic assignment of ports to the AppleTalk protocol VLAN. In this example, only static port membership is wanted, so this parameter is negated.

14. Select the add button to create the AppleTalk VLAN. The VLANs seen in Figure 14.9 will now be configured.
Figure 14.7 Protocol VLAN configuration panel
Figure 14.8 Protocol VLAN configuration panel showing member ports for the IP protocol VLAN
Figure 14.9 Enabling protocol VLANs to partition IP, IPX and AppleTalk traffic

Configuring IP Sub-net and IPX Network VLANs

EXAMPLE: The user later decides that he or she wishes to further narrow the IP and IPX broadcast domains seen in Figure 14.9 by partitioning them into IP sub-nets and IPX network VLANs to provide smaller, more defined broadcast domains, as illustrated in Figure 14.10.

NOTE: IP and IP sub-net protocol VLANs cannot operate concurrently on the system. The same is true for IPX and IPX network protocol VLANs. If the user had first configured IP and IPX protocol VLANs before deciding to partition the network by IP sub-net and IPX network VLANs, then those VLANs would first have to be deleted before the IP sub-net and IPX network VLANs are created.
Configuring VLANs

Figure 14.10 Partitioning of domains by IP sub-net and IPX networks

**USING THE CLI**

To partition the two IP sub-nets as individual VLANs instead of a single IP VLAN on module 1, the user would do the following:

```
HP9300 (config)# ip-subnet 192.75.3.0 255.255.255.0
HP9300 (config-ip-subnet)# static e 1/1 to 1/3
HP9300 (config-ip-subnet)# exit
HP9300 (config)# ip-subnet 192.75.5.0 255.255.255.0
HP9300 (config-ip-subnet)# static e 1/3 e 1/6 e 1/8
```

**syntax:** `ip-subnet <ip address> <ip mask>`
To create two IPX networks instead of an IPX VLAN, the user would do the following:

HP9300 (config)# ipx-network 500 ethernet_802.2
HP9300 (config-ipx-network)# static e 1/14
HP9300 (config-ipx-network)# exit
HP9300 (config)# ipx-network 600 ethernet_802.3
HP9300 (config-ipx-network)# static e 1/10
HP9300 (config-ipx-network)# exit

\textbf{syntax}: \texttt{ipx-network<ipx network number> <frame encapsulation type> <netbios-allow | netbios-disallow>}

\textbf{USING THE WEB MANAGEMENT INTERFACE}

\textbf{EXAMPLE}: To partition the two IP sub-nets (192.75.3.0 and 192.75.5.0) as individual VLANs instead of a single IP VLAN, the user would enter the following via the VLAN configuration sheet.

1. Select the \texttt{protocol VLAN} link on the VLAN configuration sheet. A VLAN summary panel will appear.
2. Select the \texttt{add protocol VLAN} link. The panel shown in \textbf{Figure 14.11} will appear.
3. Select \texttt{IP sub-net}.
4. Enter the \texttt{IP address} of IP sub-net 192.75.5.0 and its network \texttt{mask}.
5. Click on the \texttt{change static members} button to assign ports to the VLAN.
6. Select ports 3, 6 and 8 as \texttt{static} ports on the appropriate module. For this example, the ports on module 1 are being configured.
7. Select the \texttt{apply} button when port assignment is complete. The user will be returned to the protocol VLAN configuration panel and port membership will be seen (\textbf{Figure 14.11}).
8. Select the \texttt{add} button to create IP sub-net VLAN, 192.75.5.0.
9. Select \texttt{IP sub-net}.
10. Enter the \texttt{IP address} of IP sub-net 192.75.3.0 and its network \texttt{mask}.
11. Click on the \texttt{change static members} button to assign ports to the VLAN.
12. Select ports 1, 2 and 3 as \texttt{static} ports on the appropriate module. For this example, the ports on module 1 are being configured.
13. Select the \texttt{apply} button when port assignment is complete. The user will be returned to the protocol VLAN configuration panel.
14. Select the \texttt{add} button to apply the changes.
15. Enter the IP address of IP sub-net 192.75.3.0 and its network mask.
16. Assign ports 3, 6 and 8 as \texttt{static} ports to the VLAN. Select the slot/port range if a chassis is being configured.
17. Select the \texttt{add} button to create IP sub-net VLAN, 192.75.3.0.

\textbf{NOTE}: Selecting the \texttt{show protocol VLAN} link will display the two configured IP sub-net VLANs (\textbf{Figure 14.12}).
Figure 14.11 Assigning IP sub-net VLAN 192.75.5.0
To create two IPX networks, 500 and 600, the user would enter the following:

1. Select the protocol VLAN link on the VLAN configuration sheet. A VLAN summary panel will appear.
2. Select the add protocol VLAN link. The panel shown in Figure 14.11 will appear.
3. Select IPX network.
4. Select frame type from the pull down menu.
5. Enter 500 as the IPX network address in the network field.
6. Click on the change static members button to assign ports to the VLAN.
7. Select port 14 as a static port on the appropriate module. For this example, the ports on module 1 are being configured.
8. Select the apply button when port assignment is complete. The user will be returned to the protocol VLAN configuration panel and port membership will be seen (Figure 14.11).
9. Select the add button to create IPX Network VLAN, 500.
10. Select IPX network.
11. Select frame type from the pull down menu.
12. Enter 600 as the IPX network address in the network field.
13. Select port 10 as a static port on the appropriate module. For this example, the ports on module 1 are being configured.
14. Select the apply button when port assignment is complete. The user will be returned to the protocol VLAN configuration panel and port membership will be seen.
15. Select the add button to create IPX Network VLAN, 600.

**NOTE:** The user can view the resulting IP sub-net and IPX network VLANs by selecting the show protocol VLAN link (Figure 14.13).
<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Protocol</th>
<th>Address</th>
<th>Frame Type</th>
<th>Mask</th>
<th>Interface</th>
<th>Dynamic</th>
<th>Static</th>
<th>Exclude</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP Subnet</td>
<td>192.75.3.0</td>
<td></td>
<td>255.255.255.0</td>
<td>None</td>
<td>No</td>
<td>1/1,1/2,1/3</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>IP Subnet</td>
<td>192.75.6.0</td>
<td></td>
<td>255.255.255.0</td>
<td>None</td>
<td>No</td>
<td>1/3,1/6,1/8</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>IPX Network</td>
<td>00000000</td>
<td>Ethernet602.2</td>
<td>None</td>
<td>No</td>
<td>1/10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>IPX Network</td>
<td>00000000</td>
<td>Ethernet602.2</td>
<td>None</td>
<td>No</td>
<td>1/14</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 14.13** Show protocol VLAN summary
**Configuring Protocol-based VLANs within Port-based VLANs**

If the user is going to use port-based VLANs with protocol-based VLANs, port-based VLANs must first be created. Once a port-based VLAN is created, then the user can assign Layer 3 protocol VLANs. Generally, a user creates port-based VLANs to allow separate spanning tree domains.

**EXAMPLE:** A user wants to create two port-based VLANs. One will have ports 1-8 (VLAN 222) and the other ports 9-16 (VLAN 333). All ports within those VLANs will be untagged, as seen in Figure 14.14.

![Figure 14.14 Port-based protocols, VLAN 222 and VLAN 333](image)

Additionally, the user wants to create an IP and IPX Layer 3 protocol VLAN within the Layer 2 protocol, VLAN 222. The IP protocol VLAN will include ports 1-6, and IPX traffic will comprise of ports 7 and 8, as seen in Figure 14.15. Ports 9 through 16 will be placed in port-based VLAN 333.
Configuring VLANs

Figure 14.15 Protocol VLANs overlaid on port-based VLANs 222 and 333

USING THE CLI
To create the two port-based VLANs and the protocol VLANs seen in Figure 14.15, the user would enter the following:

HP9300 (config)# vlan 222 by port
HP9300 (config-vlan-222)# untag e1 to 8

NOTE: Once the port-based VLAN is created, the user can create the IP and IPX protocol VLANs within VLAN 222.

HP9300 (config-vlan-222)# ip-proto
HP9300 (config-vlan-ip-proto)# static e 1/1 to 1/6
HP9300 (config-vlan-ip-proto)# exit
HP9300 (config-vlan-222)# ipx-proto
HP9300 (config-vlan-ipx-proto)# static e 1/7 to 1/8
HP9300 (config-vlan-ipx-proto)# exit
HP9300 (config-vlan-222)# vlan 333 by port
HP9300 (config-vlan-333)# untag e 1/9 to 1/16

syntax: vlan <vlan ID> by port
syntax: untagged ethernet <portnumber> [to <port number | ethernet <portnumber>]
syntax: <ip-proto | ipx-proto | atalk-proto | decnet-proto | netbios-proto | other-proto> <static | exclude | dynamic> <ethernet> <number> [to <number>]

USING THE WEB MANAGEMENT INTERFACE
To create the two port-based VLANs and the protocol VLANs seen in Figure 14.15, the user would enter the following:

1. Verify that both port-based and L3 protocol VLANs are enabled on the System configuration sheet.
2. Select the VLAN link from the main menu. A VLAN summary panel will appear.
3. Select the add port VLAN link from the summary panel.
**NOTE**: As a reminder, whenever both port and protocol VLANs are being defined on a system, port-based VLANs must be assigned first. Additionally, all protocol VLANs must be assigned within the boundaries of a port-based VLAN, when both types of VLAN co-exist on a network.

4. Enter 222 as the **VLAN ID**.

5. To assign port membership to the VLAN, click on the **select port members** button. The panel seen in **Figure 14.4** will appear.

6. Select ports 1 through 8.

7. Select the **apply** button to assign the ports to VLAN 222. The user will be returned to the port VLAN configuration panel.

8. Assign a **name** to the VLAN if desired, (optional).

9. Modify the **QoS** (priority) of the VLAN if desired. Possible values are 0 to 7. An assignment of 7 provides the highest priority. The default value is 0.

10. Enable or disable **STP** for the VLAN. The default value is disabled.

11. Assign a virtual **router interface** if routing between VLANs is desired. For this example no routing is desired, so the default value of none is left unchanged.

12. Select the **add** button to create the VLAN. The user is now ready to create VLAN 333.

13. Enter 333 as the **VLAN ID**.

14. Click on the **select port members** button. The panel seen in **Figure 14.4** will appear.

15. Select ports 9 through 16.

16. Select the **apply** button to assign the ports to VLAN 333.

17. Repeat steps 8 through 11 for VLAN 333.

18. Select the **add** button when all information for the VLAN is entered. The user will now have created two VLANs, 222 and 333.

19. To assign the IP and IPX protocol VLANs, select the **protocol VLAN** link.

20. Select **IP** as the protocol.

21. Click on the **change static members** button to assign ports to the VLAN.

22. Select ports 1-6 as **static** ports on the appropriate module. For this example, the ports on module 1 are being configured.

23. Select the **apply** button when port assignment is complete. The user will be returned to the protocol VLAN configuration panel.

24. Select the **add** button to create the IP protocol VLAN. The user is now ready to define the IPX protocol VLAN.

25. Select **IPX** as the protocol.

26. Assign ports 7 and 8 as **static** ports on the appropriate module (module 1 for this example) by following steps 5-7 above.

27. Select the **add** button to create the IPX protocol VLAN.

**Routing between VLANs using Virtual Interfaces**

To route between IP sub-nets 192.75.3.0 and 192.75.5.0 shown in **Figure 14.16**, a virtual router interface is defined for each sub-net. Similarly, to allow routing between IPX networks 500 and 600, the user would assign a virtual interface for each of the IPX network VLANs. A virtual interface can be any unassigned number between 1 and 24.
To configure the IP sub-net VLANs as seen in Figure 14.16, the user would enter the following commands at the CONFIG level of the CLI:

```
HP9300 (config)# ip-subnet 192.75.3.0 255.255.255.0
HP9300 (config-ip-subnet)# static e 1/1 to 3
HP9300 (config-ip-subnet)# router-interface ve 3
HP9300 (config)# ip-subnet 192.75.5.0 255.255.255.0
HP9300 (config-ip-subnet)# static e 1/3 to 1/4 e 1/6 e 1/8
HP9300 (config-ip-subnet)# router-interface ve 5
```

**NOTE:** Both IP and IPX routing must be enabled on the system to allow routing between VLANs.

**NOTE:** Once the IP sub-nets are assigned and their corresponding virtual interfaces identified, an IP address must be assigned to a virtual interface, as shown in the example below. Other IP parameters such as routing protocols and filter groups may also be configured on a virtual interface.
To configure the IPX networks seen in Figure 14.16, the user would enter the following commands at the CONFIG level of the CLI:

HP9300 (config)# ipx-network 500 ethernet_ii
HP9300 (config-ipx-network)# static e 1/14
HP9300 (config-ipx-network)# router-interface ve 6
HP9300 (config-ipx-network)# ipx-network 600 ethernet_snap
HP9300 (config-ipx-network)# static e 1/10
HP9300 (config-ipx-network)# router-interface ve 7

**NOTE:** The virtual interface (ve) number assigned is directly tied to the number of interfaces supported on a module.

**NOTE:** Once the IPX networks are assigned and their corresponding virtual interfaces identified, an IPX network number and frame type must be assigned to a virtual interface, as shown in the example below. Other IPX parameters such as routing protocols and filter groups may also be configured on a virtual interface.

To assign IPX network addresses to the virtual interfaces 6 and 7, the user would enter the following:

HP9300 (config)# int ve 6
HP9300 (config-vif-6)# ipx network 500 ethernet_ii
HP9300 (config-vif-6)# int ve 7
HP9300 (config-vif-7)# ipx network 600 ethernet_snap
USING THE WEB MANAGEMENT INTERFACE

To route between IP sub-nets 192.75.3.0 and 192.75.5.0 shown in Figure 14.16, a virtual router interface is defined for each sub-net. Similarly, to allow routing between IPX Networks 500 and 600, the user would assign a virtual interface for each of the IPX network VLANs. A virtual interface can be any number in the range of 1 to 24.

To define virtual interfaces for the IP sub-nets and IPX networks listed above, the user would follow the steps outlined for the Web management interface in the Configuring Protocol-based VLANs within Protocol VLAN section with one exception. Instead of assigning the value of "none" to the router interface, he or she would select an available virtual router interface (v1) from the pull down menu as seen in Figure 14.17.

NOTE: Virtual interfaces can be defined only for those protocol VLANs that are routed.

Figure 14.17 Assigning a virtual router interface to IP sub-net 192.75.3.0 to support routing between VLANs