



Configuring STP and Prestandard IEEE 802.1s MST

This chapter describes how to configure the Spanning Tree Protocol (STP) and prestandard IEEE 802.1s Multiple Spanning Tree (MST) protocol on Cisco 7600 series routers.



Note

- The IEEE 802.1s MST protocol has transitioned from a prestandard state to a released state. [Chapter 19, “Configuring Standard-Compliant IEEE MST,”](#) describes the standard-compliant MST implementation supported in Release 12.2(18)SXF and later releases. This chapter describes the prestandard MST implementation supported in releases earlier than Release 12.2(18)SXF.
- For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco 7600 Series Router Cisco IOS Command Reference* at this URL:
http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

This chapter consists of these sections:

- [Understanding How STP Works, page 20-1](#)
- [Understanding How IEEE 802.1w RSTP Works, page 20-13](#)
- [Understanding How Prestandard IEEE 802.1s MST Works, page 20-14](#)
- [Default STP Configuration, page 20-21](#)
- [STP and MST Configuration Guidelines and Restrictions, page 20-21](#)
- [Configuring STP, page 20-22](#)
- [Configuring Prestandard IEEE 802.1s MST, page 20-33](#)



Note

For information on configuring the PortFast, UplinkFast, and BackboneFast STP enhancements, see [Chapter 21, “Configuring Optional STP Features.”](#)

Understanding How STP Works

These sections describe how STP works:

- [STP Overview, page 20-2](#)
- [Understanding the Bridge ID, page 20-2](#)
- [Understanding Bridge Protocol Data Units, page 20-4](#)

- [Election of the Root Bridge, page 20-4](#)
- [STP Protocol Timers, page 20-5](#)
- [Creating the Spanning Tree Topology, page 20-5](#)
- [STP Port States, page 20-6](#)
- [STP and IEEE 802.1Q Trunks, page 20-12](#)

STP Overview

STP is a Layer 2 link-management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. STP operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

Cisco 7600 series routers use STP (the IEEE 802.1D bridge protocol) on all VLANs. By default, a single instance of STP runs on each configured VLAN (provided you do not manually disable STP). You can enable and disable STP on a per-VLAN basis.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The STP algorithm calculates the best loop-free path throughout a switched Layer 2 network. Layer 2 LAN ports send and receive STP frames at regular intervals. Network devices do not forward these frames, but use the frames to construct a loop-free path.

Multiple active paths between end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages and network devices might learn end station MAC addresses on multiple Layer 2 LAN ports. These conditions result in an unstable network.

STP defines a tree with a root bridge and a loop-free path from the root to all network devices in the Layer 2 network. STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the STP algorithm recalculates the spanning tree topology and activates the standby path.

When two Layer 2 LAN ports on a network device are part of a loop, the STP port priority and port path cost setting determine which port is put in the forwarding state and which port is put in the blocking state. The STP port priority value represents the location of a port in the network topology and how efficiently that location allows the port to pass traffic. The STP port path cost value represents media speed.

Understanding the Bridge ID

Each VLAN on each network device has a unique 64-bit bridge ID consisting of a bridge priority value, an extended system ID, and an STP MAC address allocation.

This section contains these topics:

- [Bridge Priority Value, page 20-3](#)
- [Extended System ID, page 20-3](#)
- [STP MAC Address Allocation, page 20-3](#)

Bridge Priority Value

The bridge priority is a 4-bit value when the extended system ID is enabled (see [Table 20-2 on page 20-3](#) and the “[Configuring the Bridge Priority of a VLAN](#)” section on page 20-30).

Extended System ID

A 12-bit extended system ID field is part of the bridge ID (see [Table 20-2 on page 20-3](#)). Chassis that support only 64 MAC addresses always use the 12-bit extended system ID. On chassis that support 1024 MAC addresses, you can enable use of the extended system ID. STP uses the VLAN ID as the extended system ID. See the “[Enabling the Extended System ID](#)” section on page 20-24.

Table 20-1 Bridge Priority Value with the Extended System ID Disabled

Bridge Priority Value															
Bit 16	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Table 20-2 Bridge Priority Value and Extended System ID with the Extended System ID Enabled

Bridge Priority Value				Extended System ID (Set Equal to the VLAN ID)											
Bit 16	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

STP MAC Address Allocation

Cisco 7600 series router chassis have either 64 or 1024 MAC addresses available to support software features such as STP. To view the MAC address range on your chassis, enter the **show catalyst6000 chassis-mac-address** command.

For chassis with 64 MAC addresses, STP uses the extended system ID plus a MAC address to make the bridge ID unique for each VLAN.

When the extended system ID is not enabled, STP uses one MAC address per VLAN to make the bridge ID unique for each VLAN.

If you have a network device in your network with the extended system ID enabled, you should also enable the extended system ID on all other Layer 2 connected network devices to avoid undesirable root bridge election and spanning tree topology issues.

When the extended system ID is enabled, the root bridge priority becomes a multiple of 4096 plus the VLAN ID. With the extended system ID enabled, a router bridge ID (used by the spanning tree algorithm to determine the identity of the root bridge, the lowest being preferred) can only be specified as a multiple of 4096. Only the following values are possible: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

If another bridge in the same spanning tree domain does not have the extended system ID enabled, it could win root bridge ownership because of the finer granularity in the selection of its bridge ID.

Understanding Bridge Protocol Data Units

Bridge protocol data units (BPDUs) are transmitted in one direction from the root bridge. Each network device sends configuration BPDUs to communicate and compute the spanning tree topology. Each configuration BPDU contains the following minimal information:

- The unique bridge ID of the network device that the transmitting network device believes to be the root bridge
- The STP path cost to the root
- The bridge ID of the transmitting bridge
- Message age
- The identifier of the transmitting port
- Values for the hello, forward delay, and max-age protocol timers

When a network device transmits a BPDU frame, all network devices connected to the LAN on which the frame is transmitted receive the BPDU. When a network device receives a BPDU, it does not forward the frame but instead uses the information in the frame to calculate a BPDU, and, if the topology changes, initiate a BPDU transmission.

A BPDU exchange results in the following:

- One network device is elected as the root bridge.
- The shortest distance to the root bridge is calculated for each network device based on the path cost.
- A designated bridge for each LAN segment is selected. This is the network device closest to the root bridge through which frames are forwarded to the root.
- A root port is selected. This is the port providing the best path from the bridge to the root bridge.
- Ports included in the spanning tree are selected.

Election of the Root Bridge

For each VLAN, the network device with the highest-priority bridge ID (the lowest numerical ID value) is elected as the root bridge. If all network devices are configured with the default priority (32768), the network device with the lowest MAC address in the VLAN becomes the root bridge. The bridge priority value occupies the most significant bits of the bridge ID.

When you change the bridge priority value, you change the probability that the router will be elected as the root bridge. Configuring a higher-priority value increases the probability; a lower-priority value decreases the probability.

The STP root bridge is the logical center of the spanning tree topology in a Layer 2 network. All paths that are not needed to reach the root bridge from anywhere in the Layer 2 network are placed in STP blocking mode.

BPDUs contain information about the transmitting bridge and its ports, including bridge and MAC addresses, bridge priority, port priority, and path cost. STP uses this information to elect the root bridge for the Layer 2 network, to elect the root port leading to the root bridge, and to determine the designated port for each Layer 2 segment.

STP Protocol Timers

Table 20-3 describes the STP protocol timers that affect STP performance.

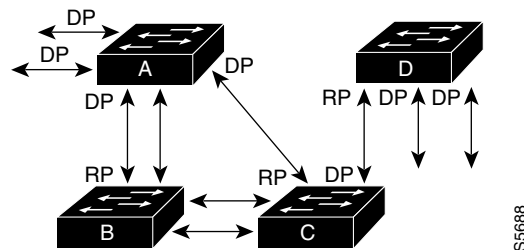
Table 20-3 STP Protocol Timers

Variable	Description
Hello timer	Determines how often the network device broadcasts hello messages to other network devices.
Forward delay timer	Determines how long each of the listening and learning states last before the port begins forwarding.
Maximum age timer	Determines the amount of time protocol information received on an port is stored by the network device.

Creating the Spanning Tree Topology

In Figure 20-1, Switch A is elected as the root bridge because the bridge priority of all the network devices is set to the default (32768) and Switch A has the lowest MAC address. However, due to traffic patterns, number of forwarding ports, or link types, Switch A might not be the ideal root bridge. By increasing the priority (lowering the numerical value) of the ideal network device so that it becomes the root bridge, you force an STP recalculation to form a new spanning tree topology with the ideal network device as the root.

Figure 20-1 Spanning Tree Topology



RP = Root Port
DP = Designated Port

When the spanning tree topology is calculated based on default parameters, the path between source and destination end stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change. The goal is to make the fastest link the root port.

For example, assume that one port on Switch B is a fiber-optic link, and another port on Switch B (an unshielded twisted-pair [UTP] link) is the root port. Network traffic might be more efficient over the high-speed fiber-optic link. By changing the STP port priority on the fiber-optic port to a higher priority (lower numerical value) than the root port, the fiber-optic port becomes the new root port.

STP Port States

These sections describe the STP port states:

- [STP Port State Overview, page 20-6](#)
- [Blocking State, page 20-8](#)
- [Listening State, page 20-9](#)
- [Learning State, page 20-10](#)
- [Forwarding State, page 20-11](#)
- [Disabled State, page 20-12](#)

STP Port State Overview

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When a Layer 2 LAN port transitions directly from nonparticipation in the spanning tree topology to the forwarding state, it can create temporary data loops. Ports must wait for new topology information to propagate through the switched LAN before starting to forward frames. They must allow the frame lifetime to expire for frames that have been forwarded using the old topology.

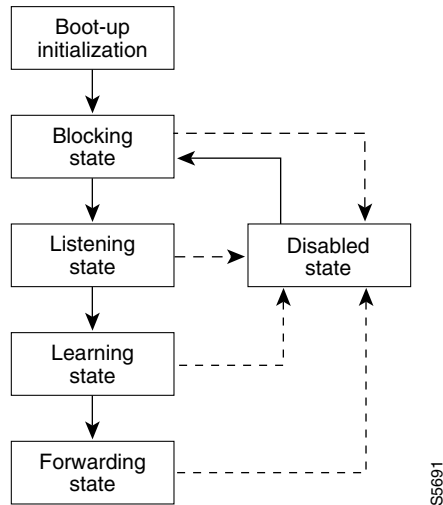
Each Layer 2 LAN port on a Cisco 7600 series router using STP exists in one of the following five states:

- **Blocking**—The Layer 2 LAN port does not participate in frame forwarding.
- **Listening**—First transitional state after the blocking state when STP determines that the Layer 2 LAN port should participate in frame forwarding.
- **Learning**—The Layer 2 LAN port prepares to participate in frame forwarding.
- **Forwarding**—The Layer 2 LAN port forwards frames.
- **Disabled**—The Layer 2 LAN port does not participate in STP and is not forwarding frames.

A Layer 2 LAN port moves through these five states as follows:

- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

[Figure 20-2](#) illustrates how a Layer 2 LAN port moves through the five states.

Figure 20-2 STP Layer 2 LAN Interface States

When you enable STP, every port in the Cisco 7600 series router, VLAN, and network goes through the blocking state and the transitory states of listening and learning at power up. If properly configured, each Layer 2 LAN port stabilizes to the forwarding or blocking state.

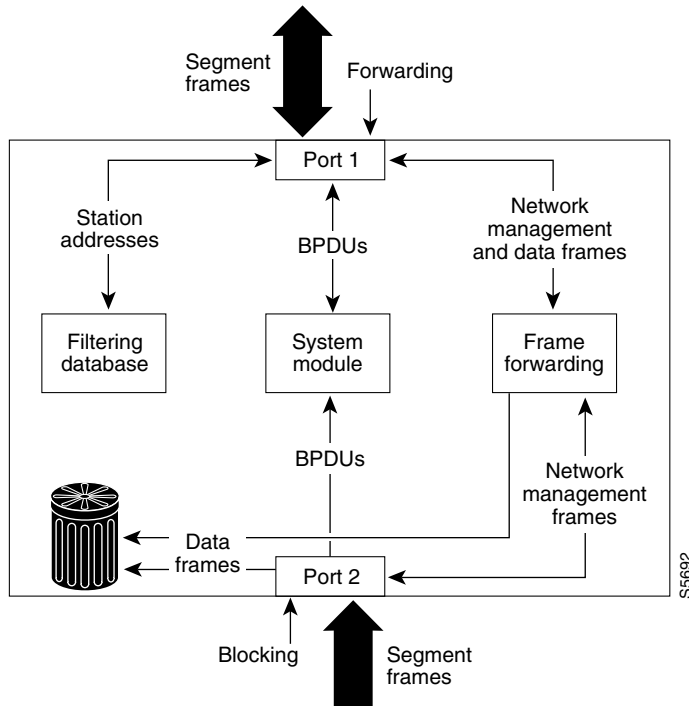
When the STP algorithm places a Layer 2 LAN port in the forwarding state, the following process occurs:

1. The Layer 2 LAN port is put into the listening state while it waits for protocol information that suggests it should go to the blocking state.
2. The Layer 2 LAN port waits for the forward delay timer to expire, moves the Layer 2 LAN port to the learning state, and resets the forward delay timer.
3. In the learning state, the Layer 2 LAN port continues to block frame forwarding as it learns end station location information for the forwarding database.
4. The Layer 2 LAN port waits for the forward delay timer to expire and then moves the Layer 2 LAN port to the forwarding state, where both learning and frame forwarding are enabled.

Blocking State

A Layer 2 LAN port in the blocking state does not participate in frame forwarding, as shown in Figure 20-3. After initialization, a BPDU is sent out to each Layer 2 LAN port. A network device initially assumes it is the root until it exchanges BPDUs with other network devices. This exchange establishes which network device in the network is the root or root bridge. If only one network device is in the network, no exchange occurs, the forward delay timer expires, and the ports move to the listening state. A port always enters the blocking state following initialization.

Figure 20-3 Interface 2 in Blocking State



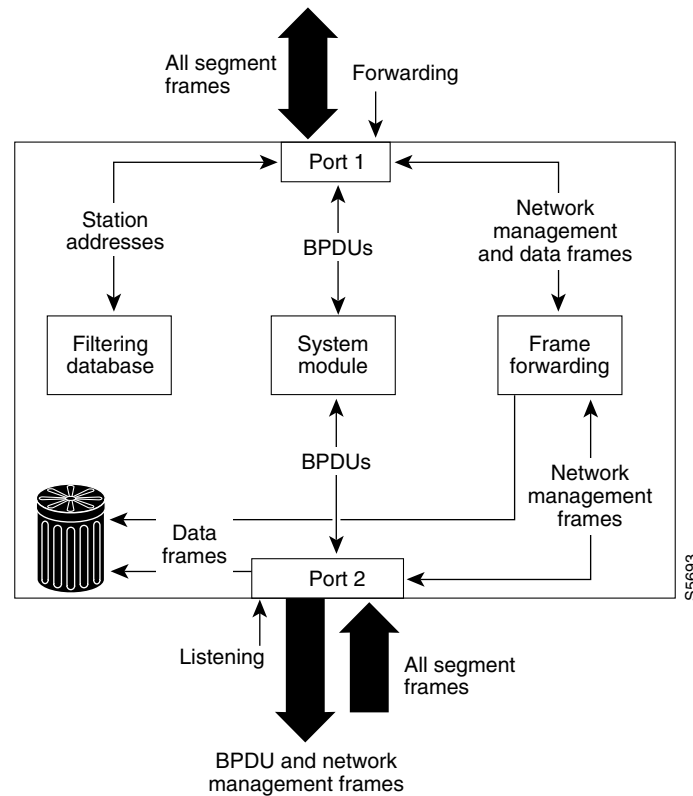
A Layer 2 LAN port in the blocking state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate end station location into its address database. (There is no learning on a blocking Layer 2 LAN port, so there is no address database update.)
- Receives BPDUs and directs them to the system module.
- Does not transmit BPDUs received from the system module.
- Receives and responds to network management messages.

Listening State

The listening state is the first transitional state a Layer 2 LAN port enters after the blocking state. The Layer 2 LAN port enters this state when STP determines that the Layer 2 LAN port should participate in frame forwarding. Figure 20-4 shows a Layer 2 LAN port in the listening state.

Figure 20-4 Interface 2 in Listening State



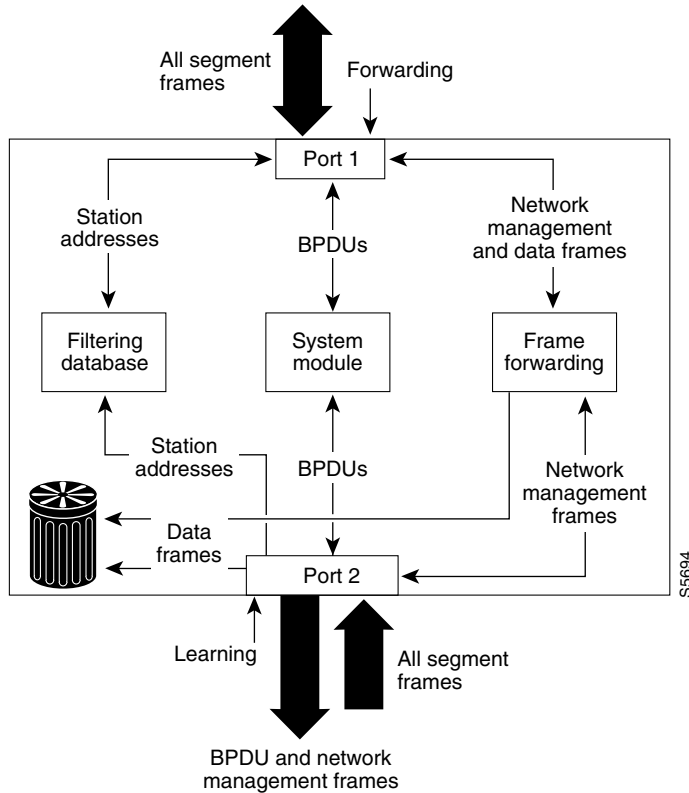
A Layer 2 LAN port in the listening state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another LAN port for forwarding.
- Does not incorporate end station location into its address database. (There is no learning at this point, so there is no address database update.)
- Receives BPDUs and directs them to the system module.
- Receives, processes, and transmits BPDUs received from the system module.
- Receives and responds to network management messages.

Learning State

A Layer 2 LAN port in the learning state prepares to participate in frame forwarding. The Layer 2 LAN port enters the learning state from the listening state. Figure 20-5 shows a Layer 2 LAN port in the learning state.

Figure 20-5 Interface 2 in Learning State



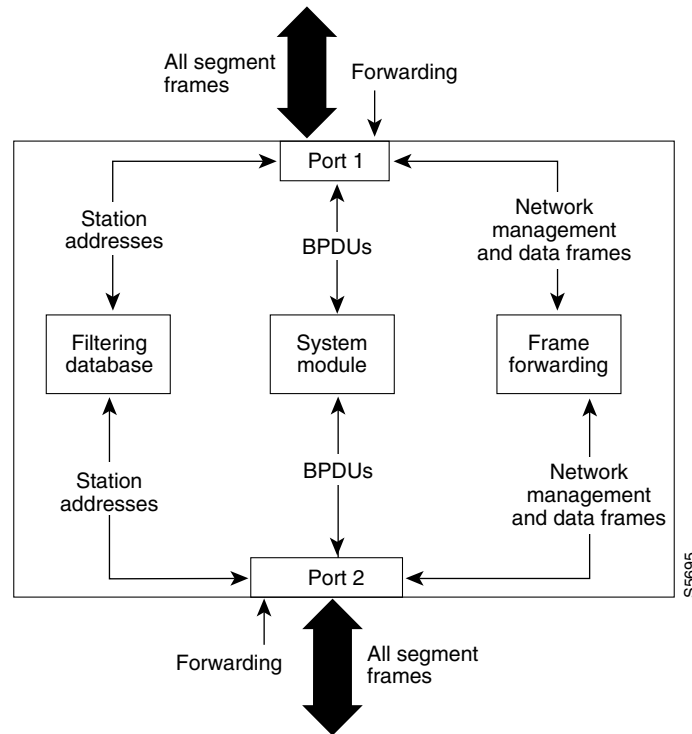
A Layer 2 LAN port in the learning state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Incorporates end station location into its address database.
- Receives BPDUs and directs them to the system module.
- Receives, processes, and transmits BPDUs received from the system module.
- Receives and responds to network management messages.

Forwarding State

A Layer 2 LAN port in the forwarding state forwards frames, as shown in Figure 20-6. The Layer 2 LAN port enters the forwarding state from the learning state.

Figure 20-6 Interface 2 in Forwarding State



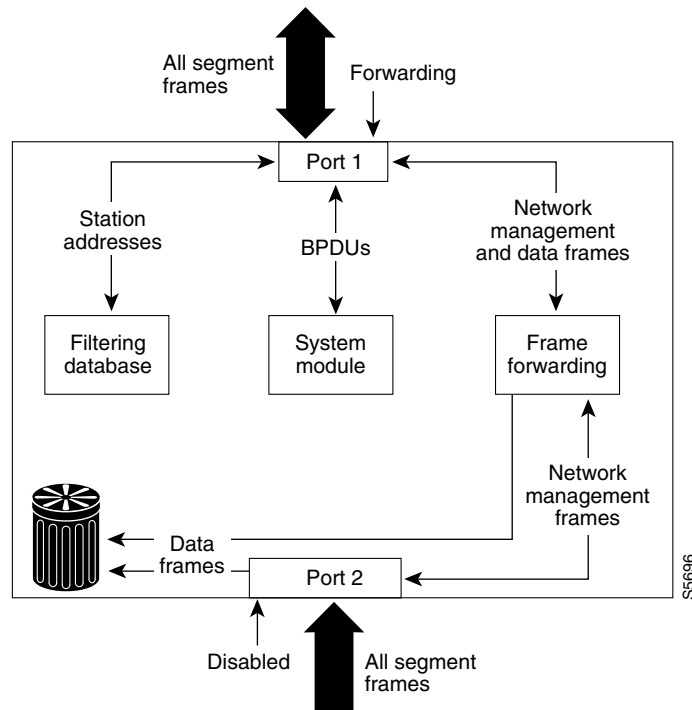
A Layer 2 LAN port in the forwarding state performs as follows:

- Forwards frames received from the attached segment.
- Forwards frames switched from another port for forwarding.
- Incorporates end station location information into its address database.
- Receives BPDUs and directs them to the system module.
- Processes BPDUs received from the system module.
- Receives and responds to network management messages.

Disabled State

A Layer 2 LAN port in the disabled state does not participate in frame forwarding or STP, as shown in Figure 20-7. A Layer 2 LAN port in the disabled state is virtually nonoperational.

Figure 20-7 Interface 2 in Disabled State



A disabled Layer 2 LAN port performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate end station location into its address database. (There is no learning, so there is no address database update.)
- Does not receive BPDUs.
- Does not receive BPDUs for transmission from the system module.

STP and IEEE 802.1Q Trunks

802.1Q trunks impose some limitations on the STP strategy for a network. In a network of Cisco network devices connected through 802.1Q trunks, the network devices maintain one instance of STP for each VLAN allowed on the trunks. However, non-Cisco 802.1Q network devices maintain only one instance of STP for all VLANs allowed on the trunks.

When you connect a Cisco network device to a non-Cisco device through an 802.1Q trunk, the Cisco network device combines the STP instance of the 802.1Q VLAN of the trunk with the STP instance of the non-Cisco 802.1Q network device. However, all per-VLAN STP information is maintained by Cisco network devices separated by a cloud of non-Cisco 802.1Q network devices. The non-Cisco 802.1Q cloud separating the Cisco network devices is treated as a single trunk link between the network devices.

For more information on 802.1Q trunks, see [Chapter 10, “Configuring LAN Ports for Layer 2 Switching.”](#)

Understanding How IEEE 802.1w RSTP Works



Note

RSTP is available as a standalone protocol in Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) mode. In this mode, the router runs an RSTP instance on each VLAN, which follows the usual PVST+ approach.

These sections describe Rapid Spanning Tree Protocol (RSTP):

- [IEEE 802.1w RSTP Overview, page 20-13](#)
- [RSTP Port Roles, page 20-13](#)
- [RSTP Port States, page 20-14](#)
- [Rapid-PVST, page 20-14](#)

IEEE 802.1w RSTP Overview

RSTP significantly reduces the time to reconfigure the active topology of the network when changes occur to the physical topology or its configuration parameters. RSTP selects one router as the root of a spanning tree-connected active topology and assigns port roles to individual ports of the router, depending on whether that port is part of the active topology.

RSTP provides rapid connectivity following the failure of a router, router port, or a LAN. A new root port and the designated port on the other side of the bridge transition to forwarding using an explicit handshake between them. RSTP allows router port configuration so that the ports can transition to forwarding directly when the router reinitializes.

RSTP as specified in 802.1w supersedes STP specified in 802.1D, but remains compatible with STP.

RSTP provides backward compatibility with 802.1D bridges as follows:

- RSTP selectively sends 802.1D-configured BPDUs and topology change notification (TCN) BPDUs on a per-port basis.
- When a port initializes, the migration-delay timer starts and RSTP BPDUs are transmitted. While the migration-delay timer is active, the bridge processes all BPDUs received on that port.
- If the bridge receives an 802.1D BPDU after a port's migration-delay timer expires, the bridge assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
- When RSTP uses 802.1D BPDUs on a port and receives an RSTP BPDU after the migration-delay expires, RSTP restarts the migration-delay timer and begins using RSTP BPDUs on that port.

RSTP Port Roles

RSTP uses the following definitions for port roles:

- Root—A forwarding port elected for the spanning tree topology.
- Designated—A forwarding port elected for every switched LAN segment.
- Alternate—An alternate path to the root bridge to that provided by the current root port.

- Backup—A backup for the path provided by a designated port toward the leaves of the spanning tree. Backup ports can exist only where two ports are connected together in a loopback by a point-to-point link or bridge with two or more connections to a shared LAN segment.
- Disabled—A port that has no role within the operation of spanning tree.

Port roles are assigned as follows:

- A root port or designated port role includes the port in the active topology.
- An alternate port or backup port role excludes the port from the active topology.

RSTP Port States

The port state controls the forwarding and learning processes and provides the values of discarding, learning, and forwarding. [Table 20-4](#) provides a comparison between STP port states and RSTP port states.

Table 20-4 Comparison Between STP and RSTP Port States

Operational Status	STP Port State	RSTP Port State	Port Included in Active Topology
Enabled	Blocking ¹	Discarding ²	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

1. IEEE 802.1D port state designation.

2. IEEE 802.1w port state designation. Discarding is the same as blocking in RSTP and MST.

In a stable topology, RSTP ensures that every root port and designated port transition to forwarding, and ensures that all alternate ports and backup ports are always in the discarding state.

Rapid-PVST

Rapid-PVST uses the existing configuration for PVST+; however, Rapid-PVST uses RSTP to provide faster convergence. Independent VLANs run their own RSTP instance.

Dynamic entries are flushed immediately on a per-port basis upon receiving a topology change.

UplinkFast and BackboneFast configurations are ignored in Rapid-PVST mode; both features are included in RSTP.

Understanding How Prestandard IEEE 802.1s MST Works

These sections describe Multiple Spanning Tree (MST):

- [IEEE 802.1s MST Overview, page 20-15](#)
- [MST-to-PVST Interoperability, page 20-16](#)
- [Common Spanning Tree, page 20-18](#)

- [MST Instances, page 20-18](#)
- [MST Configuration Parameters, page 20-18](#)
- [MST Regions, page 20-19](#)
- [Message Age and Hop Count, page 20-20](#)
- [Default STP Configuration, page 20-21](#)

IEEE 802.1s MST Overview

MST in this release is based on the draft version of the IEEE standard. 802.1s for MST is an amendment to 802.1Q. MST extends the IEEE 802.1w rapid spanning tree (RST) algorithm to multiple spanning trees. This extension provides both rapid convergence and load balancing in a VLAN environment. MST converges faster than PVST+. MST is backward compatible with 802.1D STP, 802.1w (rapid spanning tree protocol [RSTP]), and the Cisco PVST+ architecture.

MST allows you to build multiple spanning trees over trunks. You can group and associate VLANs to spanning tree instances. Each instance can have a topology independent of other spanning tree instances. This new architecture provides multiple forwarding paths for data traffic and enables load balancing. Network fault tolerance is improved because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

In large networks, you can more easily administer the network and use redundant paths by locating different VLAN and spanning tree instance assignments in different parts of the network. A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments. You must configure a set of bridges with the same MST configuration information, which allows them to participate in a specific set of spanning tree instances. Interconnected bridges that have the same MST configuration are referred to as an *MST region*.

MST uses the modified RSTP version called the Multiple Spanning Tree Protocol (MSTP). The MST feature has these characteristics:

- MST runs a variant of spanning tree called internal spanning tree (IST). IST augments the common spanning tree (CST) information with internal information about the MST region. The MST region appears as a single bridge to adjacent single spanning tree (SST) and MST regions.
- A bridge running MST provides interoperability with single spanning tree bridges as follows:
 - MST bridges run IST, which augments the common spanning tree (CST) information with internal information about the MST region.
 - IST connects all the MST bridges in the region and appears as a subtree in the CST that includes the whole bridged domain. The MST region appears as a virtual bridge to adjacent SST bridges and MST regions.
 - The common and internal spanning tree (CIST) is the collection of ISTs in each MST region, the CST that interconnects the MST regions, and the SST bridges. CIST is the same as an IST inside an MST region and the same as CST outside an MST region. The STP, RSTP, and MSTP together elect a single bridge as the root of the CIST.

- MST establishes and maintains additional spanning trees within each MST region. These spanning trees are referred to as MST instances (MSTIs). The IST is numbered 0, and the MSTIs are numbered 1,2,3, and so on. Any MSTI is local to the MST region that is independent of MSTIs in another region, even if the MST regions are interconnected. MST instances combine with the IST at the boundary of MST regions to become the CST as follows:

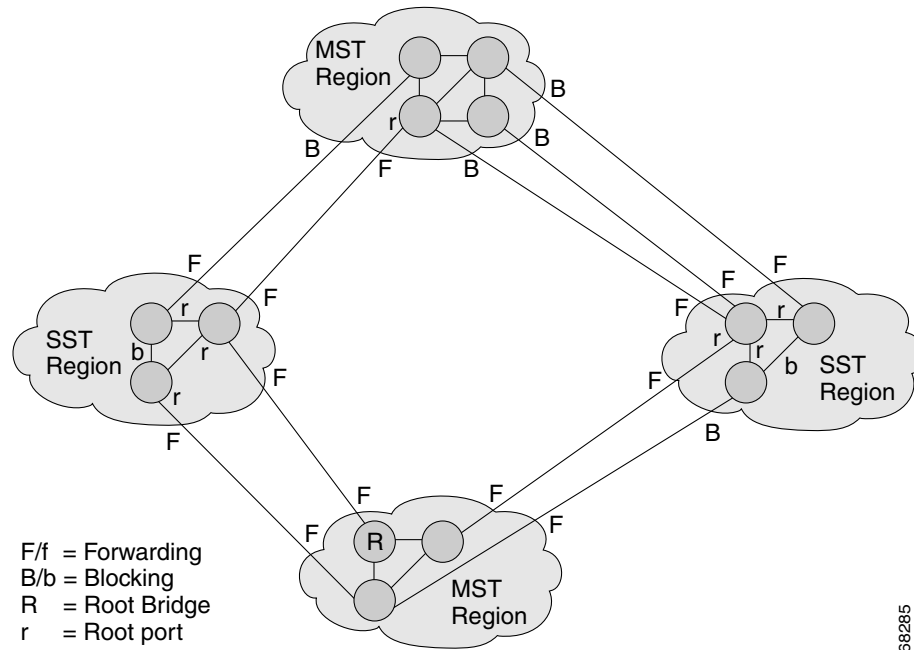
Spanning tree information for an MSTI is contained in an MSTP record (M-record). M-records are always encapsulated within MST BPDUs (MST BPDUs). The original spanning trees computed by MSTP are called M-trees. M-trees are active only within the MST region. M-trees merge with the IST at the boundary of the MST region and form the CST.

- MST provides interoperability with PVST+ by generating PVST+ BPDUs for the non-CST VLANs.
- MST supports some of the PVST+ extensions in MSTP as follows:
 - UplinkFast and BackboneFast are not available in MST mode; they are included in RSTP.
 - PortFast is supported.
 - BPDU filter and BPDU guard are supported in MST mode.
 - Loop guard and root guard are supported in MST. MST preserves the VLAN 1 disabled functionality except that BPDUs are still transmitted in VLAN 1.
 - MST switches operate as if MAC reduction is enabled.
 - For private VLANs (PVLANS), secondary VLANs must be mapped to the same instance as the primary.

MST-to-PVST Interoperability

A virtual bridged LAN may contain interconnected regions of single spanning tree (SST) and MST bridges. [Figure 20-8](#) shows this relationship.

Figure 20-8 Network with Interconnected SST and MST Regions



An MST region appears as an SST or pseudobridge to STP running in the SST region. Pseudobridges operate as follows:

- The same values for root identifiers and root path costs are sent in all BPDUs of all the pseudobridge ports. Pseudobridges differ from a single SST bridge as follows:
 - The pseudobridge BPDUs have different bridge identifiers. This difference does not affect STP operation in the neighboring SST regions because the root identifier and root cost are the same.
 - BPDUs sent from the pseudobridge ports may have significantly different message ages. Because the message age increases by 1 second for each hop, the difference in the message age is in the order of seconds.
- Data traffic from one port of a pseudobridge (a port at the edge of a region) to another port follows a path entirely contained within the pseudobridge or MST region.
- Data traffic belonging to different VLANs may follow different paths within the MST regions established by MST.
- Loop prevention is achieved by either of the following:
 - Blocking the appropriate pseudobridge ports by allowing one forwarding port on the boundary and blocking all other ports.
 - Setting the CST partitions to block the ports of the SST regions.
- A pseudobridge differs from a single SST bridge because the BPDUs sent from the pseudobridge's ports have different bridge identifiers. The root identifier and root cost are the same for both bridges.

These guidelines apply in a topology where you configure MST switches (all in the same region) to interact with PVST+ switches:

- Configure the root for all VLANs inside the MST region as shown in this example:

```
Router# show spanning-tree mst interface gigabitethernet 1/1
```

```
GigabitEthernet1/1 of MST00 is root forwarding
```

```

Edge port: no                (trunk)                port guard : none          (default)
Link type: point-to-point   (auto)                bpdu filter: disable      (default)
Boundary : boundary         (PVST)                bpdu guard : disable      (default)
Bpdus sent 10, received 310

```

```

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-----
0          Root FWD 20000   128.1   1-2,4-2999,4000-4094
3          Boun FWD 20000   128.1   3,3000-3999

```

The ports that belong to the MST router at the boundary simulate PVST+ and send PVST+ BPDUs for all the VLANs.

If you enable loop guard on the PVST+ switches, the ports might change to a loop-inconsistent state when the MST switches change their configuration. To correct the loop-inconsistent state, you must disable and reenable loop guard on that PVST+ router.

- Do not locate the root for some or all of the VLANs inside the PVST+ side of the MST router because when the MST router at the boundary receives PVST+ BPDUs for all or some of the VLANs on its designated ports, root guard sets the port to the blocking state. Do not designate switches with a slower CPU running PVST+ as a router running MST.

When you connect a PVST+ router to two different MST regions, the topology change from the PVST+ router does not pass beyond the first MST region. In this case, the topology changes are only propagated in the instance to which the VLAN is mapped. The topology change stays local to the first MST region and the CAM entries in the other region are not flushed. To make the topology change visible throughout other MST regions, you can map that VLAN to IST or connect the PVST+ router to the two regions through access links.

Common Spanning Tree

CST (802.1Q) is a single spanning tree for all the VLANs. In a Cisco 7600 series router running PVST+, the VLAN 1 spanning tree corresponds to CST. In a Cisco 7600 series router running MST, IST (instance 0) corresponds to CST.

MST Instances

This release supports up to 16 instances; each spanning tree instance is identified by an instance ID that ranges from 0 to 15. Instance 0 is mandatory and is always present. Instances 1 through 15 are optional.

MST Configuration Parameters

MST configuration includes these three parts:

- Name—A 32-character string (null padded) identifying the MST region.
- Revision number—An unsigned 16-bit number that identifies the revision of the current MST configuration.



Note You must set the revision number when required as part of the MST configuration. The revision number is not incremented automatically each time you commit the MST configuration.

- **MST configuration table**—An array of 4096 bytes. Each byte, interpreted as an unsigned integer, corresponds to a VLAN. The value is the instance number to which the VLAN is mapped. The first byte that corresponds to VLAN 0 and the 4096th byte that corresponds to VLAN 4095 are unused and always set to zero.

You must configure each byte manually. You can use SNMP or the CLI to perform the configuration.

MST BPDUs contain the MST configuration ID and the checksum. An MST bridge accepts an MST BPDU only if the MST BPDU configuration ID and the checksum match its own MST region configuration ID and checksum. If one value is different, the MST BPDU is considered to be an SST BPDU.

MST Regions

These sections describe MST regions:

- [MST Region Overview, page 20-19](#)
- [Boundary Ports, page 20-19](#)
- [IST Master, page 20-20](#)
- [Edge Ports, page 20-20](#)
- [Link Type, page 20-20](#)

MST Region Overview

Interconnected bridges that have the same MST configuration are referred to as an MST region. There is no limit on the number of MST regions in the network.

To form an MST region, bridges can be either of the following:

- An MST bridge that is the only member of the MST region.
- An MST bridge interconnected by a LAN. A LAN's designated bridge has the same MST configuration as an MST bridge. All the bridges on the LAN can process MST BPDUs.

If you connect two MST regions with different MST configurations, the MST regions do the following:

- Load balance across redundant paths in the network. If two MST regions are redundantly connected, all traffic flows on a single connection with the MST regions in a network.
- Provide an RSTP handshake to enable rapid connectivity between regions. However, the handshaking is not as fast as between two bridges. To prevent loops, all the bridges inside the region must agree upon the connections to other regions. This situation introduces a delay. We do not recommend partitioning the network into a large number of regions.

Boundary Ports

A boundary port is a port that connects to a LAN, the designated bridge, of which is either an SST bridge, or a bridge with a different MST configuration. A designated port knows that it is on the boundary if it detects an STP bridge or receives an agreement message from an RST or MST bridge with a different configuration.

At the boundary, the role of MST ports do not matter; their state is forced to be the same as the IST port state. If the boundary flag is set for the port, the MSTP port-role selection process assigns a port role to the boundary and assigns the same state as the state of the IST port. The IST port at the boundary can take up any port role except a backup port role.

IST Master

The IST master of an MST region is the bridge with the lowest bridge identifier and the least path cost to the CST root. If an MST bridge is the root bridge for CST, then it is the IST master of that MST region. If the CST root is outside the MST region, then one of the MST bridges at the boundary is selected as the IST master. Other bridges on the boundary that belong to the same region eventually block the boundary ports that lead to the root.

If two or more bridges at the boundary of a region have an identical path to the root, you can set a slightly lower bridge priority to make a specific bridge the IST master.

The root path cost and message age inside a region stay constant, but the IST path cost is incremented and the IST remaining hops are decremented at each hop. To display the information about the IST master, path cost, and remaining hops for the bridge, enter the **show spanning-tree mst** command.

Edge Ports

An edge port is a port that is connected to a nonbridging device (for example, a host or a router). A port that connects to a hub is also an edge port if the hub or any LAN that is connected by it does not have a bridge. An edge port can start forwarding as soon as the link is up.

MST requires that you configure all ports for each host or router. To establish rapid connectivity after a failure, you need to block the non-edge designated ports of an intermediate bridge. If the port connects to another bridge that can send back an agreement, then the port starts forwarding immediately. Otherwise, the port needs twice the forward delay time to start forwarding again. You must explicitly configure the ports that are connected to the hosts and routers as edge ports while using MST.

To prevent a misconfiguration, the PortFast operation is turned off if the port receives a BPDU. To display the configured and operational status of PortFast, enter the **show spanning-tree mst interface** command.

Link Type

Rapid connectivity is established only on point-to-point links. You must configure ports explicitly to a host or router. However, cabling in most networks meets this requirement, and you can avoid explicit configuration by treating all full-duplex links as point-to-point links by entering the **spanning-tree linktype** command.

Message Age and Hop Count

IST and MST instances do not use the message age and maximum age timer settings in the BPDU. IST and MST use a separate hop-count process that is very similar to the IP TTL process. You can configure each MST bridge with a maximum hop count. The root bridge of the instance sends a BPDU (or M-record) with the remaining hop count that is equal to the maximum hop count. When a bridge receives a BPDU (or M-record), it decrements the received remaining hop count by one. The bridge discards the BPDU (M-record) and ages out the information held for the port if the count reaches zero after decrementing. The nonroot bridges propagate the decremented count as the remaining hop count in the BPDUs (M-records) they generate.

The message age and maximum age timer settings in the RST portion of the BPDU remain the same throughout the region, and the same values are propagated by the region's designated ports at the boundary.

Default STP Configuration

Table 20-5 shows the default STP configuration.

Table 20-5 STP Default Configuration

Feature	Default Value
Enable state	STP enabled for all VLANs
Bridge priority	32768
STP port priority (configurable on a per-port basis—used on LAN ports configured as Layer 2 access ports)	128
STP port cost (configurable on a per-port basis—used on LAN ports configured as Layer 2 access ports)	<ul style="list-style-type: none"> • 10-Gigabit Ethernet: 2 • Gigabit Ethernet: 4 • Fast Ethernet: 19 • Ethernet: 100
STP VLAN port priority (configurable on a per-VLAN basis—used on LAN ports configured as Layer 2 trunk ports)	128
STP VLAN port cost (configurable on a per-VLAN basis—used on LAN ports configured as Layer 2 trunk ports)	<ul style="list-style-type: none"> • 10-Gigabit Ethernet: 2 • Gigabit Ethernet: 4 • Fast Ethernet: 19 • Ethernet: 100
Hello time	2 seconds
Forward delay time	15 seconds
Maximum aging time	20 seconds
Mode	PVST

STP and MST Configuration Guidelines and Restrictions

When configuring MST, follow these guidelines and restrictions:

- Do not disable spanning tree on any VLAN in any of the PVST bridges.
- Do not use PVST bridges as the root of CST.
- Ensure that all PVST spanning tree root bridges have lower (numerically higher) priority than the CST root bridge.
- Ensure that trunks carry all of the VLANs mapped to an instance or do not carry any VLANs at all for this instance.
- Do not connect switches with access links because access links may partition a VLAN.
- Any MST configuration involving a large number of either existing or new logical VLAN ports should be completed during a maintenance window because the complete MST database gets reinitialized for any incremental change (such as adding new VLANs to instances or moving VLANs across instances).

Configuring STP

These sections describe how to configure STP on VLANs:

- [Enabling STP, page 20-22](#)
- [Enabling the Extended System ID, page 20-24](#)
- [Configuring the Root Bridge, page 20-24](#)
- [Configuring a Secondary Root Bridge, page 20-26](#)
- [Configuring STP Port Priority, page 20-27](#)
- [Configuring STP Port Cost, page 20-28](#)
- [Configuring the Bridge Priority of a VLAN, page 20-30](#)
- [Configuring the Hello Time, page 20-31](#)
- [Configuring the Forward-Delay Time for a VLAN, page 20-32](#)
- [Configuring the Maximum Aging Time for a VLAN, page 20-32](#)
- [Enabling Rapid-PVST, page 20-33](#)



Note

The STP commands described in this chapter can be configured on any LAN port, but they are in effect only on LAN ports configured with the **switchport** keyword.



Caution

We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree serves as a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

Enabling STP



Note

STP is enabled by default on VLAN 1 and on all newly created VLANs.

You can enable STP on a per-VLAN basis. The Cisco 7600 series router maintains a separate instance of STP for each VLAN (except on VLANs on which you disable STP).

To enable STP on a per-VLAN basis, perform this task:

	Command	Purpose
Step 1	Router(config)# spanning-tree vlan <i>vlan_ID</i>	Enables STP on a per-VLAN basis. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 20-5 on page 20-21).
	Router(config)# default spanning-tree vlan <i>vlan_ID</i>	Reverts all STP parameters to default values for the specified VLAN.
	Router(config)# no spanning-tree vlan <i>vlan_ID</i>	Disables STP on the specified VLAN; see the following Cautions for information regarding this command.

	Command	Purpose
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show spanning-tree vlan <i>vlan_ID</i>	Verifies that STP is enabled.

**Caution**

Do not disable spanning tree on a VLAN unless all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the VLAN. This action can have unexpected results because switches and bridges with spanning tree enabled will have incomplete information regarding the physical topology of the network.

**Caution**

We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree serves as a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

This example shows how to enable STP on VLAN 200:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200
Router(config)# end
Router#
```

**Note**

Because STP is enabled by default, entering a **show running** command to view the resulting configuration does not display the command you entered to enable STP.

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200

VLAN0200
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     00d0.00b8.14c8
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768
             Address     00d0.00b8.14c8
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface          Role Sts Cost      Prio.Nbr Status
-----
Fa4/4              Desg FWD 200000    128.196 P2p
Fa4/5              Back BLK 200000    128.197 P2p

Router#
```

**Note**

You must have at least one interface that is active in VLAN 200 to create a VLAN 200 spanning tree. In this example, two interfaces are active in VLAN 200.

Enabling the Extended System ID


Note

The extended system ID is enabled permanently on chassis that support 64 MAC addresses.

You can enable the extended system ID on chassis that support 1024 MAC addresses (see the [“Understanding the Bridge ID” section on page 20-2](#)).

To enable the extended system ID, perform this task:

	Command	Purpose
Step 1	Router(config)# spanning-tree extend system-id	Enables the extended system ID.
	Router(config)# no spanning-tree extend system-id	Disables the extended system ID. Note You cannot disable the extended system ID on chassis that support 64 MAC addresses or when you have configured extended range VLANs (see “STP Default Configuration” section on page 20-21).
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show spanning-tree vlan <i>vlan_ID</i>	Verifies the configuration.


Note

When you enable or disable the extended system ID, the bridge IDs of all active STP instances are updated, which might change the spanning tree topology.

This example shows how to enable the extended system ID:

```
Router# configure terminal
Router(config)# spanning-tree extend system-id
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree summary | include Extended
Extended system ID is enabled.
```

Configuring the Root Bridge

Cisco 7600 series routers maintain a separate instance of STP for each active VLAN. A bridge ID, consisting of the bridge priority and the bridge MAC address, is associated with each instance. For each VLAN, the network device with the highest-priority (lowest-numerical) bridge ID becomes the root bridge for that VLAN.

To configure a VLAN instance to become the root bridge, enter the **spanning-tree vlan** *vlan_ID* **root** command to modify the bridge priority from the default value (32768) to a significantly lower value.

When you enter the **spanning-tree vlan *vlan_ID* root** command, the router checks the bridge priority of the current root bridges for each VLAN. When the extended system ID is disabled, the router sets the bridge priority for the specified VLANs to 8192 if this value will cause the router to become the root for the specified VLANs. When the extended system ID is enabled, the router sets the bridge priority for the specified VLANs to 24576 if this value will cause the router to become the root for the specified VLANs.

If the extended system ID is disabled and if any root bridge for the specified VLANs has a bridge priority lower than 8192, the router sets the bridge priority for the specified VLANs to 1 less than the lowest bridge priority.

If the extended system ID is enabled and if any root bridge for the specified VLANs has a bridge priority lower than 24576, the router sets the bridge priority for the specified VLANs to 4096 less than the lowest bridge priority. (4096 is the value of the least significant bit of a 4-bit bridge priority value; see [Table 20-2 on page 20-3](#).)

**Note**

The **spanning-tree vlan *vlan_ID* root** command fails if the value required to be the root bridge is less than 1.

The **spanning-tree vlan *vlan_ID* root** command can cause the following effects:

- If the extended system ID is disabled, and if all network devices in VLAN 100 have the default priority of 32768, entering the **spanning-tree vlan 100 root primary** command on the router sets the bridge priority for VLAN 100 to 8192, which causes the router to become the root bridge for VLAN 100.
- If the extended system ID is enabled, and if all network devices in, for example, VLAN 20 have the default priority of 32768, entering the **spanning-tree vlan 20 root primary** command on the router sets the bridge priority to 24576, which causes the router to become the root bridge for VLAN 20.

**Caution**

The root bridge for each instance of STP should be a backbone or distribution router. Do not configure an access router as the STP primary root.

Use the **diameter** keyword to specify the Layer 2 network diameter (that is, the maximum number of bridge hops between any two end stations in the Layer 2 network). When you specify the network diameter, the Cisco 7600 series router automatically selects an optimal hello time, forward delay time, and maximum age time for a network of that diameter, which can significantly reduce the STP convergence time. You can use the **hello** keyword to override the automatically calculated hello time.

**Note**

To preserve a stable STP topology, we recommend that you avoid configuring the hello time, forward delay time, and maximum age time manually after configuring the Cisco 7600 series router as the root bridge.

To configure a Cisco 7600 series router as the root bridge, perform this task:

	Command	Purpose
Step 1	Router(config)# spanning-tree vlan <i>vlan_ID</i> root primary [diameter <i>hops</i> [hello-time <i>seconds</i>]]	Configures a Cisco 7600 series router as the root bridge. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 20-5 on page 20-21).
	Router(config)# no spanning-tree vlan <i>vlan_ID</i> root	Clears the root bridge configuration.
Step 2	Router(config)# end	Exits configuration mode.

This example shows how to configure the Cisco 7600 series router as the root bridge for VLAN 10, with a network diameter of 4:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# end
Router#
```

Configuring a Secondary Root Bridge

When you configure a Cisco 7600 series router as the secondary root, the STP bridge priority is modified from the default value (32768) so that the router is likely to become the root bridge for the specified VLANs if the primary root bridge fails (assuming the other network devices in the network use the default bridge priority of 32768).

If the extended system ID is enabled, STP sets the bridge priority to 28672. If the extended system ID is disabled, STP sets the bridge priority to 16384.

You can run this command on more than one Cisco 7600 series router to configure multiple backup root bridges. Use the same network diameter and hello time values as you used when configuring the primary root bridge.

To configure a Cisco 7600 series router as the secondary root bridge, perform this task:

	Command	Purpose
Step 1	Router(config)# [no] spanning-tree vlan <i>vlan_ID</i> root secondary [diameter <i>hops</i> [hello-time <i>seconds</i>]]	Configures a Cisco 7600 series router as the secondary root bridge. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
	Router(config)# no spanning-tree vlan <i>vlan_ID</i> root	Clears the root bridge configuring.
Step 2	Router(config)# end	Exits configuration mode.

This example shows how to configure the Cisco 7600 series router as the secondary root bridge for VLAN 10, with a network diameter of 4:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root secondary diameter 4
Router(config)# end
Router#
```

Configuring STP Port Priority

If a loop occurs, STP considers port priority when selecting a LAN port to put into the forwarding state. You can assign higher priority values to LAN ports that you want STP to select first and lower priority values to LAN ports that you want STP to select last. If all LAN ports have the same priority value, STP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports. The possible priority range is 0 through 240 (default 128), configurable in increments of 16.

When the LAN port is configured as a trunk port, you can specify a different port priority for each VLAN carried by the trunk. VLANs not configured with a VLAN port priority default to using the spanning-tree port priority. Do not configure VLAN port priority for access ports.

To configure the STP port priority of a Layer 2 LAN interface, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {{type ¹ slot/port} {port-channel port_channel_number}}	Selects an interface to configure.
Step 2	Router(config-if)# spanning-tree port-priority port_priority Router(config-if)# no spanning-tree port-priority	Configures the port priority for the LAN interface. The <i>port_priority</i> value can be from 0 to 240 in increments of 16. Reverts to the default port priority value.
Step 3	Router(config-if)# spanning-tree vlan vlan_ID port-priority port_priority Router(config-if)# [no] spanning-tree vlan vlan_ID port-priority	Configures the VLAN port priority for the LAN interface. The <i>port_priority</i> value can be from 0 to 240 in increments of 16. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2). Reverts to the default VLAN port priority value.
Step 4	Router(config-if)# end	Exits configuration mode.
Step 5	Router# show spanning-tree interface {type ¹ slot/port} {port-channel port_channel_number} Router# show spanning-tree vlan vlan_ID	Verifies the configuration.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to configure the STP port priority of Fast Ethernet port 4/4:

```
Router# configure terminal
Router(config)# interface fastethernet 4/4
Router(config-if)# spanning-tree port-priority 160
Router(config-if)# end
Router#
```

This example shows how to verify the configuration of Fast Ethernet port 4/4:

```
Router# show spanning-tree interface fastethernet 4/4
Vlan          Role Sts Cost      Prio.Nbr Status
-----
VLAN0001      Back BLK 200000   160.196 P2p
VLAN0006      Back BLK 200000   160.196 P2p
...
VLAN0198      Back BLK 200000   160.196 P2p
VLAN0199      Back BLK 200000   160.196 P2p
VLAN0200      Back BLK 200000   160.196 P2p
Router#
```

FastEthernet 4/4 is a trunk. Several VLANs are configured and active as shown in the example. The port priority configuration applies to all VLANs on this interface.

**Note**

The **show spanning-tree interface** command only displays information if the port is connected and operating. If this condition is not met, enter a **show running-config interface** command to verify the configuration.

This example shows how to configure the VLAN port priority of Fast Ethernet port 4/4:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree vlan 200 port-priority 64
Router(config-if)# ^Z
Router#
```

The configuration entered in the example only applies to VLAN 200. All VLANs other than 200 still have a port priority of 160.

This example shows how to verify the configuration:

```
Router# show spanning-tree interface fastEthernet 4/4
Vlan          Role Sts Cost      Prio.Nbr Status
-----
VLAN0001      Back BLK 200000    160.196 P2p
VLAN0006      Back BLK 200000    160.196 P2p
...
VLAN0199      Back BLK 200000    160.196 P2p
VLAN0200      Desg FWD 200000     64.196  P2p

Router#
```

You also can display spanning tree information for VLAN 200 using the following command:

```
Router# show spanning-tree vlan 200 interface fastEthernet 4/4
Interface     Role Sts Cost      Prio.Nbr Status
-----
Fa4/4         Desg LRN 200000    64.196  P2p
```

Configuring STP Port Cost

The STP port path cost default value is determined from the media speed of a LAN interface. If a loop occurs, STP considers port cost when selecting a LAN interface to put into the forwarding state. You can assign lower cost values to LAN interfaces that you want STP to select first and higher cost values to LAN interfaces that you want STP to select last. If all LAN interfaces have the same cost value, STP puts the LAN interface with the lowest LAN interface number in the forwarding state and blocks other LAN interfaces. The possible cost range is 0 through 200000000 (the default is media specific).

STP uses the port cost value when the LAN interface is configured as an access port and uses VLAN port cost values when the LAN interface is configured as a trunk port.

To configure the STP port cost of a Layer 2 LAN interface, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {{type ¹ slot/port} {port-channel port_channel_number}}	Selects an interface to configure.
Step 2	Router(config-if)# spanning-tree cost port_cost Router(config-if)# no spanning-tree cost	Configures the port cost for the LAN interface. The <i>port_cost</i> value can be from 1 to 200000000 (1 to 65535 in Release 12.1(2)E and earlier releases). Reverts to the default port cost.
Step 3	Router(config-if)# [no] spanning-tree vlan vlan_ID cost port_cost	Configures the VLAN port cost for the LAN interface. The <i>port_cost</i> value can be from 1 to 200000000. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
Step 4	Router(config-if)# no spanning-tree vlan vlan_ID cost	Reverts to the default VLAN port cost.
Step 5	Router(config-if)# end	Exits configuration mode.
Step 6	Router# show spanning-tree interface {type ¹ slot/port} {port-channel port_channel_number} show spanning-tree vlan vlan_ID	Verifies the configuration.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to change the STP port cost of Fast Ethernet port 4/4:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree cost 1000
Router(config-if)# ^Z
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree interface fastEthernet 4/4
Vlan          Role Sts Cost      Prio.Nbr Status
-----
VLAN0001      Back BLK 1000     160.196 P2p
VLAN0006      Back BLK 1000     160.196 P2p
VLAN0007      Back BLK 1000     160.196 P2p
VLAN0008      Back BLK 1000     160.196 P2p
VLAN0009      Back BLK 1000     160.196 P2p
VLAN0010      Back BLK 1000     160.196 P2p
Router#
```

This example shows how to configure the port priority at an individual port VLAN cost for VLAN 200:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree vlan 200 cost 2000
Router(config-if)# ^Z
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 interface fastEthernet 4/4
Interface      Role Sts Cost      Prio.Nbr Status
-----
-----
```

```
Fa4/4          Desg FWD 2000          64.196 P2p
```

**Note**

In the following output other VLANs (VLAN 1 for example) have not been affected by this configuration.

```
Router# show spanning-tree vlan 1 interface fastEthernet 4/4
Interface      Role Sts Cost          Prio.Nbr Status
-----
Fa4/4          Back BLK 1000         160.196 P2p
Router#
```

**Note**

The **show spanning-tree** command only displays information for ports that are in link-up operative state and are appropriately configured for DTP. If these conditions are not met, you can enter a **show running-config** command to confirm the configuration.

Configuring the Bridge Priority of a VLAN

**Note**

Be careful when using this command. For most situations, we recommend that you enter the **spanning-tree vlan *vlan_ID* root primary** and the **spanning-tree vlan *vlan_ID* root secondary** commands to modify the bridge priority.

To configure the STP bridge priority of a VLAN when the extended system ID is disabled, perform this task:

	Command	Purpose
Step 1	Router(config)# spanning-tree vlan <i>vlan_ID</i> priority <i>bridge_priority</i> Router(config)# no spanning-tree vlan <i>vlan_ID</i> priority	Configures the bridge priority of a VLAN when the extended system ID is disabled. The <i>bridge_priority</i> value can be from 1 to 65535. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2). Reverts to the default bridge priority value.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show spanning-tree vlan <i>vlan_ID</i> bridge [detail]	Verifies the configuration.

To configure the STP bridge priority of a VLAN when the extended system ID is enabled, perform this task:

	Command	Purpose
Step 1	Router(config)# [no] spanning-tree vlan <i>vlan_ID</i> priority {0 4096 8192 12288 16384 20480 24576 28672 32768 36864 40960 45056 49152 53248 57344 61440} Router(config)# no spanning-tree vlan <i>vlan_ID</i> priority	Configures the bridge priority of a VLAN when the extended system ID is enabled. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2). Reverts to the default bridge priority value.

	Command	Purpose
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show spanning-tree vlan <i>vlan_ID</i> bridge [detail]	Verifies the configuration.

This example shows how to configure the bridge priority of VLAN 200 to 33792 when the extended system ID is disabled:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 priority 33792
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 bridge
Vlan                Bridge ID           Hello Max  Fwd
Time  Age  Delay  Protocol
-----
VLAN200            33792 0050.3e8d.64c8   2    20    15  ieee
Router#
```

Configuring the Hello Time



Note

Be careful when using this command. For most situations, we recommend that you use the **spanning-tree vlan *vlan_ID* root primary** and **spanning-tree vlan *vlan_ID* root secondary** commands to modify the hello time.

To configure the STP hello time of a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# spanning-tree vlan <i>vlan_ID</i> hello-time <i>hello_time</i>	Configures the hello time of a VLAN. The <i>hello_time</i> value can be from 1 to 10 seconds. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
	Router(config)# no spanning-tree vlan <i>vlan_ID</i> hello-time	Reverts to the default hello time.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show spanning-tree vlan <i>vlan_ID</i> bridge [detail]	Verifies the configuration.

This example shows how to configure the hello time for VLAN 200 to 7 seconds:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 hello-time 7
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 bridge
Hello Max  Fwd
```

```

Vlan                Bridge ID           Time  Age Delay  Protocol
-----
VLAN200            49152 0050.3e8d.64c8  7   20   15  ieee
Router#

```

Configuring the Forward-Delay Time for a VLAN

To configure the STP forward delay time for a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# spanning-tree vlan <i>vlan_ID</i> forward-time <i>forward_time</i>	Configures the forward time of a VLAN. The <i>forward_time</i> value can be from 4 to 30 seconds. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
	Router(config)# no spanning-tree vlan <i>vlan_ID</i> forward-time	Reverts to the default forward time.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show spanning-tree vlan <i>vlan_ID</i> bridge [detail]	Verifies the configuration.

This example shows how to configure the forward delay time for VLAN 200 to 21 seconds:

```

Router# configure terminal
Router(config)# spanning-tree vlan 200 forward-time 21
Router(config)# end
Router#

```

This example shows how to verify the configuration:

```

Router# show spanning-tree vlan 200 bridge
Vlan                Bridge ID           Hello Max  Fwd
Time  Age Delay  Protocol
-----
VLAN200            49152 0050.3e8d.64c8  2   20   21  ieee
Router#

```

Configuring the Maximum Aging Time for a VLAN

To configure the STP maximum aging time for a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# spanning-tree vlan <i>vlan_ID</i> max-age <i>max_age</i>	Configures the maximum aging time of a VLAN. The <i>max_age</i> value can be from 6 to 40 seconds. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
	Router(config)# no spanning-tree vlan <i>vlan_ID</i> max-age	Reverts to the default maximum aging time.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show spanning-tree vlan <i>vlan_ID</i> bridge [detail]	Verifies the configuration.

This example shows how to configure the maximum aging time for VLAN 200 to 36 seconds:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 max-age 36
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 bridge
```

Vlan	Bridge ID	Hello Time	Max Age	Fwd Delay	Protocol
VLAN200	49152 0050.3e8d.64c8	2	36	15	ieee

```
Router#
```

Enabling Rapid-PVST

Rapid-PVST uses the existing PVST+ framework for configuration and interaction with other features. It also supports some of the PVST+ extensions.

To enable Rapid-PVST mode on the router, enter the **spanning-tree mode rapid-pvst** command in privileged mode. To configure the router in Rapid-PVST mode, see the “Configuring STP” section on page 20-22.

Specifying the Link Type

Rapid connectivity is established only on point-to-point links. Spanning tree views a point-to-point link as a segment connecting only two switches running the spanning tree algorithm. Because the router assumes that all full-duplex links are point-to-point links and that half-duplex links are shared links, you can avoid explicitly configuring the link type. To configure a specific link type, enter the **spanning-tree linktype** command.

Restarting Protocol Migration

A router running both MSTP and RSTP supports a built-in protocol migration process that enables the router to interoperate with legacy 802.1D switches. If this router receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MSTP router can also detect that a port is at the boundary of a region when it receives a legacy BPDU, or an MST BPDU (version 3) associated with a different region, or an RST BPDU (version 2).

However, the router does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether the legacy router has been removed from the link unless the legacy router is the designated router. A router also might continue to assign a boundary role to a port when the router to which it is connected has joined the region.

To restart the protocol migration process (force the renegotiation with neighboring switches) on the entire router, you can use the **clear spanning-tree detected-protocols** privileged EXEC command. To restart the protocol migration process on a specific interface, enter the **clear spanning-tree detected-protocols interface** *interface-id* privileged EXEC command.

Configuring Prestandard IEEE 802.1s MST

Release 12.2SX supports MST. These sections describe how to configure MST:

- [Enabling MST, page 20-34](#)
- [Displaying MST Configurations, page 20-35](#)
- [Configuring MST Instance Parameters, page 20-39](#)
- [Configuring MST Instance Port Parameters, page 20-40](#)
- [Restarting Protocol Migration, page 20-40](#)

Enabling MST

To enable and configure MST, perform these tasks in privileged mode:

	Command	Purpose
Step 1	Router# show spanning-tree mst configuration	Displays the current MST configuration.
Step 2	Router(config)# spanning-tree mode mst	Configures MST mode.
Step 3	Router(config)# spanning-tree mst configuration Router(config)# no spanning-tree mst configuration	Configures the MST region by entering the MST configuration submenu. Clears the MST configuration.
Step 4	Router(config-mst)# show current	Displays the current MST configuration from within the MST configuration submenu.
Step 5	Router(config-mst)# name name revision revision_number instance instance_number vlan vlan_range	Enters the MST configuration.
Step 6	Router(config-mst)# no instance instance_number	(Optional) Unmaps all VLANs that were mapped to an instance.
Step 7	Router(config-mst)# no instance instance_number vlan vlan_number	(Optional) Unmaps a VLAN from an instance.
Step 8	Router(config-mst)# end	Applies the configuration and exit configuration mode.
Step 9	Router# show spanning-tree mst config	Shows the MST configuration from the global configuration mode.

These examples show how to enable MST:

```
Router# show spanning-tree mst configuration
% Switch is not in mst mode
Name      []
Revision  0
Instance  Vlans mapped
-----
0         1-4094
-----

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# spanning-tree mode mst

Router(config)# spanning-tree mst configuration

Router(config-mst)# show current
Current MST configuration
Name      []
Revision  0
Instance  Vlans mapped
```

```

-----
0          1-4094
-----
Router(config-mst)# name cisco
Router(config-mst)# revision 2
Router(config-mst)# instance 1 vlan 1
Router(config-mst)# instance 2 vlan 1-1000
Router(config-mst)# show pending
Pending MST configuration
Name      [cisco]
Revision  2
Instance  Vlans mapped
-----
0          1001-4094
2          1-1000
-----
Router(config-mst)# no instance 2
Router(config-mst)# show pending
Pending MST configuration
Name      [cisco]
Revision  2
Instance  Vlans mapped
-----
0          1-4094
-----
Router(config-mst)# instance 1 vlan 2000-3000
Router(config-mst)# no instance 1 vlan 2500
Router(config-mst)# show pending
Pending MST configuration
Name      [cisco]
Revision  2
Instance  Vlans mapped
-----
0          1-1999,2500,3001-4094
1          2000-2499,2501-3000
-----
Router(config)# exit
Router(config)# no spanning-tree mst configuration
Router(config)# do show spanning-tree mst configuration
Name      []
Revision  0
Instance  Vlans mapped
-----
0          1-4094
-----

```

Displaying MST Configurations

To display MST configurations, perform these tasks in MST mode:

	Command	Purpose
Step 1	Router# show spanning-tree mst configuration	Displays the active configuration.
Step 2	Router# show spanning-tree mst [<i>detail</i>]	Displays information about the MST instances currently running.
Step 3	Router# show spanning-tree mst <i>instance-id</i> [<i>detail</i>]	Displays information about a specific MST instance.
Step 4	Router# show spanning-tree mst interface <i>interface name</i> [<i>detail</i>]	Displays information for a given port.

	Command	Purpose
Step 5	Router# show spanning-tree mst <i>number</i> interface <i>interface name</i> [detail]	Displays MST information for a given port and a given instance.
Step 6	Router# show spanning-tree mst [<i>x</i>] [<i>interface Y</i>] detail	Displays detailed MST information.
Step 7	Router# show spanning-tree vlan <i>vlan_ID</i>	Displays VLAN information in MST mode.

These examples show how to display spanning tree VLAN configurations in MST mode:

```
Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 1-10
Router(config-mst)# name cisco
Router(config-mst)# revision 1
Router(config-mst)# ^Z
```

```
Router# show spanning-tree mst configuration
```

```
Name      [cisco]
Revision  1
Instance  Vlans mapped
-----  -----
0         11-4094
1         1-10
-----  -----
```

```

Router# show spanning-tree mst

##### MST00          vlans mapped: 11-4094
Bridge      address 00d0.00b8.1400  priority 32768 (32768 sysid 0)
Root       address 00d0.004a.3c1c  priority 32768 (32768 sysid 0)
           port    Fa4/48          path cost 203100
IST master  this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface      Role Sts Cost      Prio.Nbr Status
-----
Fa4/4          Back BLK 1000    160.196 P2p
Fa4/5          Desg FWD 200000  128.197 P2p
Fa4/48        Root FWD 200000  128.240 P2p Bound(STP)

##### MST01          vlans mapped: 1-10
Bridge      address 00d0.00b8.1400  priority 32769 (32768 sysid 1)
Root       this switch for MST01

Interface      Role Sts Cost      Prio.Nbr Status
-----
Fa4/4          Back BLK 1000    160.196 P2p
Fa4/5          Desg FWD 200000  128.197 P2p
Fa4/48        Boun FWD 200000  128.240 P2p Bound(STP)

Router# show spanning-tree mst 1

##### MST01          vlans mapped: 1-10
Bridge      address 00d0.00b8.1400  priority 32769 (32768 sysid 1)
Root       this switch for MST01

Interface      Role Sts Cost      Prio.Nbr Status
-----
Fa4/4          Back BLK 1000    160.196 P2p
Fa4/5          Desg FWD 200000  128.197 P2p
Fa4/48        Boun FWD 200000  128.240 P2p Bound(STP)

Router# show spanning-tree mst interface fastEthernet 4/4

FastEthernet4/4 of MST00 is backup blocking
Edge port:no          (default)          port guard :none          (default)
Link type:point-to-point (auto)          bpdu filter:disable      (default)
Boundary :internal    bpdu guard :disable      (default)
Bpdus sent 2, received 368

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-----
0        Back BLK 1000    160.196 11-4094
1        Back BLK 1000    160.196 1-10

Router# show spanning-tree mst 1 interface fastEthernet 4/4

FastEthernet4/4 of MST01 is backup blocking
Edge port:no          (default)          port guard :none          (default)
Link type:point-to-point (auto)          bpdu filter:disable      (default)
Boundary :internal    bpdu guard :disable      (default)
Bpdus (MRecords) sent 2, received 364

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-----
1        Back BLK 1000    160.196 1-10

```

```

Router# show spanning-tree mst 1 detail

##### MST01          vlans mapped: 1-10
Bridge          address 00d0.00b8.1400  priority 32769 (32768 sysid 1)
Root            this switch for MST01

FastEthernet4/4 of MST01 is backup blocking
Port info          port id          160.196  priority 160  cost      1000
Designated root   address 00d0.00b8.1400  priority 32769  cost      0
Designated bridge address 00d0.00b8.1400  priority 32769  port id 128.197
Timers:message expires in 5 sec, forward delay 0, forward transitions 0
Bpdus (MRecords) sent 123, received 1188

FastEthernet4/5 of MST01 is designated forwarding
Port info          port id          128.197  priority 128  cost      200000
Designated root   address 00d0.00b8.1400  priority 32769  cost      0
Designated bridge address 00d0.00b8.1400  priority 32769  port id 128.197
Timers:message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 1188, received 123

FastEthernet4/48 of MST01 is boundary forwarding
Port info          port id          128.240  priority 128  cost      200000
Designated root   address 00d0.00b8.1400  priority 32769  cost      0
Designated bridge address 00d0.00b8.1400  priority 32769  port id 128.240
Timers:message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 78, received 0

Router# show spanning-tree vlan 10

MST01
  Spanning tree enabled protocol mstp
  Root ID   Priority   32769
           Address   00d0.00b8.1400
           This bridge is the root
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID Priority   32769 (priority 32768 sys-id-ext 1)
           Address   00d0.00b8.1400
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface          Role Sts Cost          Prio.Nbr Status
-----
Fa4/4              Back BLK 1000          160.196 P2p
Fa4/5              Desg FWD 200000          128.197 P2p

Router# show spanning-tree summary
Root bridge for:MST01
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is disabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long

Name              Blocking Listening Learning Forwarding STP Active
-----
MST00              1          0          0          2          3
MST01              1          0          0          2          3
-----
2 msts            2          0          0          4          6
Router#

```

Configuring MST Instance Parameters

To configure MST instance parameters, perform these tasks:

	Command	Purpose
Step 1	Router(config)# spanning-tree mst X priority Y	Configures the priority for an MST instance.
Step 2	Router(config)# spanning-tree mst X root [primary secondary]	Configures the bridge as root for an MST instance.
Step 3	Router# show spanning-tree mst	Verifies the configuration.

This example shows how to configure MST instance parameters:

```

Router(config)# spanning-tree mst 1 priority ?
    <0-61440> bridge priority in increments of 4096

Router(config)# spanning-tree mst 1 priority 1
% Bridge Priority must be in increments of 4096.
% Allowed values are:
    0      4096  8192  12288  16384  20480  24576  28672
    32768  36864  40960  45056  49152  53248  57344  61440

Router(config)# spanning-tree mst 1 priority 49152
Router(config)#

Router(config)# spanning-tree mst 0 root primary
mst 0 bridge priority set to 24576
mst bridge max aging time unchanged at 20
mst bridge hello time unchanged at 2
mst bridge forward delay unchanged at 15
Router(config)# ^Z
Router#

Router# show spanning-tree mst

##### MST00          vlans mapped: 11-4094
Bridge      address 00d0.00b8.1400  priority 24576 (24576 sysid 0)
Root        this switch for CST and IST
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface    Role Sts Cost      Prio.Nbr Status
-----
Fa4/4        Back BLK 1000      160.196 P2p
Fa4/5        Desg FWD 200000     128.197 P2p
Fa4/48       Desg FWD 200000     128.240 P2p Bound(STP)

##### MST01          vlans mapped: 1-10
Bridge      address 00d0.00b8.1400  priority 49153 (49152 sysid 1)
Root        this switch for MST01

Interface    Role Sts Cost      Prio.Nbr Status
-----
Fa4/4        Back BLK 1000      160.196 P2p
Fa4/5        Desg FWD 200000     128.197 P2p
Fa4/48       Boun FWD 200000     128.240 P2p Bound(STP)

Router#

```

Configuring MST Instance Port Parameters

To configure MST instance port parameters, perform these tasks:

	Command	Purpose
Step 1	Router(config-if)# spanning-tree mst x cost y	Configures the MST instance port cost.
Step 2	Router(config-if)# spanning-tree mst x port-priority y	Configures the MST instance port priority.
Step 3	Router# show spanning-tree mst x interface y	Verifies the configuration.

This example shows how to configure MST instance port parameters:

```
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree mst 1 ?
    cost          Change the interface spanning tree path cost for an instance
    port-priority Change the spanning tree port priority for an instance

Router(config-if)# spanning-tree mst 1 cost 1234567
Router(config-if)# spanning-tree mst 1 port-priority 240
Router(config-if)# ^Z

Router# show spanning-tree mst 1 interface fastEthernet 4/4

FastEthernet4/4 of MST01 is backup blocking
Edge port:no          (default)          port guard :none          (default)
Link type:point-to-point (auto)          bpdu filter:disable      (default)
Boundary :internal    bpdu guard :disable      (default)
Bpdus (MRecords) sent 125, received 1782

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-----
1          Back BLK 1234567  240.196  1-10

Router#
```

Restarting Protocol Migration

A router running both MSTP and RSTP supports a built-in protocol migration mechanism that enables the router to interoperate with legacy 802.1D switches. If this router receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MSTP router can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (version 3) associated with a different region, or an RST BPDU (version 2).

However, the router does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether the legacy router has been removed from the link unless the legacy router is the designated router. A router also might continue to assign a boundary role to a port when the router to which it is connected has joined the region.

To restart the protocol migration process (force the renegotiation with neighboring switches) on the entire router, you can use the **clear spanning-tree detected-protocols** privileged EXEC command. Use the **clear spanning-tree detected-protocols interface *interface-id*** privileged EXEC command to restart the protocol migration process on a specific interface.

This example shows how to restart protocol migration:

```
Router# clear spanning-tree detected-protocols interface fastEthernet 4/4
Router#
```

