# Chapter 8
# Configuring Spanning Tree Protocol (STP) and Advanced STP Features

The Spanning Tree Protocol (STP) eliminates Layer 2 loops in networks, by selectively blocking some ports and allowing other ports to forward traffic, based on global (bridge) and local (port) parameters you can configure.

This chapter describes how to configure Spanning Tree Protocol (STP) parameters on HP ProCurve Routing Switches.

This chapter also describes advanced Layer 2 features that enable you to overcome limitations in the standard 802.1d Spanning Tree Protocol (STP). These are the advanced features:

- Fast Port Span
- Fast Uplink Span
- Single-instance STP
- SuperSpan
- STP per VLAN group
- Per VLAN Spanning Tree (PVST) and PVST+ Compatibility

Configuration procedures are provided for the standard STP bridge and port parameters as well as advanced STP parameters.

- To configure standard STP parameters, see “Configuring Standard STP Parameters”.
- To configure advanced parameters, see “Configuring Advanced STP Features” on page 8-19.

## Configuring Standard STP Parameters

HP Routing Switches support standard STP as described in the IEEE 802.1D specification. STP is disabled by default on Routing Switches.

By default, each port-based VLAN on an HP device runs a separate spanning tree (a separate instance of STP). An HP device has one port-based VLAN (VLAN 1) by default that contains all the device’s ports. Thus, by default each HP device has one spanning tree. However, if you configure additional port-based VLANs on an HP device, then each of those VLANs on which STP is enabled and VLAN 1 all run separate spanning trees.

If you configure a port-based VLAN on the device, the VLAN has the same STP state as the default STP state on the device. On Routing Switches, new VLANs have STP disabled by default. You can enable or disable STP in each VLAN separately. In addition, you can enable or disable STP on individual ports.

## STP Parameters and Defaults

Table 8.1 lists the default STP states for HP devices.

**Table 8.1: Default STP States**

| Default STP Type | Default STP State | Default STP State of New VLANs[a] |
|---|---|---|
| MSTP | Disabled | Disabled |

a.When you create a port-based VLAN, the new VLAN's STP state is the same as the default STP state on the device. The new VLAN does not inherit the STP state of the default VLAN.

Table 8.2 lists the default STP bridge parameters. The bridge parameters affect the entire spanning tree. If you are using MSTP, the parameters affect the VLAN. If you are using SSTP, the parameters affect all VLANs that are members of the single spanning tree.

**Table 8.2: Default STP Bridge Parameters**

| Parameter | Description | Default and Valid Values |
|---|---|---|
| Forward Delay | The period of time a bridge will wait (the listen and learn period) before beginning to forward data packets. | 15 seconds<br>Possible values: 4 – 30 seconds |
| Maximum Age | The interval a bridge will wait for a hello packet from the root bridge before initiating a topology change. | 20 seconds<br>Possible values: 6 – 40 seconds |
| Hello Time | The interval of time between each configuration BPDU sent by the root bridge. | 2 seconds<br>Possible values: 1 – 10 seconds |
| Priority | A parameter used to identify the root bridge in a spanning tree (instance of STP). The bridge with the lowest value has the highest priority and is the root.<br>A higher numerical value means a lower priority; thus, the highest priority is 0. | 32768<br>Possible values: 0 – 65535 |

**NOTE:** If you plan to change STP bridge timers, HP recommends that you stay within the following ranges, from section 8.10.2 of the IEEE STP specification.

2 * (forward_delay -1) >= max_age

max_age >= 2 * (hello_time +1 )

Table 8.3 lists the default STP port parameters. The port parameters affect individual ports and are separately configurable on each port.

**Table 8.3: Default STP Port Parameters**

| Parameter | Description | Default and Valid Values |
|---|---|---|
| Priority | The preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree.<br>A higher numerical value means a lower priority; thus, the highest priority is 8. | 128<br>Possible values: 8 – 252<br>(configurable in increments of 4) |
| Path Cost | The cost of using the port to reach the root bridge. When selecting among multiple links to the root bridge, STP chooses the link with the lowest path cost and blocks the other paths. Each port type has its own default STP path cost. | 10 Mbps – 100<br>100 Mbps – 19<br>Gigabit – 4<br>10 Gigabit – 2<br>Possible values are 0 – 65535 |

## Enabling or Disabling the Spanning Tree Protocol (STP)

You can enable or disable STP on the following levels:

- Globally – Affects all ports on the device.
- Port-based VLAN – Affects all ports within the specified port-based VLAN. When you enable or disable STP within a port-based VLAN, the setting overrides the global setting. Thus, you can enable STP for the ports within a port-based VLAN even when STP is globally disabled, or disable the ports within a port-based VLAN when STP is globally enabled.
- Individual port – Affects only the individual port. However, if you change the STP state of the primary port in a trunk group, the change affects all ports in the trunk group.

### Enabling or Disabling STP Globally

Use the following methods to enable or disable STP on a device on which you have not configured port-based VLANs.

**NOTE:** When you configure a VLAN, the VLAN inherits the global STP settings. However, once you begin to define a VLAN, you can no longer configure standard STP parameters globally using the CLI. From that point on, you can configure STP only within individual VLANs.

*USING THE CLI*

To enable STP for all ports in all VLANs on an HP device, enter the following command:

```
HP9300(config)# spanning-tree
```

This command enables a separate spanning tree in each VLAN, including the default VLAN.

***Syntax:*** [no] spanning-tree

*USING THE WEB MANAGEMENT INTERFACE*

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select Enable next to Spanning Tree.

**NOTE:** For information about the Single and Fast checkboxes, see “Single Spanning Tree (SSTP)” on page 8-62 and “Fast Uplink Span” on page 8-21.

3. Click Apply to save the changes to the device’s running-config file.
4. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

### Enabling or Disabling STP in a Port-Based VLAN

Use the following procedure to disable or enable STP on a device on which you have configured a port-based VLAN. Changing the STP state in a VLAN affects only that VLAN.

*USING THE CLI*

To enable STP for all ports in a port-based VLAN, enter commands such as the following:

```
HP9300(config)# vlan 10
HP9300(config-vlan-10)# spanning-tree
```

***Syntax:*** [no] spanning-tree

*USING THE WEB MANAGEMENT INTERFACE*

You cannot enable or disable STP on individual VLANs using the Web management interface.

### Enabling or Disabling STP on an Individual Port

Use the following procedure to disable or enable STP on an individual port.

**NOTE:** If you change the STP state of the primary port in a trunk group, the change affects all ports in the trunk group.

*USING THE CLI*

To enable STP on an individual port, enter commands such as the following:

```
HP9300(config)# interface 1/1
HP9300(config-if-1/1)# spanning-tree
```

***Syntax:*** [no] spanning-tree

*USING THE WEB MANAGEMENT INTERFACE*

You cannot enable or disable STP on individual ports using the Web management interface.

## Changing STP Bridge and Port Parameters

Table 8.2 on page 8-2 and Table 8.3 on page 8-3 list the default STP parameters. If you need to change the default value for an STP parameter, use the following procedures.

### Changing STP Bridge Parameters

To change STP bridge parameters, use either of the following methods.

**NOTE:** If you plan to change STP bridge timers, HP recommends that you stay within the following ranges, from section 8.10.2 of the IEEE STP specification.

2 * (forward_delay -1) >= max_age

max_age >= 2 * (hello_time +1 )

*USING THE CLI*

To change an HP device’s STP bridge priority to the highest value to make the device the root bridge, enter the following command:

```
HP9300(config)# spanning-tree priority 0
```

The command in this example changes the priority on a device on which you have not configured port-based VLANs. The change applies to the default VLAN. If you have configured a port-based VLAN on the device, you can configure the parameters only at the configuration level for individual VLANs. Enter commands such as the following:

```
HP9300(config)# vlan 20
HP9300(config-vlan-20)# spanning-tree priority 0
```

To make this change in the default VLAN, enter the following commands:

```
HP9300(config)# vlan 1
HP9300(config-vlan-1)# spanning-tree priority 0
```

***Syntax:*** [no] spanning-tree [forward-delay <value>] | [hello-time <value>] | [maximum-age <value>] | [priority <value>]

The **forward-delay** <value> parameter specifies the forward delay and can be a value from 4 – 30 seconds. The default is 15 seconds.

---

**NOTE:** You can configure an HP device for faster convergence (including a shorter forward delay) using Fast Span or Fast Uplink Span. See “Configuring Advanced STP Features” on page 8-19.

---

The **hello-time** <value> parameter specifies the hello time and can be a value from 1 – 10 seconds. The default is 2 seconds.

---

**NOTE:** This parameter applies only when this device or VLAN is the root bridge for its spanning tree.

---

The **maximum-age** <value> parameter specifies the amount of time the device waits for receipt of a hello packet before initiating a topology change. You can specify from 6 – 40 seconds. The default is 20 seconds.

The **priority** <value> parameter specifies the priority and can be a value from 0 – 65535. A higher numerical value means a lower priority. Thus, the highest priority is 0. The default is 32768.

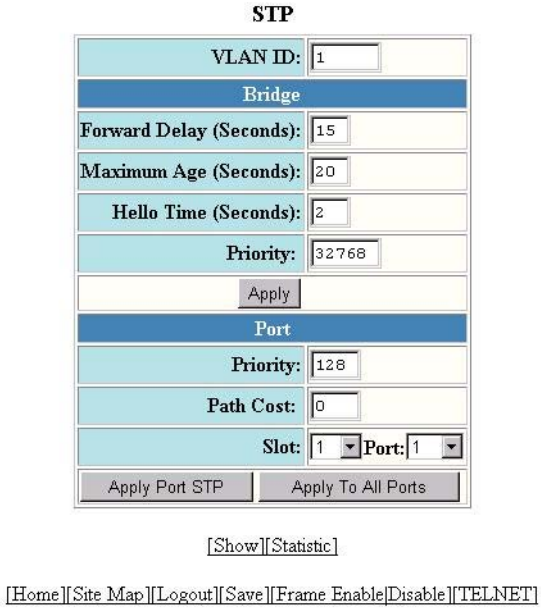
You can specify some or all of these parameters on the same command line. If you specify more than one parameter, you must specify them in the order shown above, from left to right.

*USING THE WEB MANAGEMENT INTERFACE*

To modify the STP parameters:

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to display the configuration options.
3. Select the STP link to display the STP bridge and port parameters.

4. Click the Modify button in the STP bridge parameters table to display the STP configuration panel, as shown in the following example. If the device has multiple port-based VLANs, select the Modify button next to the VLAN on which you want to change the parameters. A dialog such as the following is displayed.




5. Modify the bridge STP parameters to the values desired.
6. Click Apply to save the changes to the device's running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

## Changing STP Port Parameters

To change STP port parameters, use either of the following methods.

### *USING THE CLI*

To change the path and priority costs for a port, enter commands such as the following:

```
HP9300(config)# vlan 10
HP9300(config-vlan-10)# spanning-tree ethernet 1/5 path-cost 15 priority 64
```

***Syntax:*** spanning-tree ethernet <portnum> path-cost <value> | priority <value> | disable | enable

The **ethernet** <portnum> parameter specifies the interface.

The **path-cost** <value> parameter specifies the port's cost as a path to the spanning tree's root bridge. STP prefers the path with the lowest cost. You can specify a value from 0 – 65535.

The default depends on the port type:

- 10 Mbps – 100
- 100 Mbps – 19
- Gigabit – 4
- 10 Gigabit – 2

The **priority** <value> parameter specifies the preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree. You can specify a value from 8 – 252, in increments of 4. If you enter a

value that is not divisible by four the software rounds to the nearest value that is. The default is 128. A higher numerical value means a lower priority; thus, the highest priority is 8.

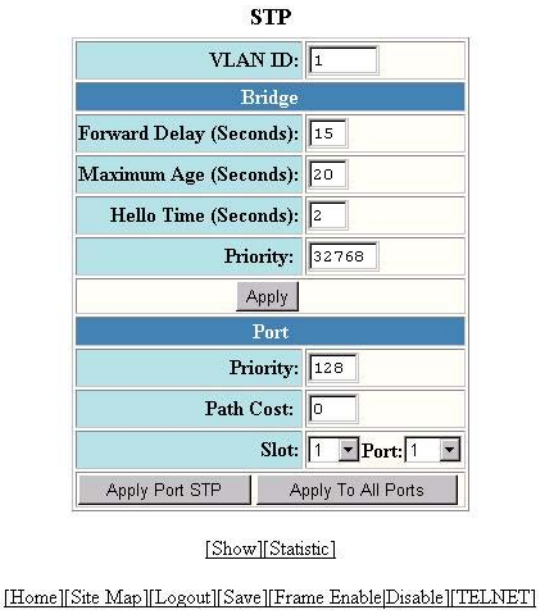
**NOTE:** The range in software releases earlier than 07.5.04 is 0 – 255. If you are upgrading a device that has a configuration saved under an earlier software release, and the configuration contains a value from 0 – 7 for a port's STP priority, the software changes the priority to the default when you save the configuration while running the new release.

The **disable | enable** parameter disables or re-enables STP on the port. The STP state change affects only this VLAN. The port's STP state in other VLANs is not changed.

*USING THE WEB MANAGEMENT INTERFACE*

To modify the STP port parameters:

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to display the configuration options.
3. Select the STP link to display the STP bridge and port parameters.
4. Click the Modify button in the STP port parameters table to display the STP configuration panel, as shown in the following example. If the device has multiple port-based VLANs, select the Modify button next to the VLAN on which you want to change the parameters. A dialog such as the following is displayed.




5. Select the port (and slot if applicable) from the Port and Slot pulldown lists.
6. Enter the desired changes to the priority and path cost fields.
7. Click Apply STP Port to apply the changes to only the selected port or select Apply To All Ports to apply the changes to all the ports.

   **NOTE:** If you want to save the priority and path costs of one port to all other ports on the device or within the selected VLAN, you can click the Apply To All Ports button.

8. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

## Displaying STP Information

You can display the following STP information:

- All the global and interface STP settings
- CPU utilization statistics
- Detailed STP information for each interface
- STP state information for a port-based VLAN
- STP state information for an individual interface

### Displaying STP Information for an Entire Device

To display STP information for an entire device, use either of the following methods.

*USING THE CLI*

To display STP information, enter the following command at any level of the CLI:

```
HP9300# show span

VLAN 1 BPDU cam_index is 3 and the Master DMA Are(HEX)
STP instance owned by VLAN 1

Global STP (IEEE 802.1D) Parameters:

VLAN Root              Root Root Prio Max He- Ho- Fwd Last     Chg  Bridge
 ID   ID               Cost Port rity Age llo ld  dly Chang    cnt  Address
                              Hex  sec sec sec sec sec
   1 800000e0804d4a00 0    Root 8000 20  2   1   15  689      1    00e0804d4a00

Port STP Parameters:

Port  Prio Path  State      Fwd    Design   Designated       Designated
Num   rity Cost             Trans  Cost     Root             Bridge
      Hex
1     80   19    FORWARDING 1      0        800000e0804d4a00 800000e0804d4a00
2     80   0     DISABLED   0      0        0000000000000000 0000000000000000
3     80   0     DISABLED   0      0        0000000000000000 0000000000000000
4     80   0     DISABLED   0      0        0000000000000000 0000000000000000
5     80   19    FORWARDING 1      0        800000e0804d4a00 800000e0804d4a00
6     80   19    BLOCKING   0      0        800000e0804d4a00 800000e0804d4a00
7     80   0     DISABLED   0      0        0000000000000000 0000000000000000
 <lines for remaining ports excluded for brevity>
```

***Syntax:*** show span [vlan <vlan-id>] | [pvst-mode] | [<num>] |
[detail [vlan <vlan-id> [ ethernet <portnum> ] | <num>]]

The **vlan** <vlan-id> parameter displays STP information for the specified port-based VLAN.

The **pvst-mode** parameter displays STP information for the device's Per VLAN Spanning Tree (PVST+) compatibility configuration. See "PVST/PVST+ Compatibility" on page 8-75.

The <num> parameter displays only the entries after the number you specify. For example, on a device with three port-based VLANs, if you enter 1, then information for the second and third VLANs is displayed, but information for the first VLAN is not displayed. Information is displayed according to VLAN number, in ascending order. The entry number is not the same as the VLAN number. For example, if you have port-based VLANs 1, 10, and 2024, then the command output has three STP entries. To display information for VLANs 10 and 2024 only, enter **show span 1**.

The **detail** parameter and its additional optional parameters display detailed information for individual ports. See “Displaying Detailed STP Information for Each Interface” on page 8-14.

The **show span** command shows the following information.

**Table 8.4: CLI Display of STP Information**

| This Field... | Displays... |
|---|---|
| **Global STP Parameters** | |
| VLAN ID | The port-based VLAN that contains this spanning tree (instance of STP). VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all STP information is for VLAN 1. |
| Root ID | The ID assigned by STP to the root bridge for this spanning tree. |
| Root Cost | The cumulative cost from this bridge to the root bridge. If this device is the root bridge, then the root cost is 0. |
| Root Port | The port on this device that connects to the root bridge. If this device is the root bridge, then the value is “Root” instead of a port number. |
| Priority Hex | This device or VLAN’s STP priority. The value is shown in hexadecimal format.<br>**Note**: If you configure this value, specify it in decimal format. See “Changing STP Bridge Parameters” on page 8-4. |
| Max age sec | The number of seconds this device or VLAN waits for a hello message from the root bridge before deciding the root has become unavailable and performing a reconvergence. |
| Hello sec | The interval between each configuration BPDU sent by the root bridge. |
| Hold sec | The minimum number of seconds that must elapse between transmissions of consecutive Configuration BPDUs on a port. |
| Fwd dly sec | The number of seconds this device or VLAN waits following a topology change and consequent reconvergence. |
| Last Chang sec | The number of seconds since the last time a topology change occurred. |
| Chg cnt | The number of times the topology has changed since this device was reloaded. |
| Bridge Address | The STP address of this device or VLAN.<br>**Note**: If this address is the same as the Root ID, then this device or VLAN is the root bridge for its spanning tree. |
| **Port STP Parameters** | |
| Port Num | The port number. |
| Priority Hex | The port’s STP priority, in hexadecimal format.<br>**Note**: If you configure this value, specify it in decimal format. See “Changing STP Port Parameters” on page 8-6. |
| Path Cost | The port’s STP path cost. |

**Table 8.4: CLI Display of STP Information (Continued)**

| This Field... | Displays... |
|---|---|
| State | The port's STP state. The state can be one of the following:<br>• BLOCKING – STP has blocked Layer 2 traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is FORWARDING. When a port is in this state, the port does not transmit or receive user frames, but the port does continue to receive STP BPDUs.<br>• DISABLED – The port is not participating in STP. This can occur when the port is disconnected or STP is disabled on the port.<br>• FORWARDING – STP is allowing the port to send and receive frames.<br>• LISTENING – STP is responding to a topology change and this port is listening for a BPDU from neighboring bridge(s) in order to determine the new topology. No user frames are transmitted or received during this state.<br>• LEARNING – The port has passed through the LISTENING state and will change to the BLOCKING or FORWARDING state, depending on the results of STP's reconvergence. The port does not transmit or receive user frames during this state. However, the device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table. |
| Fwd Trans | The number of times STP has changed the state of this port between BLOCKING and FORWARDING. |
| Design Cost | The cost to the root bridge as advertised by the designated bridge that is connected to this port. If the designated bridge is the root bridge itself, then the cost is 0. The identity of the designated bridge is shown in the Design Bridge field. |
| Design Root | The root bridge as recognized on this port. The value is the same as the root bridge ID listed in the Root ID field. |
| Design Bridge | The designated bridge to which this port is connected. The designated bridge is the device that connects the network segment on the port to the root bridge. |

### *USING THE WEB MANAGEMENT INTERFACE*

To display STP information:

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Monitor in the tree view to display the monitoring options.
3. Select the STP link to display the STP bridge and port parameters.

**Table 8.5: Web Management Display of STP Information**

| This Field... | Displays... |
|---|---|
| **STP Bridge Parameters (global parameters)** | |
| VLAN ID | The port-based VLAN that contains this spanning tree (instance of STP). VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all STP information is for VLAN 1. |
| Root ID | The ID assigned by STP to the root bridge for this spanning tree. |
| Root Cost | The cumulative cost from this bridge to the root bridge. If this device is the root bridge, then the root cost is 0. |
| Root Port | The port on this device that connects to the root bridge. If this device is the root bridge, then the value is “Root” instead of a port number. |
| Priority | This device or VLAN’s STP priority. The value is shown in hexadecimal format.<br>**Note**: If you configure this value, specify it in decimal format. See “Changing STP Bridge Parameters” on page 8-4. |
| Max Age | The number of seconds this device or VLAN waits for a hello message from the root bridge before deciding the root has become unavailable and performing a reconvergence. |
| Hello Time | The interval between each configuration BPDU sent by the root bridge. |
| Hold Time | The minimum number of seconds that must elapse between transmissions of consecutive Configuration BPDUs on a port. |
| Forward Delay | The number of seconds this device or VLAN waits following a topology change and consequent reconvergence. |
| Topology Last Change | The number of seconds since the last time a topology change occurred. |
| Topology Change Counter | The number of times the topology has changed since this device was reloaded. |
| Bridge Address | The STP address of this device or VLAN.<br>**Note**: If this address is the same as the Root ID, then this device or VLAN is the root bridge for its spanning tree. |
| **STP Port Parameters** | |
| VLAN | The VLAN that the port is in. |
| Port | The port number. |
| Priority | The port’s STP priority, in hexadecimal format.<br>**Note**: If you configure this value, specify it in decimal format. See “Changing STP Port Parameters” on page 8-6. |
| Path Cost | The port’s STP path cost. |

**Table 8.5: Web Management Display of STP Information (Continued)**

| This Field... | Displays... |
|---|---|
| State | The port's STP state. The state can be one of the following:<br>• BLOCKING – STP has blocked Layer 2 traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is FORWARDING. When a port is in this state, the port does not transmit or receive user frames, but the port does continue to receive STP BPDUs.<br>• DISABLED – The port is not participating in STP. This can occur when the port is disconnected or STP is disabled on the port.<br>• FORWARDING – STP is allowing the port to send and receive frames.<br>• LISTENING – STP is responding to a topology change and this port is listening for a BPDU from neighboring bridge(s) in order to determine the new topology. No user frames are transmitted or received during this state.<br>• LEARNING – The port has passed through the LISTENING state and will change to the BLOCKING or FORWARDING state, depending on the results of STP's reconvergence. The port does not transmit or receive user frames during this state. However, the device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table. |
| Transition | The number of times STP has changed the state of this port between BLOCKING and FORWARDING. |
| Cost | The cost to the root bridge as advertised by the designated bridge that is connected to this port. If the designated bridge is the root bridge itself, then the cost is 0. The identity of the designated bridge is shown in the Design Bridge field. |
| Root | The root bridge as recognized on this port. The value is the same as the root bridge ID listed in the Root ID field. |
| Bridge | The designated bridge to which this port is connected. The designated bridge is the device that connects the network segment on the port to the root bridge. |

## Displaying CPU Utilization Statistics

You can display CPU utilization statistics for STP and the IP protocols.

*USING THE CLI*

To display CPU utilization statistics for STP for the previous one-second, one-minute, five-minute, and fifteen-minute intervals, enter the following command at any level of the CLI:

```
HP9300# show process cpu
Process Name    5Sec(%)    1Min(%)    5Min(%)    15Min(%)    Runtime(ms)
ARP               0.01       0.03       0.09       0.22              9
BGP               0.04       0.06       0.08       0.14             13
GVRP              0.00       0.00       0.00       0.00              0
ICMP              0.00       0.00       0.00       0.00              0
IP                0.00       0.00       0.00       0.00              0
OSPF              0.00       0.00       0.00       0.00              0
RIP               0.00       0.00       0.00       0.00              0
STP               0.00       0.03       0.04       0.07              4
VRRP              0.00       0.00       0.00       0.00              0
```

If the software has been running less than 15 minutes (the maximum interval for utilization statistics), the command indicates how long the software has been running. Here is an example:

```
HP9300# show process cpu
The system has only been up for 6 seconds.
Process Name    5Sec(%)    1Min(%)    5Min(%)    15Min(%)    Runtime(ms)
ARP               0.01       0.00       0.00       0.00              0
BGP               0.00       0.00       0.00       0.00              0
GVRP              0.00       0.00       0.00       0.00              0
ICMP              0.01       0.00       0.00       0.00              1
IP                0.00       0.00       0.00       0.00              0
OSPF              0.00       0.00       0.00       0.00              0
RIP               0.00       0.00       0.00       0.00              0
STP               0.00       0.00       0.00       0.00              0
VRRP              0.00       0.00       0.00       0.00              0
```

To display utilization statistics for a specific number of seconds, enter a command such as the following:

```
HP9300# show process cpu 2
Statistics for last 1 sec and 80 ms
Process Name    Sec(%)    Time(ms)
ARP               0.00           0
BGP               0.00           0
GVRP              0.00           0
ICMP              0.01           1
IP                0.00           0
OSPF              0.00           0
RIP               0.00           0
STP               0.01           0
VRRP              0.00           0
```

When you specify how many seconds' worth of statistics you want to display, the software selects the sample that most closely matches the number of seconds you specified. In this example, statistics are requested for the previous two seconds. The closest sample available is actually for the previous 1 second plus 80 milliseconds.

***Syntax:*** show process cpu [<num>]

The <num> parameter specifies the number of seconds and can be from 1 – 900. If you use this parameter, the command lists the usage statistics only for the specified number of seconds. If you do not use this parameter, the command lists the usage statistics for the previous one-second, one-minute, five-minute, and fifteen-minute intervals.

*USING THE WEB MANAGEMENT INTERFACE*

You cannot display this information using the Web management interface.

## Displaying the STP State of a Port-Based VLAN

When you display information for a port-based VLAN, that information includes the STP state of the VLAN. Use either of the following methods to display port-based VLAN information.

*USING THE CLI*

To display information for a port-based VLAN, enter a command such as the following at any level of the CLI. The STP state is shown in bold type in this example.

```
HP9300(config)# show vlans

Total PORT-VLAN entries: 2
Maximum PORT-VLAN entries: 16

legend: [S=Slot]

PORT-VLAN 1, Name DEFAULT-VLAN, Priority level0, Spanning tree On
 Untagged Ports: (S3)  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16
 Untagged Ports: (S3) 17 18 19 20 21 22 23 24
 Untagged Ports: (S4)  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17
 Untagged Ports: (S4) 18 19 20 21 22 23 24
   Tagged Ports: None
   Uplink Ports: None

PORT-VLAN 2, Name greenwell, Priority level0, Spanning tree Off
 Untagged Ports: (S1)  1  2  3  4  5  6  7  8
 Untagged Ports: (S4)  1
   Tagged Ports: None
   Uplink Ports: None
```

***Syntax:*** show vlans [<vlan-id> | ethernet <portnum>]

The <vlan-id> parameter specifies a VLAN for which you want to display the configuration information.

The **ethernet** <portnum> parameter specifies a port. If you use this parameter, the command lists all the VLAN memberships for the port.

*USING THE WEB MANAGEMENT INTERFACE*

To display STP information for a specific VLAN:

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view.
3. Click on the plus sign next to VLAN in the tree view
4. Select the Port link to display configuration information for the device's port-based VLANs. The STP state is shown in the STP column.

## Displaying Detailed STP Information for Each Interface

To display detailed STP information for individual ports, use the following CLI method.

*USING THE CLI*

To display the detailed STP information, enter the following command at any level of the CLI:

```
HP9300# show span detail
========================================================================
VLAN 1 - MULTIPLE SPANNING TREE (MSTP) ACTIVE
========================================================================
Bridge identifier    - 0x800000e0804d4a00
Active global timers - Hello: 0

Port 1/1 is FORWARDING
  Port - Path cost: 19, Priority: 128, Root: 0x800000e052a9bb00
  Designated - Bridge: 0x800000e052a9bb00, Interface: 1, Path cost: 0
  Active Timers - None
  BPDUs - Sent: 11, Received: 0
Port 1/2 is DISABLED
Port 1/3 is DISABLED
Port 1/4 is DISABLED
<lines for remaining ports excluded for brevity>
```

If a port is disabled, the only information shown by this command is “DISABLED”. If a port is enabled, this display shows the following information.

***Syntax:*** show span detail [vlan <vlan-id> [ ethernet <portnum> ] | <num>]

The **vlan** <vlan-id> parameter specifies a VLAN.

The **ethernet** <portnum> parameter specifies an individual port within the VLAN (if specified).

The <num> parameter specifies the number of VLANs you want the CLI to skip before displaying detailed STP information. For example, if the device has six VLANs configured (VLAN IDs 1, 2, 3, 99, 128, and 256) and you enter the command **show span detail 4**, detailed STP information is displayed for VLANs 128 and 256 only.

**NOTE:** If the configuration includes VLAN groups, the **show span detail** command displays the master VLANs of each group but not the member VLANs within the groups. However, the command does indicate that the VLAN is a master VLAN. The **show span detail vlan** <vlan-id> command displays the information for the VLAN even if it is a member VLAN. To list all the member VLANs within a VLAN group, enter the **show vlan-group** [<group-id>] command.

The **show span detail** command shows the following information.

**Table 8.6: CLI Display of Detailed STP Information for Ports**

| This Field... | Displays... |
|---|---|
| Active Spanning Tree protocol | The VLAN that contains the listed ports and the active Spanning Tree protocol.<br>The STP type can be one of the following:<br>• MULTIPLE SPANNNG TREE (MSTP)<br>• GLOBAL SINGLE SPANNING TREE (SSTP)<br>**Note**: If STP is disabled on a VLAN, the command displays the following message instead: “Spanning-tree of port-vlan <vlan-id> is disabled.” |
| Bridge identifier | The STP identity of this device. |

**Table 8.6: CLI Display of Detailed STP Information for Ports (Continued)**

| This Field... | Displays... |
|---|---|
| Active global timers | The global STP timers that are currently active, and their current values. The following timers can be listed:<br>• Hello – The interval between Hello packets. This timer applies only to the root bridge.<br>• Topology Change (TC) – The amount of time during which the topology change flag in Hello packets will be marked, indicating a topology change. This timer applies only to the root bridge.<br>• Topology Change Notification (TCN) – The interval between Topology Change Notification packets sent by a non-root bridge toward the root bridge. This timer applies only to non-root bridges. |
| Port number and STP state | The internal port number and the port's STP state.<br>The internal port number is one of the following:<br>• The port's interface number, if the port is the designated port for the LAN.<br>• The interface number of the designated port from the received BPDU, if the interface is not the designated port for the LAN.<br>The state can be one of the following:<br>• BLOCKING – STP has blocked Layer 2 traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is FORWARDING. When a port is in this state, the port does not transmit or receive user frames, but the port does continue to receive STP BPDUs.<br>• DISABLED – The port is not participating in STP. This can occur when the port is disconnected or STP is administratively disabled on the port.<br>• FORWARDING – STP is allowing the port to send and receive frames.<br>• LISTENING – STP is responding to a topology change and this port is listening for a BPDU from neighboring bridge(s) in order to determine the new topology. No user frames are transmitted or received during this state.<br>• LEARNING – The port has passed through the LISTENING state and will change to the BLOCKING or FORWARDING state, depending on the results of STP's reconvergence. The port does not transmit or receive user frames during this state. However, the device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table.<br>**Note**: If the state is DISABLED, no further STP information is displayed for the port. |
| Port Path cost | The port's STP path cost. |
| Port Priority | This port's STP priority. The value is shown as a hexadecimal number. |

**Table 8.6: CLI Display of Detailed STP Information for Ports (Continued)**

| This Field... | Displays... |
|---|---|
| Root | The ID assigned by STP to the root bridge for this spanning tree. |
| Designated Bridge | The MAC address of the designated bridge to which this port is connected. The designated bridge is the device that connects the network segment on the port to the root bridge. |
| Designated Port | The port number sent from the designated bridge. |
| Designated Path Cost | The cost to the root bridge as advertised by the designated bridge that is connected to this port. If the bridge is the root bridge itself, then the cost is 0. The identity of the designated bridge is shown in the Designated Bridge field. |
| Active Timers | The current values for the following timers, if active:<br>• Message age – The number of seconds this port has been waiting for a hello message from the root bridge.<br>• Forward delay – The number of seconds that have passed since the last topology change and consequent reconvergence.<br>• Hold time – The number of seconds that have elapsed since transmission of the last Configuration BPDU. |
| BPDUs Sent and Received | The number of BPDUs sent and received on this port since the software was reloaded. |

### *Displaying Detailed STP Information for a Single Port in a Specific VLAN*

Enter a command such as the following to display STP information for an individual port in a specific VLAN.

```
HP9300(config)# show span detail vlan 1 ethernet 7/1
Port 7/1 is FORWARDING
  Port - Path cost: 19, Priority: 128, Root: 0x800000e052a9bb00
  Designated - Bridge: 0x800000e052a9bb00, Interface: 7, Path cost: 0
  Active Timers - None
  BPDUs - Sent: 29, Received: 0
```

***Syntax:*** show span detail [vlan <vlan-id> [ ethernet <portnum> ] | <num>]

*USING THE WEB MANAGEMENT INTERFACE*

The detailed display is not supported in the Web management interface.

## Displaying STP State Information for an Individual Interface

To display STP state information for an individual port, you can use the methods in “Displaying STP Information for an Entire Device” on page 8-8 or “Displaying Detailed STP Information for Each Interface”. You also can display STP state information for a specific port using either of the following methods.

*USING THE CLI*

To display information for a specific port, enter a command such as the following at any level of the CLI:

```
HP9300(config)# show interface ethernet 3/11

FastEthernet3/11 is up, line protocol is up
  Hardware is FastEthernet, address is 00e0.52a9.bb49 (bia 00e0.52a9.bb49)
  Configured speed auto, actual 100Mbit, configured duplex fdx, actual fdx
  Member of L2 VLAN ID 1, port is untagged, port state is FORWARDING
  STP configured to ON, priority is level0, flow control enabled
  mirror disabled, monitor disabled
  Not member of any active trunks
  Not member of any configured trunks
  No port name
  MTU 1518 bytes, encapsulation ethernet
  5 minute input rate: 352 bits/sec, 0 packets/sec, 0.00% utilization
  5 minute output rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
  1238 packets input, 79232 bytes, 0 no buffer
  Received 686 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 ignored
  529 multicast
  918 packets output, 63766 bytes, 0 underruns
  0 output errors, 0 collisions
```

The STP information is shown in bold type in this example.

***Syntax:*** show interfaces [ethernet <portnum>] | [loopback <num>] | [slot <slot-num>] | [ve <num>] | [brief]

You also can display the STP states of all ports by entering a command such as the following, which uses the **brief** parameter:

```
HP9300(config)# show interface brief

Port  Link State     Dupl Speed Trunk Tag Priori MAC            Name
1/1   Down None      None None  None  No  level0 00e0.52a9.bb00
1/2   Down None      None None  None  No  level0 00e0.52a9.bb01
1/3   Down None      None None  None  No  level0 00e0.52a9.bb02
1/4   Down None      None None  None  No  level0 00e0.52a9.bb03
1/5   Down None      None None  None  No  level0 00e0.52a9.bb04
1/6   Down None      None None  None  No  level0 00e0.52a9.bb05
1/7   Down None      None None  None  No  level0 00e0.52a9.bb06
1/8   Down None      None None  None  No  level0 00e0.52a9.bb07


.
.  some rows omitted for brevity
.
3/10  Down None      None None  None  No  level0 00e0.52a9.bb4a
3/11  Up   Forward   Full 100M  None  No  level0 00e0.52a9.bb49
```

In this example, only one port, 3/11, is forwarding traffic toward the root bridge.

*USING THE WEB MANAGEMENT INTERFACE*

To display STP information for a specific port, use the same method as the one described in “Displaying STP Information for an Entire Device” on page 8-8:

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Monitor in the tree view to display the monitoring options.
3. Select the STP link to display the STP bridge and port parameters.

# Configuring Advanced STP Features

This section describes how to configure the following features:

- Fast Port Span – see “Fast Port Span”
- Fast Uplink Span – see “Fast Uplink Span” on page 8-21
- 802.1W Rapid Spanning Tree (RSTP) – see “802.1W Rapid Spanning Tree (RSTP)” on page 8-22
- 802.1W Draft 3 RSTP – see “802.1W Draft 3” on page 8-58
- Single-instance STP – see “Single Spanning Tree (SSTP)” on page 8-62
- SuperSpan – see “SuperSpan” on page 8-64
- STP per VLAN group – see “STP per VLAN Group” on page 8-71
- Per VLAN Spanning Tree+ (PVST+) Compatibility – see “PVST/PVST+ Compatibility” on page 8-75

## Fast Port Span

When STP is running on a device, message forwarding is delayed during the spanning tree recalculation period following a topology change. The STP forward delay parameter specifies the period of time a bridge waits before forwarding data packets. The forward delay controls the listening and learning periods of STP reconvergence. You can configure the forward delay to a value from 4 – 30 seconds. The default is 15 seconds. Thus, using the standard forward delay, convergence requires 30 seconds (15 seconds for listening and an additional 15 seconds for learning) when the default value is used.

This slow convergence is undesirable and unnecessary in some circumstances. The Fast Port Span feature allows certain ports to enter the forwarding state in four seconds. Specifically, Fast Port Span allows faster convergence on ports that are attached to end stations and thus do not present the potential to cause Layer 2 forwarding loops. Because the end stations cannot cause forwarding loops, they can safely go through the STP state changes (blocking to listening to learning to forwarding) more quickly than is allowed by the standard STP convergence time. Fast Port Span performs the convergence on these ports in four seconds (two seconds for listening and two seconds for learning).

In addition, Fast Port Span enhances overall network performance in the following ways:

- Fast Port Span reduces the number of STP topology change notifications on the network. When an end station attached to a Fast Span port comes up or down, the HP device does not generate a topology change notification for the port. In this situation, the notification is unnecessary since a change in the state of the host does not affect the network’s topology.
- Fast Port Span eliminates unnecessary MAC cache aging that can be caused by topology change notifications. Bridging devices age out the learned MAC addresses in their MAC caches if the addresses are unrefreshed for a given period of time, sometimes called the MAC aging interval. When STP sends a topology change notification, devices that receive the notification use the value of the STP forward delay to quickly age out their MAC caches. For example, if a device’s normal MAC aging interval is 5 minutes, the aging interval changes temporarily to the value of the forward delay (for example, 15 seconds) in response to an STP topology change.

  In normal STP, the accelerated cache aging occurs even when a single host goes up or down. Because Fast Port Span does not send a topology change notification when a host on a Fast Port Span port goes up or down, the unnecessary cache aging that can occur in these circumstances under normal STP is eliminated.

Fast Port Span is a system-wide parameter and is enabled by default. Thus, when you boot a device with software release 06.6.05 or later, all the ports that are attached only to end stations run Fast Port Span. For ports

that are not eligible for Fast Port Span, such as ports connected to other networking devices, the device automatically uses the normal STP settings. If a port matches any of the following criteria, the port is ineligible for Fast Port Span and uses normal STP instead:

- The port is 802.1q tagged
- The port is a member of a trunk group
- The port has learned more than one active MAC address
- An STP Configuration BPDU has been received on the port, thus indicating the presence of another bridge on the port.

You also can explicitly exclude individual ports from Fast Port Span if needed. For example, if the only uplink ports for a wiring closet switch are Gigabit ports, you can exclude the ports from Fast Port Span.

### Disabling and Re-enabling Fast Port Span

Fast Port Span is a system-wide parameter and is enabled by default. Thus all ports that are eligible for Fast Port Span use it.

To disable or re-enable Fast Port Span, use one of the following methods.

*USING THE CLI*

To disable Fast Port Span, enter the following commands:

```
HP9300(config)# no fast port-span
HP9300(config)# write memory
```

***Syntax:*** [no] fast port-span

---

**NOTE:** The **fast port-span** command has additional parameters that let you exclude specific ports. These parameters are shown in the following section.

---

To re-enable Fast Port Span, enter the following commands:

```
HP9300(config)# fast port-span
HP9300(config)# write memory
```

*USING THE WEB MANAGEMENT INTERFACE*

1. Log on to the device using a valid user name and password for read-write access.
2. Click the Fast checkbox next to Spanning Tree to remove the checkmark from the box.
3. Click Apply to apply the change to the device's running-config.
4. Select the Save link at the bottom of the panel. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

### Excluding Specific Ports from Fast Port Span

You can exclude individual ports from Fast Port Span while leaving Fast Port Span enabled globally. To do so, use one of the following methods.

*USING THE CLI*

To exclude a port from Fast Port Span, enter commands such as the following:

```
HP9300(config)# fast port-span exclude ethernet 1/1
HP9300(config)# write memory
```

To exclude a set of ports from Fast Port Span, enter commands such as the following:

```
HP9300(config)# fast port-span exclude ethernet 1/1 ethernet 2/1 ethernet 3/2
HP9300(config)# write memory
```

To exclude a contiguous (unbroken) range of ports from Fast Span, enter commands such as the following:

```
HP9300(config)# fast port-span exclude ethernet 1/1 to 1/24
```

```
HP9300(config)# write memory
```

***Syntax:*** [no] fast port-span [exclude ethernet <portnum> [ethernet <portnum>… | to <portnum>]]

To re-enable Fast Port Span on a port, enter a command such as the following:

```
HP9300(config)# no fast port-span exclude ethernet 1/1
HP9300(config)# write memory
```

This command re-enables Fast Port Span on port 1/1 only and does not re-enable Fast Port Span on other excluded ports. You also can re-enable Fast Port Span on a list or range of ports using the syntax shown above this example.

To re-enable Fast Port Span on all excluded ports, disable and then re-enable Fast Port Span by entering the following commands:

```
HP9300(config)# no fast port-span
HP9300(config)# fast port-span
HP9300(config)# write memory
```

Disabling and then re-enabling Fast Port Span clears the exclude settings and thus enables Fast Port Span on all eligible ports. To make sure Fast Port Span remains enabled on the ports following a system reset, save the configuration changes to the startup-config file after you re-enable Fast Port Span. Otherwise, when the system resets, those ports will again be excluded from Fast Port Span.

*USING THE WEB MANAGEMENT INTERFACE*

You cannot exclude individual ports from Fast Span using the Web management interface.

## Fast Uplink Span

The Fast Port Span feature described in the previous section enhances STP performance for end stations. The Fast Uplink feature enhances STP performance for wiring closet switches with redundant uplinks. Using the default value for the standard STP forward delay, convergence following a transition from an active link to a redundant link can take 30 seconds (15 seconds for listening and an additional 15 seconds for learning).

You can use the Fast Uplink feature on an HP device deployed as a wiring closet switch to decrease the convergence time for the uplink ports to another device to just four seconds (two seconds for listening and two seconds for learning). The wiring closet switch must be an HP device but the device at the other end of the link can be an HP device or another vendor's switch. Configuration of the Fast Uplink Span feature takes place entirely on the HP device.

To configure the Fast Uplink Span feature, specify a group of ports that have redundant uplinks on the wiring closet switch (HP device) as members of a Fast Uplink Group. If the active link becomes unavailable, the Fast Uplink Span feature transitions the forwarding to one of the other ports in four seconds. You can configure one Fast Uplink Span group on the device. All Fast Uplink Span ports are members of the same Fast Uplink Span group.

---

**NOTE:** To avoid the potential for temporary bridging loops, Hewlett-Packard recommends that you use the Fast Uplink feature only for wiring closet switches (switches at the edge of the network cloud). In addition, enable the feature only on a group of ports intended for redundancy, so that at any given time only one of the ports is expected to be in the forwarding state.

---

### Fast Uplink Span Rules for Trunk Groups

If you add a port to a Fast Uplink Span group that is a member of a trunk group, the following rules apply:

- If you add the primary port of a trunk group to the Fast Uplink Span group, all other ports in the trunk group are automatically included in the group. Similarly, if you remove the primary port in a trunk group from the Fast Uplink Span group, the other ports in the trunk group are automatically removed from the Fast Uplink Span group.
- You cannot add a subset of the ports in a trunk group to the Fast Uplink Span group. All ports in a trunk group have the same Fast Uplink Span property, as they do for other port properties.

- If the working trunk group is partially down but not completely down, no switch-over to the backup occurs. This behavior is the same as in the standard STP feature.
- If the working trunk group is completely down, a backup trunk group can go through an accelerated transition only if the following are true:
  - The trunk group is included in the fast uplink group.
  - All other ports except those in this trunk group are either disabled or blocked. The accelerated transition applies to all ports in this trunk group.
- When the original working trunk group comes back (partially or fully), the transition back to the original topology is accelerated if the conditions listed above are met.

### Configuring a Fast Uplink Port Group

To enable Fast Uplink, use one of the following methods.

*USING THE CLI*

To configure a group of ports for Fast Uplink Span, enter the following commands:

```
HP9300(config)# fast uplink-span ethernet 4/1 to 4/4
HP9300(config)# write memory
```

***Syntax:*** [no] fast uplink-span [ethernet <portnum> [ethernet <portnum>… | to <portnum>]]

This example configures four ports, 4/1 – 4/4, as a Fast Uplink Span group. In this example, all four ports are connected to a wiring closet switch. Only one of the links is expected to be active at any time. The other links are redundant. For example, if the link on port 4/1 is the active link on the wiring closet switch but becomes unavailable, one of the other links takes over. Because the ports are configured in a Fast Uplink Span group, the STP convergence takes about four seconds instead of taking 30 seconds or longer using the standard STP forward delay.

If you add a port that is the primary port of a trunk group, all ports in the trunk group become members of the Fast Uplink Span group.

You can add ports to a Fast Uplink Span group by entering the **fast uplink-span** command additional times with additional ports. The device can have only one Fast Uplink Span group, so all the ports you identify as Fast Uplink Span ports are members of the same group.

To remove a Fast Uplink Span group or to remove individual ports from a group, use “no” in front of the appropriate **fast uplink-span** command. For example, to remove ports 4/3 and 4/4 from the Fast Uplink Span group configured above, enter the following commands:

```
HP9300(config)# no fast uplink-span ethernet 4/3 to 4/4
HP9300(config)# write memory
```

If you delete a port that is the primary port of a trunk group, all ports in the trunk group are removed from the Fast Uplink Span group.

*USING THE WEB MANAGEMENT INTERFACE*

You cannot configure the Fast Uplink Span feature using the Web management interface.

## 802.1W Rapid Spanning Tree (RSTP)

HP’s earlier implementation of Rapid Spanning Tree Protocol (RSTP), which was 802.1W Draft 3, provided only a subset of the IEEE 802.1W standard; whereas the 802.1W RSTP feature provides the full standard. The implementation of the 802.1W Draft 3 is referred to as RSTP Draft 3.

RSTP Draft3 will continue to be supported on HP devices for backward compatibility. However, customers who are currently using RSTP Draft 3 should migrate to 802.1W.

The 802.1W feature is supported on all Chassis devices. It provides rapid traffic reconvergence for point-to-point links within a few milliseconds (0 – 500 milliseconds), following the failure of a bridge or bridge port. This reconvergence occurs more rapidly than the reconvergence provided by the 802.1D (Spanning Tree Protocol (STP)) or by RSTP Draft 3.

**NOTE:** This rapid convergence will not occur on ports connected to shared media devices, such as hubs. To take advantage of the rapid convergence provided by 802.1W, make sure to explicitly configure all point-to-point links in a topology.

The convergence provided by the standard 802.1W protocol occurs more rapidly than the convergence provided by previous spanning tree protocols because:

- Classic or legacy 802.1D STP protocol requires a newly selected Root port to go through listening and learning stages before traffic convergence can be achieved. The 802.1D traffic convergence time is calculated using the following formula:

  *2 x FORWARD_DELAY + BRIDGE_MAX_AGE.*

  If default values are used in the parameter configuration, convergence can take up to 50 seconds. (In this document STP will be referred to as 802.1D.)

- RSTP Draft 3 works only on bridges that have Alternate ports, which are the precalculated “next best root port”. (Alternate ports provide back up paths to the root bridge.) Although convergence occurs from 0 – 500 milliseconds in RSTP Draft 3, the spanning tree topology reverts to the 802.1D convergence if an Alternate port is not found.

- Convergence in 802.1w bridge is not based on any timer values. Rather, it is based on the explicit handshakes between Designated ports and their connected Root ports to achieve convergence in less than 500 milliseconds.

## Bridges and Bridge Port Roles

A bridge in an 802.1W rapid spanning tree topology is assigned as the root bridge if it has the highest priority (lowest bridge identifier) in the topology. Other bridges are referred to as non-root bridges.

Unique roles are assigned to ports on the root and non-root bridges. Role assignments are based on the following information contained in the Rapid Spanning Tree Bridge Packet Data Unit (RST BPDU):

- Root bridge ID
- Path cost value
- Transmitting bridge ID
- Designated port ID

802.1W algorithm uses this information to determine if the RST BPDU received by a port is superior to the RST BPDU that the port transmits. The two values are compared in the order as given above, starting with the Root bridge ID. The RST BPDU with a lower value is considered superior. The superiority and inferiority of the RST BPDU is used to assign a role to a port.

If the value of the received RST BPDU is the same as that of the transmitted RST BPDU, then the port ID in the RST BPDUs are compared. The RST BPDU with the lower port ID is superior. Port roles are then calculated appropriately.

The port’s role is included in the BPDU that it transmits. The BPDU transmitted by an 802.1W port is referred to as an RST BPDU, while it is operating in 802.1W mode.

Ports can have one of the following roles:

- Root – Provides the lowest cost path to the root bridge from a specific bridge
- Designated – Provides the lowest cost path to the root bridge from a LAN to which it is connected
- Alternate – Provides an alternate path to the root bridge when the root port goes down
- Backup – Provides a backup to the LAN when the Designated port goes down
- Disabled – Has no role in the topology

### *Assignment of Port Roles*

At system start-up, all 802.1W-enabled bridge ports assume a Designated role. Once start-up is complete, 802.1W algorithm calculates the superiority or inferiority of the RST BPDU that is received and transmitted on a port.

On a root bridge, each port is assigned a ***Designated port*** role, except for ports on the same bridge that are physically connected together. In these type of ports, the port that receives the superior RST BPDU becomes the ***Backup port***, while the other port becomes the ***Designated port***.

On non-root bridges, ports are assigned as follows:

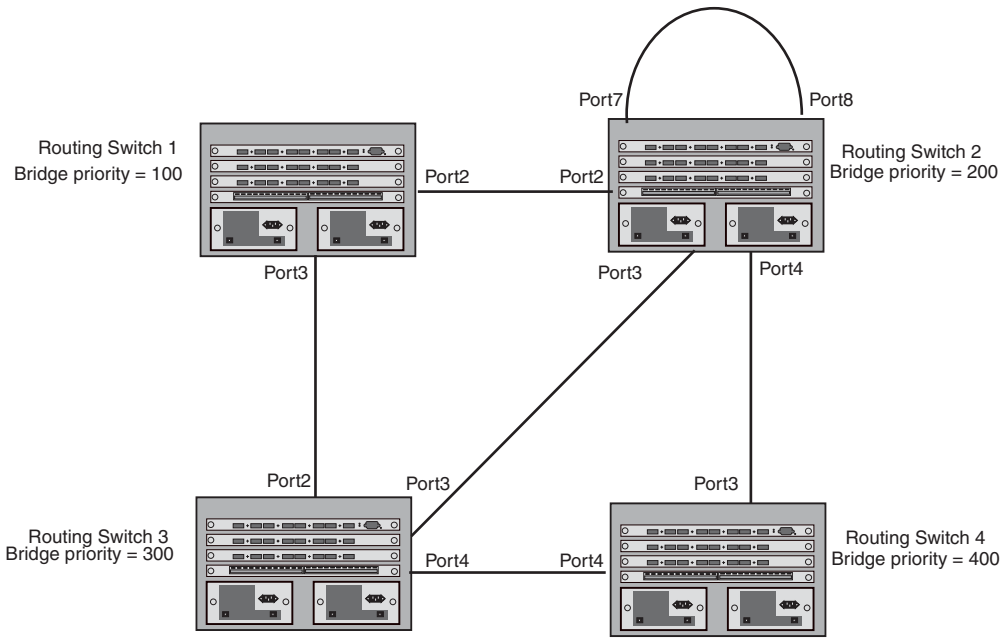
- The port that receives the RST BPDU with the lowest path cost from the root bridge becomes the ***Root port***.
- If two ports on the same bridge are physically connected, the port that receives the superior RST BPDU becomes the ***Backup port***, while the other port becomes the ***Designated port***.
- If a non-root bridge already has a Root port, then the port that receives an RST BPDU that is superior to those it can transmit becomes the ***Alternate port***.
- If the RST BPDU that a port receives is inferior to the RST BPDUs it transmits, then the port becomes a ***Designated port***.
- If the port is down or if 802.1W is disabled on the port, that port is given the role of ***Disabled port***. Disabled ports have no role in the topology. However, if 802.1W is enabled on a port with a link down and the link of that port comes up, then that port assumes one of the following port roles: Root, Designated, Alternate, or Backup.

The following example (Figure 8.1) explains role assignments in a simple RSTP topology.

**NOTE:** All examples in this document assume that all ports in the illustrated topologies are point-to-point links and are homogeneous (they have the same path cost value) unless otherwise specified.

The topology in Figure 8.1 contains four bridges. Routing Switch 1 is the root bridge since it has the lowest bridge priority. Routing Switch 2 through Routing Switch 4 are non-root bridges.

**Figure 8.1 Simple 802.1W Topology**




### *Ports on Routing Switch 1*

All ports on Routing Switch 1, the root bridge, are assigned Designated port roles.

#### *Ports on Routing Switch 2*

Port2 on Routing Switch 2 directly connects to the root bridge; therefore, Port2 is the Root port.

Routing Switch 2's bridge priority value is superior to that of Routing Switch 3 and Routing Switch 4; therefore, the ports on Routing Switch 2 that connect to Routing Switch 3 and Routing Switch 4 are given the Designated port role.

Furthermore, Port7 and Port8 on Routing Switch 2 are physically connected. The RST BPDUs transmitted by Port7 are superior to those Port8 transmits. Therefore, Routing Switch 2 is the Backup port and Port7 is the Designated port.

#### *Ports on Routing Switch 3*

Port2 on Routing Switch 3 directly connects to the Designated port on the root bridge; therefore, it assumes the Root port role.

The root path cost of the RST BPDUs received on Port4/Routing Switch 3 is inferior to the RST BPDUs transmitted by the port; therefore, Port4/Routing Switch 3 becomes the Designated port.

Similarly Routing Switch 3 has a bridge priority value inferior to Routing Switch 2. Port3 on Routing Switch 3 connects to Port 3 on Routing Switch 2. This port will be given the Alternate port role, since a Root port is already established on this bridge.

#### *Ports Routing Switch 4*

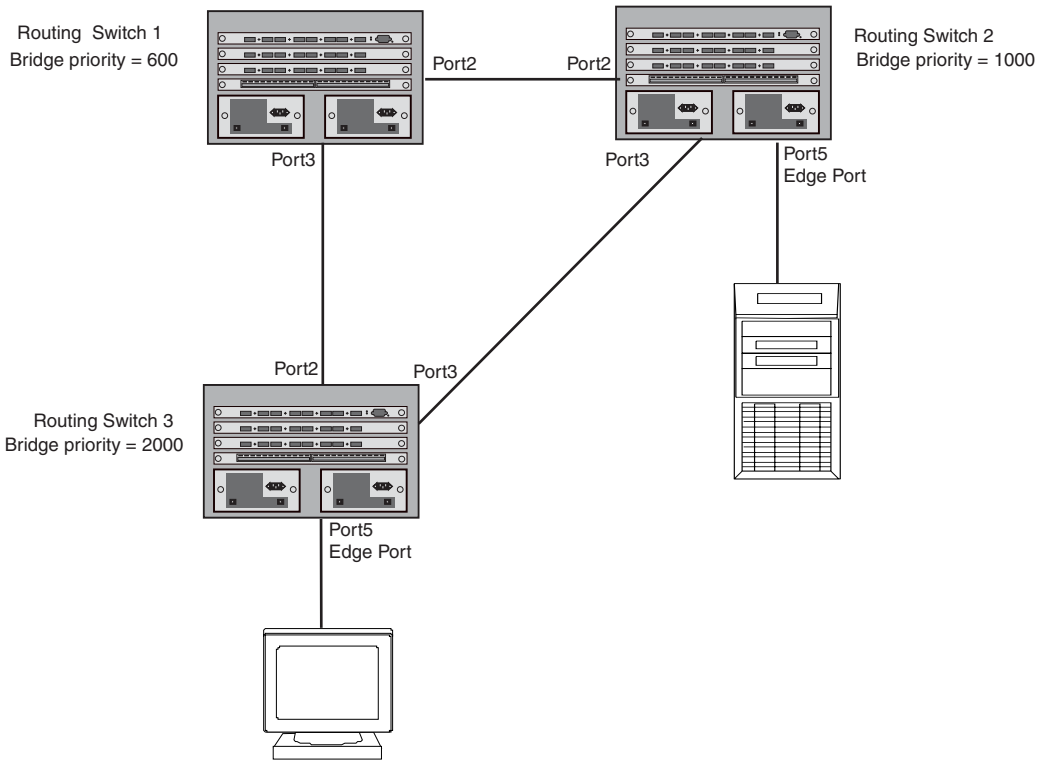
Routing Switch 4 is not directly connected to the root bridge. It has two ports with superior incoming RST BPDUs from two separate LANs: Port3 and Port4. The RST BPDUs received on Port3 are superior to the RST BPDUs received on port 4; therefore, Port3 becomes the Root port and Port4 becomes the Alternate port.

### Edge Ports and Edge Port Roles

HP's implementation of 802.1W allows ports that are configured as Edge ports to be present in an 802.1W topology. (Figure 8.2). Edge ports are ports of a bridge that connect to workstations or computers. Edge ports do not register any incoming BPDU activities.

Edge ports assume Designated port roles. Port flapping does not cause any topology change events on Edge ports since 802.1W does not consider Edge ports in the spanning tree calculations.

**Figure 8.2 Topology with Edge Ports**




However, if any incoming RST BPDU is received from a previously configured Edge port, 802.1W automatically makes the port as a non-edge port. This is extremely important to ensure a loop free Layer 2 operation since a non-edge port is part of the active RSTP topology.

The 802.1W protocol can auto-detect an Edge port and a non-edge port. An administrator can also configure a port to be an Edge port using the CLI. It is recommended that Edge ports are configured explicitly to take advantage of the Edge port feature, instead of allowing the protocol to auto-detect them.

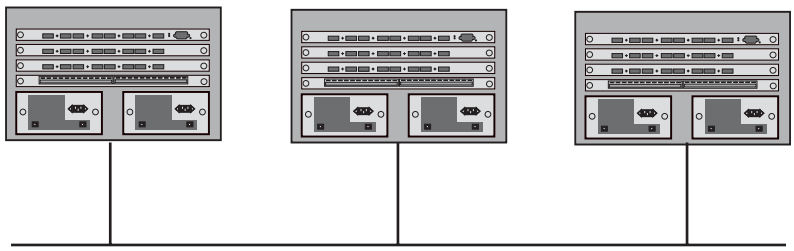
## Point-to-Point Ports

To take advantage of the 802.1W features, ports on an 802.1W topology should be explicitly configured as point-to-point links using the CLI. Shared media should not be configured as point-to-point links.

**NOTE:** Configuring shared media or non-point-to-point links as point-to-point links could lead to Layer 2 loops.

The topology in Figure 8.3 is an example of shared media that should not be configured as point-to-point links. In Figure 8.3, a port on a bridge communicates or is connected to at least two ports.

**Figure 8.3 Example of Shared Media**



## Bridge Port States

Ports roles can have one of the following states:

- Forwarding – 802.1W is allowing the port to send and receive all packets.
- Discarding – 802.1W has blocked data traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is forwarding. When a port is in this state, the port does not transmit or receive data frames, but the port does continue to receive RST BPDUs. This state corresponds to the listening and blocking states of 802.1D.
- Learning – 802.1W is allowing MAC entries to be added to the filtering database but does not permit forwarding of data frames. The device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table.
- Disabled – The port is not participating in 802.1W. This can occur when the port is disconnected or 802.1W is administratively disabled on the port.

A port on a non-root bridge with the role of Root port is always in a forwarding state. If another port on that bridge assumes the Root port role, then the old Root port moves into a discarding state as it assumes another port role.

A port on a non-root bridge with a Designated role starts in the discarding state. When that port becomes elected to the Root port role, 802.1W quickly places it into a forwarding state. However, if the Designated port is an Edge port, then the port starts and stays in a forwarding state and it cannot be elected as a Root port.

A port with an Alternate or Backup role is always in a discarding state. If the port's role changes to Designated, then the port changes into a forwarding state.

If a port on one bridge has a Designated role and that port is connected to a port on another bridge that has an Alternate or Backup role, the port with a Designated role cannot be given a Root port role until two instances of the forward delay timer expires on that port.

## Edge Port and Non-Edge Port States

As soon as a port is configured as an Edge port using the CLI, it goes into a forwarding state instantly (in less than 100 msec):

When the link to a port comes up and 802.1W detects that the port is an Edge port, that port instantly goes into a forwarding state.

If 802.1W detects that port as a non-edge port, the port goes into a forwarding state within four seconds of link up or after two hello timer expires on the port.

## Changes to Port Roles and States

To achieve convergence in a topology, a port's role and state changes as it receives and transmits new RST BPDUs. Changes in a port's role and state constitute a topology change. Besides the superiority and inferiority of the RST BPDU, bridge-wide and per-port state machines are used to determine a port's role as well as a port's state. Port state machines also determine when port role and state changes occur.

### *State Machines*

The bridge uses the Port Role Selection state machine to determine if port role changes are required on the bridge. This state machine performs a computation when one of the following events occur:

- New information is received on any port on the bridge
- The timer expires for the current information on a port on the bridge

Each port uses the following state machines:

- Port Information – This state machine keeps track of spanning-tree information currently used by the port. It records the origin of the information and ages out any information that was derived from an incoming BPDU.
- Port Role Transition – This state machine keeps track of the current port role and transitions the port to the appropriate role when required. It moves the Root port and the Designated port into forwarding states and moves the Alternate and Backup ports into discarding states.
- Port Transmit – This state machine is responsible for BPDU transmission. It checks to ensure only the

maximum number of BPDUs per hello interval are sent every second. Based on what mode it is operating in, it sends out either legacy BPDUs or RST BPDUs. In this document legacy BPDUs are also referred to as STP BPDUs.

- Port Protocol Migration – This state machine deals with compatibility with 802.1D bridges. When a legacy BPDU is detected on a port, this state machine configures the port to transmit and receive legacy BPDUs and operate in the legacy mode.
- Topology Change – This state machine detects, generates, and propagates topology change notifications. It acknowledges Topology Change Notice (TCN) messages when operating in 802.1D mode. It also flushes the MAC table when a topology change event takes place.
- Port State Transition – This state machine transitions the port to a discarding, learning, or forwarding state and performs any necessary processing associated with the state changes.
- Port Timers – This state machine is responsible for triggering any of the state machines described above, based on expiration of specific port timers.

In contrast to the 802.1D standard, the 802.1W standard does not have any bridge specific timers. All timers in the CLI are applied on a per-port basis, even though they are configured under bridge parameters.

802.1W state machines attempt to quickly place the ports into either a forwarding or discarding state. Root ports are quickly placed in forwarding state when both of the following events occur:

- It is assigned to be the Root port.
- It receives an RST BPDU with a proposal flag from a Designated port. The proposal flag is sent by ports with a Designated role when they are ready to move into a forwarding state.

When a the role of Root port is given to another port, the old Root port is instructed to reroot. The old Root port goes into a discarding state and negotiates with its peer port for a new role and a new state. A peer port is the port on the other bridge to which the port is connected. For example, in Figure 8.4, Port1 of Routing Switch 200 is the peer port of Port2 of Routing Switch 100.

A port with a Designated role is quickly placed into a forwarding state if one of the following occurs:

- The Designated port receives an RST BPDU that contains an agreement flag from a Root port
- The Designated port is an Edge port

However, a Designated port that is attached to an Alternate port or a Backup port must wait until the forward delay timer expires twice on that port while it is still in a Designated role, before it can proceed to the forwarding state.

Backup ports are quickly placed into discarding states.

Alternate ports are quickly placed into discarding states.

A port operating in 802.1W mode may enter a learning state to allow MAC entries to be added to the filtering database; however, this state is transient and lasts only a few milliseconds, if the port is operating in 802.1W mode and if the port meets the conditions for rapid transition.

### *Handshake Mechanisms*

To rapidly transition a Designated or Root port into a forwarding state, the Port Role Transition state machine uses handshake mechanisms to ensure loop free operations. It uses one type of handshake if no Root port has been assigned on a bridge, and another type if a Root port has already been assigned.

### *Handshake When No Root Port is Elected*

If a Root port has not been assigned on a bridge, 802.1W uses the Proposing -> Proposed -> Sync -> Synced -> Agreed handshake:

- Proposing – The Designated port on the root bridge sends an RST BPDU packet to its peer port that contains a proposal flag. The proposal flag is a signal that indicates that the Designated port is ready to put itself in a forwarding state (Figure 8.4). The Designated port continues to send this flag in its RST BPDU until it is placed in a forwarding state (Figure 8.7) or is forced to operate in 802.1D mode. (See “Compatibility of 802.1W with 802.1D” on page 48.)
- Proposed – When a port receives an RST BPDU with a proposal flag from the Designated port on its point-to-

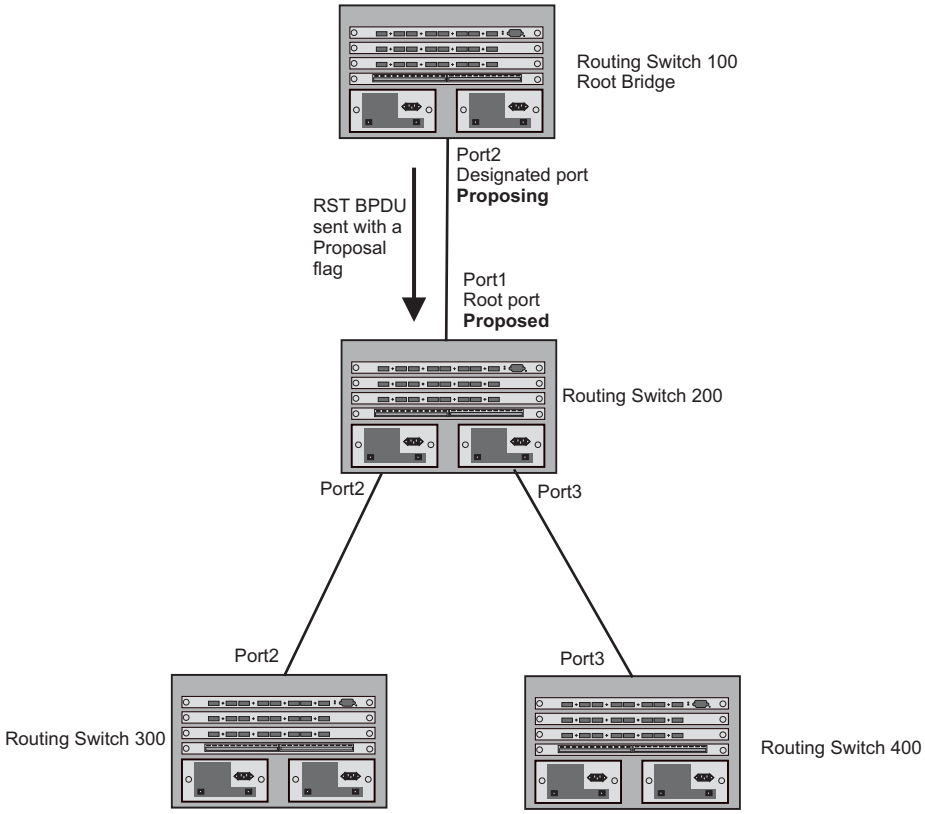
point link, it asserts the Proposed signal and one of the following occurs (Figure 8.4):

- If the RST BPDU that the port receives is superior to what it can transmit, the port assumes the role of a Root port. (See the section on “Bridges and Bridge Port Roles” on page 8-23.)
- If the RST BPDU that the port receives is inferior to what it can transmit, then the port is given the role of Designated port.

**NOTE:** Proposed will never be asserted if the port is connected on a shared media link.

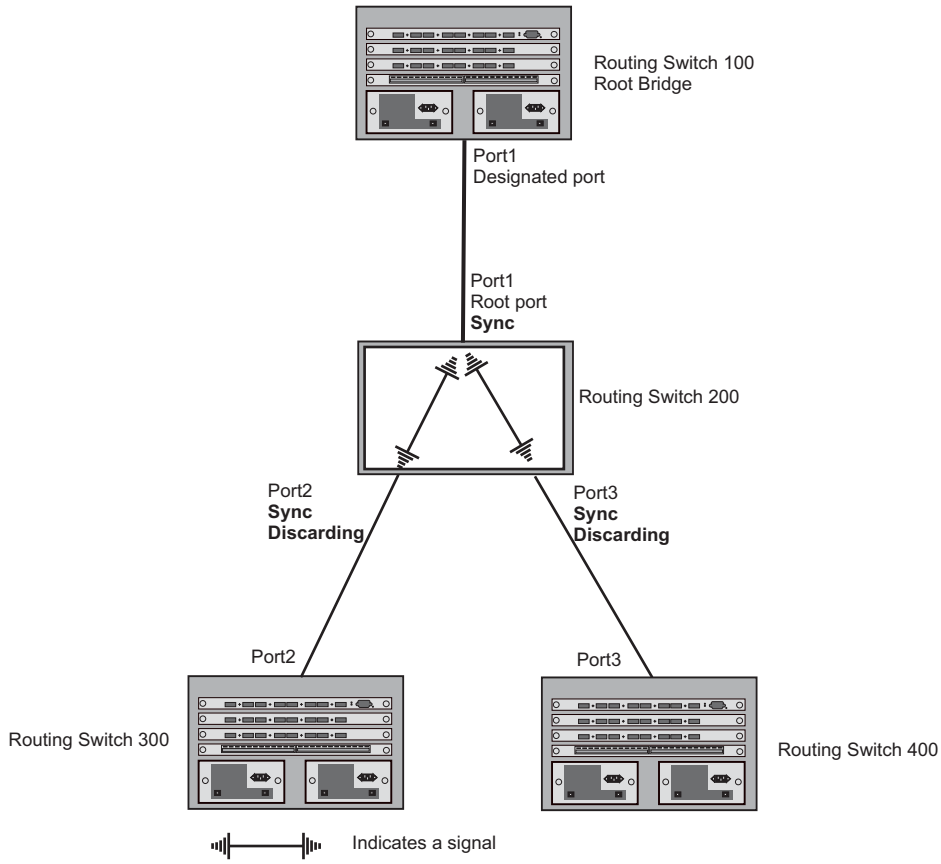
In Figure 8.4, Port3/Routing Switch 200 is elected as the Root port

**Figure 8.4 Proposing and Proposed Stage**



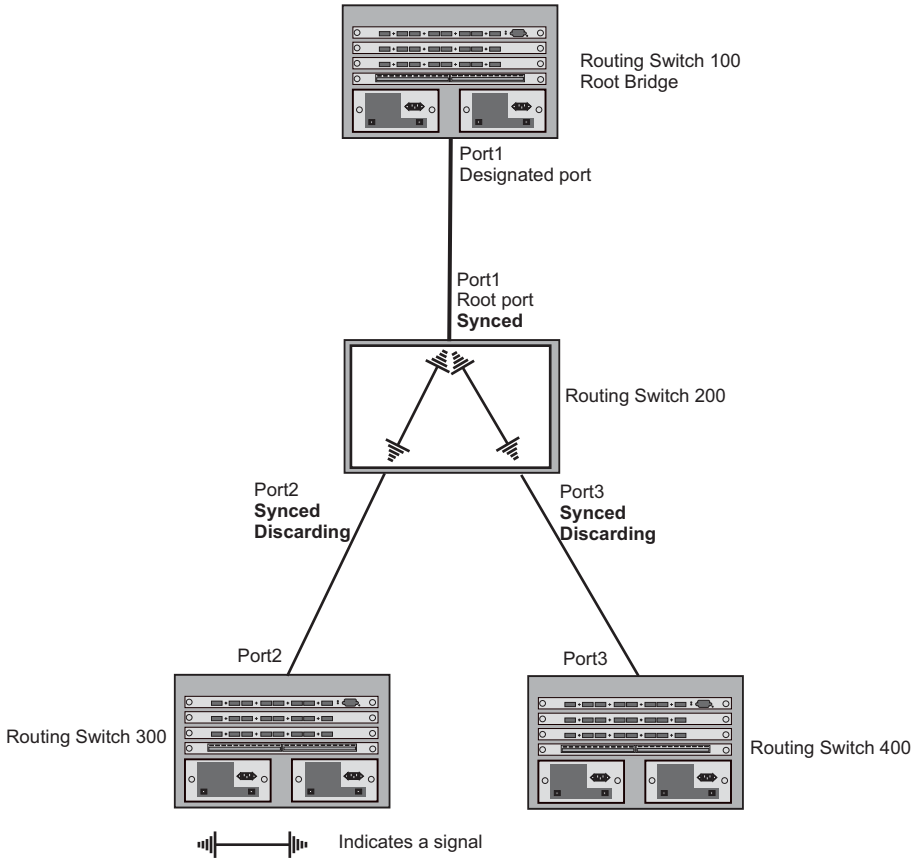
- Sync – Once the Root port is elected, it sets a sync signal on all the ports on the bridge. The signal tells the ports to synchronize their roles and states (Figure 8.5). Ports that are non-edge ports with a role of Designated port change into a discarding state. These ports have to negotiate with their peer ports to establish their new roles and states.

**Figure 8.5 Sync Stage**



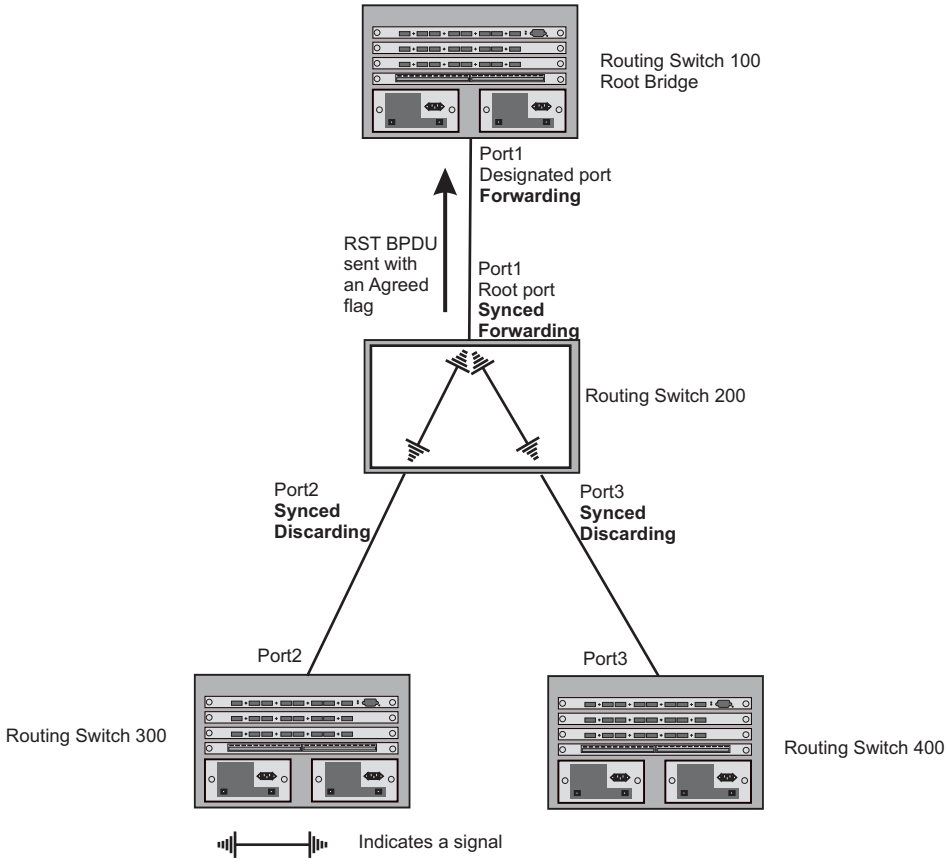
- Synced – Once the Designated port changes into a discarding state, it asserts a synced signal. Immediately, Alternate ports and Backup ports are synced. The Root port monitors the synced signals from all the bridge ports. Once all bridge ports asserts a synced signal, the Root port asserts its own synced signal (Figure 8.6).

**Figure 8.6 Synced Stage**



- Agreed – The Root port sends back an RST BPDU containing an agreed flag to its peer Designated port and moves into the forwarding state. When the peer Designated port receives the RST BPDU, it rapidly transitions into a forwarding state.

**Figure 8.7 Agree Stage**




At this point, the handshake mechanism is complete between Routing Switch 100, the root bridge, and Routing Switch 200.

Routing Switch 200 updates the information on the Routing Switch 200's Designated ports (Port2 and Port3) and identifies the new root bridge. The Designated ports send RST BPDUs, containing proposal flags, to their downstream bridges, without waiting for the hello timers to expire on them. This process starts the handshake with the downstream bridges.

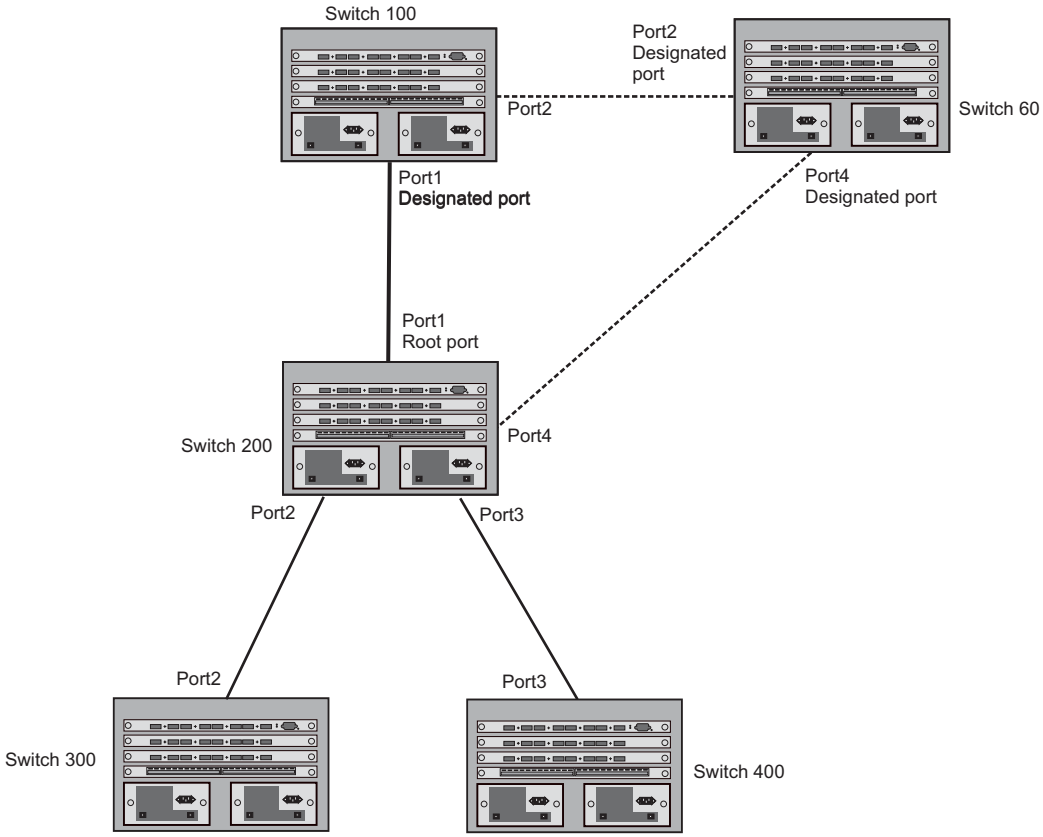
For example, Port2/Routing Switch 200 sends an RST BPDU to Port2/Routing Switch 300 that contains a proposal flag. Port2/Routing Switch 300 asserts a proposed signal. Ports in Routing Switch 300 then set sync signals on the ports to synchronize and negotiate their roles and states. Then the ports assert a synced signal and when the Root port in Routing Switch 300 asserts it's synced signal, it sends an RST BPDU to Routing Switch 200 with an agreed flag.

This handshake is repeated between Routing Switch 200 and Routing Switch 400 until all Designated and Root ports are in forwarding states.

### *Handshake When a Root Port Has Been Elected*

If a non-root bridge already has a Root port, 802.1W uses a different type of handshake. For example, in Figure 8.8, a new root bridge is added to the topology.

**Figure 8.8 Addition of a New Root Bridge**

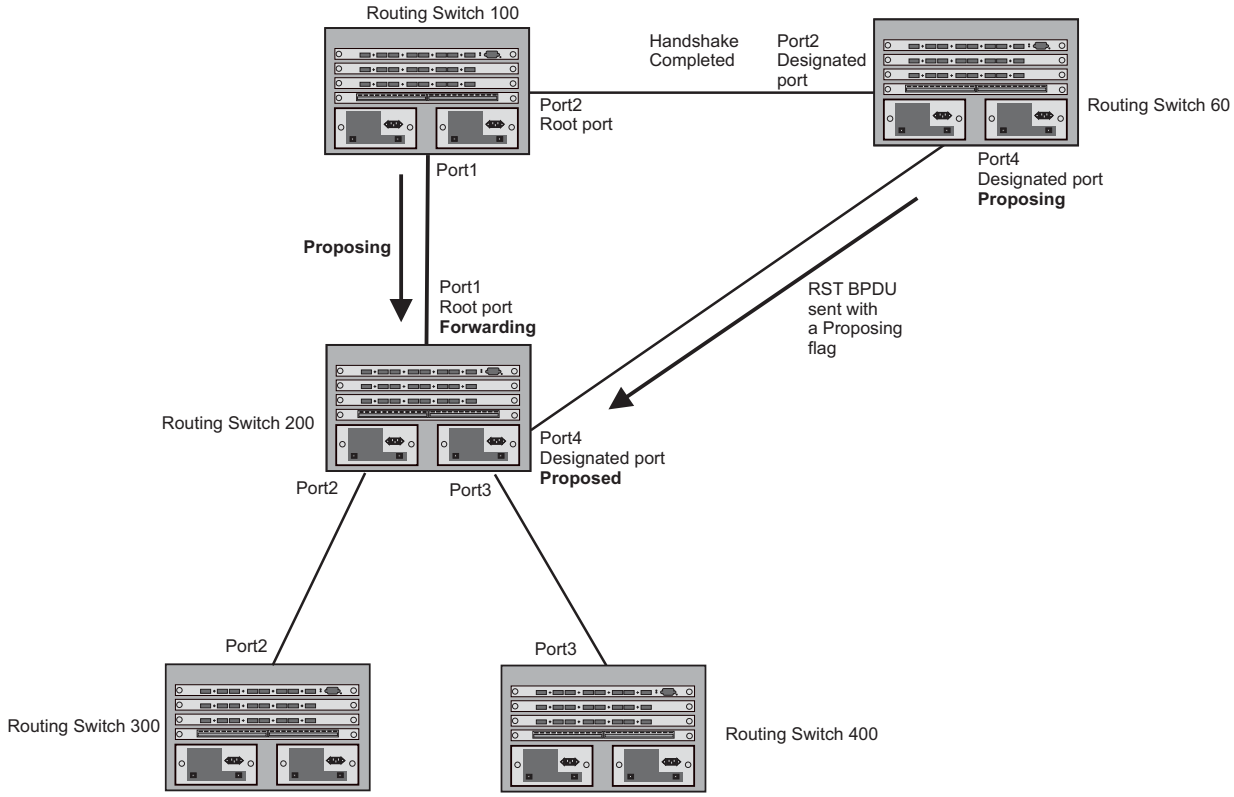


The handshake that occurs between Routing Switch 60 and Routing Switch 100 follows the one described in the previous section (“Handshake When No Root Port is Elected” on page 8-28). The former root bridge becomes a non-root bridge and establishes a Root port (Figure 8.9).

However, since Routing Switch 200 already had a Root port in a forwarding state, 802.1W uses the Proposing -> Proposed -> Sync and Reroot -> Sync and Rerooted -> Rerooted and Synced -> Agreed handshake:

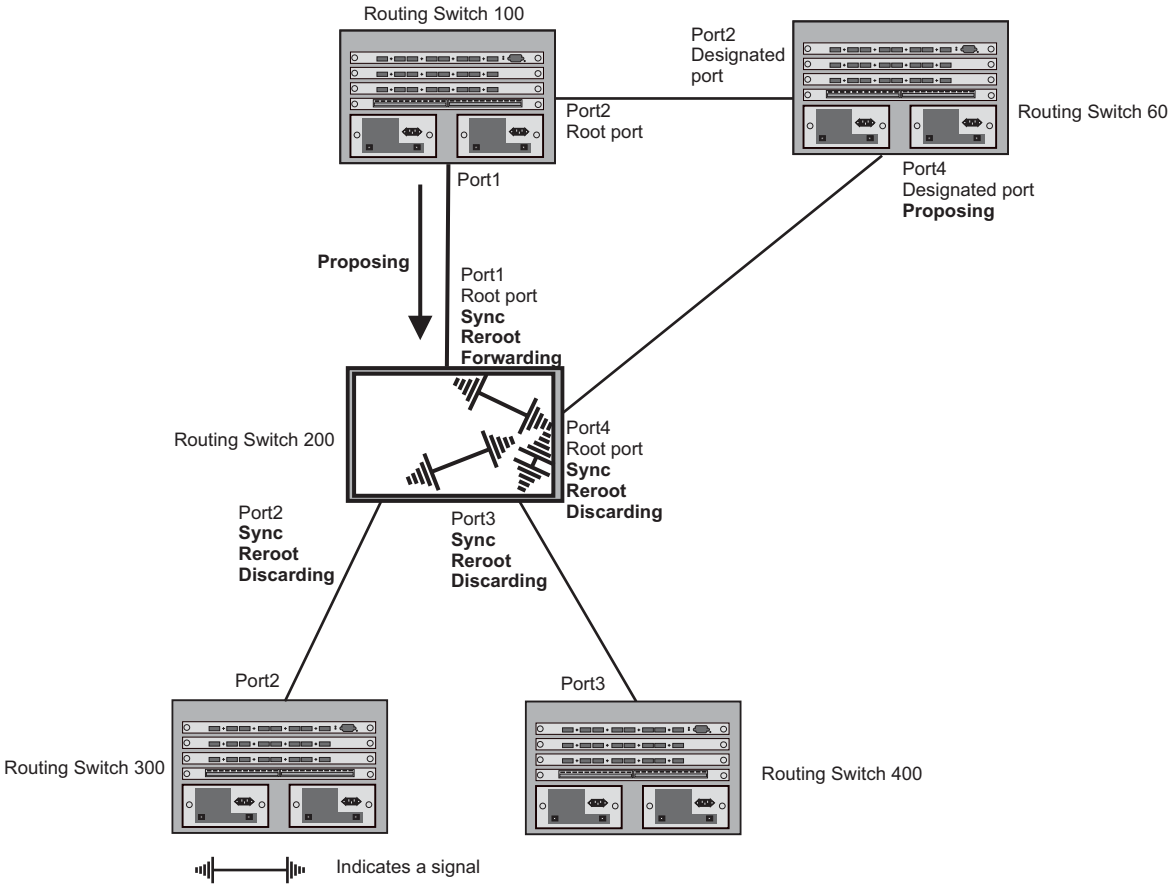
- Proposing and Proposed – The Designated port on the new root bridge (Port4/Routing Switch 60) sends an RST BPDU that contains a proposing signal to Port4/Routing Switch 200 to inform the port that it is ready to put itself in a forwarding state (Figure 8.9). 802.1W algorithm determines that the RST BPDU that Port4/ Routing Switch 200 received is superior to what it can generate, so Port4/Routing Switch 200 assumes a Root port role.

**Figure 8.9 New Root Bridge Sending a Proposal Flag**



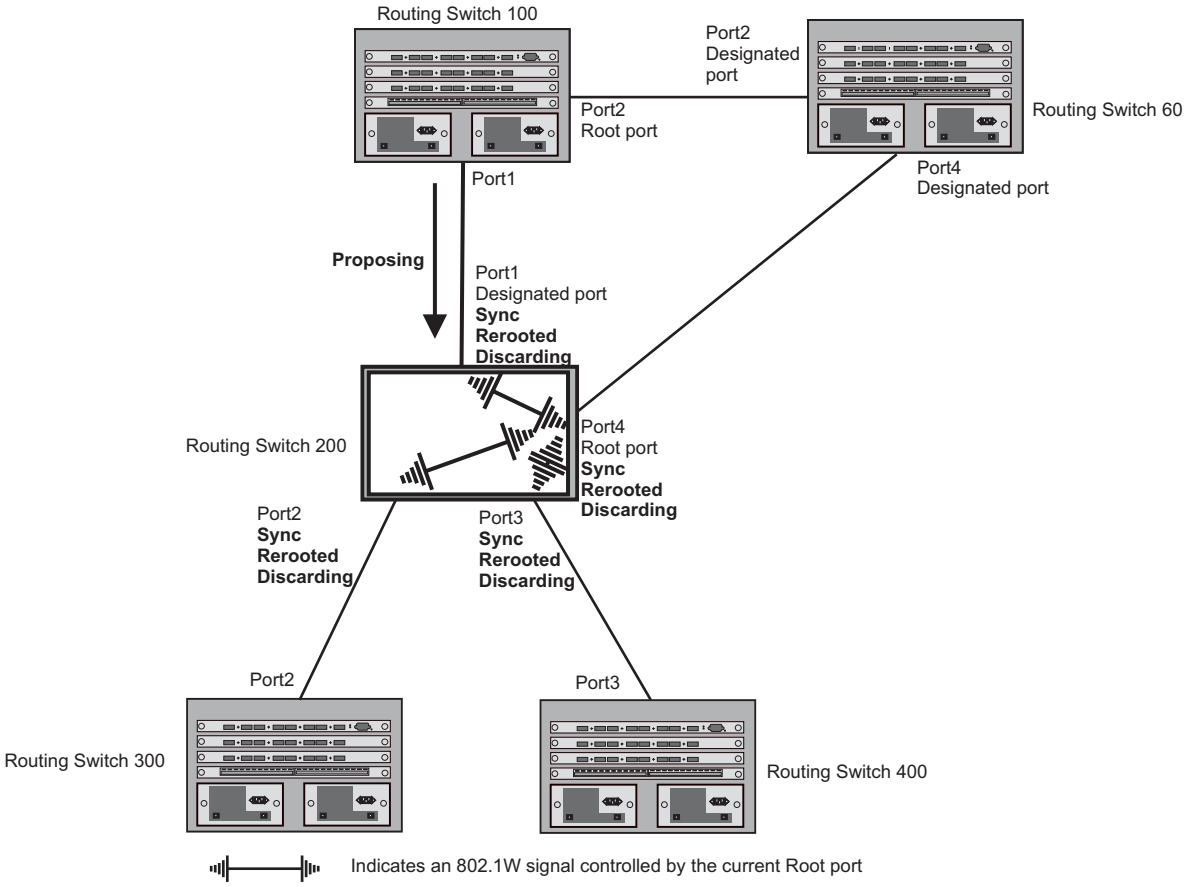
- Sync and Reroot – The Root port then asserts a sync and a reroot signal on all the ports on the bridge. The signal tells the ports that a new Root port has been assigned and they are to renegotiate their new roles and states. The other ports on the bridge assert their sync and reroot signals. Information about the old Root port is discarded from all ports. Designated ports change into discarding states (Figure 8.10).

**Figure 8.10 Sync and Reroot**



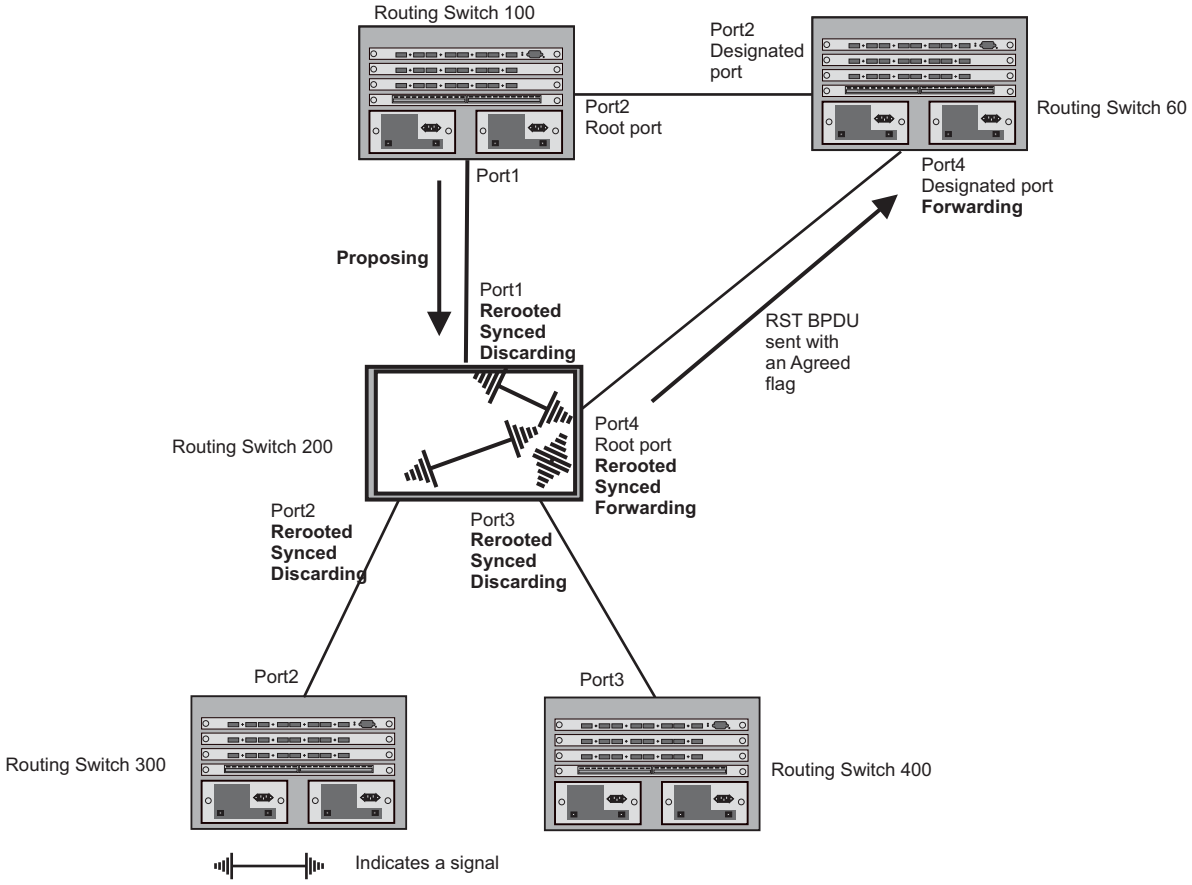
- Sync and Rerooted – When the ports on Routing Switch 200 have completed the reroot phase, they assert their rerooted signals and continue to assert their sync signals as they continue in their discarding states. They also continue to negotiate their roles and states with their peer ports (Figure 8.11).

**Figure 8.11 Sync and Rerooted**



- Synced and Agree – When all the ports on the bridge assert their synced signals, the new Root port asserts its own synced signal and sends an RST BPDU to Port4/Routing Switch 60 that contains an agreed flag (Figure 8.11). The Root port also moves into a forwarding state.

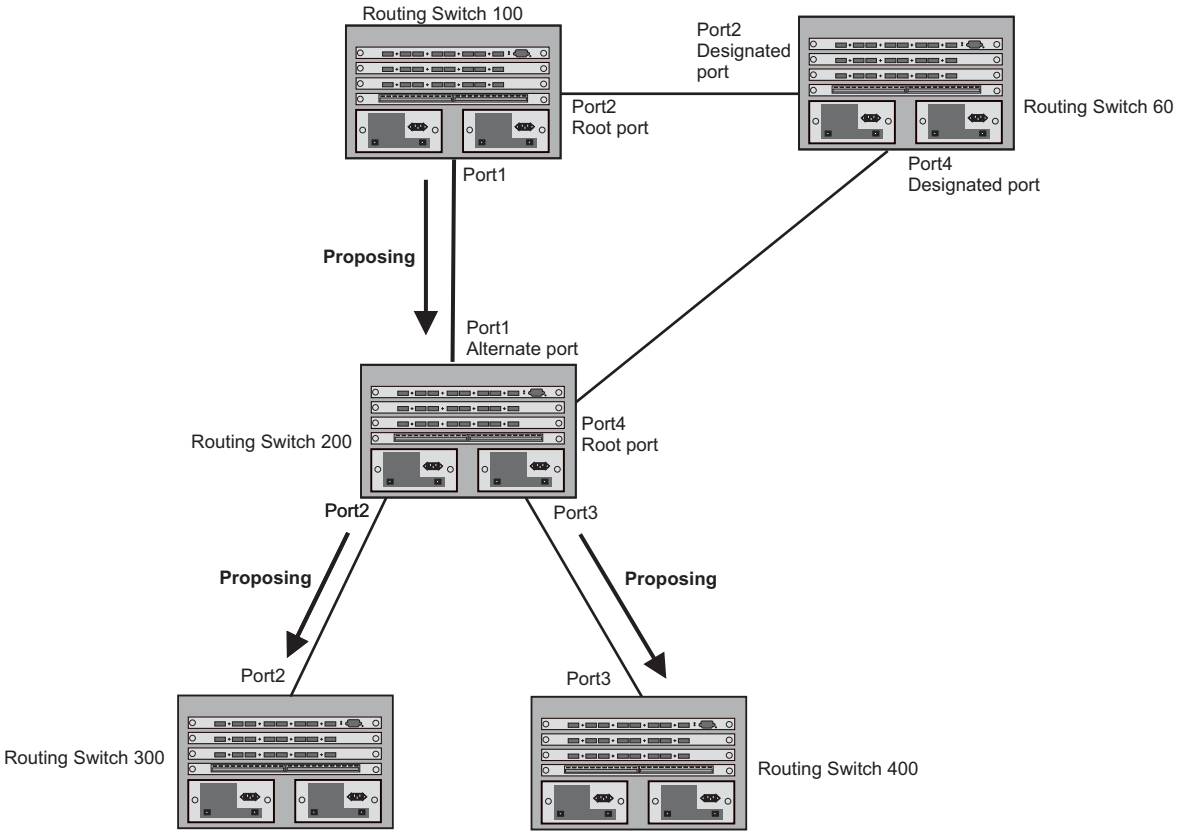
**Figure 8.12 Rerooted, Synced, and Agreed**




The old Root port on Routing Switch 200 becomes an Alternate Port (Figure 8.13). Other ports on that bridge are elected to appropriate roles.

The Designated port on Routing Switch 60 goes into a forwarding state once it receives the RST BPDU with the agreed flag.

**Figure 8.13 Handshake Completed After Election of New Root Port**




Recall that Routing Switch 200 sent the agreed flag to Port4/Routing Switch 60 and not to Port1/Routing Switch 100 (the port that connects Routing Switch 100 to Routing Switch 200). Therefore, Port1/Routing Switch 100 does not go into forwarding state instantly. It waits until two instances of the forward delay timer expires on the port before it goes into forwarding state.

At this point the handshake between the Routing Switch 60 and Routing Switch 200 is complete.

The remaining bridges (Routing Switch 300 and Routing Switch 400) may have to go through the reroot handshake if a new Root port needs to be assigned.

## Convergence in a Simple Topology

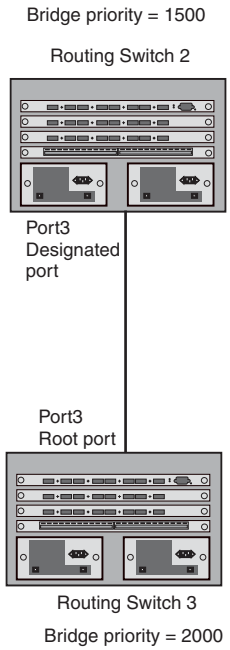
The examples in this section illustrate how 802.1W convergence occurs in a simple Layer 2 topology at start-up.

**NOTE:** The remaining examples assume that the appropriate handshake mechanisms occur as port roles and states change.

### *Convergence at Start Up*

In Figure 8.14, two bridges Routing Switch 2 and Routing Switch 3 are powered up. There are point-to-point connections between Port3/Routing Switch 2 and Port3/Routing Switch 3.

**Figure 8.14 Convergence Between Two Bridges**




At power up, all ports on Routing Switch 2 and Routing Switch 3 assume Designated port roles and are at discarding states before they receive any RST BPDU.

Port3/Routing Switch 2, with a Designated role, transmits an RST BPDU with a proposal flag to Port3/Routing Switch 3. A ports with a Designated role sends the proposal flag in its RST BPDU when they are ready to move to a forwarding state.

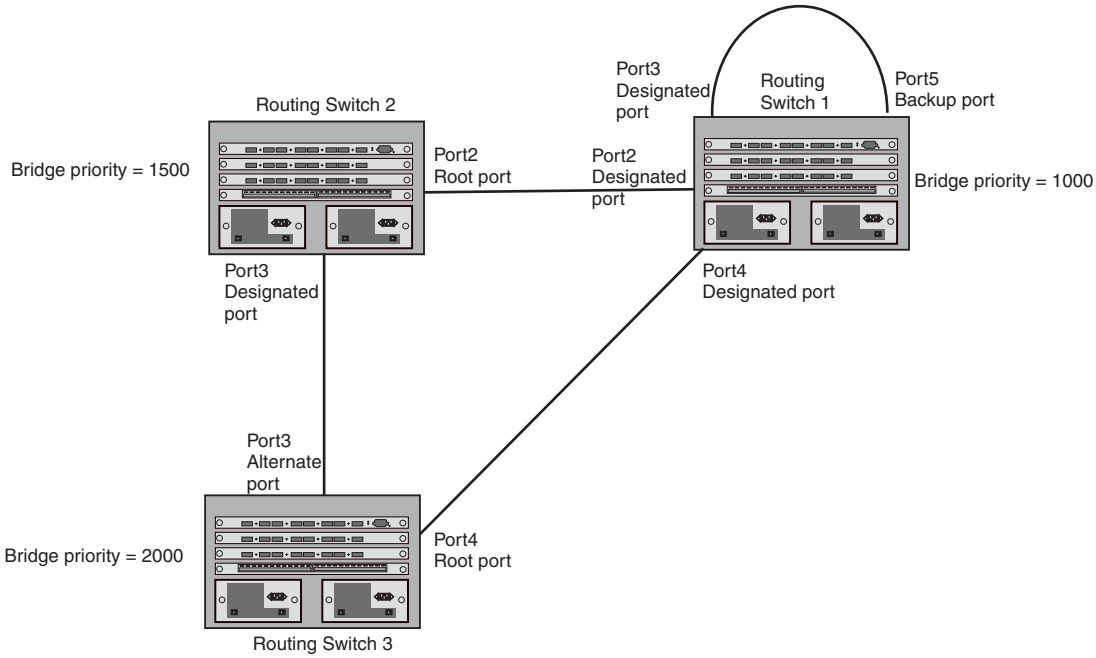
Port3/Routing Switch 3, which starts with a role of Designated port, receives the RST BPDU and finds that it is superior to what it can transmit; therefore, Port3/Routing Switch 3 assumes a new port role, that of a Root port. Port3/Routing Switch 3 transmits an RST BPDU with an agreed flag back to Routing Switch 2 and immediately goes into a forwarding state.

Port3/Routing Switch 2 receives the RST BPDU from Port3/Routing Switch 3 and immediately goes into a forwarding state.

Now 802.1W has fully converged between the two bridges, with Port3/Routing Switch 3 as an operational root port in forwarding state and Port3/Routing Switch 2 as an operational Designated port in forwarding state.

Next, Routing Switch 1 is powered up (Figure 8.15).

**Figure 8.15 Simple Layer 2 Topology**




The point-to-point connections between the three bridges are as follows:

- Port2/Routing Switch 1 and Port2/Routing Switch 2
- Port4/Routing Switch 1 and Port4/Routing Switch 3
- Port3/Routing Switch 2 and Port3/Routing Switch 3

Ports 3 and 5 on Routing Switch 1 are physically connected together.

At start up, the ports on Routing Switch 1 assume Designated port roles, which are in discarding state. They begin sending RST BPDUs with proposal flags to move into a forwarding state.

When Port4/Routing Switch 3 receives these RST BPDUs 802.1W algorithm determines that they are better than the RST BPDUs that were previously received on Port3/Routing Switch 3. Port4/Routing Switch 3 is now selected as Root port. This new assignment signals Port3/Routing Switch 3 to begin entering the discarding state and to assume an Alternate port role. As it goes through the transition, Port3/Routing Switch 3 negotiates a new role and state with its peer port, Port3/Routing Switch 2.

Port4/Routing Switch 3 sends an RST BPDU with an agreed flag to Port4/Routing Switch 1. Both ports go into forwarding states.

Port2/Routing Switch 2 receives an RST BPDU. The 802.1W algorithm determines that these RST BPDUs that are superior to any that any port on Routing Switch 2 can transmit; therefore, Port2/Routing Switch 2 assumes the role of a Root port.

The new Root port then signals all ports on the bridge to start synchronization. Since none of the ports are Edge ports, they all enter the discarding state and assume the role of Designated ports. Port3/Routing Switch 2, which previously had a Designated role with a forwarding state, starts the discarding state. They also negotiate port roles and states with their peer ports. Port3/Routing Switch 2 also sends an RST BPU to Port3/Routing Switch 3 with a proposal flag to request permission go into a forwarding state.

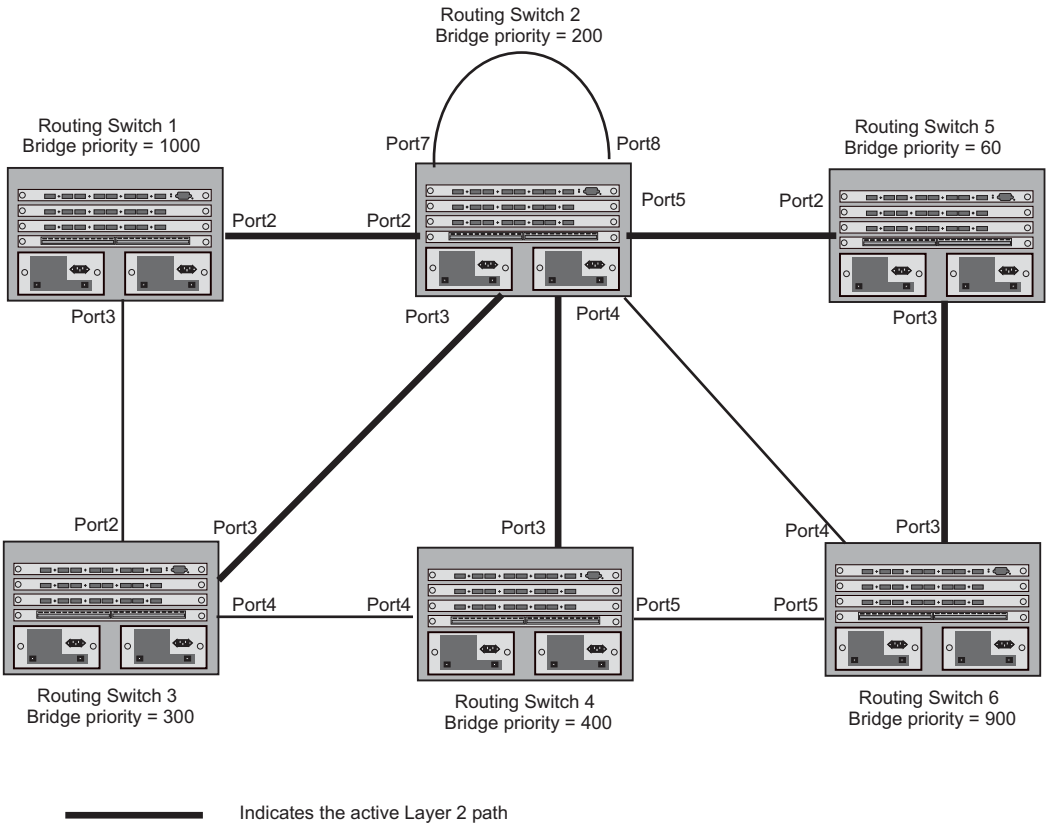
The Port2/Routing Switch 2 bridge also sends an RST BPDU with an agreed flag Port2/Routing Switch 1 that Port2 is the new Root port. Both ports go into forwarding states.

Now, Port3/Routing Switch 3 is currently in a discarding state and is negotiating a port role. It received RST BPDUs from Port3/Routing Switch 2. The 802.1W algorithm determines that the RST BPDUs Port3/Routing Switch 3 received are superior to those it can transmit; however, they are not superior to those that are currently being received by the current Root port (Port4). Therefore, Port3 retains the role of Alternate port.

Ports 3/Routing Switch 1 and Port5/Routing Switch 1 are physically connected. Port5/Routing Switch 1 received RST BPDUs that are superior to those received on Port3/Routing Switch 1; therefore, Port5/Routing Switch 1 is given the Backup port role while Port3 is given the Designated port role. Port3/Routing Switch 1, does not go directly into a forwarding state. It waits until the forward delay time expires twice on that port before it can proceed to the forwarding state.

Once convergence is achieved, the active Layer 2 forwarding path converges as shown in Figure 8.16.

**Figure 8.16 Active Layer 2 Path**

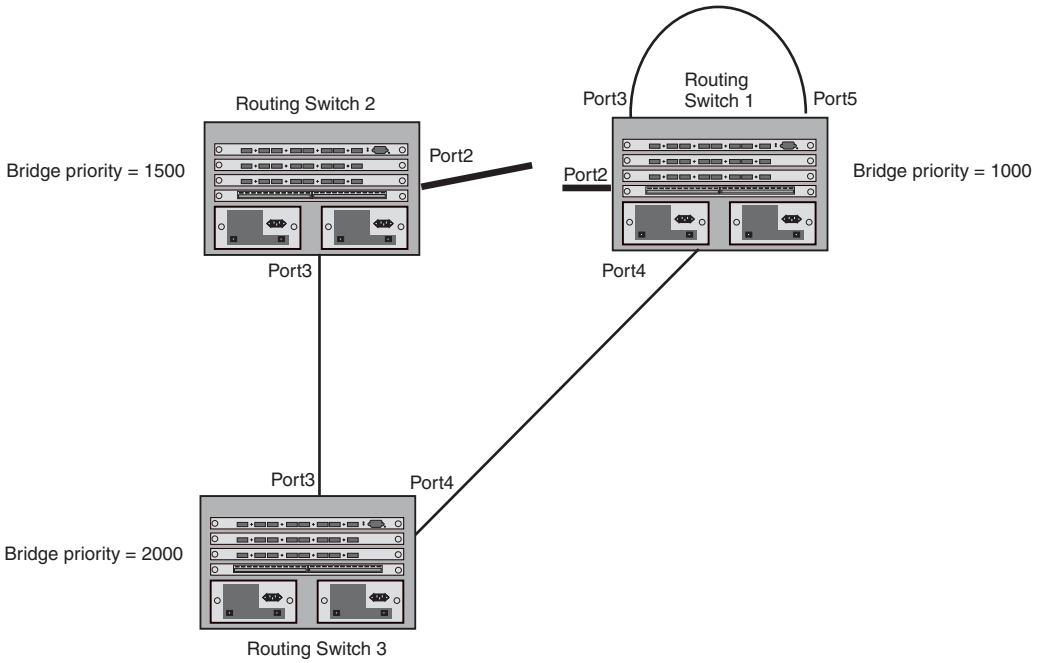


## Convergence After a Link Failure

What happens if a link in the 802.1W topology fails?

For example, Port2/Routing Switch , which is the port that connects Routing Switch 2 to the root bridge (Routing Switch 1), fails. Both Routing Switch 2 and Routing Switch 1 notice the topology change (Figure 8.17).

**Figure 8.17 Link Failure in the Topology**




Routing Switch 1 sets its Port2 into a discarding state.

At the same time, Routing Switch 2 assumes the role of a root bridge since its root port failed and it has no operational Alternate port. Port3/Routing Switch 2, which currently has a Designated port role, sends an RST BPDU to Routing Switch 3. The RST BPDU contains a proposal flag and a bridge ID of Routing Switch 2 as its root bridge ID.

When Port3/Routing Switch 3 receives the RST BPDUs, 802.1W algorithm determines that they are inferior to those that the port can transmit. Therefore, Port3/Routing Switch 3 is given a new role, that of a Designated port. Port3/Routing Switch 3 then sends an RST BPDU with a proposal flag to Routing Switch 2, along with the new role information. However, the root bridge ID transmitted in the RST BPDU is still Routing Switch 1.

When Port3/Routing Switch 2 receives the RST BPDU, 802.1W algorithm determines that it is superior to the RST BPDU that it can transmit; therefore, Port3/Routing Switch 2 receives a new role; that of a Root port. Port3/ Routing Switch 2 then sends an RST BPDU with an agreed flag to Port3/Routing Switch 3. Port3/Routing Switch 2 goes into a forwarding state.

When Port3/Routing Switch 3 receives the RST BPDU that Port3/Routing Switch 2 sent, Port3/Routing Switch 3 changes into a forwarding state, which then completes the full convergence of the topology.

## Convergence at Link Restoration

When Port2/Routing Switch 2 is restored, both Routing Switch 2 and Routing Switch 1 recognize the change. Port2/Routing Switch 1 starts assuming the role of a Designated port and sends an RST BPDU containing a proposal flag to Port2/Routing Switch 2.

When Port2/Routing Switch 2 receives the RST BPDUs, 802.1W algorithm determines that the RST BPDUs the port received are better than those received on Port3/Routing Switch 3; therefore, Port2/Routing Switch 2 is given the role of a Root port. All the ports on Routing Switch 2 are informed that a new Root port has been assigned which then signals all the ports to synchronize their roles and states. Port3/Routing Switch 2, which was the

previous Root port, enters a discarding state and negotiates with other ports on the bridge to establish its new role and state, until it finally assumes the role of a Designated port.

Next, the following happens:

- Port3/Routing Switch 2, the Designated port, sends an RST BPDU, with a proposal flag to Port3/Routing Switch 3.
- Port2/Routing Switch 2 also sends an RST BPDU with an agreed flag to Port2/Routing Switch 1 and then places itself into a forwarding state.

When Port2/Routing Switch 1 receives the RST BPDU with an agreed flag sent by Port2/Routing Switch 2, it puts that port into a forwarding state. The topology is now fully converged.

When Port3/Routing Switch 3 receives the RST BPDU that Port3/Routing Switch 2 sent, 802.1W algorithm determines that these RST BPDUs are superior to those that Port3/Routing Switch 3 can transmit. Therefore, Port3/Routing Switch 3 is given a new role, that of an Alternate port. Port3/Routing Switch 3 immediately enters a discarding state.

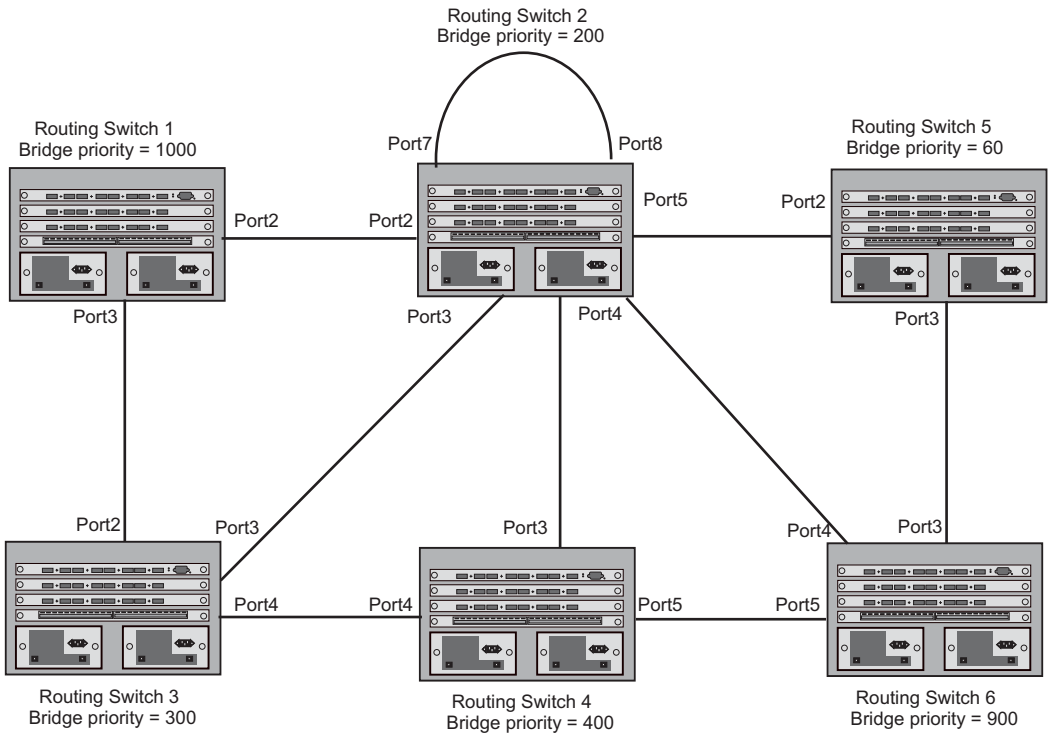
Now Port3/Routing Switch 2 does not go into a forwarding state instantly like the Root port. It waits until the forward delay timer expires twice on that port while it is still in a Designated role, before it can proceed to the forwarding state. The wait, however, does not cause a denial of service, since the essential connectivity in the topology has already been established.

When fully restored, the topology is the same as that shown on Figure 8.15.

## Convergence in a Complex 802.1W Topology

The following is an example of a complex 802.1W topology.

**Figure 8.18 Complex 802.1W Topology**




In Figure 8.18, Routing Switch 5 is selected as the root bridge since it is the bridge with the highest priority. Lines in the figure show the point-to-point connection to the bridges in the topology.

Routing Switch 5 sends an RST BPDU that contains a proposal flag to Port5/Routing Switch 2. When handshakes are completed in Routing Switch 5, Port5/Routing Switch 2 is selected as the Root port on Routing Switch 2. All other ports on Routing Switch 2 are given Designated port role with discarding states.

Port5/Routing Switch 2 then sends an RST BPDU with an agreed flag to Routing Switch 5 to confirm that it is the new Root port and the port enters a forwarding state. Port7 and Port8 are informed of the identity of the new Root port. 802.1W algorithm selects Port7 as the Designated port while Port8 becomes the Backup port.

Port3/Routing Switch 5 sends an RST BPDU to Port3/Routing Switch 6 with a proposal flag. When Port3/Routing Switch 5 receives the RST BPDU, handshake mechanisms select Port3 as the Root port of Routing Switch 6. All other ports are given a Designated port role with discarding states. Port3/Routing Switch 6 then sends an RST BPDU with an agreed flag to Port3/Routing Switch 5 to confirm that it is the Root port. The Root port then goes into a forwarding state.

Now, Port4/Routing Switch 6 receives RST BPDUs that are superior to what it can transmit; therefore, it is given the Alternate port role. The port remains in discarding state.

Port5/Routing Switch 6 receives RST BPDUs that are inferior to what it can transmit. The port is then given a Designated port role.

Next Routing Switch 2 sends RST BPDUs with a proposal flag to Port3/Routing Switch 4. Port3 becomes the Root port for the bridge; all other ports are given a Designated port role with discarding states. Port3/Routing Switch 4 sends an RST BPDU with an agreed flag to Routing Switch 2 to confirm that it is the new Root port. The port then goes into a forwarding state.

Now Port4/Routing Switch 4 receives an RST BPDU that is superior to what it can transmit. The port is then given an Alternate port role, and remains in discarding state.

Likewise, Port5/Switch 4 receives an RST BPDU that is superior to what it can transmit. The port is also given an Alternate port role, and remains in discarding state.

Port2/Routing Switch 2 transmits an RST BPDU with a proposal flag to Port2/Routing Switch 1. Port2/Routing Switch 1 becomes the Root port. All other ports on Routing Switch 1 are given Designated port roles with discarding states.

Port2/Routing Switch 1 sends an RST BPDU with an agreed flag to Port2/Routing Switch 2 and Port2/Routing Switch 1 goes into a forwarding state.

Port3/Routing Switch 1 receives an RST BPDUs that is inferior to what it can transmit; therefore, the port retains its Designated port role and goes into forwarding state only after the forward delay timer expires twice on that port while it is still in a Designated role.

Port3/Routing Switch 2 sends an RST BPDU to Port3/Routing Switch 3 that contains a proposal flag. Port3/Routing Switch 3 becomes the Root port, while all other ports on Routing Switch 3 are given Designated port roles and go into discarding states. Port3/Routing Switch 3 sends an RST BPDU with an agreed flag to Port3/Routing Switch 2 and Port3/Routing Switch 3 goes into a forwarding state.

Now, Port2/Routing Switch 3 receives an RST BPDUs that is superior to what it can transmit so that port is given an Alternate port state.

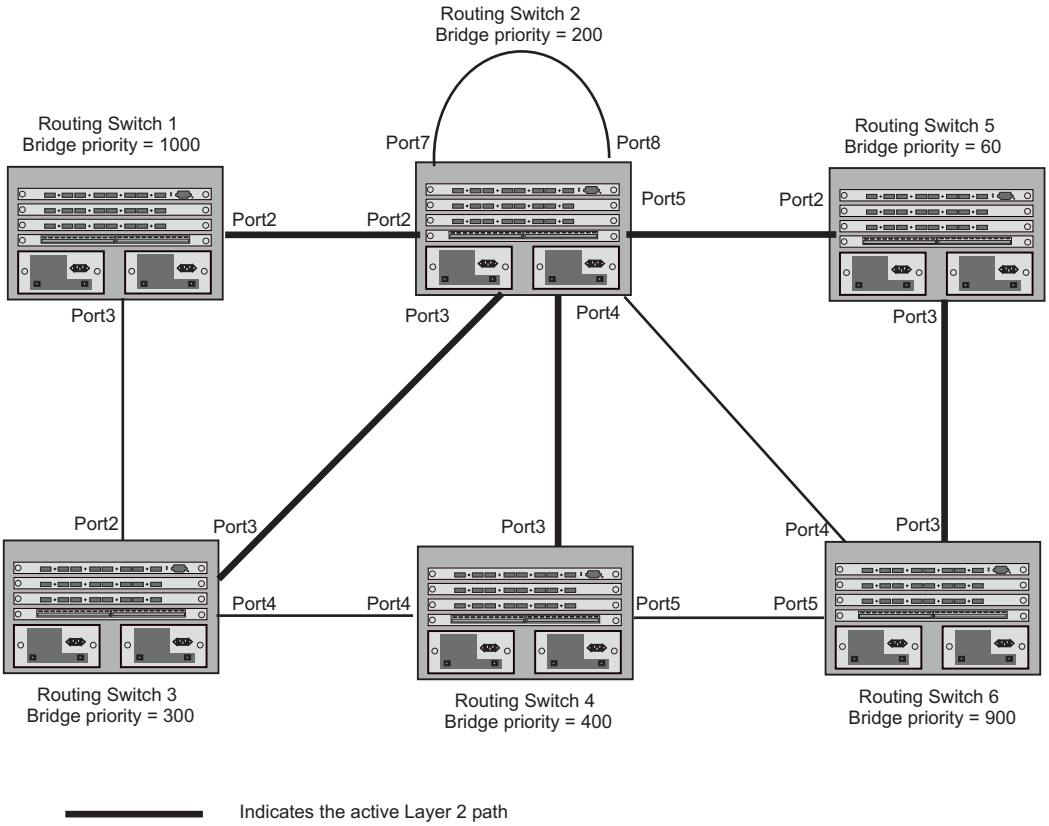
Port4/Routing Switch 3 receives an RST BPDU that is inferior to what it can transmit; therefore, the port retains its Designated port role.

Ports on all the bridges in the topology with Designated port roles that received RST BPDUs with agreed flags go into forwarding states instantly. However, Designated ports that did not receive RST BPDUs with agreed flags must wait until the forward delay timer expires twice on those port. Only then will these port move into forwarding states.

The entire 802.1W topology converges in less than 300 msec and the essential connectivity is established between the designated ports and their connected root ports.

After convergence is complete, Figure 8.19 shows the active Layer 2 path of the topology in Figure 8.18.

**Figure 8.19 Active Layer 2 Path in Complex Topology**




## Propagation of Topology Change

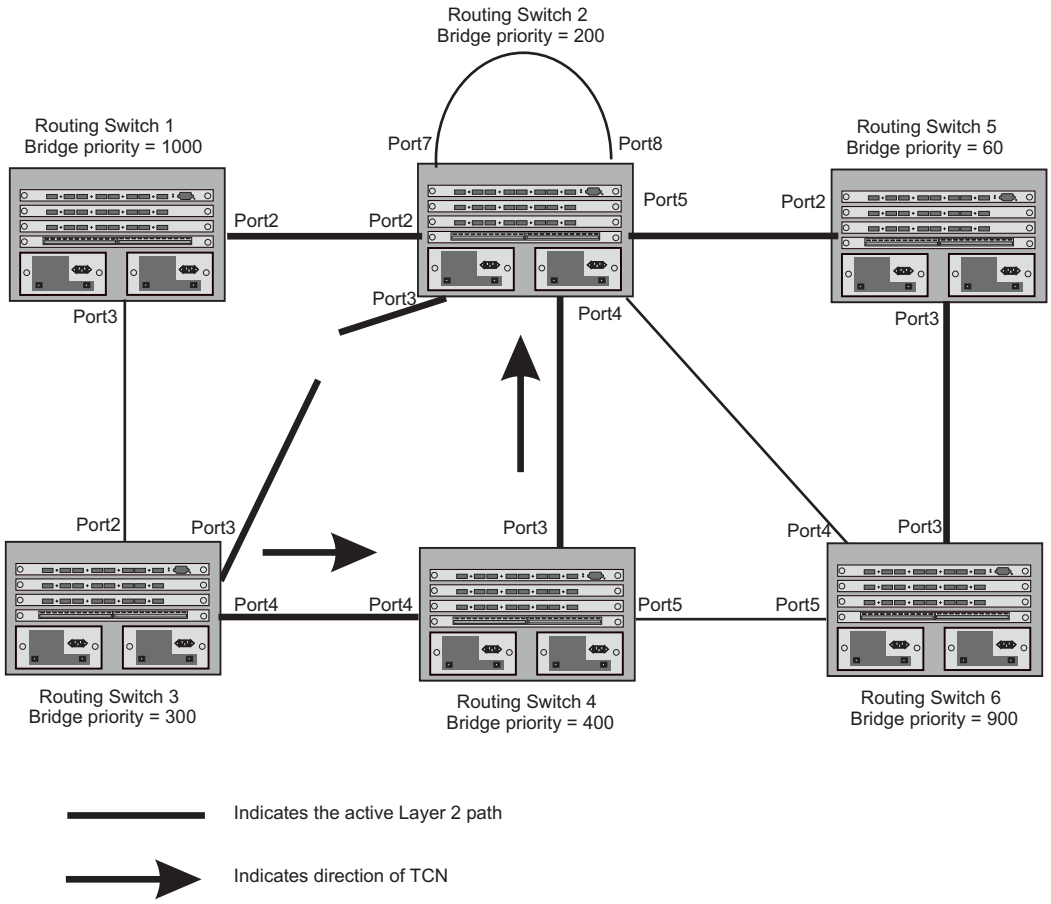
The Topology Change state machine generates and propagates the topology change notification messages on each port. When a Root port or a Designated port goes into a forwarding state, the Topology Change state machine on those ports send a topology change notice (TCN) to all the bridges in the topology to propagate the topology change.

**NOTE:** Edge ports, Alternate ports, or Backup ports do not need to propagate a topology change.

The TCN is sent in the RST BPDU that a port sends. Ports on other bridges in the topology then acknowledge the topology change once they receive the RST BPDU, and send the TCN to other bridges until all the bridges are informed of the topology change.

For example, Port3/Routing Switch 2 in Figure 8.20, fails. Port4/Routing Switch 3 becomes the new Root port. Port4/Routing Switch 3 sends an RST BPDU with a TCN to Port4/Routing Switch 4. To propagate the topology change, Port4/Routing Switch 4 then starts a TCN timer on itself, on the bridge's Root port, and on other ports on that bridge with a Designated role. Then Port3/Routing Switch 4 sends RST BPDU with the TCN to Port4/Routing Switch 2. (Note the new active Layer 2 path in Figure 8.20.)

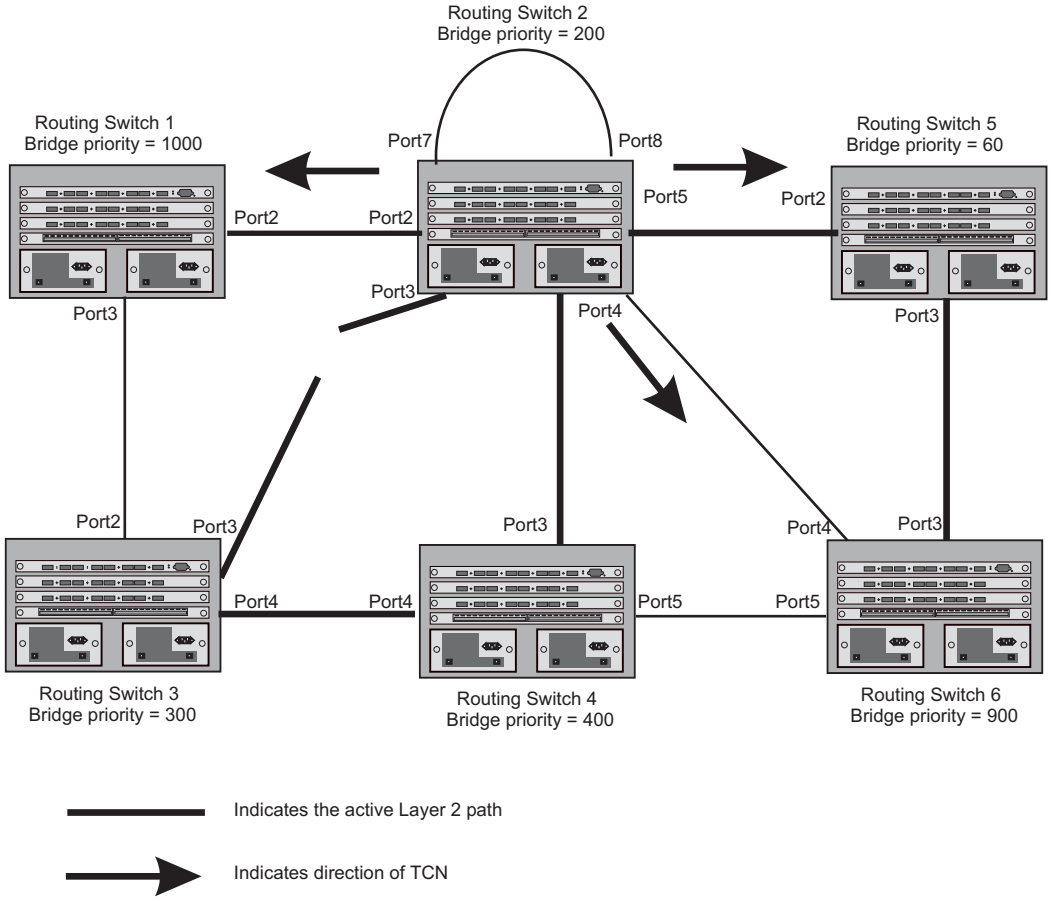
**Figure 8.20 Beginning of Topology Change Notice**



Routing Switch 2 then starts the TCN timer on the Designated ports and sends RST BPDUs that contain the TCN as follows (Figure 8.21):

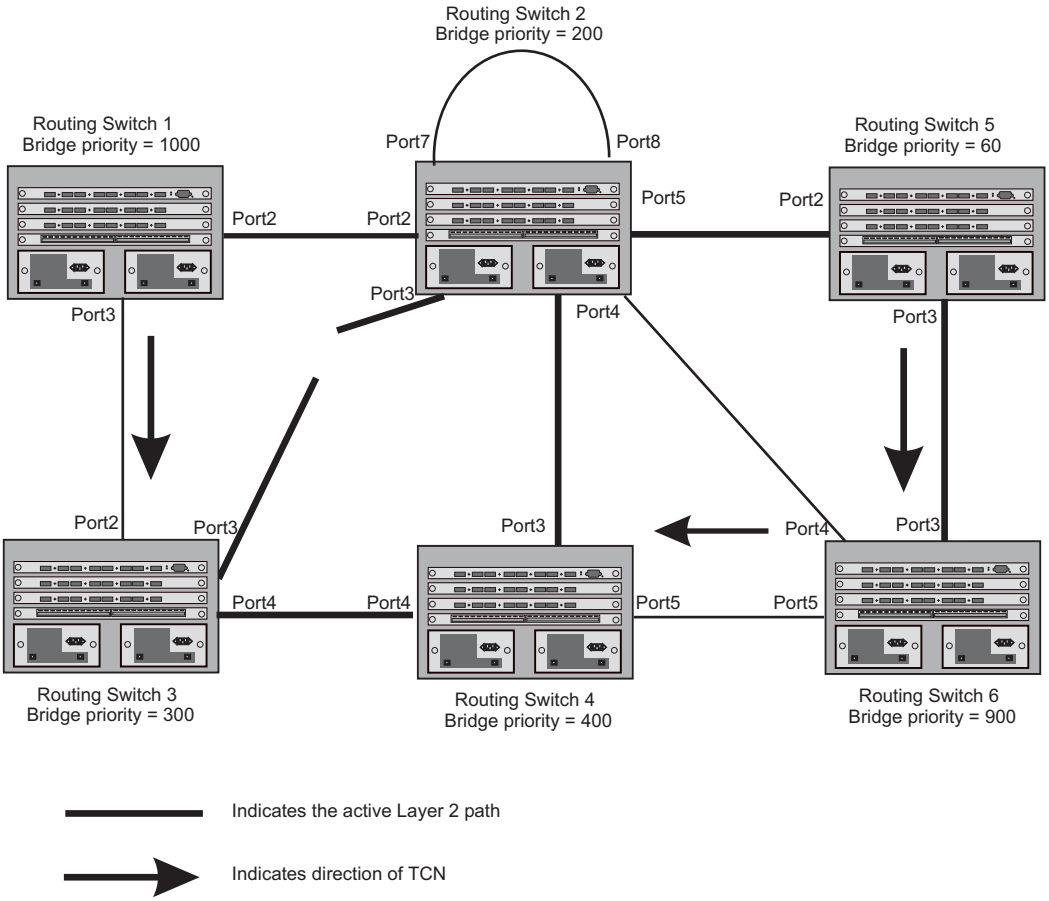
- Port5/Routing Switch 2 sends the TCN to Port2/Routing Switch 5
- Port4/Routing Switch 2 sends the TCN to Port4/Routing Switch 6
- Port2/Routing Switch 2 sends the TCN to Port2/Routing Switch 1

**Figure 8.21 Sending TCN to Bridges Connected to Routing Switch 2**



Then FRY1, Routing Switch 5, and Routing Switch 6 send RST BPDUs that contain the TCN to Routing Switch 3 and Routing Switch 4 to complete the TCN propagation (Figure 8.22).

**Figure 8.22 Completing the TCN Propagation**




## Compatibility of 802.1W with 802.1D

802.1W-enabled bridges are backward compatible with IEEE 802.1D bridges. This compatibility is managed on a per-port basis by the Port Migration state machine. **However, intermixing the two types of bridges in the network topology is not advisable if you want to take advantage of the rapid convergence feature.**

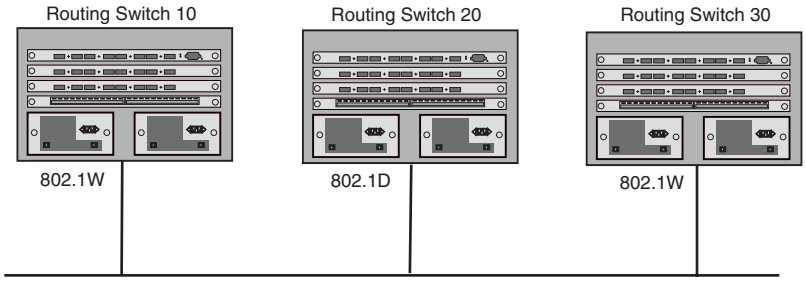
Compatibility with 802.1D means that an 802.1W-enabled port can send BPDUs in the STP or 802.1D format when one of the following events occur:

- The port receives a legacy BPDU. A legacy BPDU is an STP BPDU or a BPDU in an 802.1D format. The port that receives the legacy BPDU automatically configures itself to behave like a legacy port. It sends and receives legacy BPDUs only.
- The entire bridge is configured to operate in an 802.1D mode when an administrator sets the
- bridge parameter to zero at the CLI, forcing all ports on the bridge to send legacy BPDUs only.

Once a port operates in the 802.1D mode, 802.1D convergence times are used and rapid convergence is not realized.

For example, in Figure 8.23, Routing Switch 10 and Routing Switch 30 receive legacy BPDUs from Routing Switch 20. Ports on Routing Switch 10 and Routing Switch 30 begin sending BPDUs in STP format to allow them to operate transparently with Routing Switch 20.

**Figure 8.23 802.1W Bridges with an 802.1D Bridge**




Once Routing Switch 20 is removed from the LAN, Routing Switch 10 and Routing Switch 30 receive and transmit BPDUs in the STP format to and from each other. This state will continue until the administrator enables the **force-migration-check** command to force the bridge to send RSTP BPDU during a migrate time period. If ports on the bridges continue to hear only STP BPDUs after this migrate time period, those ports will return to sending STP BPDUs. However, when the ports receive RST BPDUs during the migrate time period, the ports begin sending RST BPDUs. The migrate time period is non-configurable. It has a value of three seconds.

**NOTE:** The IEEE standards state that 802.1W bridges need to interoperate with 802.1D bridges. IEEE standards set the path cost of 802.1W bridges to be between 1 and 200,000,000; whereas path cost of 802.1D bridges are set between 1 and 65,535. In order for the two bridge types to be able to interoperate in the same topology, the administrator needs to configure the bridge path cost appropriately. Path costs for either 802.1W bridges or 802.1D bridges need to be changed; in most cases, path costs for 802.1W bridges need to be changed.

## Configuring 802.1W Parameters on an HP Device

The remaining 802.1W sections explain how to configure the 802.1W protocol in an HP Chassis device.

Chassis devices are shipped from the factory with 802.1W disabled. Use the following methods to enable or disable 802.1W. You can enable or disable 802.1W at the following levels:

- Port-based VLAN – Affects all ports within the specified port-based VLAN. When you enable or disable 802.1W within a port-based VLAN, the setting overrides the global setting. Thus, you can enable 802.1W for the ports within a port-based VLAN even when 802.1W is globally disabled, or disable the ports within a port-based VLAN when 802.1W is globally enabled.
- Individual port – Affects only the individual port. However, if you change the 802.1W state of the primary port in a trunk group, the change affects all ports in the trunk group.

### *Enabling or Disabling 802.1W in a Port-Based VLAN*

Use the following procedure to disable or enable 802.1W on a device on which you have configured a port-based VLAN. Changing the 802.1W state in a VLAN affects only that VLAN.

#### *USING THE CLI*

To enable 802.1W for all ports in a port-based VLAN, enter commands such as the following:

```
HP9300(config)# vlan 10
HP9300(config-vlan-10)# spanning-tree 802-1w
```

***Syntax:*** [no] spanning-tree 802-1w

#### *USING THE WEB MANAGEMENT INTERFACE*

You cannot enable or disable 802.1W on port-based VLAN using the Web management interface.

### *Enabling or Disabling 802.1W on a Single Spanning Tree*

To enable 802.1W for all ports of a single spanning tree, use the procedure in this section.

*USING THE CLI*

Enter a command such as the following:

```
HP9300(config-vlan-10)# spanning-tree single 802-1w
```

***Syntax:*** [no] spanning-tree single 802-1w

*USING THE WEB MANAGEMENT INTERFACE*

You cannot enable or disable 802.1W on a single spanning tree using the Web management interface.

### *Disabling or Enabling 802.1W on an Individual Port*

The **spanning-tree 802-1w** or **spanning-tree single 802-1w** command must be used to initially enable 802.1W on ports. Both commands enable 802.1W on all ports that belong to the VLAN or to the single spanning tree.

Once 802.1W is enabled on a port, it can be disabled on individual ports. 802.1W that have been disabled on individual ports can then be enabled as required.

---

**NOTE:** If you change the 802.1W state of the primary port in a trunk group, the change affects all ports in that trunk group.

---

*USING THE CLI*

To disable or enable 802.1W on an individual port, enter commands such as the following:

```
HP9300(config)# interface 1/1
HP9300(config-if-1/1)# no spanning-tree
```

***Syntax:*** [no] spanning-tree

*USING THE WEB MANAGEMENT INTERFACE*

You cannot enable or disable 802.1W on individual ports using the Web management interface.

### *Changing 802.1W Bridge Parameters*

When you make changes to 802.1W bridge parameters, the changes are applied to individual ports on the bridge. To change 802.1W bridge parameters, use the following methods.

*USING THE CLI*

To designate a priority for a bridge, enter a command such as the following:

```
HP9300(config)# spanning-tree 802-1w priority 10
```

The command in this example changes the priority on a device on which you have not configured port-based VLANs. The change applies to the default VLAN. If you have configured a port-based VLAN on the device, you can configure the parameters only at the configuration level for individual VLANs. Enter commands such as the following:

```
HP9300(config)# vlan 20
HP9300(config-vlan-20)# spanning-tree 802-1w priority 0
```

To make this change in the default VLAN, enter the following commands:

```
HP9300(config)# vlan 1
HP9300(config-vlan-1)# spanning-tree 802-1w priority 0
```

***Syntax:*** spanning-tree 802-1w [forward-delay <value>] | [hello-time <value>] | [max-age <time>] | [force-version <value>] | [priority <value>]

The **forward-delay** <value> parameter specifies how long a port waits before it forwards an RST BPDU after a topology change. This can be a value from 4 – 30 seconds. The default is 15 seconds.

The **hello-time** <value> parameter specifies the interval between two hello packets. This parameter can have a value from 1 – 10 seconds. The default is 2 seconds; however, set this value to at least 4 seconds to provide enough time for BPDUs to reach the root bridge before the timeout period expires on a non-root bridge port.

The **max-age** <value> parameter specifies the amount of time the device waits to receive a hello packet before it initiates a topology change. You can specify a value from 6 – 40 seconds. The default is 20 seconds.

Beginning with software release 07.6.04, the value of **max-age** must be greater than the value of **forward-delay** to ensure that the downstream bridges do not age out faster than the upstream bridges (those bridges that are closer to the root bridge).

The **force-version** <value> parameter forces the bridge to send BPDUs in a specific format. You can specify one of the following values:

- 0 – The STP compatibility mode. Only STP (or legacy) BPDUs will be sent.
- 2 – The default. RST BPDUs will be sent unless a legacy bridge is detected. If a legacy bridge is detected, STP BPDUs will be sent instead.

The default is 2.

The **priority** <value> parameter specifies the priority of the bridge. You can enter a value from 0 – 65535. A lower numerical value means a the bridge has a higher priority. Thus, the highest priority is 0. The default is 32768.

You can specify some or all of these parameters on the same command line. If you specify more than one parameter, you must specify them in the order shown above, from left to right.

*USING THE WEB MANAGEMENT INTERFACE*

You cannot modify 802.1W bridge parameters using the Web management interface.

### *Changing Port Parameters*

The 802.1W port commands can be enabled on individual ports or on multiple ports, such as all ports that belong to a VLAN.

The 802.1W port parameters are preconfigured with default values. If the default parameters meet your network requirements, no other action is required.

You can change the following 802.1W port parameters using the following methods.

*USING CLI*

```
HP9300(config)# vlan 10
HP9300(config-vlan-10)# spanning-tree 802-1w ethernet 1/5 path-cost 15 priority 64
```

***Syntax:*** spanning-tree 802-1w ethernet <portnum> path-cost <value> | priority <value> | [admin-edge-port] | [admin-pt2pt-mac] | [force-migration-check]

The **ethernet** <portnum> parameter specifies the interface used.

The **path-cost** <value> parameter specifies the cost of the port's path to the root bridge. 802.1W prefers the path with the lowest cost. You can specify a value from 1 – 20,000,000. Table 1 shows the recommended path cost values from the IEEE standards.

**Table 1: Recommended Path Cost Values of 802.1W**

| Link Speed | Recommended (Default) 802.1W Path Cost Values | Recommended 802.1W Path Cost Range |
|---|---|---|
| Less than 100 kilobits per second | 200,000,000 | 20,000,000 – 200,000,000 |

**Table 1: Recommended Path Cost Values of 802.1W**

| Link Speed | Recommended (Default) 802.1W Path Cost Values | Recommended 802.1W Path Cost Range |
|---|---|---|
| 1 Megabit per second | 20,000,000 | 2,000,000 – 200,000,000 |
| 10 Megabits per second | 2,000,000 | 200,000 – 200,000,000 |
| 100 Megabits per second | 200,000 | 20,000 – 200,000,000 |
| 1 Gigabit per second | 20,000 | 2,000 – 200,000,000 |
| 10 Gigabits per second | 2,000 | 200 – 20,000 |
| 100 Gigabits per second | 200 | 20 – 2,000 |
| 1 Terabits per second | 20 | 2 – 200 |
| 10 Terabits per second | 2 | 1 – 20 |

The **priority** <value> parameter specifies the preference that 802.1W gives to this port relative to other ports for forwarding traffic out of the topology. You can specify a value from 8 – 252, in increments of 4. If you enter a value that is not divisible by four the software rounds to the nearest value that is. The default is 128. A higher numerical value means a lower priority; thus, the highest priority is 8

Set the **admin-edge-port** to enabled or disabled. If set to enabled, then the port becomes an edge port in the domain.

Set the **admin-pt2pt-mac** to enabled or disabled. If set to enabled, then a port is connected to another port through a point-to-point link. The point-to-point link increases the speed of convergence. This parameter, however, does not auto-detect whether or not the link is a physical point-to-point link.

The **force-migration-check** parameter forces the specified port to sent one RST BPDU. If only STP BPDUs are received in response to the sent RST BPDU, then the port will go return to sending STP BPDUs.

*USING THE WEB MANAGEMENT INTERFACE*

You cannot modify 802.1W port parameters using the Web management interface.

**EXAMPLE:**

Suppose you want to enable 802.1W on a system with no active port-based VLANs and change the hello-time from the default value of 2 to 8 seconds. Additionally, suppose you want to change the path and priority costs for port 5 only. To do so, enter the following commands.

```
HP9300(config)# spanning-tree 802-1w hello-time 8
HP9300(config)# spanning-tree 802-1w ethernet 5 path-cost 15 priority 64
```

## Displaying Information About 802-1W

You can display a summary or details of the 802.1W information.

*USING THE CLI*

To display a summary of 802-1W, use the following command:

```
HP9300(config)#show 802-1w
--- VLAN 1 [ STP Instance owned by VLAN 1 ] ---------------------------
VLAN 1 BPDU cam_index is 2 and the IGC and DMA master Are(HEX) 0 1 2 3
Bridge IEEE 802.1W Parameters:
Bridge            Bridge  Bridge Bridge Force   tx
Identifier        MaxAge  Hello  FwdDly Version Hold
hex               sec     sec    sec            cnt
800000e080541700  20      2      15     Default 3

RootBridge        RootPath   DesignatedBri-    Root  Max  Fwd  Hel
Identifier        Cost       dge Identifier    Port  Age  Dly  lo
hex                          hex                     sec  sec  sec
800000e0804c9c00  200000     800000e0804c9c00  1     20   15   2

Port IEEE 802.1W Parameters:
      <--- Config Params -->|<-------------- Current state ----------------->
Port  Pri PortPath P2P Edge Role       State      Designa- Designated
Num       Cost     Mac Port                     ted cost bridge
1     128 200000   F   F    ROOT       FORWARDING 0        800000e0804c9c00
2     128 200000   F   F    DESIGNATED FORWARDING 200000   800000e080541700
3     128 200000   F   F    DESIGNATED FORWARDING 200000   800000e080541700
4     128 200000   F   F    BACKUP     DISCARDING 200000   800000e080541700
```

***Syntax:*** show 802-1w [vlan <vlan-id>]

The **vlan** <vlan-id> parameter displays 802.1W information for the specified port-based VLAN.

The **show 802.1w display** command shows the information listed in Table 2.

**Table 2: CLI Display of 802.1W Summary**

| This Field... | Displays... |
|---|---|
| VLAN ID | The port-based VLAN that owns the STP instance. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all 802.1W information is for VLAN 1. |
| **Bridge IEEE 802.1W Parameters** | |
| Bridge Identifier | The ID of the bridge. |
| Bridge Max Age | The configured max age for this bridge. The default is 20. |
| Bridge Hello | The configured hello time for this bridge.The default is 2. |
| Bridge FwdDly | The configured forward delay time for this bridge. The default is 15. |

**Table 2: CLI Display of 802.1W Summary (Continued)**

| This Field... | Displays... |
|---|---|
| Force-Version | The configured force version value. One of the following value is displayed:<br>• 0 – The bridge has been forced to operate in an STP compatibility mode.<br>• 2 – The bridge has been forced to operate in an 802.1W mode. (This is the default.) |
| txHoldCnt | The number of BPDUs that can be transmitted per Hello Interval. The default is 3. |
| Root Bridge Identifier | ID of the Root bridge that is associated with this bridge |
| Root Path Cost | The cost to reach the root bridge from this bridge. If the bridge is the root bridge, then this parameter shows a value of zero. |
| Designated Bridge Identifier | The bridge from where the root information was received.It can be from the root bridge itself, but it could also be from another bridge. |
| Root Port | The port on which the root information was received. This is the port that is connected to the Designated Bridge. |
| Max Age | The ***max age*** is derived from the Root port. An 802.1W-enabled bridge uses this value, along with the hello and message age parameters to compute the effective age of an RST BPDU.<br>The ***message age*** parameter is generated by the Designated port and transmitted in the RST BPDU. RST BPDUs transmitted by a Designated port of the root bridge contains a message value of zero.<br>***Effective age*** is the amount of time the Root port, Alternate port, or Backup port retains the information it received from its peer Designated port. Effective age is reset every time a port receives an RST BPDU from its Designated port. If a Root port does not receive an RST BPDU from its peer Designated port for a duration more than the effective age, the Root port ages out the existing information and recomputes the topology.<br>If the port is operating in 802.1D compatible mode, then max age functionality is the same as in 802.1D (STP). |
| Fwd Dly | The number of seconds a non-edge Designated port waits until it can apply any of the following transitions, if the RST BPDU it receives does not have an agreed flag:<br>• Discarding state to learning state<br>• Learning state to forwarding state<br>When a non-edge port receives the RST BPDU it goes into forwarding state within 4 seconds or after two hello timers expire on the port.<br>Fwd Dly is also the number of seconds that a Root port waits for an RST BPDU with a proposal flag before it applies the state transitions listed above.<br>If the port is operating in 802.1D compatible mode, then forward delay functionality is the same as in 802.1D (STP). |

**Table 2: CLI Display of 802.1W Summary (Continued)**

| This Field... | Displays... |
|---|---|
| Hello | The hello value derived from the Root port. It is the number of seconds between two Hello packets. |
| **Port IEEE 802.1W Parameters** | |
| Port Num | The port number shown in a slot#/port# format. |
| Pri | The configured priority of the port. The default is 128 or 0x80. |
| Port Path Cost | The configured path cost on a link connected to this port. |
| P2P Mac | Indicates if the point-to-point-mac parameter is configured to be a point-to-point link:<br>• T – The link is configured as a point-to-point link.<br>• F – The link is not configured as a point-to-point link. This is the default. |
| Edge port | Indicates if the port is configured as an operational Edge port:<br>• T – The port is configured as an Edge port.<br>• F – The port is not configured as an Edge port. This is the default. |
| Role | The current role of the port:<br>• Root<br>• Designated<br>• Alternate<br>• Backup<br>• Disabled<br>Refer to “Bridges and Bridge Port Roles” on page 8-23 for definitions of the roles. |
| State | The port’s current 802.1W state. A port can have one of the following states:<br>• Forwarding<br>• Discarding<br>• Learning<br>• Disabled<br>Refer to “Bridge Port States” on page 8-27 and “Edge Port and Non-Edge Port States” on page 8-27. |
| Designated Cost | The best root path cost that this port received, including the best root path cost that it can transmit. |
| Designated Bridge | The ID of the bridge that sent the best RST BPDU that was received on this port. |

To display detailed information about 802-1W, using the following command:

```
HP9300(config)#show 802-1w detail
=====================================================================
VLAN 1 - MULTIPLE SPANNING TREE (MSTP - IEEE 802.1W) ACTIVE
=====================================================================
BridgeId 800000e080541700, forceVersion 2, txHoldCount 3

Port 1 - Role: ROOT - State: FORWARDING
  PathCost 200000, Priority 128, AdminOperEdge F, AdminPt2PtMac F
  DesignatedPriority - Root: 0x800000e0804c9c00, Bridge: 0x800000e080541700
  ActiveTimers - rrWhile 4 rcvdInfoWhile 4
  MachineStates - PIM: CURRENT, PRT: ROOT_PORT, PST: FORWARDING
  TCM: ACTIVE, PPM: SENDING_STP, PTX: TRANSMIT_IDLE
  Received - RST BPDUs 0, Config BPDUs 1017, TCN BPDUs 0


Port 2 - Role: DESIGNATED - State: FORWARDING
  PathCost 200000, Priority 128, AdminOperEdge F, AdminPt2PtMac F
  DesignatedPriority - Root: 0x800000e0804c9c00, Bridge: 0x800000e080541700
  ActiveTimers - helloWhen 0
  MachineStates - PIM: CURRENT, PRT: DESIGNATED_PORT, PST: FORWARDING
  TCM: ACTIVE, PPM: SENDING_RSTP, PTX: TRANSMIT_IDLE
  Received - RST BPDUs 0, Config BPDUs 0, TCN BPDUs 0
```

***Syntax:*** show 802-1w detail [vlan <vlan-id>]

The **vlan** <vlan-id> parameter displays 802.1W information for the specified port-based VLAN.

The **show spanning-tree 802.1W** command shows the following information.

| This Field... | Displays... |
|---|---|
| VLAN ID | ID of the VLAN that owns the instance of 802.1W and whether or not it is active. |
| Bridge ID | ID of the bridge. |
| forceVersion | the configured version of the bridge:<br>• 0 – The bridge has been forced to operate in an STP compatible mode.<br>• 2 – The bridge has been forced to operate in an 802.1W mode. |
| txHoldCount | The number of BPDUs that can be transmitted per Hello Interval. The default is 3. |
| Port | ID of the port in slot#/port# format. |

| This Field... | Displays... |
|---|---|
| Role | The current role of the port:<br>• Root<br>• Designated<br>• Alternate<br>• Backup<br>• Disabled<br>Refer to “Bridges and Bridge Port Roles” on page 8-23 for definitions of the roles. |
| State | The port’s current 802.1W state. A port can have one of the following states:<br>• Forwarding<br>• Discarding<br>• Learning<br>• Disabled<br>Refer to “Bridge Port States” on page 8-27 and “Edge Port and Non-Edge Port States” on page 8-27. |
| Path Cost | The configured path cost on a link connected to this port. |
| Priority | The configured priority of the port. The default is 128 or 0x80. |
| AdminOperEdge | Indicates if the port is an operational Edge port. Edge ports may either be auto-detected or configured (forced) to be Edge ports using the CLI:<br>• T – The port is and Edge port.<br>• F – The port is not an Edge port. This is the default. |
| AdminP2PMac | Indicates if the point-to-point-mac parameter is configured to be a point-to-point link:<br>• T – The link is a point-to-point link<br>• F – The link is not a point-to-point link. This is the default. |
| DesignatedPriority | Shows the following:<br>• Root – Shows the ID of the root bridge for this bridge.<br>• Bridge – Shows the ID of the Designated bridge that is associated with this port. |

| This Field... | Displays... |
|---|---|
| ActiveTimers | Shows what timers are currently active on this port and the number of seconds they have before they expire:<br>• rrWhile – Recent root timer. A non-zero value means that the port has recently been a Root port.<br>• rcvdInfoWhile – Received information timer. Shows the time remaining before the information held by this port expires (ages out). This timer is initialized with the effective age parameter. (See “Max Age” on page 8-54.)<br>• rbWhile – Recent backup timer. A non-zero value means that the port has recently been a Backup port.<br>• helloWhen – Hello period timer. The value shown is the amount of time between hello messages.<br>• tcWhile – Topology change timer. The value shown is the interval when topology change notices can be propagated on this port.<br>• fdWhile – Forward delay timer. (See the explanation for Fwd Dly on page 54.)<br>• mdelayWhile – Migration delay timer. The amount of time that a bridge on the same LAN has to synchronize its migration state with this port before another BPDU type can cause this port to change the BPDU that it transmits. |
| Machine States | The current states of the various state machines on the port:<br>• PIM – State of the Port Information state machine.<br>• PRT – State of the Port Role Transition state machine.<br>• PST – State of the Port State Transition state machine.<br>• TCM – State of the Topology Change state machine.<br>• PPM – State of the Port Protocol Migration.<br>• PTX – State of the Port Transmit state machine.<br>Refer to the section “State Machines” on page 8-27 for details on state machines. |
| Received | Shows the number of BPDU types the port has received:<br>• RST BPDU – BPDU in 802.1W format.<br>• Config BPDU – Legacy configuration BPDU (802.1D format).<br>• TCN BPDU – Legacy topology change BPDU (802.1D format). |

## 802.1W Draft 3

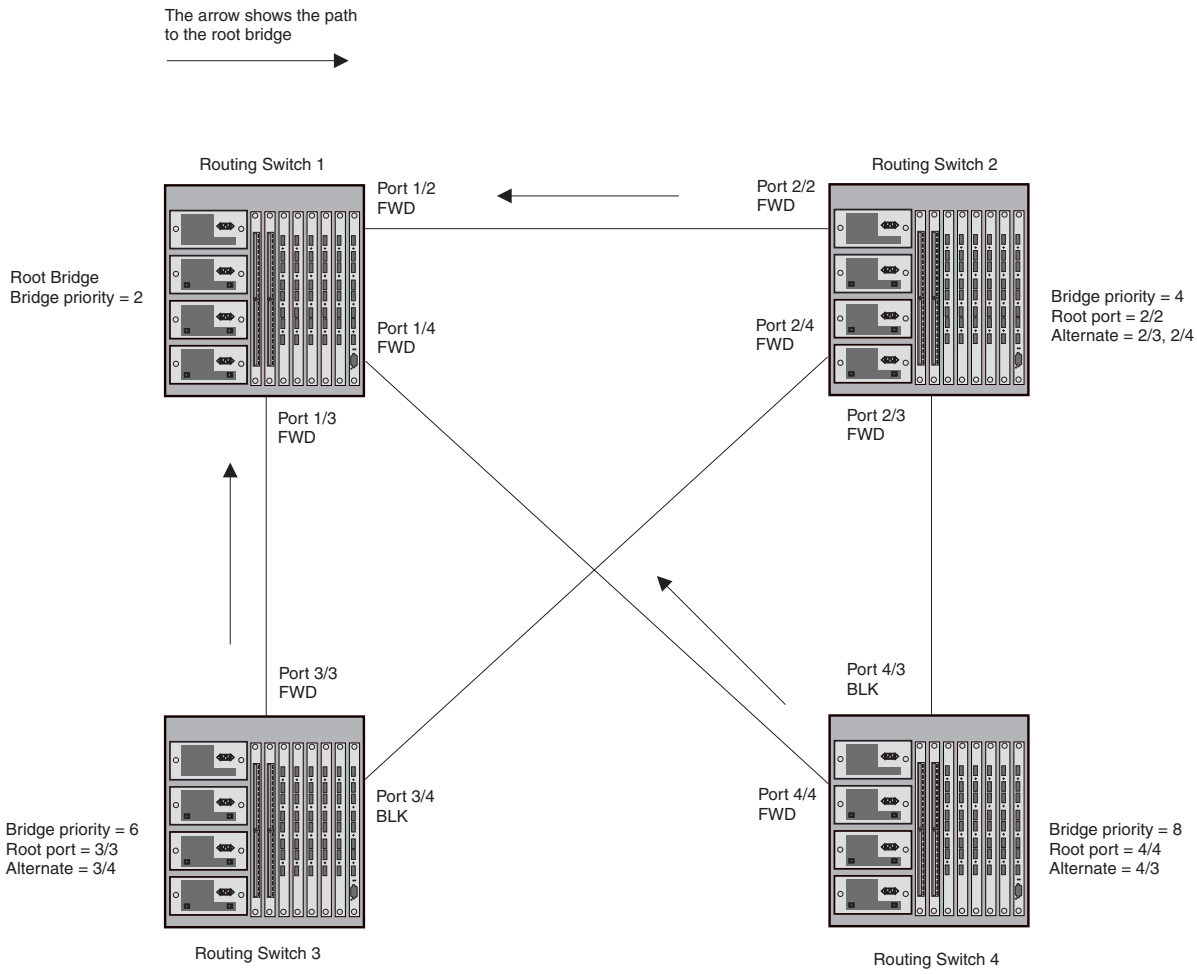
As an alternative to full 802.1W, you can configure 802.1W Draft 3. 8021.W Draft 3 provides a subset of the RSTP capabilities described in the 802.1W STP specification.

8021.W Draft 3 support is disabled by default. When the feature is enabled, if a root port on an HP device that is not the root bridge becomes unavailable, the device can automatically Routing Switch over to an alternate root port, without reconvergence delays. 8021.W Draft 3 does not apply to the root bridge, since all the root bridge’s ports are always in the forwarding state.

Figure 8.24 shows an example of an optimal STP topology. In this topology, all the non-root bridges have at least two paths to the root bridge (Routing Switch 1 in this example). One of the paths is through the root port. The

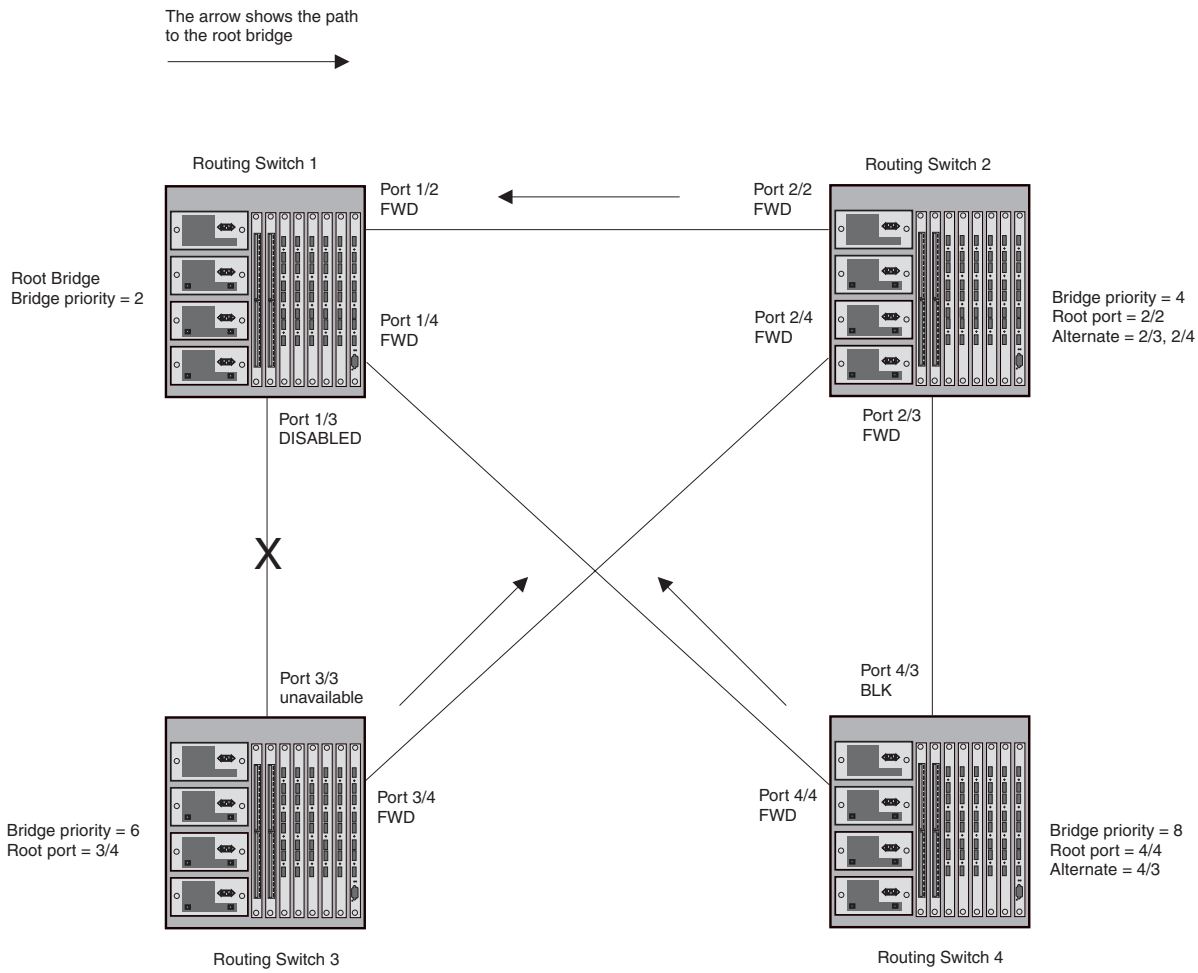
other path is a backup and is through the alternate port. While the root port is in the forwarding state, the alternate port is in the blocking state.

**Figure 8.24 802.1W Draft 3 RSTP ready for failover**




If the root port on a Routing Switch becomes unavailable, 8021.W Draft 3 immediately fails over to the alternate port, as shown in Figure 8.25.

**Figure 8.25 802.1W Draft 3 RSTP failover to alternate root port**




In this example, port 3/3 on Routing Switch 3 has become unavailable. In standard STP (802.1D), if the root port becomes unavailable, the Routing Switch must go through the listening and learning stages on the alternate port to reconverge with the spanning tree. Thus, port 3/4 must go through the listening and learning states before entering the forwarding state and thus reconverging with the spanning tree.

8021.W Draft 3 avoids the reconvergence delay by calculating an alternate root port, and immediately failing over to the alternate port if the root port becomes unavailable. The alternate port is in the blocking state as long as the root port is in the forwarding state, but moves immediately to the active state if the root port becomes unavailable. Thus, using 8021.W Draft 3, Routing Switch 3 immediately fails over to port 3/4, without the delays caused by the listening and learning states.

8021.W Draft 3 selects the port with the next-best cost to the root bridge. For example, on Routing Switch 3, port 3/3 has the best cost to the root bridge and thus is selected by STP as the root port. Port 3/4 has the next-best cost to the root bridge, and thus is selected by 8021.W Draft 3 as the alternate path to the root bridge.

Once a failover occurs, the Routing Switch no longer has an alternate root port. If the port that was an alternate port but became the root port fails, standard STP is used to reconverge with the network. You can minimize the reconvergence delay in this case by setting the forwarding delay on the root bridge to a lower value. For example, if the forwarding delay is set to 15 seconds (the default), change the forwarding delay to a value from 3 – 10 seconds.

During failover, 8021.W Draft 3 flushes the MAC addresses leaned on the unavailable root port, selects the alternate port as the new root port, and places that port in the forwarding state. If traffic is flowing in both directions on the new root port, addresses are flushed (moved) in the rest of the spanning tree automatically.

## Reconvergence Time

Spanning tree reconvergence using 8021.W Draft 3 can occur within one second.

After the spanning tree reconverges following the topology change, traffic also must reconverge on all the bridges attached to the spanning tree. This is true regardless of whether 8021.W Draft 3 or standard STP is used to reconverge the spanning tree.

Traffic reconvergence happens after the spanning tree reconvergence, and is achieved by flushing the Layer 2 information on the bridges.

- Following 8021.W Draft 3 reconvergence of the spanning tree, traffic reconvergence occurs in the time it takes for the bridge to detect the link changes plus the STP maximum age set on the bridge.
- If standard STP reconvergence occurs instead, traffic reconvergence takes two times the forward delay plus the maximum age.

**NOTE:** 8021.W Draft 3 does not apply when a failed root port comes back up. In this case, standard STP is used.

## Configuration Considerations

8021.W Draft 3 is disabled by default. To ensure optimal performance of the feature before you enable it:

- Configure the bridge priorities so that the root bridge is one that supports 8021.W Draft 3. (Use an HP device or third-party device that supports 8021.W Draft 3.)
- Change the forwarding delay on the root bridge to a value lower than the default 15 seconds. HP recommends a value from 3 – 10 seconds. The lower forwarding delay helps reduce reconvergence delays in cases where 8021.W Draft 3 is not applicable, such as when a failed root port comes back up.
- Configure the bridge priorities and root port costs so that each device has an active path to the root bridge if its root port becomes unavailable. For example, port 3/4 is connected to port 2/4 on Routing Switch 2, which has the second most favorable bridge priority in the spanning tree.

**NOTE:** If reconvergence involves changing the state of a root port on a bridge that supports 802.1D STP but not 8021.W Draft 3, then reconvergence still requires the amount of time it takes for the ports on the 802.1D bridge to change state to forwarding (as needed), and receive BPDUs from the root bridge for the new topology.

## Enabling 8021.W Draft 3

8021.W Draft 3 is disabled by default. The procedure for enabling the feature differs depending on whether single STP is enabled on the device.

**NOTE:** STP must be enabled before you can enable 8021.W Draft 3.

### *Enabling 8021.W Draft 3 When Single STP Is Not Enabled*

To enable 8021.W Draft 3 on a device that is not running single STP, use the following CLI method.

*USING THE CLI*

By default, each port-based VLAN on the device has its own spanning tree. To enable 8021.W Draft 3 in a port-based VLAN, enter commands such as the following:

```
HP9300(config)# vlan 10
HP9300(config-vlan-10)# spanning-tree rstp
```

***Syntax:*** [no] spanning-tree rstp

This command enables 8021.W Draft 3. You must enter the command separately in each port-based VLAN in which you want to run 8021.W Draft 3.

**NOTE:** This command does not also enable STP. To enable STP, first enter the **spanning-tree** command without the **rstp** parameter. After you enable STP, enter the **spanning-tree rstp** command to enable 8021.W Draft 3.

To disable 8021.W Draft 3, enter the following command:

```
HP9300(config-vlan-10)# no spanning-tree rstp
```

#### *Enabling 8021.W Draft 3 When Single STP Is Enabled*

To enable 8021.W Draft 3 on a device that is running single STP, enter the following command at the global CONFIG level of the CLI:

```
HP9300(config)# spanning-tree single rstp
```

***Syntax:*** [no] spanning-tree single rstp

This command enables 8021.W Draft 3 on the whole device.

**NOTE:** This command does not also enable single STP. To enable single STP, first enter the **spanning-tree single** command without the **rstp** parameter. After you enable single STP, enter the **spanning-tree single rstp** command to enable 8021.W Draft 3.

To disable 8021.W Draft 3 on a device that is running single STP, enter the following command:

```
HP9300(config)# no spanning-tree single rstp
```

## Single Spanning Tree (SSTP)

By default, each port-based VLAN on an HP device runs a separate spanning tree, which you can enable or disable on an individual VLAN basis.

Alternatively, you can configure an HP device to run a single spanning tree across all ports and VLANs on the device. The Single STP feature (SSTP) is especially useful for connecting an HP device to third-party devices that run a single spanning tree in accordance with the 802.1q specification.

SSTP uses the same parameters, with the same value ranges and defaults, as the default STP support on HP devices. See “STP Parameters and Defaults” on page 8-2.

### SSTP Defaults

SSTP is disabled by default. When you enable the feature, all VLANs on which STP is enabled become members of a single spanning tree. All VLANs on which STP is disabled are excluded from the single spanning tree.

- To add a VLAN to the single spanning tree, enable STP on that VLAN.
- To remove a VLAN from the single spanning tree, disable STP on that VLAN.

When you enable SSTP, all the ports that are in port-based VLANs with STP enabled become members of a single spanning tree domain. Thus, the ports share a single BPDU broadcast domain. The HP device places all the ports in a non-configurable VLAN, 4094, to implement the SSTP domain. However, this VLAN does not affect port membership in the port-based VLANs you have configured. Other broadcast traffic is still contained within the individual port-based VLANs. Therefore, you can use SSTP while still using your existing VLAN configurations without changing your network. In addition, SSTP does not affect 802.1q tagging. Tagged and untagged ports alike can be members of the single spanning tree domain.

**NOTE:** When SSTP is enabled, the BPDUs on tagged ports go out untagged.

If you disable SSTP, all VLANs that were members of the single spanning tree run MSTP instead. In MSTP, each VLAN has its own spanning tree. VLANs that were not members of the single spanning tree were not enabled for STP. Therefore, STP remains disabled on those VLANs.

### Enabling SSTP

To enable SSTP, use one of the following methods.

**NOTE:** If the device has only one port-based VLAN (the default VLAN), then the device is already running a single instance of STP. In this case, you do not need to enable SSTP. You need to enable SSTP only if the device contains more than one port-based VLAN and you want all the ports to be in the same STP broadcast domain.

*USING THE CLI*

To configure the HP device to run a single spanning tree, enter the following command at the global CONFIG level.

```
HP9300(config)# spanning-tree single
```

**NOTE:** If the device has only one port-based VLAN, the CLI command for enabling SSTP is not listed in the CLI. The command is listed only if you have configured a port-based VLAN.

To change a global STP parameter, enter a command such as the following at the global CONFIG level:

```
HP9300(config) spanning-tree single priority 2
```

This command changes the STP priority for all ports to 2.

To change an STP parameter for a specific port, enter commands such as the following:

```
HP9300(config) spanning-tree single ethernet 1/1 priority 10
```

The commands shown above override the global setting for STP priority and set the priority to 10 for port 1/1.

Here is the syntax for the global STP parameters.

***Syntax:*** [no] spanning-tree single [forward-delay <value>]
[hello-time <value>] | [maximum-age <time>] | [priority <value>]

Here is the syntax for the STP port parameters.

***Syntax:*** [no] spanning-tree single [ethernet <portnum> path-cost <value> | priority <value>]

**NOTE:** Both commands listed above are entered at the global CONFIG level.

*USING THE WEB MANAGEMENT INTERFACE*

1. Log on to the device using a valid user name and password for read-write access.
2. Click the Single checkbox next to Spanning Tree to place a checkmark in the box.
3. Make sure Enable, not Disable, is selected next to Spanning Tree.
4. Click Apply to apply the change to the device's running-config.
5. Select the Save link at the bottom of the panel. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

## Displaying SSTP information

To verify that SSTP is in effect, enter the following commands at any level of the CLI:

```
HP9300(config)# show span
```

***Syntax:*** show span [vlan <vlan-id>] | [pvst-mode] | [<num>] |
[detail [vlan <vlan-id> [ ethernet <portnum> ] | <num>]]

The **vlan** <vlan-id> parameter displays STP information for the specified port-based VLAN.

The **pvst-mode** parameter displays STP information for the device's Per VLAN Spanning Tree (PVST+) compatibility configuration. See "PVST/PVST+ Compatibility" on page 8-75.

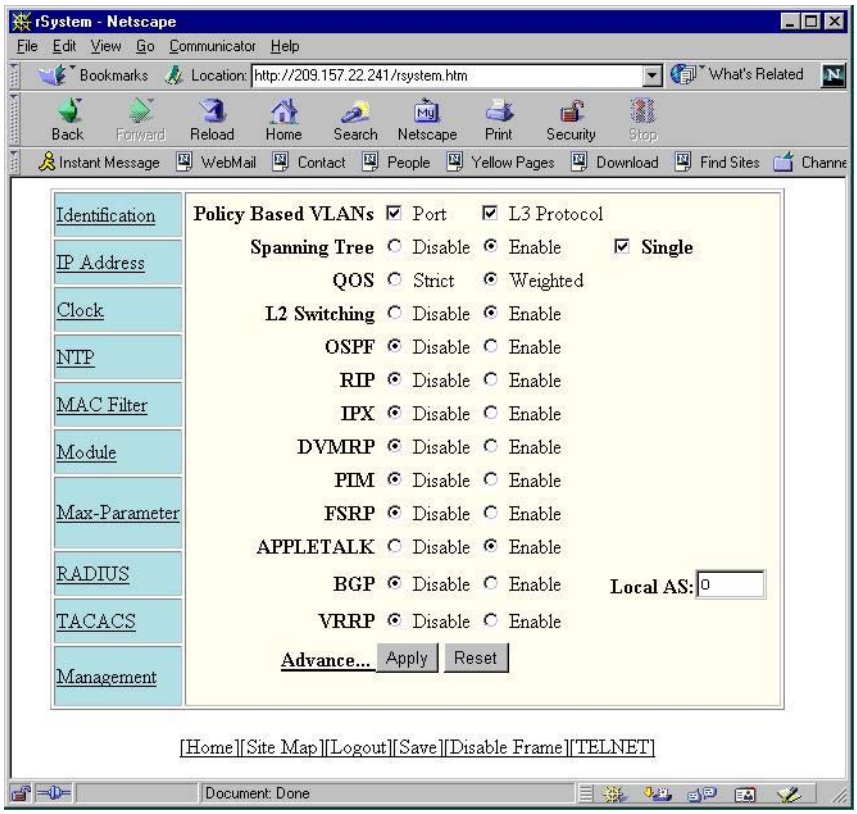
The <num> parameter displays only the entries after the number you specify. For example, on a device with three port-based VLANs, if you enter 1, then information for the second and third VLANs is displayed, but information for the first VLAN is not displayed. Information is displayed according to VLAN number, in ascending order. The entry number is not the same as the VLAN number. For example, if you have port-based VLANs 1, 10, and 2024,

then the command output has three STP entries. To display information for VLANs 10 and 2024 only, enter **show span 1**.

The **detail** parameter and its additional optional parameters display detailed information for individual ports. See “Displaying Detailed STP Information for Each Interface” on page 8-14.

*USING THE WEB MANAGEMENT INTERFACE*

1. Log on to the device using a valid user name and password for read-write access. The System configuration dialog is displayed.
2. Click on the Single checkbox next to Spanning Tree to place a checkmark in the box, as shown in the following example.




3. Click Apply to apply the change to the device’s running-config.
4. Select the Save link at the bottom of the panel. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

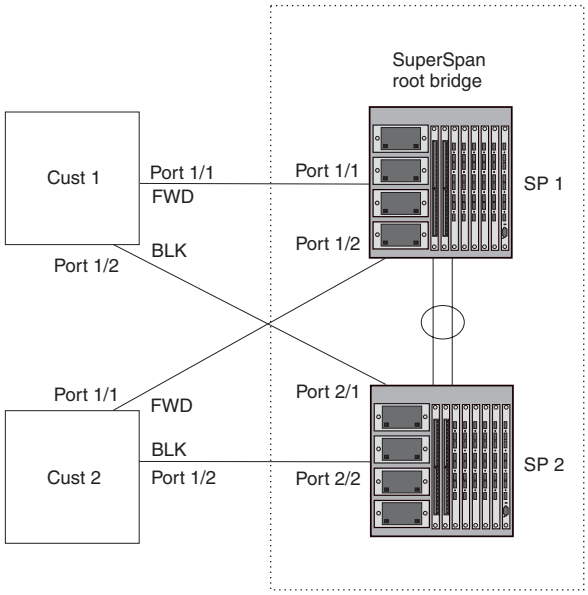
## SuperSpan

SuperSpan is an HP STP enhancement that allows Service Providers (SPs) to use STP in both SP networks and customer networks. The SP devices are HP devices and are configured to tunnel each customers' STP BPDUs through the SP. From the customer's perspective, the SP network is a loop-free non-blocking device or network. The SP network behaves like a hub in the sense that the necessary blocking occurs in the customer network, not in the SP.

The HP interfaces that connect the SP to a customer's network are configured as SuperSpan boundary interfaces. Each SuperSpan boundary interface is configured with a customer ID, to uniquely identify the customer's network within SuperSpan.

Figure 8.26 shows an example SuperSpan implementation. In this example, an SP's network is connected to multiple customers. Each customer network is running its own instance of standard STP. The HP devices in the SP are running SuperSpan.

**Figure 8.26 SuperSpan example**




In this example, the SP network contains two devices that are running SuperSpan. The SP is connected to two customer networks. Each customer network is running its own instance of STP. SuperSpan prevents Layer 2 loops in the traffic flow with each customer while at the same time isolating each customer's traffic and spanning tree from the traffic and spanning trees of other customers. For example, the SP devices provide loop prevention for Customer 1 while ensuring that Customer 1's traffic is never forwarded to Customer 2. In this example, customer 1 has two interfaces to the SP network, ports 1/1 and 1/2 connected to SP 1. The SP network behaves like a non-blocking hub. BPDUs are tunneled through the network. To prevent a Layer 2 loop, customer 1's port 1/2 enters the blocking state.

## Customer ID

SuperSpan uses a SuperSpan customer ID to uniquely identify and forward traffic for each customer. You assign the customer ID as part of the SuperSpan configuration of the HP devices in the SP. In Figure 8.26, the spanning trees of customer 1 and customer 2 do not interfere with one another because the SP network isolates each customer's spanning tree based on the SuperSpan customer IDs in the traffic.

## BPDU Forwarding

When an HP device receives a customer's BPDU on a boundary interface, the device changes the destination MAC address of the BPDU from the bridge group address (01-80-c2-00-00-00) as follows:

- The first byte (locally administered bit) is changed from 01 to 03, to indicate that the BPDU needs to be tunneled.
- The fourth and fifth bytes are changed to the customer STP ID specified on the boundary interface.

For example, if the customer's STP ID is 1, the destination MAC address of the customer's BPDUs is changed to the following: 03-80-c2-00-01-00.

Each HP device that is configured for SuperSpan forwards the BPDU using the changed destination MAC address. At the other end of the tunnel, the HP device connected to the customer's network changes the destination MAC address back to the bridge group address (01-80-c2-00-00-00).

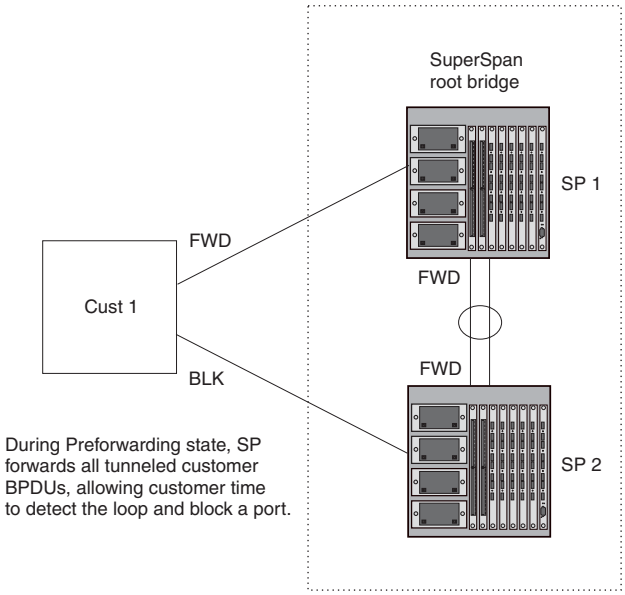
## Preforwarding State

To ensure that the customer's network has time to converge at Layer 2 and prevent loops, the HP devices configured for SuperSpan use a special forwarding state, Preforwarding. The Preforwarding state occurs between the Learning and Forwarding states and by default lasts for five seconds. During the Preforwarding state, the HP device forwards tunneled BPDUs from customers only and does not forward data traffic. This ensures that the customer's network will detect the Layer 2 loop and block a port. The SP network remains unblocked. After the Preforwarding state, the HP ports change to the Forwarding state and forward data traffic as well as BPDUs.

The default length of the Preforwarding state is five seconds. You can change the length of the Preforwarding state to a value from 3 – 30 seconds.

Figure 8.27 shows an example of how the Preforwarding state is used.

**Figure 8.27 SuperSpan Preforwarding state**




In this example, a customer has two links to the SP. Since the SP is running SuperSpan, the SP ports enter the Preforwarding state briefly to allow the customer ports connected to the SP to detect the Layer 2 loop and block one of the ports.

**NOTE:** If you add a new device to a network that is already running SuperSpan, you must enable SuperSpan on the new device, at least on the VLANs that will be tunneling the customer traffic. Otherwise, the new device does not use the Preforwarding state. This can cause the wrong ports to be blocked.

## Mixing Single STP and Multiple Spanning Trees

You can use SuperSpan in any of the following combinations:

- Customer and SP networks both use multiple spanning trees (a separate spanning tree in each VLAN).
- Customer uses multiple spanning trees but SP uses Single STP (all STP-enabled VLANs are in the same spanning tree).
- Customer uses Single STP but SP uses multiple spanning trees.
- Customer and SP networks both use Single STP.

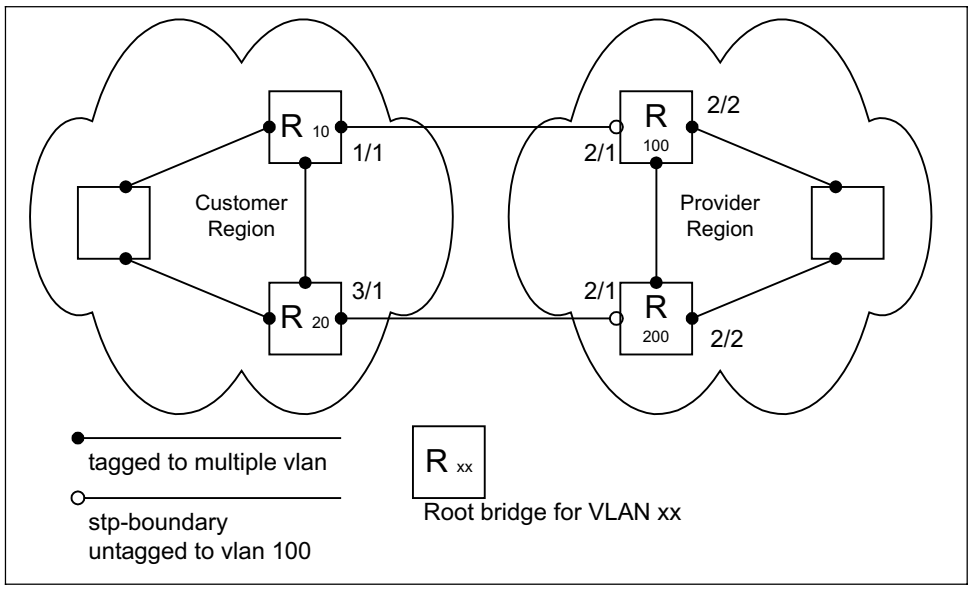
The following sections provide an example of each combination.

**NOTE:** All the combinations listed above are supported when the boundary ports joining the SP SuperSpan domain to the client spanning trees are untagged. For example, all these combinations are valid in super aggregated VLAN configurations. If the boundary ports are tagged, you cannot use Single STP in the client network in combination with multiple spanning trees in the SP SuperSpan domain.

### *Customer and SP Use Multiple Spanning Trees*

Figure 8.28 shows an example of SuperSpan where both the customer network and the SP network use multiple spanning trees (a separate spanning tree in each port-based VLAN).

**Figure 8.28 Customer and SP using multiple spanning trees**




Both the customer and SP regions are running multiple spanning trees (one per port-based VLAN) in the Layer 2 switched network. The customer network contains VLANs 10 and 20 while the SP network contains VLANs 100 and 200. Customer traffic from VLAN 10 and VLAN 20 is aggregated by VLAN 100 in the SP since the boundary ports, 2/1 on R100 and R200, are untagged members of VLAN 100. By adjusting the bridge priority on VLANs 10 and 20, the customer can select a different root bridge for each spanning tree running in the customer network.

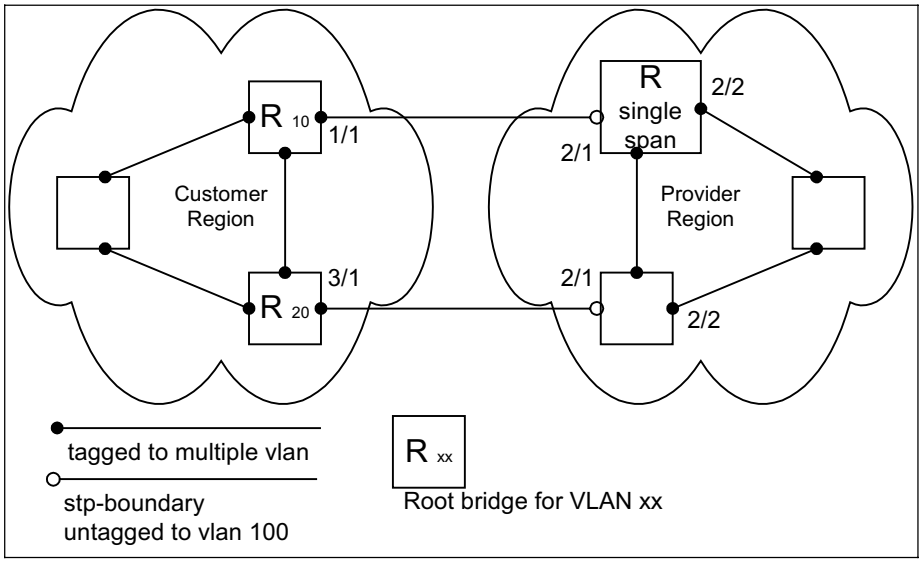
In the above example, STP in VLAN 10 will select R10 as the root bridge and make 1/1 on R10 forwarding while blocking port 3/1 on R20. The opposite occurs for STP in VLAN 20. As a result, both links connecting the customer and SP regions are fully utilized and serve as backup links at the same time, providing loop-free, non-blocking connectivity. In the SP network, multiple STP instances are running (one for VLAN 100 and one for VLAN 200) to ensure loop-free, non-blocking connectivity in each VLAN.

SuperSPAN boundaries are configured at port 2/1 of R100 and R200. Since the customer's traffic will be aggregated into VLAN 100 at the SP, the SP network appears to the customer to be a loop-free non-blocking hub to the customer network when port 2/2 on R200 is blocked by STP in VLAN 100.

### *Customer Uses Multiple Spanning Trees But SP Uses Single STP*

Figure 8.29 shows an example of SuperSpan where the customer network uses multiple spanning trees while the SP network uses Single STP.

**Figure 8.29 Customer using multiple spanning trees and SP using Single STP**



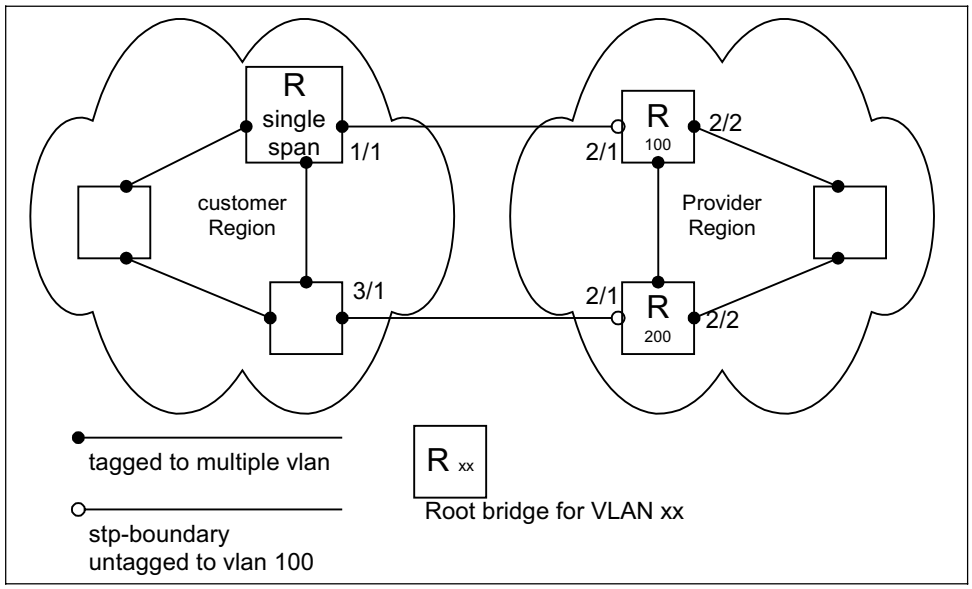

Customer traffic from different VLANs is maintained by different spanning trees, while the SP network is maintained by a single spanning tree. The SP can still use multiple VLANs at the core to separate traffic from different customers. However, all VLANs will have the same network topology because they are all calculated by the single spanning tree. The loop-free, non-blocking network acts like a hub for the customer network, with boundary ports 2/1 on each device being untagged members of VLAN 100.

Traffic from all VLANs in the customer network will be aggregated through VLAN 100 at the SP. This setup leaves the customer network's switching pattern virtually unchanged from the scenario in "Customer and SP Use Multiple Spanning Trees" on page 8-67, since the SP network still is perceived as a virtual hub, and maintenance of the hub's loop-free topology is transparent to the customer network.

### *Customer Uses Single STP But SP Uses Multiple Spanning Trees*

Figure 8.30 shows an example of SuperSpan where the customer network uses Single STP while the SP uses multiple spanning trees.

**Figure 8.30 Customer using Single STP and SP using multiple spanning trees**

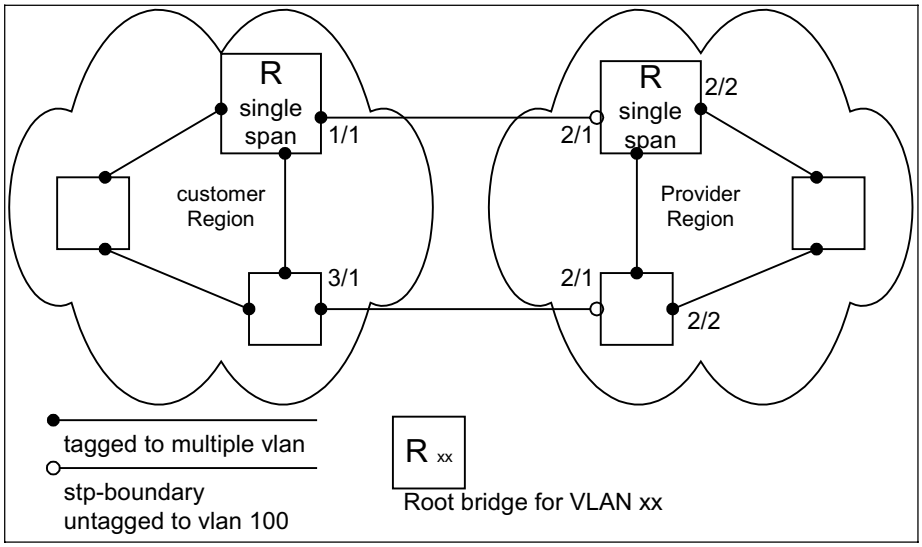



In this setup, the customer network is running a single spanning tree for VLANs 10 and 20. The traffic from VLAN 10 and 20 will be carried, or aggregated by VLAN 100 at the SP's network. The main difference between this scenario and the previous tow scenarios is that all traffic at the customer's network now follows the same path, having the same STP root bridge in all VLANs. Therefore, the customer network will not have the ability to maximize network utilization on all its links. On the other hand, loop-free, non-blocking topology is still separately maintained by the customer network's single spanning tree and the SP's per-VLAN spanning tree on VLAN 100.

### *Customer and SP Use Single STP*

Figure 8.31 shows an example of SuperSpan where the customer network and SP both use Single STP.

**Figure 8.31 Customer and SP using Single STP**




In this setup, both the customer and SP networks are running a single spanning tree at Layer 2. The traffic from VLAN 10 and 20 will be carried, or aggregated by VLAN 100 at the SP network as in the previous scenario. Loop-free, non-blocking topology is still separately maintained by the customer's single spanning tree and the SP's single spanning tree.

## Configuring SuperSpan

To configure an HP device for SuperSpan:

- Configure each interface on the HP device that is connected to customer equipment as a boundary interface. This step enables the interface to convert the destination MAC address in the customer's BPDUs.

  The software requires you to specify a SuperSpan customer ID when configuring the boundary interface. Use an ID from 1 – 65535. The customer ID uniquely identifies the customer. Use the same customer ID for each SP interface with the same customer. When tunneling BPDUs through the HP network, the devices use the customer ID to ensure that BPDUs are forwarded only to the customer's devices, and not to other customers' devices.

- Globally enable SuperSpan. This step enables the Preforwarding state.

### *Configuring a Boundary Interface*

To configure the boundary interfaces on SP 1 in Figure 8.26 on page 8-65, enter the following commands:

```
HP9300(config)# interface 1/1
HP9300(config-if-e1000-1/1)# stp-boundary 1
HP9300(config)# interface 1/2
HP9300(config-if-e1000-1/2)# stp-boundary 2
```

These commands configure two interfaces on the HP device as SuperSpan boundary interfaces. Interface 1/1 is a boundary interface with customer 1. Interface 1/2 is a boundary interface with customer 2. Each boundary interface is associated with a number, which is the SuperSpan ID. The SuperSpan ID identifies the instance of SuperSpan you are associating with the interface. Use the same SuperSpan ID for each boundary interface with the same customer. Use a different SuperSpan ID for each customer. For example, use SuperSpan ID 1 for all the boundary interfaces with customer 1 and use SuperSpan ID 2 for all boundary interfaces with customer 2.

***Syntax:*** [no] stp-boundary <num>

The <num> parameter specifies the SuperSpan ID. You can specify a number from 1 – 65535.

To configure the boundary interfaces on SP 2 in Figure 8.26 on page 8-65, enter the following commands:

```
HP9300(config)# interface 2/1
HP9300(config-if-e1000-2/1)# stp-boundary 1
HP9300(config)# interface 2/2
HP9300(config-if-e1000-2/2)# stp-boundary 2
```

### *Enabling SuperSpan*

After you configure the SuperSpan boundary interfaces, enable SuperSpan. You can enable SuperSpan globally or on an individual VLAN level. If you enable the feature globally, the feature is enabled on all VLANs.

---

**NOTE:** If you enable the feature globally, then create a new VLAN, the new VLAN inherits the global SuperSpan state. For example, if SuperSpan is globally enabled when you create a VLAN, SuperSpan also is enabled in the new VLAN.

---

You also can change the length of the Preforwarding state to a value from 3 – 30 seconds. The default is 5 seconds.

To globally enable SuperSpan, enter the following command:

```
HP9300(config)# super-span-global
```

***Syntax:*** [no] super-span-global [preforward-delay <secs>]

The <secs> parameter specifies the length of the Preforwarding state. You can specify from 3 – 30 seconds. The default is 5 seconds.

SuperSpan is enabled in all VLANs on the device. To disable SuperSpan in an individual VLAN, enter commands such as the following:

```
HP9300(config)# vlan 10
```

```
HP9300(config-vlan-10)# no super-span
```

***Syntax:*** [no] super-span

### Displaying SuperSpan Information

To display the boundary interface configuration and BPDU statistics, enter the following command:

```
HP9300(config)# show super-span
CID 1 Boundary Ports:
     Port   C-BPDU   C-BPDU   T-BPDU   T-BPDU
            Rxed     Txed     Rxed     Txed
     1/1    1        0        0        0
     1/2    0        0        0        0
     Total  1        0        0        0

CID 2 Boundary Ports:
     Port   C-BPDU   C-BPDU   T-BPDU   T-BPDU
            Rxed     Txed     Rxed     Txed
     2/1    0        0        3        0
     2/2    0        0        0        0
     Total  0        0        3        0
```

In this example, the device has two SuperSpan customer IDs.

***Syntax:*** show superspan [cid <num>]

The **cid** <num> parameter specifies a SuperSpan customer ID. If you do not specify a customer ID, information for all the customer IDs configured on the device is shown.

This command shows the following information.

**Table 8.7: CLI Display of SuperSpan Customer ID Information**

| This Field... | Displays... |
|---|---|
| CID | The SuperSpan customer ID number. |
| Port | The boundary port number. |
| C-BPDU Rxed | The number of BPDUs received from the client spanning tree. |
| C-BPDU Txed | The number of BPDUs sent to the client spanning tree. |
| T-BPDU Rxed | The number of BPDUs received from the SuperSpan tunnel. |
| T-BPDU Txed | The number of BPDUs sent to the SuperSpan tunnel. |

To display general STP information, see “Displaying STP Information” on page 8-8.

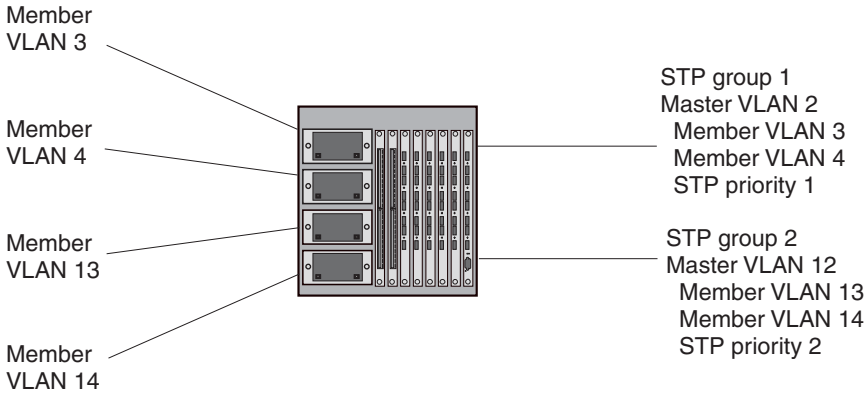
## STP per VLAN Group

STP per VLAN group is an STP enhancement that provides scalability while overcoming the limitations of the following scalability alternatives:

- Standard STP – You can configure only 128 instances of standard STP on an HP device. It is possible to need more instances of STP than this in large configurations. Using STP per VLAN group, you can aggregate STP instances.
- Single STP – Single STP allows all the VLANs to run STP, but each VLAN runs the same instance of STP, resulting in numerous blocked ports that do not pass any Layer 2 traffic. STP per VLAN group uses all available links by load balancing traffic for different instances of STP on different ports. A port that blocks traffic for one spanning tree forwards traffic for another spanning tree.

STP per VLAN group allows you to group VLANs and apply the same STP parameter settings to all the VLANs in the group. Figure 8.32 shows an example of a STP per VLAN group implementation.

**Figure 8.32 STP per VLAN Group Example**




A master VLAN contains one or more member VLANs. Each of the member VLANs in a master VLAN runs the same instance of STP and uses the STP parameters configured for the master VLAN. In this example, the HP device is configured with VLANs 3, 4, 13, and 14. VLANs 3 and 4 are grouped in master VLAN 2, which is in STP group 1. VLANs 13 and 14 are grouped in master VLAN 12, which is in STP group 2. The VLANs in STP group 1 all share the same spanning tree. The VLANs in STP group 2 share a different spanning tree.

All the ports in the VLANs are tagged. The ports must be tagged so that they can be in both a member VLAN and the member's master VLAN. For example, ports 1/1 – 1/4 are in member VLAN 3 and also in master VLAN 2 (since master VLAN 2 contains member VLAN 3).

## STP Load Balancing

Notice that the STP groups each have different STP priorities. In configurations that use the STP groups on multiple devices, you can use the STP priorities to load balance the STP traffic. By setting the STP priorities for the same STP group to different values on each device, you can cause each of the devices to be the root bridge for a different STP group. This type of configuration distributes the traffic evenly across the devices and also ensures that ports that are blocked in one STP group's spanning tree are used by another STP group's spanning tree for forwarding. See "Configuration Example for STP Load Sharing" on page 8-74 for an example using STP load sharing.

## Configuring STP per VLAN Group

To configure STP per VLAN group:

- Configure the member VLANs.
- Optionally, configure master VLANs to contain the member VLANs. This is useful when you have a lot of member VLANs and you do not want to individually configure STP on each one. Each of the member VLANs in a master VLAN uses the STP settings of the master VLAN.
- Configure the STP groups. Each STP group runs a separate instance of STP.

Here are the CLI commands for implementing the STP per VLAN group configuration shown in Figure 8.32. The following commands configure the member VLANs (3, 4, 13, and 14) and the master VLANs (2 and 12). Notice that changes to STP parameters are made in the master VLANs only, not in the member VLANs.

```
HP9300(config)# vlan 2
HP9300(config-vlan-2)# spanning-tree priority 1
HP9300(config-vlan-2)# tagged ethernet 1/1 ethernet to 1/4
HP9300(config-vlan-2)# vlan 3
HP9300(config-vlan-3)# tagged ethernet 1/1 ethernet to 1/4
HP9300(config-vlan-3)# vlan 4
HP9300(config-vlan-4)# tagged ethernet 1/1 ethernet to 1/4
HP9300(config-vlan-4)# vlan 12
```

```
HP9300(config-vlan-12)# spanning-tree priority 2
HP9300(config-vlan-12)# tagged ethernet 1/1 ethernet to 1/4
HP9300(config-vlan-12)# vlan 13
HP9300(config-vlan-13)# tagged ethernet 1/1 ethernet to 1/4
HP9300(config-vlan-13)# vlan 14
HP9300(config-vlan-14)# tagged ethernet 1/1 ethernet to 1/4
HP9300(config-vlan-14)# exit
```

The following commands configure the STP groups.

```
HP9300(config)# stp-group 1
HP9300(config-stp-group-1)# master-vlan 2
HP9300(config-stp-group-1)# member-vlan 3 to 4
HP9300(config-stp-group-1)# exit
HP9300(config)# stp-group 2
HP9300(config-stp-group-2)# master-vlan 12
HP9300(config-stp-group-2)# member-vlan 13 to 14
```

***Syntax:*** [no] stp-group <num>

This command changes the CLI to the STP group configuration level. The following commands are valid at this level. The <num> parameter specifies the STP group ID and can be from 1 – 32.

***Syntax:*** [no] master-vlan <num>

This command adds a master VLAN to the STP group. The master VLAN contains the STP settings for all the VLANs in the STP per VLAN group. The <num> parameter specifies the VLAN ID. An STP group can contain one master VLAN.

**NOTE:** If you delete the master VLAN from an STP group, the software automatically assigns the first member VLAN in the group to be the new master VLAN for the group.

***Syntax:*** [no] member-vlan <num> [to <num>]

This command adds additional VLANs to the STP group. These VLANs also inherit the STP settings of the master VLAN in the group.

***Syntax:*** [no] member-group <num>

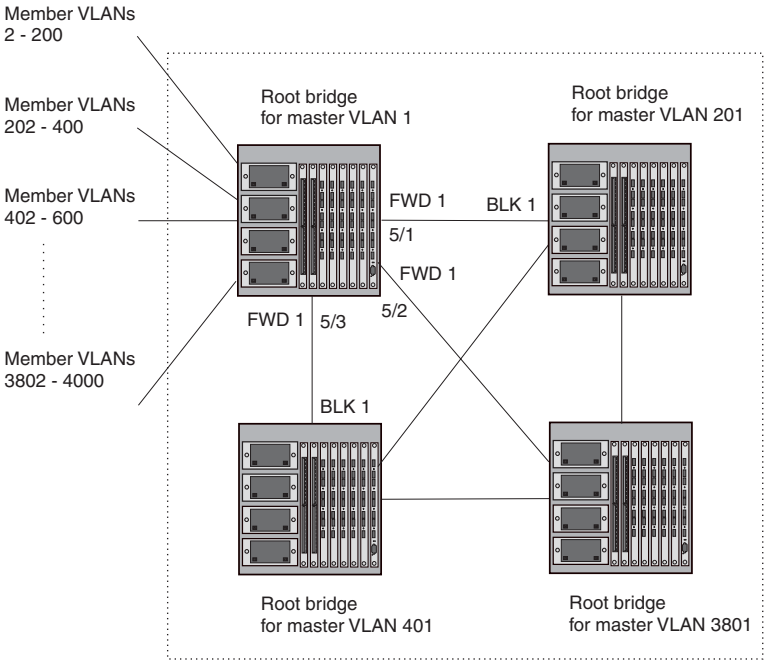
This command adds a member group (a VLAN group) to the STP group. All the VLANs in the member group inherit the STP settings of the master VLAN in the group. The <num> parameter specifies the VLAN group ID.

**NOTE:** This command is optional and is not used in the example above. For an example of this command, see “Configuration Example for STP Load Sharing”.

## Configuration Example for STP Load Sharing

Figure 8.33 shows another example of a STP per VLAN group implementation.

**Figure 8.33 More Complex STP per VLAN Group Example**




In this example, each of the devices in the core is configured with a common set of master VLANs, each of which contains one or more member VLANs. Each of the member VLANs in a master VLAN runs the same instance of STP and uses the STP parameters configured for the master VLAN.

The STP group ID identifies the STP instance. All VLANs within an STP group run the same instance of STP. The master VLAN specifies the bridge STP parameters for the STP group, including the bridge priority. In this example, each of the devices in the core is configured to be the default root bridge for a different master VLAN. This configuration ensures that each link can be used for forwarding some traffic. For example, all the ports on the root bridge for master VLAN 1 are configured to forward BPDUs for master VLAN's spanning tree. Ports on the other devices block or forward VLAN 1's traffic based on STP convergence. All the ports on the root bridge for VLAN 2 forward VLAN 2's traffic, and so on.

All the ports in the VLANs are tagged. The ports must be tagged so that they can be in both a member VLAN and the member's master VLAN. For example, port 1/1 – and ports 5/1, 5/2, and 5/3 are in member VLAN 2 and master VLAN 1 (since master VLAN a contains member VLAN 2).

Here are the commands for configuring the root bridge for master VLAN 1 in figure Figure 8.32 for STP per VLAN group. The first group of commands configures the master VLANs. Notice that the STP priority is set to a different value for each VLAN. In addition, the same VLAN has a different STP priority on each device. This provides load balancing by making each of the devices a root bridge for a different spanning tree.

```
HP9300(config)# vlan 1
HP9300(config-vlan-1)# spanning-tree priority 1
HP9300(config-vlan-1)# tag ethernet 1/1 ethernet 5/1 to 5/3
HP9300(config-vlan-1)# vlan 201
HP9300(config-vlan-201)# spanning-tree priority 2
HP9300(config-vlan-201)# tag ethernet 1/2 ethernet 5/1 to 5/3
HP9300(config-vlan-201)# vlan 401
HP9300(config-vlan-401)# spanning-tree priority 3
HP9300(config-vlan-401)# tag ethernet 1/3 ethernet 5/1 to 5/3
...
HP9300(config-vlan-3601)# vlan 3801
```

```
HP9300(config-vlan-3801)# spanning-tree priority 20
HP9300(config-vlan-3801)# tag ethernet 1/20 ethernet 5/1 to 5/3
HP9300(config-vlan-3801)# exit
```

The next group of commands configures VLAN groups for the member VLANs. Notice that the VLAN groups do not contain the VLAN numbers assigned to the master VLANs. Also notice that no STP parameters are configured for the groups of member VLANs. Each group of member VLANs will inherit its STP settings from its master VLAN.

Set the bridge priority for each master VLAN to the highest priority (1) on one of the devices in the STP per VLAN group configuration. By setting the bridge priority to the highest priority, you make the device the default root bridge for the spanning tree. To ensure STP load balancing, make each of the devices the default root bridge for a different master VLAN.

```
HP9300(config)# vlan-group 1 vlan 2 to 200
HP9300(config-vlan-group-1)# tag ethernet 1/1 ethernet 5/1 to 5/3
HP9300(config-vlan-group-1)# vlan-group 2 vlan 202 to 400
HP9300(config-vlan-group-2)# tag ethernet 1/2 ethernet 5/1 to 5/3
HP9300(config-vlan-group-2)# vlan-group 3 vlan 402 to 600
HP9300(config-vlan-group-2)# tag ethernet 1/3 ethernet 5/1 to 5/3
...
HP9300(config-vlan-group-19)# vlan-group 20 vlan 3082 to 4000
HP9300(config-vlan-group-20)# tag ethernet 1/20 ethernet 5/1 to 5/3
HP9300(config-vlan-group-20)# exit
```

The following group of commands configures the STP groups. Each STP group in this configuration contains one master VLAN, which contains a VLAN group. This example shows that an STP group also can contain additional VLANs (VLANs not configured in a VLAN group).

```
HP9300(config)# stp-group 1
HP9300(config-stp-group-1)# master-vlan 1
HP9300(config-stp-group-1)# member-group 1
HP9300(config-stp-group-1)# member-vlan 4001 4004 to 4010
HP9300(config-stp-group-1)# stp-group 2
HP9300(config-stp-group-2)# master-vlan 201
HP9300(config-stp-group-2)# member-group 2
HP9300(config-stp-group-2)# member-vlan 4002 4003 4011 to 4015
HP9300(config-stp-group-2)# stp-group 3
HP9300(config-stp-group-3)# master-vlan 401
HP9300(config-stp-group-3)# member-group 3
...
HP9300(config-stp-group-19)# stp-group 20
HP9300(config-stp-group-20)# master-vlan 3081
HP9300(config-stp-group-20)# member-group 20
```

# PVST/PVST+ Compatibility

The following sections describe the Per VLAN Spanning Tree (PVST) and PVST+ compatibility features on HP devices. Use the section that matches the software release you are using:

- For release 07.6.04 and later, see “PVST/PVST+ Compatibility – 07.6.04 and Later”.
- For releases 07.1.10 – 07.6.00, see “PVST/PVST+ Compatibility – Earlier Than 07.6.01b” on page 8-81.

## PVST/PVST+ Compatibility – 07.6.04 and Later

Software release 07.6.04 enhances HP support for Cisco's Per VLAN Spanning Tree plus (PVST+), by allowing an HP device to run multiple spanning trees (MSTP) while also interoperating with IEEE 802.1Q devices[1].

1.Cisco user documentation for PVST/PVST+ refers to the IEEE 802.1Q spanning tree as the ***Common Spanning Tree (CST)***.

Previous releases allow an HP device to interoperate with IEEE 802.1Q devices only when the HP device is configured for Single STP (SSTP). In this case, the HP device is operating as an IEEE 802.1Q device but cannot run multiple spanning trees. The current release and previous releases allow the HP device to interoperate with PVST when the HP device is configured for MSTP.

**NOTE:** HP ports automatically detect PVST+ BPDUs and enable support for the BPDUs once detected. You do not need to perform any configuration steps to enable PVST+ support. However, to support the IEEE 802.1Q BPDUs, you might need to enable dual-mode support.

HP's support for Cisco's Per VLAN Spanning Tree plus (PVST+), allows an HP device to run multiple spanning trees (MSTP) while also interoperating with IEEE 802.1Q devices. HP ports automatically detect PVST+ BPDUs and enable support for the BPDUs once detected. The enhancement allows a port that is in PVST+ compatibility mode due to auto-detection to revert to the default MSTP mode when one of the following events occurs:

- The link is disconnected or broken
- The link is administratively disabled
- The link is disabled by interaction with the link-keepalive protocol

This enhancement allows a port that was originally interoperating with PVST+ to revert to MSTP when connected to an HP device.

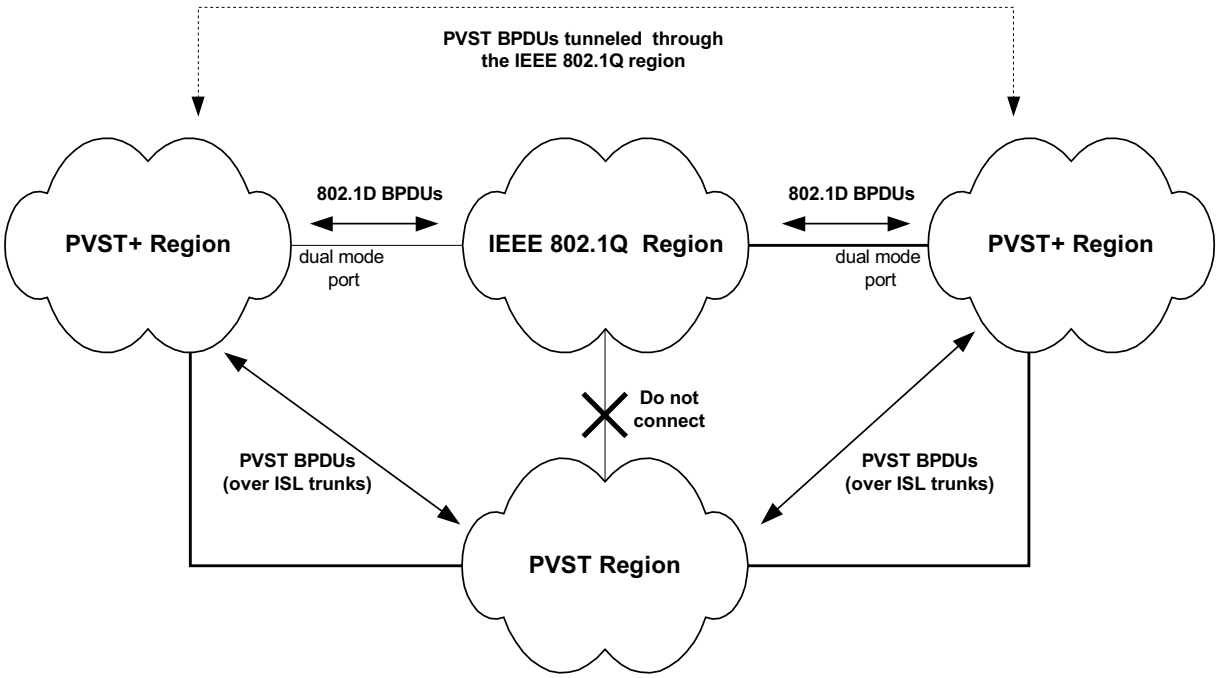
## Overview of PVST and PVST+

***Per VLAN Spanning Tree (PVST)*** is a Cisco proprietary protocol that allows a Cisco device to have multiple spanning trees. The Cisco device can interoperate with spanning trees on other PVST devices but cannot interoperate with IEEE 802.1Q devices. An IEEE 802.1Q device has all its ports running a single spanning tree. ***PVST+*** is an extension of PVST that allows a Cisco device to also interoperate with devices that are running a single spanning tree (IEEE 802.1Q).

The enhanced PVST+ support in release 07.6.04 allows an HP device to interoperate with PVST spanning trees and the IEEE 802.1Q spanning tree at the same time.

IEEE 802.1Q and PVST regions cannot interoperate directly but can interoperate indirectly through PVST+ regions. PVST BPDUs are tunneled through 802.1Q regions, while PVST BPDUs for VLAN 1 (the IEEE 802.1Q VLAN) are processed by PVST+ regions. Figure 8.34 shows the interaction of IEEE 802.1Q, PVST, and PVST+ regions.

**Figure 8.34 Interaction of IEEE 802.1Q, PVST, and PVST+ regions**




## VLAN Tags and Dual Mode

To support the IEEE 802.1Q (Common Spanning Tree) portion of PVST+, a port must be a member of VLAN 1. Cisco devices always use VLAN 1 to support the IEEE 802.1Q portion of PVST+.

For the port to also support the other VLANs (the PVST+ VLANs) in tagged mode, the dual-mode feature must be enabled on the port. The ***dual-mode*** feature enables the port to send and receive both tagged and untagged frames. When the dual-mode feature is enabled, the port is an untagged member of one of its VLANs and is at the same time a tagged member of all its other VLANs.

The untagged frames are supported on the port's ***Port Native VLAN***. By default, the Port Native VLAN is the same as the device's ***Default VLAN***[1], which by default is VLAN 1. Thus, to support IEEE 802.1Q in a typical configuration, the port must be able to send and receive untagged frames for VLAN 1 and tagged frames for the other VLANs.

If you want to use tagged frames on VLAN 1, you can change the default VLAN ID to an ID other than 1. You also can specify the VLAN on which you want the port to send and receive untagged frames (the Port Native VLAN). The Port Native VLAN ID does not need to be the same as the Default VLAN.

**NOTE:** Support for the IEEE 802.1Q spanning tree always uses VLAN 1, regardless of whether the devices are configured to use tagged or untagged frames on the VLAN.

## Configuring PVST+ Support

PVST+ support is automatically enabled when the port receives a PVST BPDU. You can manually enable the support at any time or disable the support if desired.

If you want a tagged port to also support IEEE 802.1Q BPDUs, you need to enable the dual-mode feature on the port. The dual-mode feature is disabled by default and must be enabled manually.

Starting with release 07.6.04, a port that is in PVST+ compatibility mode due to auto-detection reverts to the default MSTP mode when one of the following events occurs:

1.Cisco PVST/PVST+ documentation refers to the Default VLAN as the ***Default Native VLAN***.

- The link is disconnected or broken
- The link is administratively disabled
- The link is disabled by interaction with the link-keepalive protocol

This allows a port that was originally interoperating with PVST+ to revert to MSTP when connected to an HP device.

### *Enabling PVST+ Support Manually*

To immediately enable PVST+ support on a port, enter commands such as the following:

```
HP9300(config)# interface ethernet 1/1
HP9300(config-if-1/1)# pvst-mode
```

***Syntax:*** [no] pvst-mode

**NOTE:** If you disable PVST+ support, the software still automatically enables PVST+ support if the port receives a BPDU with PVST+ format.

### *Enabling Dual-Mode Support*

To enable the dual-mode feature on a port, enter the following command at the interface configuration level for the port:

```
HP9300(config-if-1/1)# dual-mode
```

***Syntax:*** [no] dual-mode [<vlan-id>]

The <vlan-id> specifies the port's Port Native VLAN. This is the VLAN on which the port will support untagged frames. By default, the Port Native VLAN is the same as the default VLAN (which is VLAN 1 by default).

For more information about the dual-mode feature, see "Dual-Mode VLAN Ports" on page 11-54.

## Displaying PVST+ Support Information

To display PVST+ information for ports on an HP device, enter the following command at any level of the CLI:

```
HP9300(config)# show span pvst-mode
PVST+ Enabled on:
Port      Method
1/1       Set by configuration
1/2       Set by configuration
2/10      Set by auto-detect
3/12      Set by configuration
4/24      Set by auto-detect
```

***Syntax:*** show span pvst-mode

**NOTE:** This command is present in earlier releases but the output format has been changed to reflect the feature enhancements.

This command displays the following information.

**Table 35: CLI Display of PVST+ Information**

| This Field... | Displays... |
|---|---|
| Port | The HP port number.<br>**Note**: The command lists information only for the ports on which PVST+ support is enabled. |

**Table 35: CLI Display of PVST+ Information (Continued)**

| This Field... | Displays... |
|---|---|
| Method | The method by which PVST+ support was enabled on the port. The method can be one of the following:<br>• Set by configuration – You enabled the support.<br>• Set by auto-detect – The support was enabled automatically when the port received a PVST+ BPDU. |

## Configuration Examples

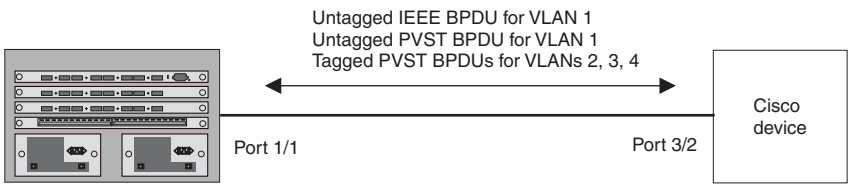
The following examples show configuration examples for two common configurations:

- Untagged IEEE 802.1Q BPDUs on VLAN 1 and tagged PVST+ BPDUs on other VLANs
- Tagged IEEE 802.1Q BPDUs on VLAN 1 and untagged BPDUs on another VLAN

### *Tagged Port Using Default VLAN 1 as its Port Native VLAN*

Figure 8.36 shows an example of a PVST+ configuration that uses VLAN 1 as the untagged default VLAN and VLANs 2, 3, and 4 as tagged VLANs.

**Figure 8.36 Default VLAN 1 for untagged BPDUs**




To implement this configuration, enter the following commands.

**Commands on the HP Device**

```
HP9300(config)# vlan-group 1 vlan 2 to 4
HP9300(config-vlan-group-1)# tagged ethernet 1/1
HP9300(config-vlan-group-1)# exit
HP9300(config)# interface ethernet 1/1
HP9300(config-if-1/1)# dual-mode
HP9300(config-if-1/1)# pvst-mode
```

These commands configure a VLAN group containing VLANs 2, 3, and 4, add port 1/1 as a tagged port to the VLANs, and enable the dual-mode feature and PVST+ support on the port. The dual-mode feature allows the port to send and receive untagged frames for the default VLAN (VLAN 1 in this case) in addition to tagged frames for VLANs 2, 3, and 4. Enabling the PVST+ support ensures that the port is ready to send and receive PVST+ BPDUs. If you do not manually enable PVST+ support, the support is not enabled until the port receives a PVST+ BPDU.

The configuration leaves the default VLAN and the port's Port Native VLAN unchanged. The default VLAN is 1 and the port's Port Native VLAN also is 1. The dual-mode feature supports untagged frames on the default VLAN only. Thus, port 1/1 can send and receive untagged BPDUs for VLAN 1 and can send and receive tagged BPDUs for the other VLANs.

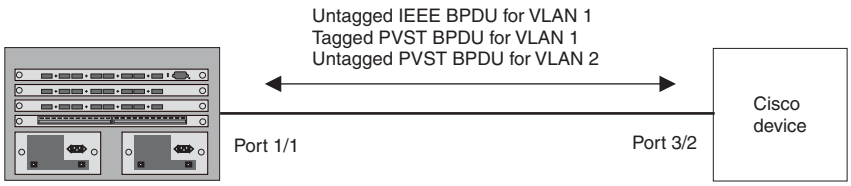
Port 1/1 will process BPDUs as follows:

- Process IEEE 802.1Q BPDUs for VLAN 1.
- Process tagged PVST BPDUs for VLANs 2, 3, and 4.
- Drop untagged PVST BPDUs for VLAN 1.

### *Untagged Port Using VLAN 2 as Port Native VLAN*

Figure 8.37 shows an example in which a port's Port Native VLAN is not VLAN 1. In this case, VLAN 1 uses tagged frames and VLAN 2 uses untagged frames.

**Figure 8.37 Port Native VLAN 2 for untagged BPDUs**




To implement this configuration, enter the following commands.

**Commands on the HP Device**

```
HP9300(config)# default-vlan-id 4000
HP9300(config)# vlan 1
HP9300(config-vlan-1)# tagged ethernet 1/1
HP9300(config-vlan-1)# exit
HP9300(config)# vlan 2
HP9300(config-vlan-2)# tagged ethernet 1/1
HP9300(config-vlan-2)# exit
HP9300(config)# interface ethernet 1/1
HP9300(config-if-1/1)# dual-mode 2
HP9300(config-if-1/1)# pvst-mode
HP9300(config-if-1/1)# exit
```

These commands change the default VLAN ID, configure port 1/1 as a tagged member of VLANs 1 and 2, and enable the dual-mode feature and PVST+ support on port 1/1. Since VLAN 1 is tagged in this configuration, the default VLAN ID must be changed from VLAN 1 to another VLAN ID. Changing the default VLAN ID from 1 allows the port to process tagged frames for VLAN 1. VLAN 2 is specified with the **dual-mode** command, which makes VLAN 2 the port's Port Native VLAN. As a result, the port processes untagged frames and untagged PVST BPDUs on VLAN 2.

---

**NOTE:** Although VLAN 2 becomes the port's untagged VLAN, the CLI still requires that you add the port to the VLAN as a tagged port, since the port is a member of more than one VLAN.

---

Port 1/1 will process BPDUs as follows:

- Process IEEE 802.1Q BPDUs for VLAN 1.
- Process untagged PVST BPDUs for VLAN 2.
- Drop tagged PVST BPDUs for VLAN 1.

Note that when VLAN 1 is not the default VLAN, the ports must have the dual-mode featured enabled in order to process IEEE 802.1Q BPDUs.

For example, the following configuration is incorrect:

```
HP9300(config)# default-vlan-id 1000
HP9300(config)# vlan 1
HP9300(config-vlan-1)# tagged ethernet 1/1 to 1/2
HP9300(config-vlan-1)# exit
HP9300(config)# interface ethernet 1/1
HP9300(config-if-1/1)# pvst-mode
HP9300(config-if-1/1)# exit
HP9300(config)# interface ethernet 1/2
HP9300(config-if-1/2)# pvst-mode
HP9300(config-if-1/2)# exit
```

In the configuration above, all PVST BPDUs associated with VLAN 1 would be discarded. Since IEEE BPDUs associated with VLAN 1 are untagged, they are discarded because the ports in VLAN 1 are tagged. Effectively, the BPDUs are never processed by the Spanning Tree Protocol. STP assumes that there is no better bridge on the network and sets the ports to FORWARDING. This could cause a Layer 2 loop.

The following configuration is correct:

```
HP9300(config)# default-vlan-id 1000
HP9300(config)# vlan 1
HP9300(config-vlan-1)# tagged ethernet 1/1 to 1/2
HP9300(config-vlan-1)# exit
HP9300(config)# interface ethernet 1/1
HP9300(config-if-1/1)# pvst-mode
HP9300(config-if-1/1)# dual-mode
HP9300(config-if-1/1)# exit
HP9300(config)# interface ethernet 1/2
HP9300(config-if-1/2)# pvst-mode
HP9300(config-if-1/2)# dual-mode
HP9300(config-if-1/2)# exit
```

Setting the ports as dual-mode ensures that the untagged IEEE 802.1Q BPDUs reach the VLAN 1 instance.

## PVST/PVST+ Compatibility – Earlier Than 07.6.01b

HP devices that are configured to support a separate spanning tree in each port-based VLAN can interoperate with Cisco devices that are running Per VLAN Spanning Tree (PVST) or PVST+, Cisco proprietary STP implementations that support separate spanning trees in each port-based VLAN.

An HP device configured to run a separate spanning tree in each port-based VLAN automatically enables PVST/PVST+ support on a port if that port receives an STP BPDU with PVST/PVST+ format. You also can enable PVST/PVST+ support statically as well as display PVST/PVST+ information for each port.

The information in this section is for reference. If you are running PVST/PVST+ on the Cisco devices and the default support for separate spanning trees in each VLAN on the HP devices, then no configuration is necessary for the devices to share spanning tree information.

**NOTE:** If you plan to use the PVST/PVST+ support, do not use VLAN 1. PVST+ uses VLAN 1 as a single STP broadcast domain and thus uses a different BPDU format than for other VLANs.

### PVST

Each spanning tree (that is, each instance of STP) has one device called the root bridge. The root bridge is the control point for the spanning tree, and sends STP status and topology change information to the other devices in the spanning tree by sending BPDUs to the other devices. The other devices forward the BPDUs as needed.

The format of an STP BPDU differs depending on whether it is a Cisco PVST BPDU or an HP BPDU. HP and Cisco devices also can support single STP BPDUs, which use another format.

- An HP device configured with a separate spanning tree in each VLAN sends BPDUs in standard IEEE 802.1D format, but includes a proprietary four-byte tag. The tag identifies the VLAN the BPDU is for.
- A Cisco device configured for PVST sends the BPDUs to multicast MAC address 01-00-0C-CC-CC-CD. If the device is configured for PVST+, then the device sends BPDUs for all VLANs except VLAN 1 to 01-00-0C-CC-CC-CD. The device sends BPDUs in VLAN 1 to 01-80-C2-00-00-00, the single STP address (see below and “PVST+”).
- An HP device configured for single STP (IEEE 802.1Q) sends untagged BPDUs to the well-known STP MAC address 01-80-C2-00-00-00.

**NOTE:** Cisco devices can be configured to interoperate with devices that support IEEE 802.1Q single STP, but the devices cannot be configured to run single STP.

HP's PVST support enables HP and Cisco devices that have separate spanning trees in each VLAN to interoperate. The HP PVST support is automatically enabled when a port receives a PVST BPDU and does not require configuration on the HP or Cisco device.

When PVST is enabled on an HP port, that port sends BPDUs in PVST format instead of HP's spanning tree format.

### PVST+

HP devices and Cisco devices support separate spanning trees on an individual port-based VLAN basis. However, until the IEEE standard for multiple spanning trees is finalized, vendors are using different methods to support multiple spanning trees within their own products. PVST+ is an extension to PVST that enables a Cisco device to interoperate with other devices that are running a single spanning tree (IEEE 802.1Q) while still running a separate spanning tree in each VLAN.

PVST+ uses 802.1Q single STP BPDUs on VLAN 1 and PVST BPDUs (which have a proprietary format) for other VLANs. In this case, the Cisco device uses devices running 802.1Q as tunnels for PVST (non-802.1Q) traffic. The 802.1Q single STP BPDUs are addressed to the well-known STP MAC address 01-80-C2-00-00-00. The PVST BPDUs for the other VLANs are addressed to multicast address 01-00-0C-CC-CC-CD.

The PVST+ method can require manual configuration of STP parameters on the 802.1Q devices to ensure that traffic for the PVST VLANs is not blocked. In addition, the opportunities to adjust STP parameters to load balance traffic on a VLAN basis are limited when using PVST+.

#### *Using HP Single STP with Cisco PVST+*

Since HP's single STP feature complies with IEEE 802.1Q (the single STP specification), you also can use an HP device running single STP to interoperate with a Cisco device running PVST+. When you enable single STP on an HP device, the PVST compatibility feature is not enabled, even if a port receives a PVST BPDU.

### Enabling PVST/PVST+ Statically

PVST/PVST+ support is automatically enabled on a port if the port receives a BPDU in PVST/PVST+ format. However, you can statically enable PVST/PVST+ support on a port if desired. In this case, the support is enabled immediately and support for HP tagged BPDUs is disabled at the same time. To enable the PVST/PVST+ support, use the following CLI method.

**NOTE:** When PVST/PVST+ support is enabled on a port, support for HP BPDUs is disabled.

#### *USING THE CLI*

To enable PVST/PVST+ support on a port, enter commands such as the following:

```
HP9300(config)# interface ethernet 1/1
HP9300(config-if-1/1)# pvst-mode
```

***Syntax:*** [no] pvst-mode

**NOTE:** If you disable PVST/PVST+ support, the software still automatically enables PVST/PVST+ support if the port receives an STP BPDU with PVST/PVST+ format.

#### *USING THE WEB MANAGEMENT INTERFACE*

You cannot enable PVST support using the Web management interface.

### Displaying PVST Information

To display PVST information, use the following CLI method.

#### *USING THE CLI*

To display PVST information for ports on an HP device, enter the following command at any level of the CLI:

```
HP9300(config)# show span pvst-mode
```

```
VLAN    Port    PVST    PVST
 ID     Num.    Cfg.    On(by cfg. or detect)
 200    10       0       1
 200    11       1       1
```

This example shows that for VLAN 200, PVST support is statically enabled on port 11. PVST is not statically enabled on Port 10, but because port 10 received an incoming PVST BPDU on its interface, the port converted to using PVST mode.

***Syntax:*** show span pvst-mode

The **show span pvst-mode** command displays the following information.

**Table 8.8: CLI Display of PVST Information**

| This Field... | Displays... |
|---|---|
| VLAN ID | The VLAN to which the PVST/PVST+ information applies. |
| Port Num. | The HP port number. |
| PVST cfg. | Whether PVST support is statically enabled on the port. The value can be one of the following:<br>• 0 – The support has not been statically enabled.<br>• 1 – The support has been statically enabled. |
| PVST on (by cfg. or detect) | Whether PVST/PVST+ support is active on the port. The value can be one of the following:<br>• 0 – PVST/PVST+ support is not enabled.<br>• 1 – PVST/PVST+ support is enabled, either because you statically enabled the support or because the port received an STP BPDU with PVST/PVST+ format. |

*USING THE WEB MANAGEMENT INTERFACE*

You cannot display PVST information using the Web management interface.