Overview of PVST+

The original IEEE 802.1D standard defines a CST that assumes only one spanning tree instance for the entire switched network, regardless of the number of VLANs. A network running CST has these characteristics:

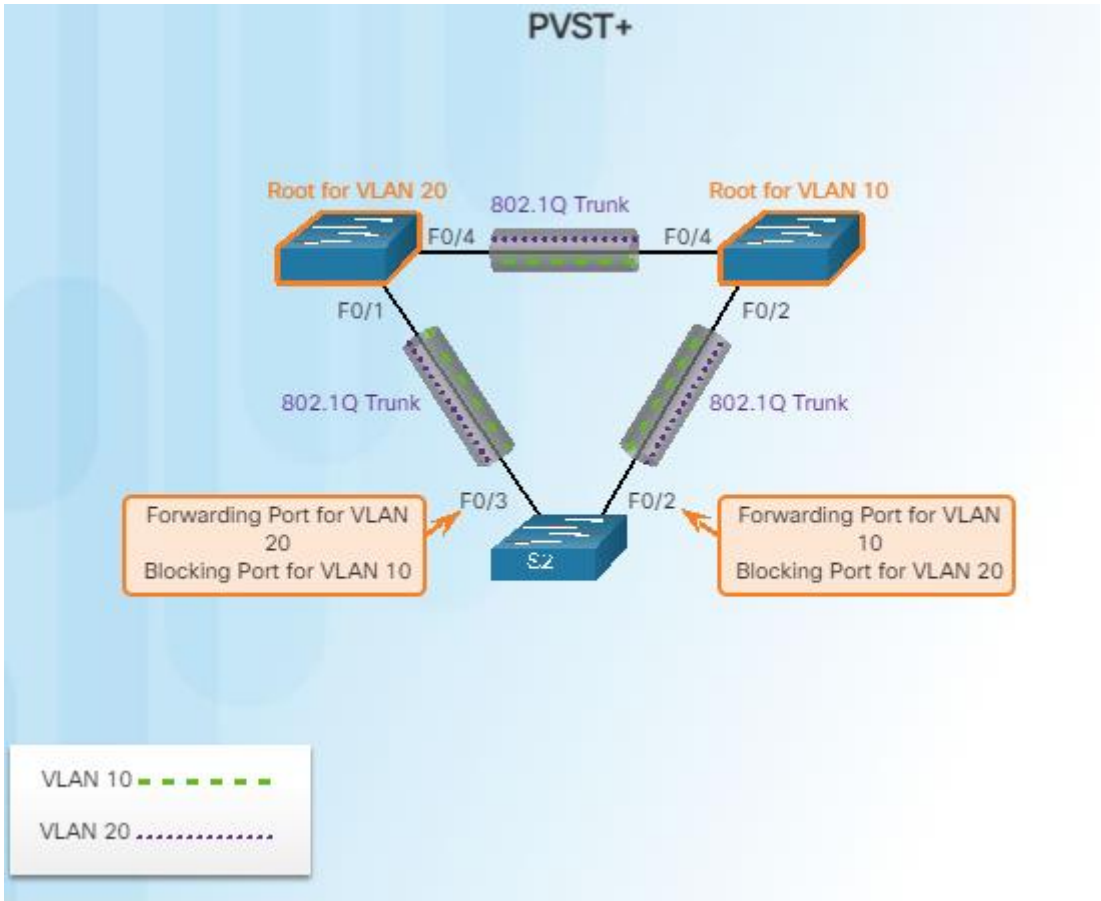
- No load sharing is possible. One uplink must block for all VLANs.
- The CPU is spared. Only one instance of spanning tree must be computed.

Cisco developed PVST+ so that a network can run an independent instance of the Cisco implementation of IEEE 802.1D for each VLAN in the network. With PVST+, it is possible for one trunk port on a switch to block for a VLAN while forwarding for other VLANs. PVST+ can be used to implement Layer 2 load balancing. The switches in a PVST+ environment require greater CPU process and BPDU bandwidth consumption than a traditional CST implementation of STP because each VLAN runs a separate instance of STP.

In a PVST+ environment, spanning tree parameters can be tuned so that half of the VLANs forward on each uplink trunk. In the figure, port F0/3 on S2 is the forwarding port for VLAN 20, and F0/2 on S2 is the forwarding port for VLAN 10. This is accomplished by configuring one switch to be elected the root bridge for half of the VLANs in the network, and a second switch to be elected the root bridge for the other half of the VLANs. In the figure, S3 is the root bridge for VLAN 20 and S1 is the root bridge for VLAN 10. Multiple STP root bridges per VLAN increases redundancy in the network.

Networks running PVST+ have these characteristics:

- Optimum load balancing can result.
- One spanning tree instance for each VLAN maintained can mean a considerable waste of CPU cycles for all the switches in the network (in addition to the bandwidth that is used for each instance to send its own BPDU). This will only be problematic if a large number of VLANs are configured.



Port States and PVST+ Operation

STP facilitates the logical loop-free path throughout the broadcast domain. The spanning tree is determined through the information learned by the exchange of the BPDU frames between the interconnected switches. To facilitate the learning of the logical spanning tree, each switch port transitions through five possible port states and three BPDU timers.

The spanning tree is determined immediately after a switch is finished booting up. If a switch port transitions directly from the blocking state to the forwarding state without information about the full topology during the transition, the port can temporarily create a data loop. For this reason, STP introduces five port states. PVST+ uses the same five port states. The figure describes the port states that ensure no loops are created during the creation of the logical spanning tree:

- **Blocking** - The port is an alternate port and does not participate in frame forwarding. The port receives BPDU frames to determine the location and root ID of the root bridge switch and which port roles each switch port should assume in the final active STP topology.

- **Listening** - Listens for the path to the root. STP has determined that the port can participate in frame forwarding according to the BPDU frames that the switch has received. The switch port receives BPDU frames, transmits its own BPDU frames, and informs adjacent switches that the switch port is preparing to participate in the active topology.

- **Learning** - Learns the MAC addresses. The port prepares to participate in frame forwarding and begins to populate the MAC address table.

- **Forwarding** - The port is considered part of the active topology. It forwards data frames and sends and receives BPDU frames.

- **Disabled** - The Layer 2 port does not participate in spanning tree and does not forward frames. The disabled state is set when the switch port is administratively disabled.

Note that the number of ports in each of the various states (blocking, listening, learning, or forwarding) can be displayed with the **show spanning-tree summary** command.

For each VLAN in a switched network, PVST+ performs four steps to provide a loop-free logical network topology:

Step 1. Elects one root bridge - Only one switch can act as the root bridge (for a given VLAN). The root bridge is the switch with the lowest bridge ID. On the root bridge, all ports are designated ports (no root ports).

Step 2. Selects the root port on each non-root bridge - PVST+ establishes one root port on each non-root bridge for each VLAN. The root port is the lowest-cost path from the non-root bridge to the root bridge, which indicates the direction of the best path to the root bridge. Root ports are normally in the forwarding state.

Step 3. Selects the designated port on each segment - On each link, PVST+ establishes one designated port for each VLAN. The designated port is selected on the switch that has the lowest-cost path to the root bridge. Designated ports are normally in the forwarding state, and forwarding traffic for the segment.

Step 4. The remaining ports in the switched network are alternate ports - Alternate ports normally remain in the blocking state, to logically break the loop topology. When a port is in the blocking state, it does not forward traffic, but it can still process received BPDU messages.

Port States

	Port State				
Operation Allowed	Blocking	Listening	Learning	Forwarding	Disabled
Can receive and process BPDUs	YES	YES	YES	YES	NO
Can forward data frames received on interface	NO	NO	NO	YES	NO
Can forward data frames switched from another interface	NO	NO	NO	YES	NO
Can learn MAC addresses	NO	NO	YES	YES	NO

Extended System ID and PVST+ Operation

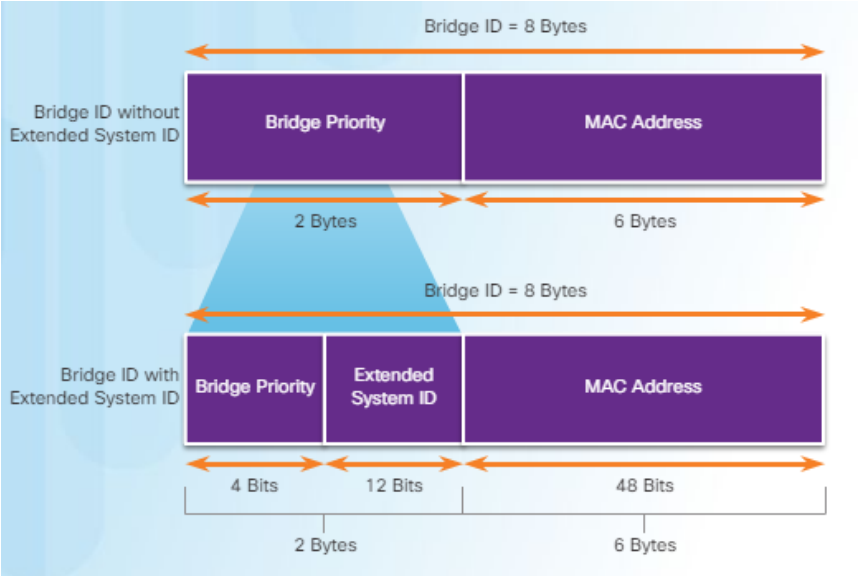
In a PVST+ environment, the extended system ID ensures each switch has a unique BID for each VLAN.

For example, the VLAN 2 default BID would be 32770 (priority 32768, plus the extended system ID of 2). If no priority has been configured, every switch has the same default priority and the election of the root bridge for each VLAN is based on the MAC address. Because the bridge ID is based on the lowest MAC address, the switch chosen to be root bridge might not be the most powerful or the most optimal switch.

There are situations where the administrator may want a specific switch selected as the root bridge. This may be for a variety of reasons, including:

- the switch is more optimally located within the LAN design in regards to the majority of traffic flow patterns for a particular VLAN;
- the switch has higher processing power, or;
- the switch is simply easier to access and manage remotely.

To manipulate the root-bridge election, assign a lower priority to the switch that should be selected as the root bridge for the desired VLAN(s).



Overview of Rapid PVST+

RSTP (IEEE 802.1w) is an evolution of the original 802.1D standard and is incorporated into the IEEE 802.1D-2004 standard. The 802.1w STP terminology remains primarily the same as the original IEEE 802.1D STP terminology. Most parameters have been left unchanged, so users that are familiar with STP can easily configure the new protocol. Rapid PVST+ is the Cisco implementation of RSTP on a per-VLAN basis. An independent instance of RSTP runs for each VLAN.

The figure shows a network running RSTP. S1 is the root bridge with two designated ports in a forwarding state. RSTP supports a new port type. Port F0/3 on S2 is an alternate port in discarding state. Notice that there are no blocking ports. RSTP does not have a blocking port state. RSTP defines port states as discarding, learning, or forwarding.

RSTP speeds the recalculation of the spanning tree when the Layer 2 network topology changes. RSTP can achieve much faster convergence in a properly configured network, sometimes in as little as a few hundred milliseconds. RSTP redefines the type of ports and their state. If a port is configured to be an alternate port or a backup port, it can immediately change to a forwarding state without waiting for the network to converge. The following briefly describes RSTP characteristics:

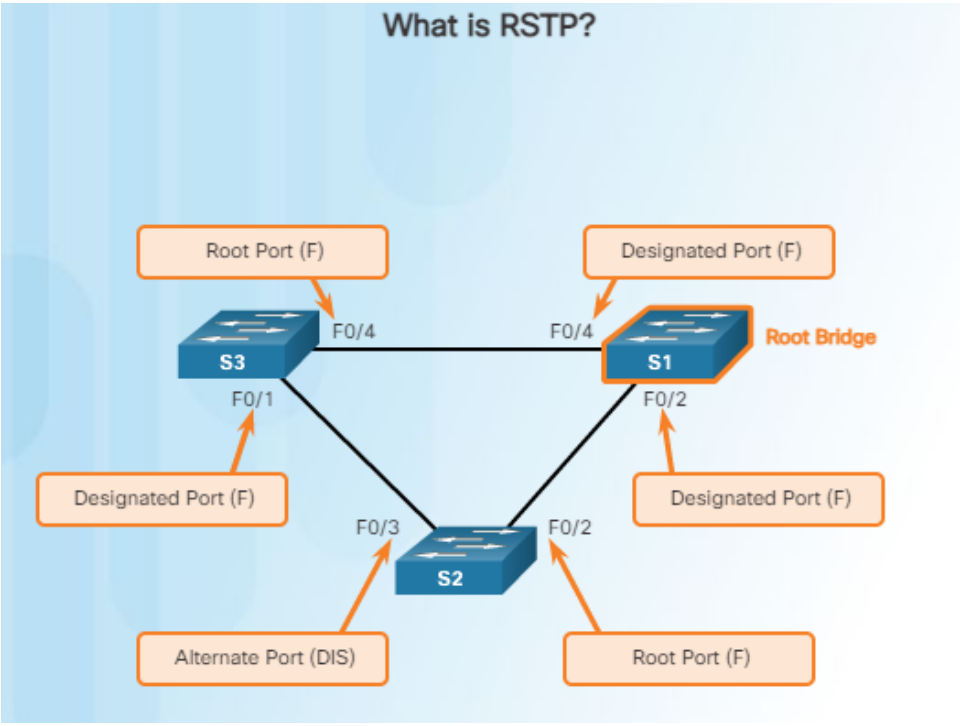
- RSTP is the preferred protocol for preventing Layer 2 loops in a switched network environment. Many of the differences were established by Cisco-proprietary enhancements to the original 802.1D. These enhancements, such as BPDUs carrying and sending information about port roles only to neighboring switches, require no additional configuration and generally perform better than the earlier Cisco-proprietary versions. They are now transparent and integrated into the protocol's operation.

- Cisco-proprietary enhancements to the original 802.1D, such as UplinkFast and BackboneFast, are not compatible with RSTP.

- RSTP (802.1w) supersedes the original 802.1D while retaining backward compatibility. Much of the original 802.1D terminology remains and most parameters are unchanged. In addition, 802.1w is capable of reverting back to legacy 802.1D to interoperate with legacy switches on a per-port basis. For example, the RSTP spanning tree algorithm elects a root bridge in exactly the same way as the original 802.1D.

- RSTP keeps the same BPDU format as the original IEEE 802.1D, except that the version field is set to 2 to indicate RSTP and the flags field uses all 8 bits.

- RSTP is able to actively confirm that a port can safely transition to the forwarding state without having to rely on a timer configuration.



RSTP BPDUs

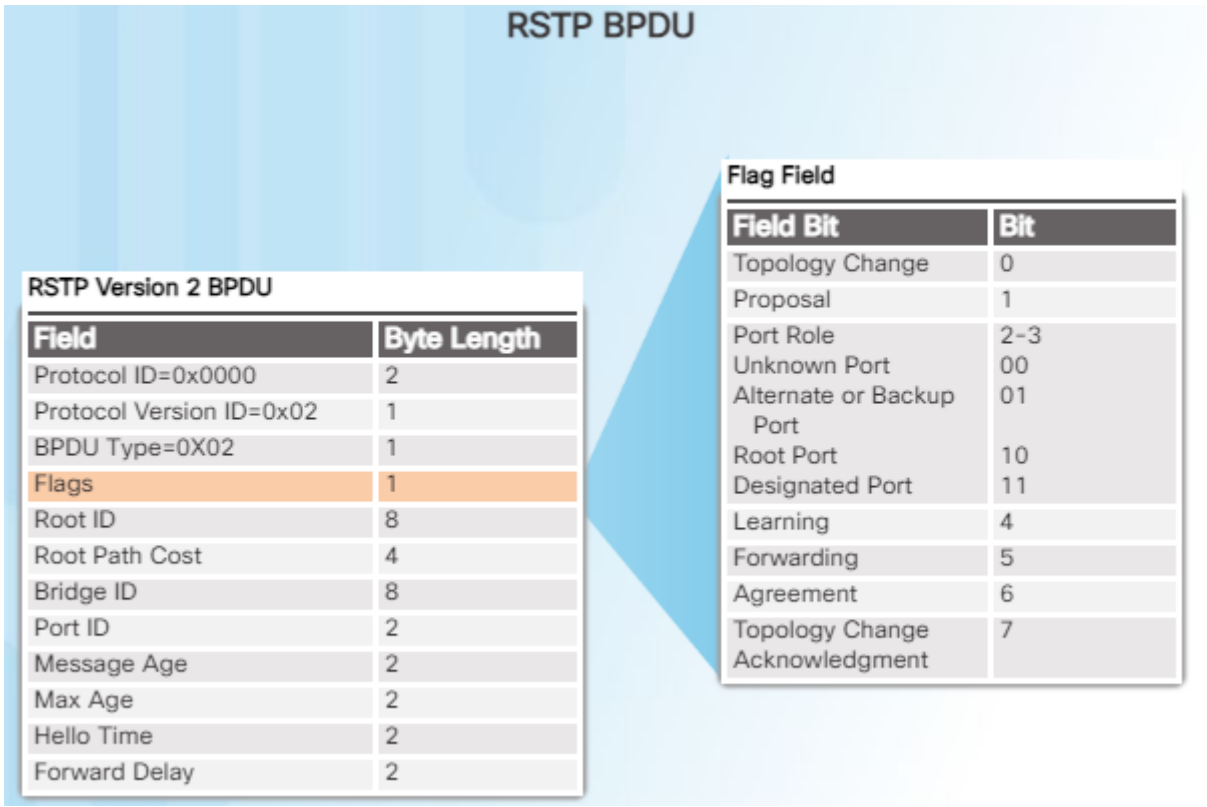
RSTP uses type 2, version 2 BPDUs. The original 802.1D STP uses type 0, version 0 BPDUs. However, a switch running RSTP can communicate directly with a switch running the original 802.1D STP. RSTP sends BPDUs and populates the flag byte in a slightly different manner than in the original 802.1D:

- Protocol information can be immediately aged on a port if Hello packets are not received for three consecutive Hello times (six seconds, by default) or if the max age timer expires.
- BPDUs are used as a keepalive mechanism. Therefore, three consecutively missed BPDUs indicate lost connectivity between a bridge and its neighboring root or designated bridge. The fast aging of the information allows failures to be detected quickly.

Note: Like STP, an RSTP switch sends a BPDU with its current information every Hello time period (two seconds, by default), even if the RSTP switch does not receive BPDUs from the root bridge.

As shown in the figure, RSTP uses the flag byte of version 2 BPDU:

- Bits 0 and 7 are used for topology change and acknowledgment. They are in the original 802.1D.
- Bits 1 and 6 are used for the Proposal Agreement process (used for rapid convergence).
- Bits 2 to 5 encode the role and state of the port.
- Bits 4 and 5 are used to encode the port role using a 2-bit code.



Edge Ports

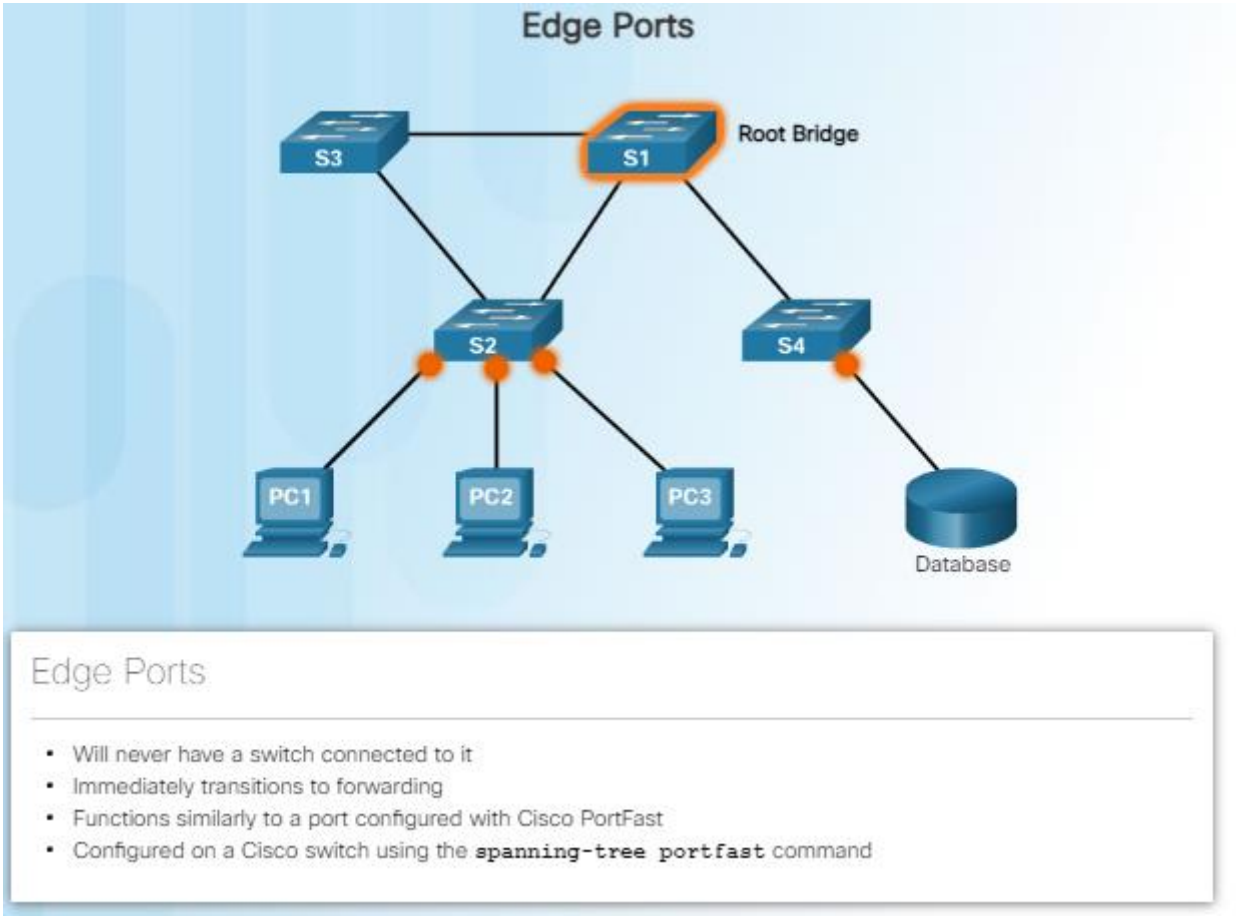
An RSTP edge port is a switch port that is never intended to be connected to another switch. It immediately transitions to the forwarding state when enabled.

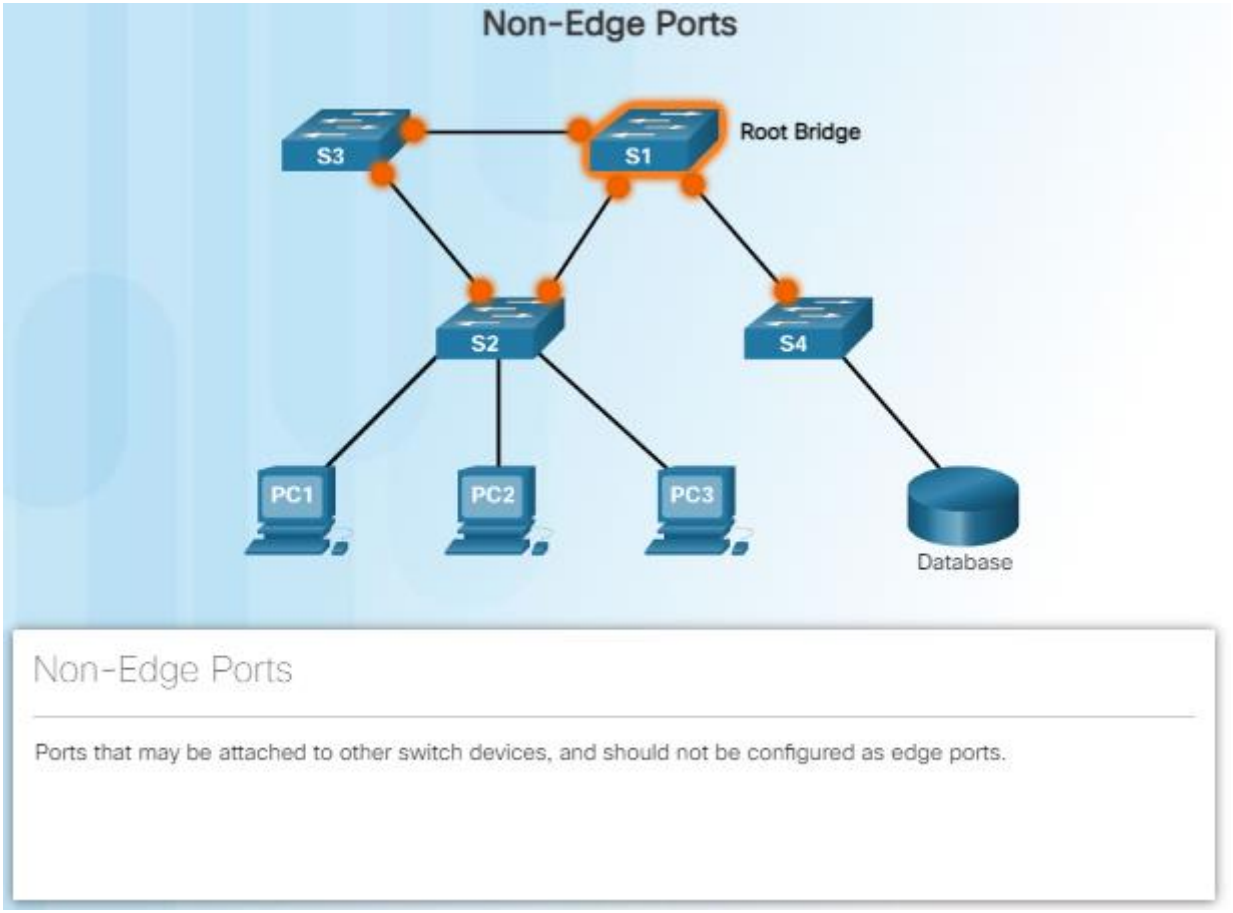
The RSTP edge port concept corresponds to the PVST+ PortFast feature. An edge port is directly connected to an end station and assumes that no switch device is connected to it. RSTP edge ports should immediately transition to the forwarding state, thereby skipping the time-consuming original 802.1D listening and learning port states.

The Cisco RSTP implementation (Rapid PVST+) maintains the PortFast keyword, using the spanning-tree portfast command for edge port configuration. This makes the transition from STP to RSTP seamless.

Figure 1 shows examples of ports that can be configured as edge ports. Figure 2 shows examples of ports that are non-edge ports.

Note: Configuring an edge port to be attached to another switch is not recommended. This can have negative implications for RSTP because a temporary loop may result, possibly delaying the convergence of RSTP.





Link Types

The link type provides a categorization for each port participating in RSTP by using the duplex mode on the port. Depending on what is attached to each port, two different link types can be identified:

- **Point-to-Point** - A port operating in full-duplex mode typically connects a switch to a switch and is a candidate for a rapid transition to a forwarding state.
- **Shared** - A port operating in half-duplex mode connects a switch to a hub that attaches multiple devices.

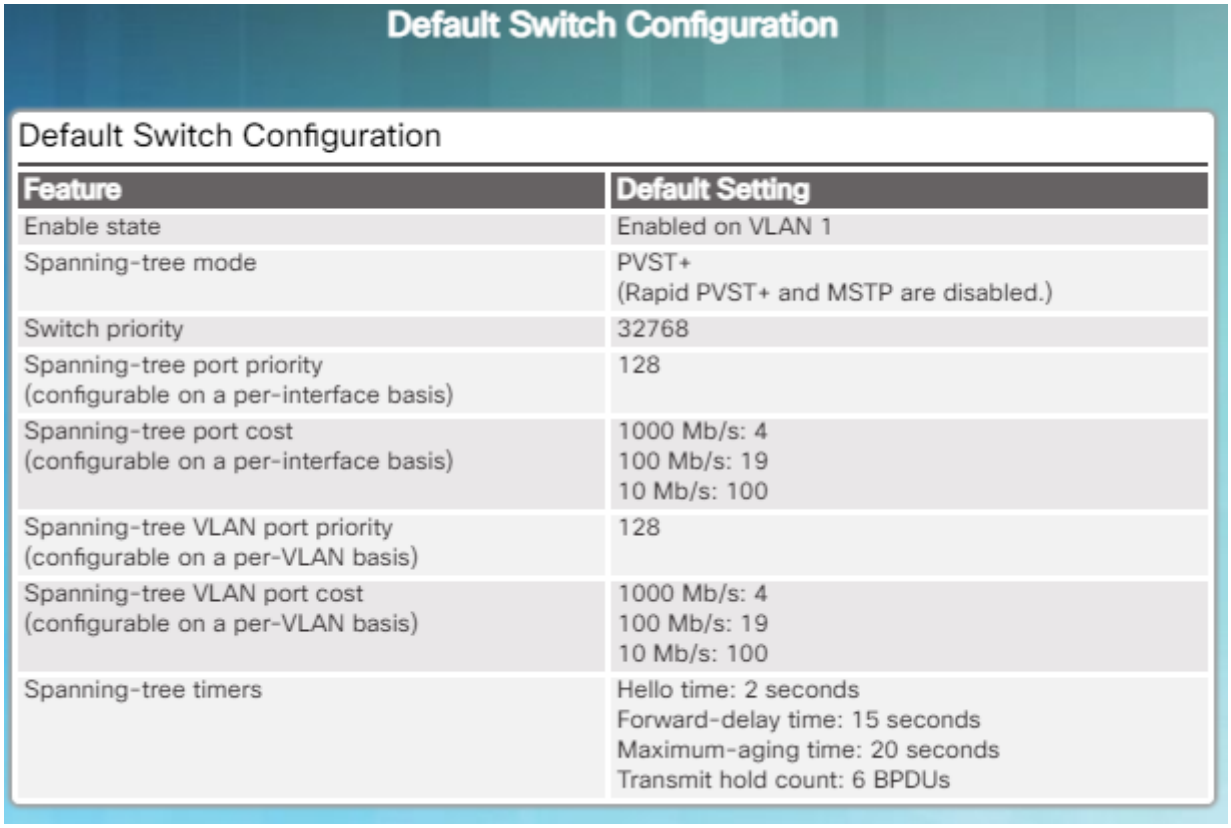
In the figure, click each link to learn about the link types.

The link type can determine whether the port can immediately transition to a forwarding state, assuming certain conditions are met. These conditions are different for edge ports and non-edge ports. Non-edge ports are categorized into two link types: point-to-point and shared. The link type is automatically determined, but can be overridden with an explicit port configuration using the **spanning-tree link-type** { **point-to-point** | **shared** } command. Characteristics of port roles, with regard to link types, include the following:

- Edge port connections and point-to-point connections are candidates for rapid transition to a forwarding state. However, before the link-type parameter is considered, RSTP must determine the port role.
- Root ports do not use the link-type parameter. Root ports are able to make a rapid transition to the forwarding state as soon as the port is in sync (receives a BPDU from the root bridge).
- Alternate and backup ports do not use the link-type parameter in most cases.
- Designated ports make the most use of the link-type parameter. A rapid transition to the forwarding state for the designated port occurs only if the link-type parameter is set to **point-to-point**.

Catalyst 2960 Default Configuration

The table shows the default spanning tree configuration for a Cisco Catalyst 2960 series switch. Notice that the default spanning tree mode is PVST+.



Default Switch Configuration

Feature	Default Setting
Enable state	Enabled on VLAN 1
Spanning-tree mode	PVST+ (Rapid PVST+ and MSTP are disabled.)
Switch priority	32768
Spanning-tree port priority (configurable on a per-interface basis)	128
Spanning-tree port cost (configurable on a per-interface basis)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Spanning-tree timers	Hello time: 2 seconds Forward-delay time: 15 seconds Maximum-aging time: 20 seconds Transmit hold count: 6 BPDUs

Configuring and Verifying the Bridge ID

When an administrator wants a specific switch to become a root bridge, the bridge priority value must be adjusted to ensure it is lower than the bridge priority values of all the other switches on the network. There are two different methods to configure the bridge priority value on a Cisco Catalyst switch.

Method 1

To ensure that the switch has the lowest bridge priority value, use the **spanning-tree vlan** *vlan-id* **root primary** command in global configuration mode. The priority for the switch is set to the predefined value of 24,576 or to the highest multiple of 4,096, less than the lowest bridge priority detected on the network.

If an alternate root bridge is desired, use the **spanning-tree vlan** *vlan-id* **root secondary** global configuration mode command. This command sets the priority for the switch to the predefined value of 28,672. This ensures that the alternate switch becomes the root bridge if the primary root bridge fails. This assumes that the rest of the switches in the network have the default 32,768 priority value defined.

In Figure 1, S1 has been assigned as the primary root bridge using the **spanning-tree vlan 1 root primary** command, and S2 has been configured as the secondary root bridge using the **spanning-tree vlan 1 root secondary** command.

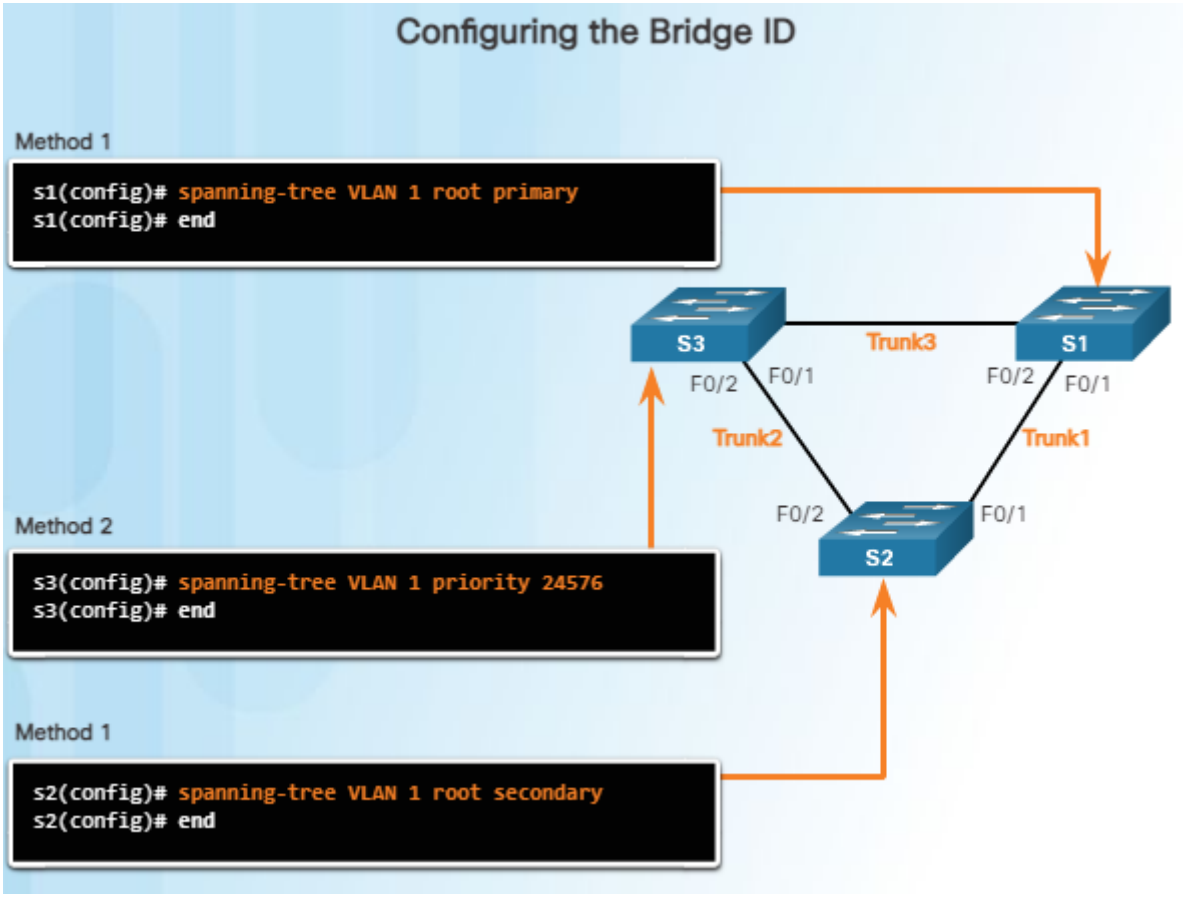
Method 2

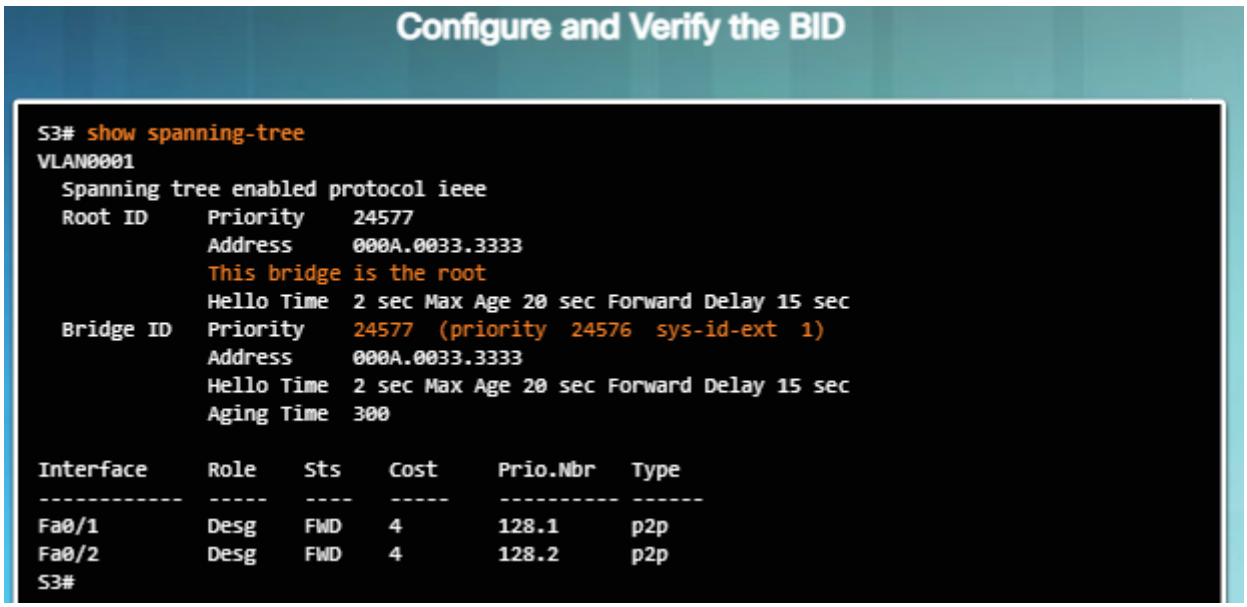
Another method for configuring the bridge priority value is using the **spanning-tree vlan** *vlan-id* **priority** *value* global configuration mode command. This command gives more granular control over the bridge priority value. The priority value is configured in increments of 4,096 between 0 and 61,440.

In the example, S3 has been assigned a bridge priority value of 24,576 using the **spanning-tree vlan 1 priority 24576** command.

To verify the bridge priority of a switch, use the **show spanning-tree** command. In Figure 2, the priority of the switch has been set to 24,576. Also notice that the switch is designated as the root bridge for the spanning tree instance.

Use the Syntax Checker in Figure 3 to configure switches S1, S2, and S3. Using Method 2 described above, configure S3 manually, setting the priority to 24,576 for VLAN 1. Using Method 1, configure S2 as the secondary root VLAN 1 and configure S1 as the primary root for VLAN 1. Verify the configuration with the **show spanning-tree** command on S1.





PortFast and BPDU Guard

PortFast is a Cisco feature for PVST+ environments. When a switch port is configured with PortFast that port transitions from blocking to forwarding state immediately, bypassing the usual 802.1D STP transition states (the listening and learning states). You can use PortFast on access ports to allow these devices to connect to the network immediately, rather than waiting for IEEE 802.1D STP to converge on each VLAN. Access ports are ports which are connected to a single workstation or to a server.

In a valid PortFast configuration, BPDUs should never be received, because that would indicate that another bridge or switch is connected to the port, potentially causing a spanning tree loop. Cisco switches support a feature called BPDU guard. When it is enabled, BPDU guard puts the port in an errdisabled (error-disabled) state on receipt of a BPDU. This will effectively shut down the port. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back into service.

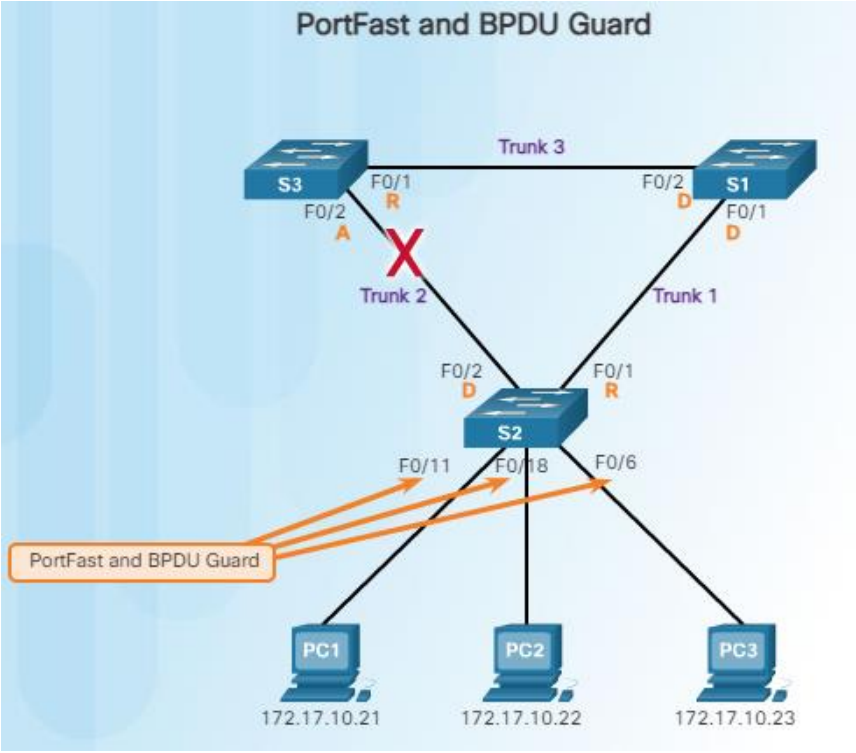
Cisco PortFast technology is useful for DHCP. Without PortFast, a PC can send a DHCP request before the port is in forwarding state, denying the host from getting a usable IP address and other information. Because PortFast immediately changes the state to forwarding, the PC always gets a usable IP address (if the DHCP server has been configured correctly and communication with the DHCP server has occurred).

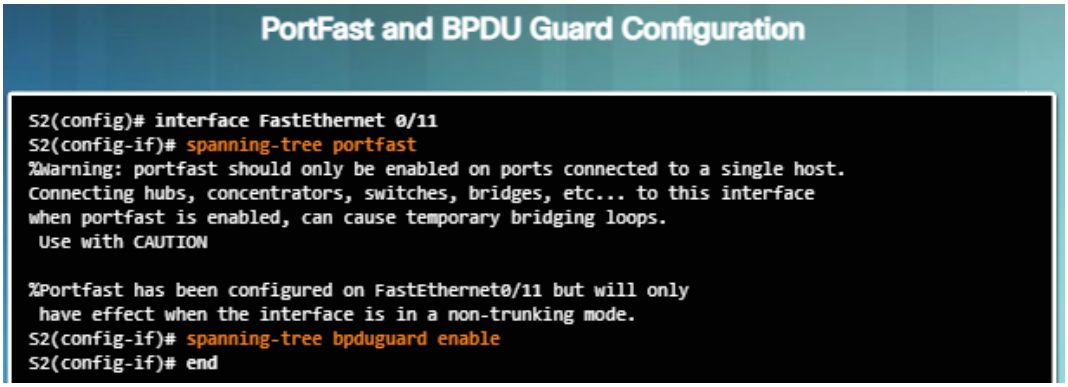
Note: Because the purpose of PortFast is to minimize the time that access ports must wait for spanning tree to converge, it should only be used on access ports. If you enable PortFast on a port connecting to another switch, you risk creating a spanning tree loop.

To configure PortFast on a switch port, enter the **spanning-tree portfast** interface configuration mode command on each interface that PortFast is to be enabled, as shown in Figure 2. The **spanning-tree portfast default** global configuration mode command enables PortFast on all nontrunking interfaces.

To configure BPDU guard on a Layer 2 access port, use the **spanning-tree bpduguard enable** interface configuration mode command. The **spanning-tree portfast bpduguard default** global configuration command enables BPDU guard on all PortFast-enabled ports.

To verify that PortFast and BPDU guard has been enabled for a switch port, use the **show running-config** command, as shown in Figure 3. PortFast and BPDU guard are disabled, by default, on all interfaces.





PVST+ Load Balancing

The topology in Figure 1 shows three switches with 802.1Q trunks connecting them. There are two VLANs, 10 and 20, that are being trunked across these links. The goal is to configure S3 as the root bridge for VLAN 20 and S1 as the root bridge for VLAN 10. Port F0/3 on S2 is the forwarding port for VLAN 20 and the blocking port for VLAN 10. Port F0/2 on S2 is the forwarding port for VLAN 10 and the blocking port for VLAN 20.

In addition to establishing a root bridge, it is also possible to establish a secondary root bridge. A secondary root bridge is a switch that may become the root bridge for a VLAN if the primary root bridge fails. Assuming the other bridges in the VLAN retain their default STP priority, this switch becomes the root bridge if the primary root bridge fails.

The steps to configure PVST+ on this example topology are:

Step 1. Select the switches you want for the primary and secondary root bridges for each VLAN. For example, in Figure 1, S3 is the primary bridge for VLAN 20 and S1 is the secondary bridge for VLAN 20.

Step 2. Configure the switch to be a primary bridge for the VLAN by using the **spanning-tree vlan** *number* **root primary** command, as shown in Figure 2.

Step 3. Configure the switch to be a secondary bridge for the VLAN by using the **spanning-tree vlan** *number* **root secondary** command.

Another way to specify the root bridge is to set the spanning tree priority on each switch to the lowest value so that the switch is selected as the primary bridge for its associated VLAN.

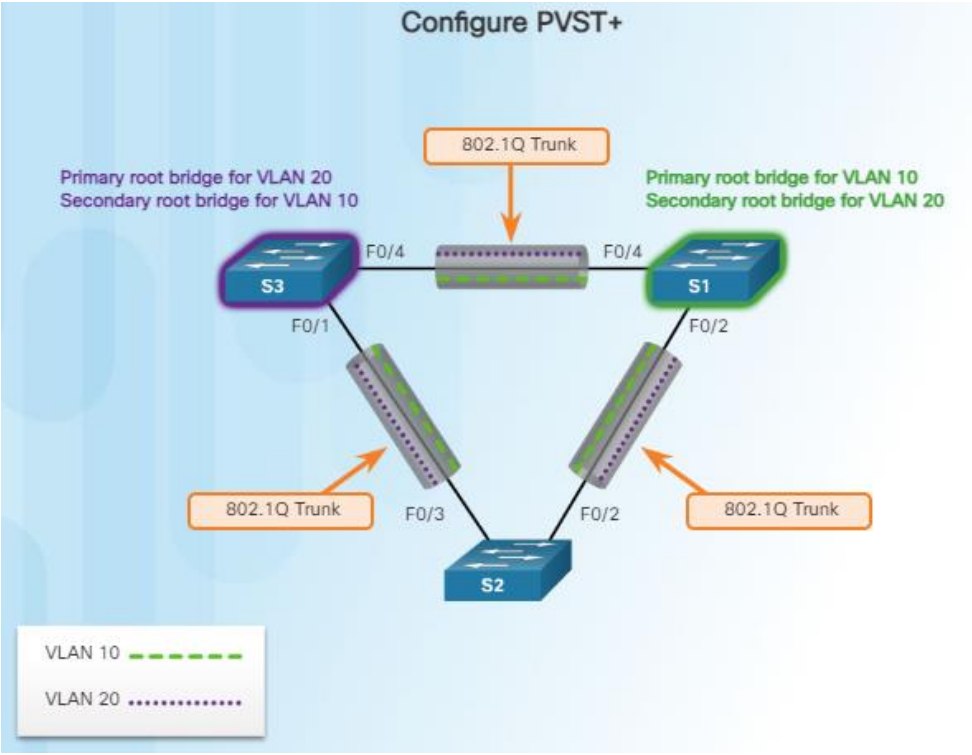
Notice that in Figure 2, S3 is configured as the primary root bridge for VLAN 20, S1 is configured as the primary root bridge for VLAN 10. S2 retained its default STP priority.

The figure also shows that S3 is configured as the secondary root bridge for VLAN 10, and S1 is configured as the secondary root bridge for VLAN 20. This configuration enables spanning tree load balancing, with VLAN 10 traffic heading toward root bridge S1 and VLAN 20 traffic heading toward root bridge S3.

Another way to specify the root bridge is to set the spanning tree priority on each switch to the lowest value so that the switch is selected as the primary bridge for its associated VLAN, as shown in Figure 3. The switch priority can be set for any spanning tree instance. This setting affects the likelihood that a switch is selected as the root bridge. A lower value increases the probability that the switch is selected. The range is 0 to 61,440 in increments of 4,096; all other values are rejected. For example, a valid priority value is 4,096 x 2 = 8,192.

As shown in Figure 4, the **show spanning-tree active** command displays spanning tree configuration details for the active interfaces only. The output shown is for S1 configured with PVST+. There are a number of Cisco IOS command parameters associated with the **show spanning-tree** command.

In Figure 5, the output shows that the priority for VLAN 10 is 4,096, the lowest of the three respective VLAN priorities.



Configure PVST+

```
S3(config)# spanning-tree vlan 20 root primary
```

This command forces S3 to be the primary root for VLAN 20.

```
S3(config)# spanning-tree vlan 10 root secondary
```

This command forces S3 to be the secondary root for VLAN 10.

```
S1(config)# spanning-tree vlan 10 root primary
```

This command forces S1 to be the primary root for VLAN 10.

```
S1(config)# spanning-tree vlan 20 root secondary
```

This command forces S1 to be the secondary root for VLAN 20.

Configure PVST+

```
S3(config)# spanning-tree vlan 20 priority 4096
```

This command sets a low priority for S3, making it likely that S3 will be the primary root for VLAN 20.

```
S1(config)# spanning-tree vlan 10 priority 4096
```

This command sets a low priority for S1, making it likely that S1 will be the primary root for VLAN 10.

Configure PVST+

```
S1# show spanning-tree active

 < output omitted >

VLAN0010
   Spanning tree enabled protocol ieee
   Root ID     Priority    4106
               Address     0019.aa9e.b000
               This bridge is the root
               Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
   Bridge ID   Priority    4106  (priority  4096  sys-id-ext  10)
               Address     0019.aa9e.b000
               Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
               Aging Time  300

Interface      Role    Sts    Cost     Prio.Nbr      Type
-----------    -----   ----   -----    ----------    ------
Fa0/2          Desg    FWD    19        128.2         p2p
Fa0/4          Desg    FWD    19        128.4         p2p

< output omitted >
```

Configure PVST+

```
S1# show running-config
Building configuration...

Current configuration : 1595 bytes
!
version 12.2

< output omitted >

!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
!
< output omitted >
```

Rapid PVST+ Spanning Tree Mode

Rapid PVST+ is the Cisco implementation of RSTP. It supports RSTP on a per-VLAN basis. The topology in Figure 1 has two VLANs: 10 and 20.

Note: The default spanning tree configuration on a Catalyst 2960 Series switch is PVST+. A Catalyst 2960 switch supports PVST+, Rapid PVST+, and MST, but only one version can be active for all VLANs at any time.

Rapid PVST+ commands control the configuration of VLAN spanning tree instances. A spanning tree instance is created when an interface is assigned to a VLAN and is removed when the last interface is moved to another VLAN. As well, you can configure STP switch and port parameters before a spanning tree instance is created. These parameters are applied when a spanning tree instance is created.

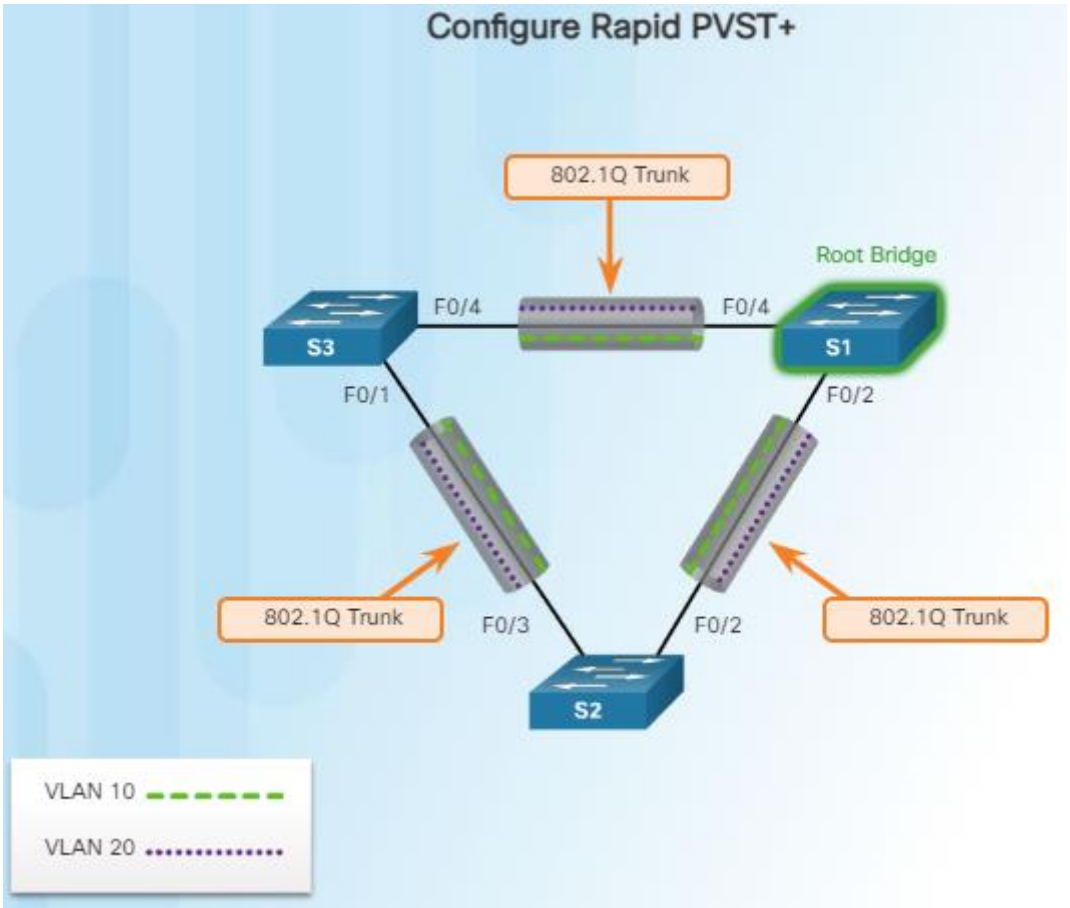
Figure 2 displays the Cisco IOS command syntax needed to configure Rapid PVST+ on a Cisco switch.
The **spanning-tree mode rapid-pvst** global configuration mode command is the one required command for the Rapid PVST+ configuration. When specifying an interface to configure, valid interfaces include physical ports, VLANs, and port channels. The VLAN ID range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. The port-channel range is 1 to 6.

Figure 3 shows Rapid PVST+ commands configured on S1.

In Figure 4, the **show spanning-tree vlan 10** command shows the spanning tree configuration for VLAN 10 on switch S1. Notice that the BID priority is set to 4,096. In the output, the statement “Spanning tree enabled protocol rstp” indicates that S1 is running Rapid PVST+. Because S1 is the root bridge for VLAN 10, all of its interfaces are designated ports.

In Figure 5, the **show running-config** command is used to verify the Rapid PVST+ configuration on S1.

Note: Generally, it is unnecessary to configure the point-to-point *link-type* parameter for Rapid PVST+, because it is unusual to have a shared *link-type*. In most cases, the only difference between configuring PVST+ and Rapid PVST+ is the **spanning-tree mode rapid-pvst** command.



Configure Rapid PVST+

Cisco IOS Command Syntax	
Enter global configuration mode.	`configure terminal`
Configure Rapid PVST+ spanning-tree mode.	`spanning-tree mode rapid-pvst`
Enter interface configuration mode and specify an interface to configure. Valid interfaces include physical ports, VLANs, and port channels.	`interface` *`interface-id`*
Specify that the link type for this port is point-to-point.	`spanning-tree link-type point-to-point`
Return to privileged EXEC mode.	`end`
Clear all detected STP.	`clear spanning-tree detected-protocols`

Configure Rapid PVST+

```
S1# configure terminal
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/2
S1(config-if)# spanning-tree link-type point-to-point
S1(config-if)# end
S1# clear spanning-tree detected-protocols
```

Configure Rapid PVST+

```
S1# show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    4106
             Address     0019.aa9e.b000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4106   (priority 4096 sys-id-ext 10)
             Address     0019.aa9e.b000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/2            Desg LRN 19        128.2    P2p
Fa0/4            Desg LRN 19        128.4    P2p


S1#
< output omitted >
```

Configure Rapid PVST+

```
S1# show run

< output omitted >

spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
!


S1#
< output omitted >
```