Configuring STP and MST

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

Note For complete syntax and usage information for the commands used in this chapter, refer to the Cisco 7600 Series Routers Command References at this URL:

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

This chapter contains these sections:

Note For information on configuring the PortFast, UplinkFast, and BackboneFast STP enhancements, see Chapter 20, "Configuring Optional STP Features."

Understanding How STP Works

These sections describe how STP works:

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

Note   In Cisco 7600 series routers, the extended system ID is always enabled.

The bridge priority is a 4-bit value when the extended system ID is enabled (see Table 19-1 on page 19-3 and the "Configuring the Bridge Priority of a VLAN" section on page 19-33).

Extended System ID

A 12-bit extended system ID field is part of the bridge ID (see Table 19-1 on page 19-3). Cisco 7600 series routers have 64 MAC addresses and always use the 12-bit extended system ID.

Table 19-1   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 routers have 64 addresses available to support software features such as STP. To view the MAC address range, enter the **show catalyst6000 chassis-mac-address** command.

STP uses the extended system ID plus a MAC address to make the bridge ID unique for each VLAN.

With MAC address reduction enabled on any device, you should also enable MAC address reduction on all other Layer 2 connected network devices to avoid undesirable root bridge election and spanning tree topology issues.

When MAC address reduction is enabled, the root bridge priority becomes a multiple of 4096 plus the VLAN ID. With MAC address reduction 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 run the MAC address reduction feature, 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 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 value increases the probability; a lower 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 19-2 describes the STP protocol timers that affect STP performance.

Table 19-2   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 19-1, 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 19-1   Spanning Tree Topology
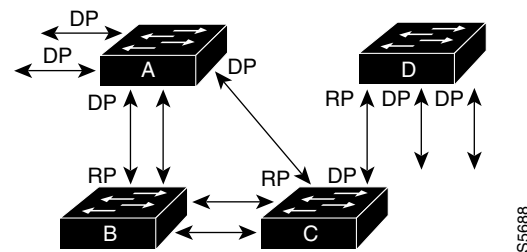
RP = Root Port
DP = Designated Port

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 19-5
- Blocking State, page 19-7
- Listening State, page 19-8
- Learning State, page 19-9
- Forwarding State, page 19-10
- Disabled State, page 19-11

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.

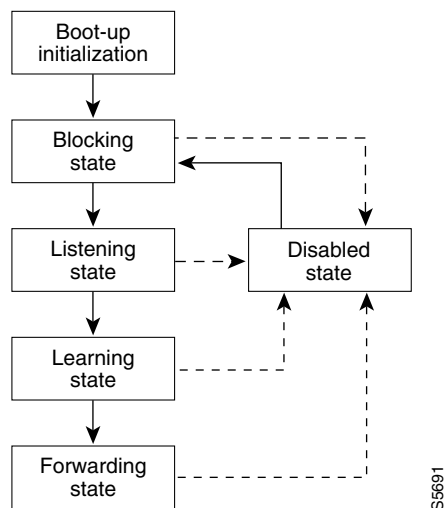Each Layer 2 LAN port on a Cisco 7600 series router using STP exists in one of the following five states:

- 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 19-2 illustrates how a Layer 2 LAN port moves through the five states.

Figure 19-2   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 19-3. 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 19-3   Interface 2 in Blocking State
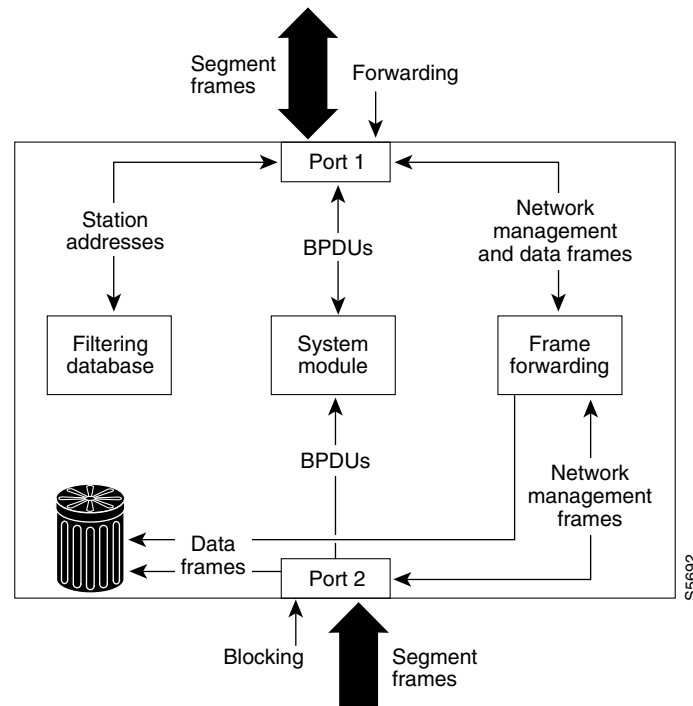
A Layer 2 LAN port in the blocking state performs as follows:

- 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 19-4 shows a Layer 2 LAN port in the listening state.

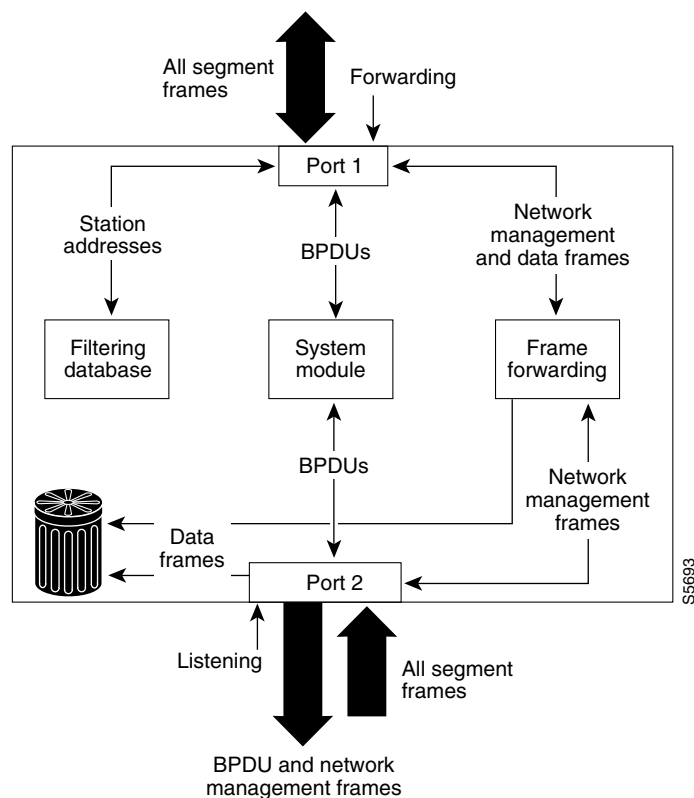*Figure 19-4   Interface 2 in Listening State*

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 19-5 shows a Layer 2 LAN port in the learning state.

Figure 19-5   Interface 2 in Learning State

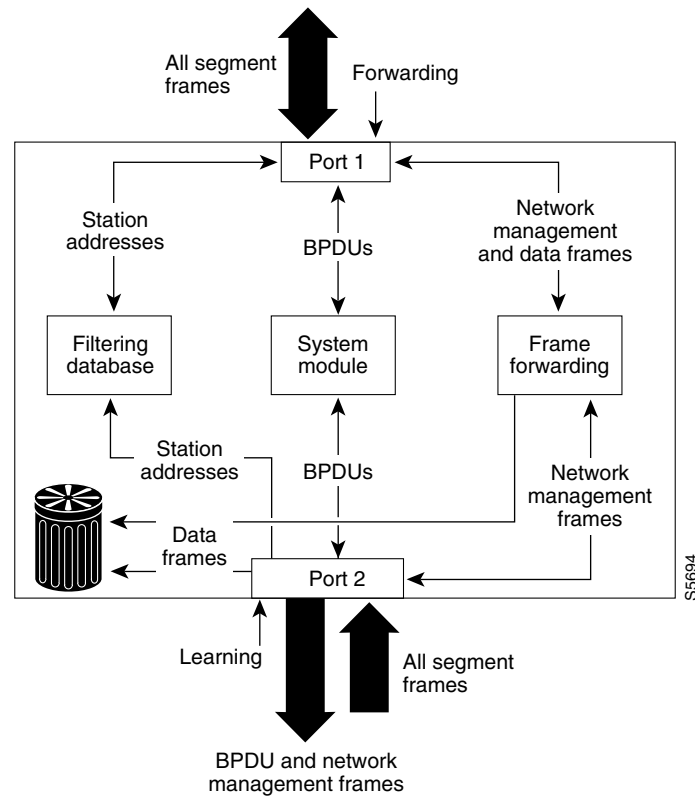

A Layer 2 LAN port in the learning state performs as follows:

- 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 19-6. The Layer 2 LAN port enters the forwarding state from the learning state.

Figure 19-6   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 19-7. A Layer 2 LAN port in the disabled state is virtually nonoperational.

Figure 19-7   Interface 2 in Disabled State

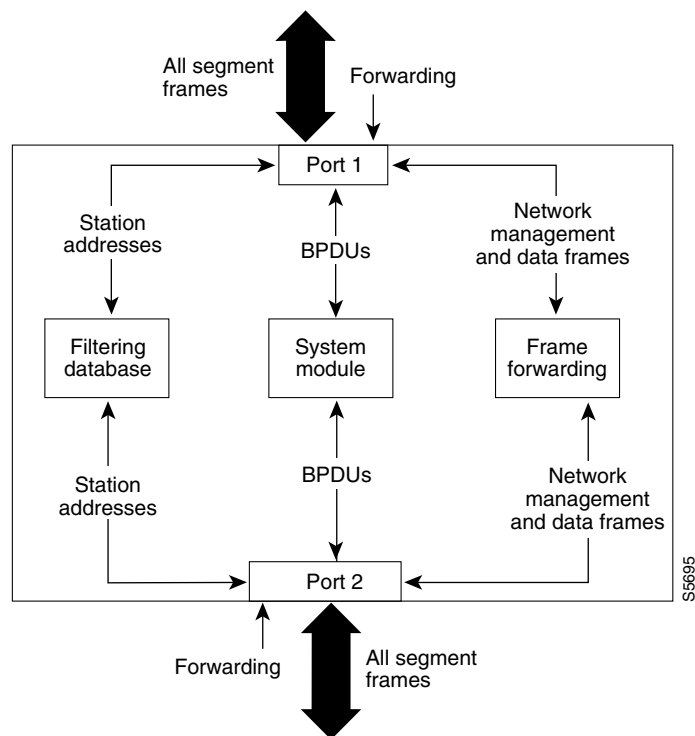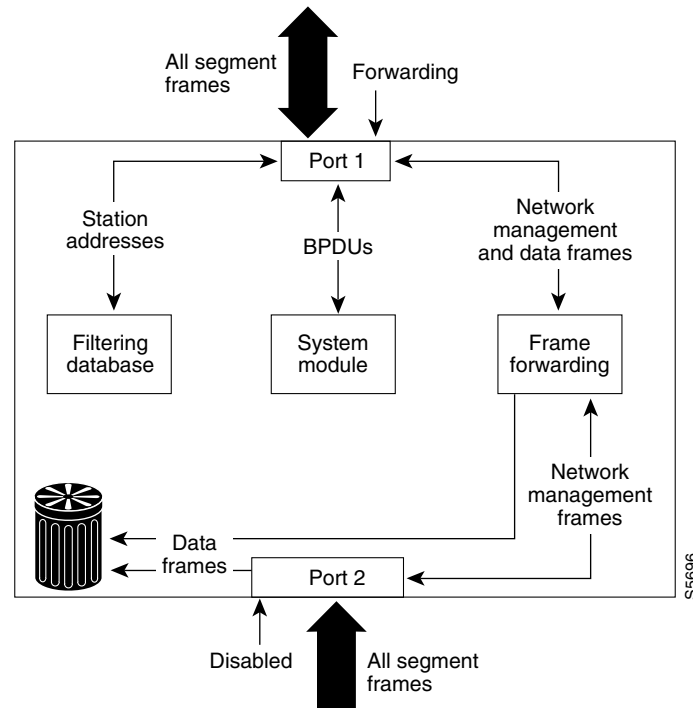A disabled Layer 2 LAN port performs as follows:

- 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

RSTP takes advantage of point-to-point wiring and provides rapid convergence of the spanning tree. Reconfiguration of the spanning tree can occur in less than 1 second (in contrast to 50 seconds with the default settings in the 802.1D spanning tree).

These section describes how the RSTP works:

- Port Roles and the Active Topology, page 19-12
- Rapid Convergence, page 19-13
- Synchronization of Port Roles, page 19-14
- Bridge Protocol Data Unit Format and Processing, page 19-15
- Topology Changes, page 19-17
- Rapid-PVST, page 19-17

Port Roles and the Active Topology

The RSTP provides rapid convergence of the spanning tree by assigning port roles and by learning the active topology. The RSTP builds upon the 802.1D STP to select the router with the highest switch priority (lowest numerical priority value) as the root bridge as described in the "Election of the Root Bridge" section on page 19-4. The RSTP then assigns one of these port roles to individual ports:

- Root port—Provides the best path (lowest cost) when the router forwards packets to the root bridge.
- Designated port—Connects to the designated router, which incurs the lowest path cost when forwarding packets from that LAN to the root bridge. The port through which the designated router is attached to the LAN is called the designated port.
- Alternate port—Offers an alternate path toward the root bridge to that provided by the current root port.
- Backup port—Acts as a backup for the path provided by a designated port toward the leaves of the spanning tree. A backup port can exist only when two ports are connected in a loopback by a point-to-point link or when a router has two or more connections to a shared LAN segment.
- Disabled port—Has no role within the operation of the spanning tree.

A port with the root or a designated port role is included in the active topology. A port with the alternate or backup port role is excluded from the active topology.

In a stable topology with consistent port roles throughout the network, the RSTP ensures that every root port and designated port immediately transition to the forwarding state while all alternate and backup ports are always in the discarding state (equivalent to blocking in 802.1D). The port state controls the operation of the forwarding and learning processes. Table 19-3 provides a comparison of 802.1D and RSTP port states.

Table 19-3   Port State Comparison

Operational Status	STP Port State (IEEE 802.1D)	RSTP Port State	Is Port Included in the Active Topology?
Enabled	Blocking	Discarding	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

To be consistent with Cisco STP implementations, this guide defines the port state as *blocking* instead of *discarding*. Designated ports start in the listening state.

Rapid Convergence

The RSTP provides for rapid recovery of connectivity following the failure of a router, a router port, or a LAN. It provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links as follows:

- Edge ports—If you configure a port as an edge port on an RSTP router by using the **spanning-tree portfast** interface configuration command, the edge port immediately transitions to the forwarding state. An edge port is the same as a Port Fast-enabled port, and you should enable it only on ports that connect to a single end station.

- Root ports—If the RSTP selects a new root port, it blocks the old root port and immediately transitions the new root port to the forwarding state.

- Point-to-point links—If you connect a port to another port through a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology.

  As shown in Figure 19-8, router A is connected to router B through a point-to-point link, and all of the ports are in the blocking state. Assume that the priority of router A is a smaller numerical value than the priority of router B. Router A sends a proposal message (a configuration BPDU with the proposal flag set) to router B, proposing itself as the designated router.

  After receiving the proposal message, router B selects as its new root port the port from which the proposal message was received, forces all nonedge ports to the blocking state, and sends an agreement message (a BPDU with the agreement flag set) through its new root port.

  After receiving router B's agreement message, router A also immediately transitions its designated port to the forwarding state. No loops in the network are formed because router B blocked all of its nonedge ports and because there is a point-to-point link between routers A and B.

  When router C is connected to router B, a similar set of handshaking messages are exchanged. Router C selects the port connected to router B as its root port, and both ends immediately transition to the forwarding state. With each iteration of this handshaking process, one more router joins the active topology. As the network converges, this proposal-agreement handshaking progresses from the root toward the leaves of the spanning tree.

The router learns the link type from the port duplex mode: a full-duplex port is considered to have a point-to-point connection and a half-duplex port is considered to have a shared connection. You can override the default setting that is controlled by the duplex setting by using the **spanning-tree link-type** interface configuration command.

Figure 19-8   Proposal and Agreement Handshaking for Rapid Convergence
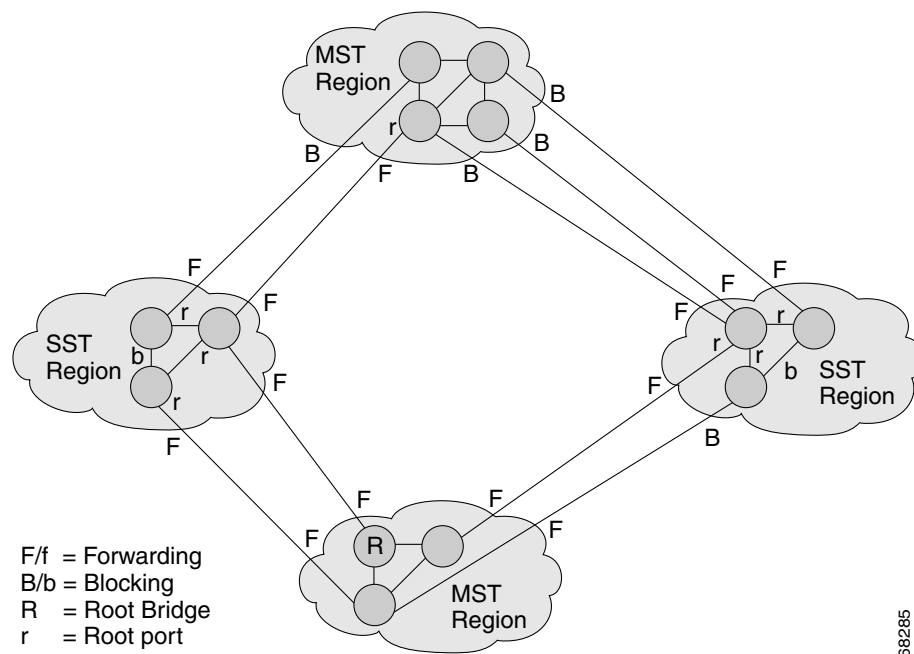
Synchronization of Port Roles

When the router receives a proposal message on one of its ports and that port is selected as the new root port, the RSTP forces all other ports to synchronize with the new root information.

The router is synchronized with superior root information received on the root port if all other ports are synchronized. An individual port on the router is synchronized if:

- That port is in the blocking state.
- It is an edge port (a port configured to be at the edge of the network).

If a designated port is in the forwarding state and is not configured as an edge port, it transitions to the blocking state when the RSTP forces it to synchronize with new root information. In general, when the RSTP forces a port to synchronize with root information and the port does not satisfy any of the above conditions, its port state is set to blocking.

After ensuring that all of the ports are synchronized, the router sends an agreement message to the designated router corresponding to its root port. When the routers connected by a point-to-point link are in agreement about their port roles, the RSTP immediately transitions the port states to forwarding. The sequence of events is shown in Figure 19-9.

Figure 19-9 *Sequence of Events During Rapid Convergence*
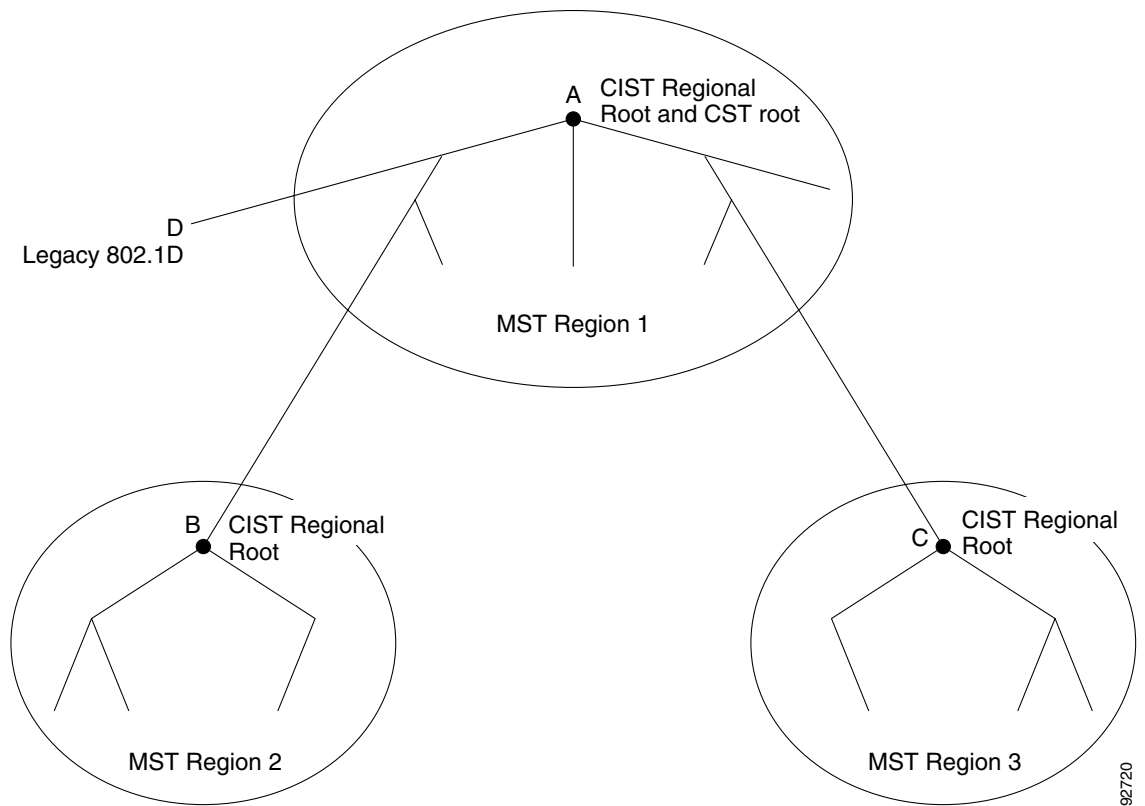
Bridge Protocol Data Unit Format and Processing

These sections describe bridge protocol data unit (BPDU) format and processing:

- BPDU Format and Processing Overview, page 19-15
- Processing Superior BPDU Information, page 19-16
- Processing Inferior BPDU Information, page 19-16

BPDU Format and Processing Overview

The RSTP BPDU format is the same as the 802.1D BPDU format except that the protocol version is set to 2. A new 1-byte Version 1 Length field is set to zero, which means that no Version 1 protocol information is present. Table 19-4 describes the RSTP flag fields.

Table 19-4 *RSTP BPDU Flags*

Bit	Function
0	Topology change (TC)
1	Proposal

Table 19-4   RSTP BPDU Flags (continued)

Bit	Function
2–3:	Port role:
00	Unknown
01	Alternate port or backup port
10	Root port
11	Designated port
4	Learning
5	Forwarding
6	Agreement
7	Topology change acknowledgement (TCA)

The sending router sets the proposal flag in the RSTP BPDU to propose itself as the designated router on that LAN. The port role in the proposal message is always set to the designated port.

The sending router sets the agreement flag in the RSTP BPDU to accept the previous proposal. The port role in the agreement message is always set to the root port.

The RSTP does not have a separate TCN BPDU. It uses the topology change (TC) flag to show the topology changes. However, for interoperability with 802.1D routers, the RSTP router processes and generates TCN BPDUs.

The learning and forwarding flags are set according to the state of the sending port.

Processing Superior BPDU Information

A superior BPDU is a BPDU with root information (such as lower switch ID or lower path cost) that is superior to what is currently stored for the port.

If a port receives a superior BPDU, the RSTP triggers a reconfiguration. If the port is proposed and is selected as the new root port, RSTP forces all the other ports to synchronize.

If the BPDU received is an RSTP BPDU with the proposal flag set, the router sends an agreement message after all of the other ports are synchronized. If the BPDU is an 802.1D BPDU, the router does not set the proposal flag and starts the forward-delay timer for the port. The new root port requires twice the forward-delay time to transition to the forwarding state.

If the superior information received on the port causes the port to become a backup port or an alternate port, RSTP sets the port to the blocking state and sends an agreement message. The designated port continues sending BPDUs with the proposal flag set until the forward-delay timer expires, at which time the port transitions to the forwarding state.

Processing Inferior BPDU Information

An inferior BPDU is a BPDU with root information (such as higher switch ID or higher path cost) that is inferior to what is currently stored for the port.

If a designated port receives an inferior BPDU, it immediately replies with its own information.

Topology Changes

These are the differences between the RSTP and the 802.1D in handling spanning tree topology changes:

- Detection—Unlike 802.1D in which *any* transition between the blocking and the forwarding state causes a topology change, *only* transitions from the blocking to the forwarding state cause a topology change with RSTP (only an increase in connectivity is considered a topology change). State changes on an edge port do not cause a topology change. When an RSTP router detects a topology change, it deletes the learned information on all of its nonedge ports except on those from which it received the TC notification.

- Notification—The RSTP does not use TCN BPDUs, unlike 802.1D. However, for 802.1D interoperability, an RSTP router processes and generates TCN BPDUs.

- Acknowledgement—When an RSTP router receives a TCN message on a designated port from an 802.1D router, it replies with an 802.1D configuration BPDU with the TCA bit set. However, if the TC-while timer (the same as the TC timer in 802.1D) is active on a root port connected to an 802.1D router and a configuration BPDU with the TCA set is received, the TC-while timer is reset.

  This method of operation is only required to support 802.1D routers. The RSTP BPDUs never have the TCA bit set.

- Propagation—When an RSTP router receives a TC message from another router through a designated or root port, it propagates the change to all of its nonedge, designated ports and to the root port (excluding the port on which it is received). The router starts the TC-while timer for all such ports and flushes the information learned on them.

- Protocol migration—For backward compatibility with 802.1D routers, RSTP selectively sends 802.1D configuration BPDUs and TCN BPDUs on a per-port basis.

  When a port is initialized, the migrate-delay timer is started (specifies the minimum time during which RSTP BPDUs are sent), and RSTP BPDUs are sent. While this timer is active, the router processes all BPDUs received on that port and ignores the protocol type.

  If the router receives an 802.1D BPDU after the port migration-delay timer has expired, it assumes that it is connected to an 802.1D router and starts using only 802.1D BPDUs. However, if the RSTP router is using 802.1D BPDUs on a port and receives an RSTP BPDU after the timer has expired, it restarts the timer and starts using RSTP BPDUs on that port.

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 MST

These sections describe MST:

MST Overview

MST maps multiple VLANs into a spanning tree instance, with each instance having a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning tree instances required to support a large number of VLANs. MST improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

The most common initial deployment of MST is in the backbone and distribution layers of a Layer 2 switched network. This deployment provides the kind of highly available network that is required in a service-provider environment.

MST provides rapid spanning tree convergence through explicit handshaking, which eliminates the 802.1D forwarding delay and quickly transitions root bridge ports and designated ports to the forwarding state.

MST improves spanning tree operation and maintains backward compatibility with these STP versions:

- Original 802.1D spanning tree
- Existing Cisco-proprietary Multiple Instance STP (MISTP)
- Existing Cisco per-VLAN spanning tree plus (PVST+)
- Rapid per-VLAN spanning tree plus (rapid PVST+)

For information about other spanning tree features such as Port Fast, UplinkFast, root guard, and so forth, see Chapter 20, "Configuring Optional STP Features."

Note
- IEEE 802.1w defined the Rapid Spanning Tree Protocol (RSTP) and was incorporated into IEEE 802.1D.
- IEEE 802.1s defined MST and was incorporated into IEEE 802.1Q.

MST Regions

For routers to participate in MST instances, you must consistently configure the routers with the same MST configuration information. A collection of interconnected routers that have the same MST configuration comprises an MST region as shown in Figure 19-10 on page 19-21.

The MST configuration controls to which MST region each router belongs. The configuration includes the name of the region, the revision number, and the MST VLAN-to-instance assignment map.

A region can have one or multiple members with the same MST configuration; each member must be capable of processing RSTP bridge protocol data units (BPDUs). There is no limit to the number of MST regions in a network, but each region can support up to 65 spanning tree instances. Instances can be identified by any number in the range from 0 to 4094. You can assign a VLAN to only one spanning tree instance at a time.

IST, CIST, and CST

These sections describe internal spanning tree (IST), common and internal spanning tree (CIST), and common spanning tree (CST):

IST, CIST, and CST Overview

Unlike other spanning tree protocols, in which all the spanning tree instances are independent, MST establishes and maintains IST, CIST, and CST spanning trees:

- An IST is the spanning tree that runs in an MST region.

  Within each MST region, MST maintains multiple spanning tree instances. Instance 0 is a special instance for a region, known as the IST. All other MST instances are numbered from 1 to 4094.

  The IST is the only spanning tree instance that sends and receives BPDUs. All of the other spanning tree instance information is contained in MSTP records (M-records), which are encapsulated within MST BPDUs. Because the MST BPDU carries information for all instances, the number of BPDUs that need to be processed to support multiple spanning tree instances is significantly reduced.

  All MST instances within the same region share the same protocol timers, but each MST instance has its own topology parameters, such as root bridge ID, root path cost, and so forth. By default, all VLANs are assigned to the IST.

  An MST instance is local to the region; for example, MST instance 1 in region A is independent of MST instance 1 in region B, even if regions A and B are interconnected.

- A CIST is a collection of the ISTs in each MST region.

- The CST interconnects the MST regions and single spanning trees.

The spanning tree computed in a region appears as a subtree in the CST that encompasses the entire switched domain. The CIST is formed by the spanning tree algorithm running among routers that support the 802.1w, 802.1s, and 802.1D standards. The CIST inside an MST region is the same as the CST outside a region.

For more information, see the "Spanning Tree Operation Within an MST Region" section on page 19-20 and the "Spanning Tree Operations Between MST Regions" section on page 19-20.

Spanning Tree Operation Within an MST Region

The IST connects all the MST routers in a region. When the IST converges, the root of the IST becomes the CIST regional root (called the *IST master* before the implementation of the 802.1s standard) as shown in Figure 19-10 on page 19-21. The CIST regional root is also the CIST root if there is only one region in the network. If the CIST root is outside the region, one of the MST routers at the boundary of the region is selected as the CIST regional root.

When an MST router initializes, it sends BPDUs that identify itself as the root of the CIST and the CIST regional root, with both of the path costs to the CIST root and to the CIST regional root set to zero. The router also initializes all of its MST instances and claims to be the root for all of them. If the router receives superior MST root information (lower switch ID, lower path cost, and so forth) than currently stored for the port, it relinquishes its claim as the CIST regional root.

During initialization, a region might have many subregions, each with its own CIST regional root. As routers receive superior IST information from a neighbor in the same region, they leave their old subregions and join the new subregion that contains the true CIST regional root, which causes all subregions to shrink except for the one that contains the true CIST regional root.

For correct operation, all routers in the MST region must agree on the same CIST regional root. Therefore, any two routers in the region only synchronize their port roles for an MST instance if they converge to a common CIST regional root.

Spanning Tree Operations Between MST Regions

If there are multiple regions or 802.1D routers within the network, MST establishes and maintains the CST, which includes all MST regions and all 802.1D STP routers in the network. The MST instances combine with the IST at the boundary of the region to become the CST.

The IST connects all the MST routers in the region and appears as a subtree in the CIST that encompasses the entire switched domain. The root of the subtree is the CIST regional root. The MST region appears as a virtual router to adjacent STP routers and MST regions.

Figure 19-10 shows a network with three MST regions and an 802.1D router (D). The CIST regional root for region 1 (A) is also the CIST root. The CIST regional root for region 2 (B) and the CIST regional root for region 3 (C) are the roots for their respective subtrees within the CIST.

Figure 19-10   MST Regions, CIST Regional Roots, and CST Root
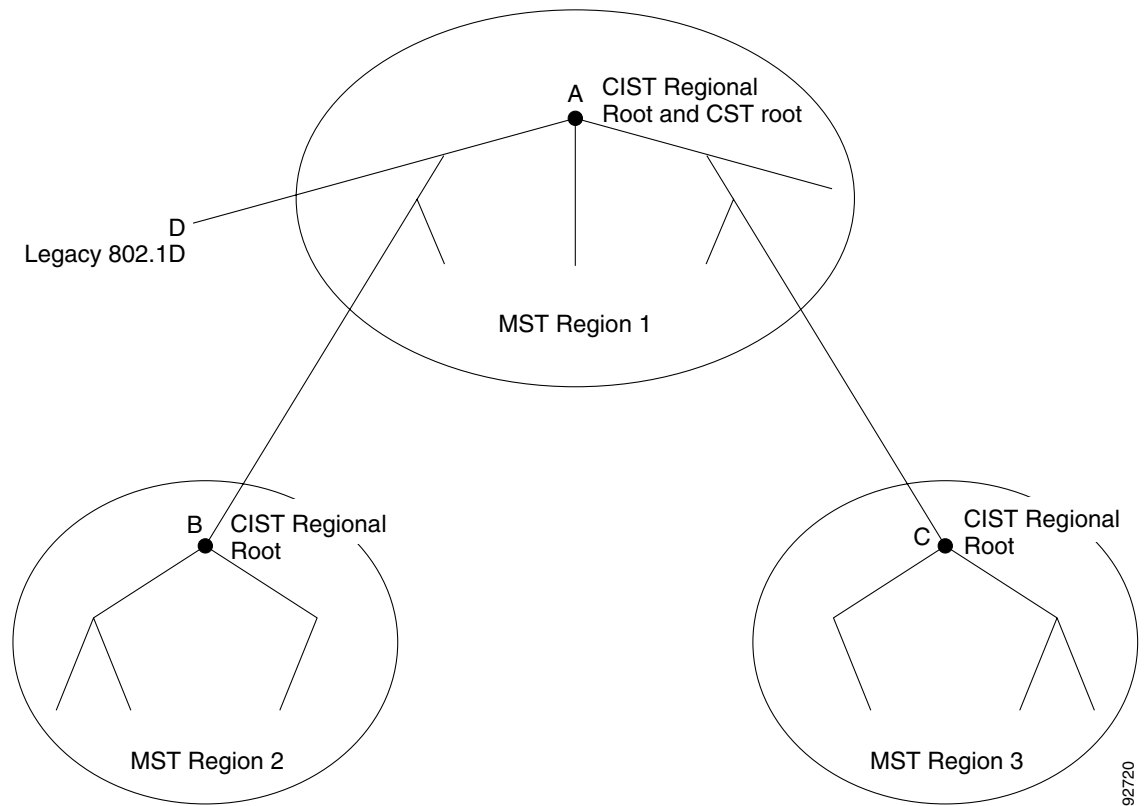
Only the CST instance sends and receives BPDUs, and MST instances add their spanning tree information into the BPDUs to interact with neighboring routers and compute the final spanning tree topology. Because of this, the spanning tree parameters related to BPDU transmission (for example, hello time, forward time, max-age, and max-hops) are configured only on the CST instance but affect all MST instances. Parameters related to the spanning tree topology (for example, switch priority, port VLAN cost, and port VLAN priority) can be configured on both the CST instance and the MST instance.

MST routers use Version 3 BPDUs or 802.1D STP BPDUs to communicate with 802.1D routers. MST routers use MST BPDUs to communicate with MST routers.

IEEE 802.1s Terminology

Some MST naming conventions used in the prestandard implementation have been changed to include identification of some *internal* and *regional* parameters. These parameters are used only within an MST region, compared to external parameters that are used throughout the whole network. Because the CIST is the only spanning tree instance that spans the whole network, only the CIST parameters require the external qualifiers and not the internal or regional qualifiers.

- The CIST root is the root bridge for the the CIST, which is the unique instance that spans the whole network.

- The CIST external root path cost is the cost to the CIST root. This cost is left unchanged within an MST region. Remember that an MST region looks like a single router to the CIST. The CIST external root path cost is the root path cost calculated between these virtual routers and routers that do not belong to any region.

- The CIST regional root was called the IST master in the prestandard implementation. If the CIST root is in the region, the CIST regional root is the CIST root. Otherwise, the CIST regional root is the closest router to the CIST root in the region. The CIST regional root acts as a root bridge for the IST.

- The CIST internal root path cost is the cost to the CIST regional root in a region. This cost is only relevant to the IST, instance 0.

Table 19-5 compares the IEEE standard and the Cisco prestandard terminology.

Table 19-5   Prestandard and Standard Terminology

IEEE Standard Definition	Cisco Prestandard Implementation	Cisco Standard Implementation
CIST regional root	IST master	CIST regional root
CIST internal root path cost	IST master path cost	CIST internal path cost
CIST external root path cost	Root path cost	Root path cost
MSTI regional root	Instance root	Instance root
MSTI internal root path cost	Root path cost	Root path cost

Hop Count

MST does not use the message-age and maximum-age information in the configuration BPDU to compute the spanning tree topology. Instead, they use the path cost to the root and a hop-count mechanism similar to the IP time-to-live (TTL) mechanism.

By using the **spanning-tree mst max-hops** global configuration command, you can configure the maximum hops inside the region and apply it to the IST and all MST instances in that region. The hop count achieves the same result as the message-age information (triggers a reconfiguration). The root bridge of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a router receives this BPDU, it decrements the received remaining hop count by one and propagates this value as the remaining hop count in the BPDUs it generates. When the count reaches zero, the router discards the BPDU and ages the information held for the port.

The message-age and maximum-age information in the RSTP portion of the BPDU remain the same throughout the region, and the same values are propagated by the region-designated ports at the boundary.

Boundary Ports

In the Cisco prestandard implementation, a boundary port connects an MST region to one of these STP regions:

- A single spanning tree region running RSTP

- A single spanning tree region running PVST+ or rapid PVST+

- Another MST region with a different MST configuration

A boundary port also connects to a LAN, the designated router of which is either a single spanning tree router or a router with a different MST configuration.

There is no definition of a boundary port in the 802.1s standard. The 802.1Q-2002 standard identifies two kinds of messages that a port can receive: internal (coming from the same region) and external. When a message is external, it is received only by the CIST. If the CIST role is root or alternate, or if the external BPDU is a topology change, it could have an impact on the MST instances. When a message

is internal, the CIST part is received by the CIST, and each MST instance receives its respective M-record. The Cisco prestandard implementation treats a port that receives an external message as a boundary port, which means a port cannot receive a mix of internal and external messages.

An MST region includes both routers and LANs. A segment belongs to the region of its designated port. Therefore, a port in a different region from the designated port for a segment is a boundary port. This definition allows two ports internal to a region to share a segment with a port belonging to a different region, creating the possibility of receiving both internal and external messages on a port.

The primary change from the Cisco prestandard implementation is that a designated port is not defined as boundary unless it is running in an STP-compatible mode.

Note   If there is an 802.1D STP router on the segment, messages are always considered external.

The other change from the prestandard implementation is that the CIST regional root bridge ID field is now inserted where an RSTP or legacy 802.1s router has the sender switch ID. The whole region performs like a single virtual router by sending a consistent sender switch ID to neighboring routers. In this example, router C would receive a BPDU with the same consistent sender switch ID of root, whether or not A or B is designated for the segment.

Standard-Compliant MST Implementation

The standard-compliant MST implementation includes features required to meet the standard, as well as some of the desirable prestandard functionality that is not yet incorporated into the published standard. These sections describe the standard-compliant MST implementation:

Changes in Port-Role Naming

The boundary role was deleted from the final MST standard, but this boundary concept is maintained in the standard-compliant implementation. However, an MST instance (MSTI) port at a boundary of the region might not follow the state of the corresponding CIST port. The following two situations currently exist:

- The boundary port is the root port of the CIST regional root—When the CIST instance port is proposed and is synchronized, it can send back an agreement and move to the forwarding state only after all the corresponding MSTI ports are synchronized (and thus forwarding). The MSTI ports now have a special *master* role.

- The boundary port is not the root port of the CIST regional root—The MSTI ports follow the state and role of the CIST port. The standard provides less information, and it might be difficult to understand why an MSTI port can be alternately blocking when it receives no BPDUs (M-records). In this situation, although the boundary role no longer exists, when you enter the **show** commands, they identify a port as boundary in the *type* column of the output.

Spanning Tree Interoperation Between Legacy and Standard-Compliant Routers

Because automatic detection of prestandard routers can fail, you can use an interface configuration command to identify prestandard ports. A region cannot be formed between a standard and a prestandard router, but they can interoperate before using the CIST. Only the capability of load balancing over different instances is lost in this specific situation. The CLI displays different flags depending on the port configuration when the port receives prestandard BPDUs. A syslog message also appears the first time a router receives a prestandard BPDU on a port that has not been configured for prestandard BPDU transmission.

Figure 19-11 illustrates a standard-compliant router connected to a prestandard router. Assume that A is the standard-compliant router and B is a prestandard router, both configured to be in the same region. A is the root bridge for the CIST, and so B has a root port (BX) on segment X and an alternate port (BY) on segment Y. If segment Y flaps, and the port on BY becomes the alternate before sending out a single prestandard BPDU, AY cannot detect that a prestandard router is connected to Y and continues to send standard BPDUs. The port BY is fixed in a boundary, and no load balancing is possible between A and B. The same problem exists on segment X, but B might transmit topology changes.

Figure 19-11   Standard-Compliant and Prestandard Router Interoperation
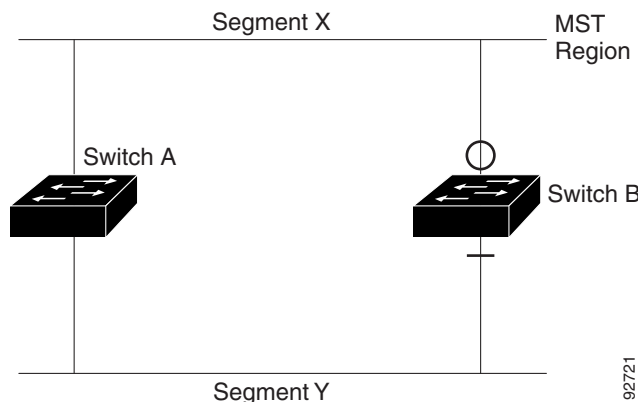
Note   We recommend that you minimize the interaction between standard and prestandard MST implementations.

Detecting Unidirectional Link Failure

This feature is not yet present in the IEEE MST standard, but it is included in the standard-compliant implemtation. The software checks the consistency of the port role and state in the received BPDUs to detect unidirectional link failures that could cause bridging loops.

When a designated port detects a conflict, it keeps its role, but reverts to a discarding state because disrupting connectivity in case of inconsistency is preferable to opening a bridging loop.

Figure 19-12 illustrates a unidirectional link failure that typically creates a bridging loop. Router A is the root bridge, and its BPDUs are lost on the link leading to router B. RSTP and MST BPDUs include the role and state of the sending port. With this information, router A can detect that router B does not react to the superior BPDUs it sends and that router B is the designated, not root bridge. As a result, router A blocks (or keeps blocking) its port, thus preventing the bridging loop.

Figure 19-12   Detecting Unidirectional Link Failure
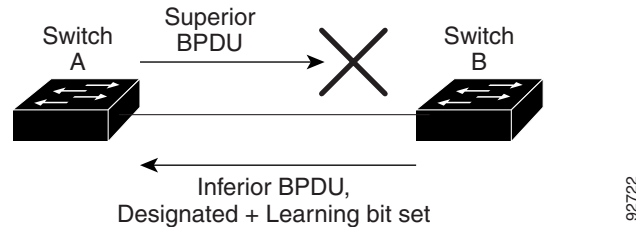
Interoperability with IEEE 802.1D-1998 STP

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

However, the router does not automatically revert to the MST mode if it no longer receives 802.1D BPDUs because it cannot detect whether the 802.1D router has been removed from the link unless the 802.1D router is the designated router. A router might also continue to assign a boundary role to a port when the router to which this router is connected has joined the region. To restart the protocol migration process (force the renegotiation with neighboring routers), use the **clear spanning-tree detected-protocols** privileged EXEC command.

If all the 802.1D routers on the link are RSTP routers, they can process MST BPDUs as if they are RSTP BPDUs. Therefore, MST routers send either a Version 0 configuration and topology change notification (TCN) BPDUs or Version 3 MST BPDUs on a boundary port. A boundary port connects to a LAN, the designated router of which is either a single spanning tree router or a router with a different MST configuration.

Configuring STP

These sections describe how to configure STP on VLANs:

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.

Default STP Configuration

Table 19-6 shows the default STP configuration.

Table 19-6   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)	• 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)	• Gigabit Ethernet: 4 • Fast Ethernet: 19 • Ethernet: 100
Hello time	2 seconds
Forward delay time	15 seconds
Maximum aging time	20 seconds
Mode	PVST

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** *vlan_ID*	Enables STP on a per-VLAN basis. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 19-6 on page 19-26).
	Router(config)# **default spanning-tree vlan** *vlan_ID*	Reverts all STP parameters to default values for the specified VLAN.
	Router(config)# **no spanning-tree vlan** *vlan_ID*	Disables STP on the specified VLAN; see the following Cautions for information regarding this command.
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show spanning-tree vlan** *vlan_ID*	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
---------------- ---- --- --------- -------- --------------------------------
Gi1/4            Desg FWD 200000    128.196  P2p
Gi1/5            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

The extended system ID is enabled permanently on Cisco 7600 series routers. 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 lowest 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. With the extended system ID 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.

With the extended system ID enabled, 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 19-1 on page 19-3.)

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

With the extended system ID enabled, 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** *vlan_ID* **root primary** [**diameter** *hops* [**hello-time** *seconds*]]	Configures a Cisco 7600 series router as the root bridge. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 19-6 on page 19-26).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **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).

With the extended system ID is enabled, STP sets the bridge priority to 28672.

You can run this command on more than one 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** *vlan_ID* **root secondary** [**diameter** *hops* [**hello-time** *seconds*]]	Configures a Cisco 7600 series router as the secondary root bridge. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **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.

Cisco IOS uses the port priority value when the LAN port is configured as an access port and uses VLAN port priority values when the LAN port is configured as a trunk port.

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

	Command	Purpose
Step 1	Router(config)# **interface** {{**gigabitethernet 1**/*port*} | {**port-channel** *port_channel_number*}}	Selects an interface to configure.
Step 2	Router(config-if)# **spanning-tree port-priority** *port_priority*	Configures the port priority for the LAN interface. The *port_priority* value can be from 1 to 252 in increments of 4.
	Router(config-if)# **no spanning-tree port-priority**	Reverts to the default port priority value.
Step 3	Router(config-if)# **spanning-tree vlan** *vlan_ID* **port-priority** *port_priority*	Configures the VLAN port priority for the LAN interface. The *port_priority* value can be from 1 to 252 in increments of 4. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
	Router(config-if)# [**no**] **spanning-tree vlan** *vlan_ID* **port-priority**	Reverts to the default VLAN port priority value.
Step 4	Router(config-if)# **end**	Exits configuration mode.

	Command	Purpose
Step 5	Router# **show spanning-tree interface** {**gigabitethernet 1**/*port*}	{**port-channel** *port_channel_number*} Router# **show spanning-tree vlan** *vlan_ID*	Verifies the configuration.

This example shows how to configure the STP port priority of Gigabit Ethernet port 1/4:

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/4
Router(config-if)# spanning-tree port-priority 160
Router(config-if)# end
Router#
```

This example shows how to verify the configuration of Gigabit Ethernet port 1/4:

```
Router# show spanning-tree interface gigabitethernet 1/4
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#
```

Gigabit Ethernet port 1/4 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 Gigabit Ethernet port 1/4:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/4
Router(config-if)# spanning-tree vlan 200 port-priority 64
Router(config-if)# end
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 gigabitethernet 1/4
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 gigabitethernet 1/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Gi1/4            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** {{**gigabitethernet 1**/*port*} | {**port-channel** *port_channel_number*}}	Selects an interface to configure.
Step 2	Router(config-if)# **spanning-tree cost** *port_cost*	Configures the port cost for the LAN interface. The *port_cost* value can be from 1 to 200000000.
	Router(config-if)# **no spanning-tree cost**	Reverts to the default port cost.
Step 3	Router(config-if)# **spanning-tree vlan** *vlan_ID* **cost** *port_cost*	Configures the VLAN port cost for the LAN interface. The *port_cost* value can be from 1 to 200000000. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
	Router(config-if)# **no spanning-tree vlan** *vlan_ID* **cost**	Reverts to the default VLAN port cost.
Step 4	Router(config-if)# **end**	Exits configuration mode.
Step 5	Router# **show spanning-tree interface** {**gigabitethernet 1**/*port*} | {**port-channel** *port_channel_number*} **show spanning-tree vlan** *vlan_ID*	Verifies the configuration.

This example shows how to change the STP port cost of Gigabit Ethernet port 1/4:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/4
Router(config-if)# spanning-tree cost 1000
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree interface gigabitethernet 1/4
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 gigabitethernet 1/4
Router(config-if)# spanning-tree vlan 200 cost 2000
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 interface gigabitethernet 1/4
Interface       Role Sts Cost       Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Gi1/4           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 gigabitethernet 1/4
Interface       Role Sts Cost       Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Gi1/4           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, perform this task:

	Command	Purpose
Step 1	Router(config)# **spanning-tree vlan** *vlan_ID* **priority** {**0** | **4096** | **8192** | **12288** | **16384** | **20480** | **24576** | **28672** | **32768** | **36864** | **40960** | **45056** | **49152** | **53248** | **57344** | **61440**}	Configures the bridge priority of a VLAN when the extended system ID is enabled. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **priority**	Reverts to the default bridge priority value.
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show spanning-tree vlan** *vlan_ID* **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 32768
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          32768 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** *vlan_ID* **hello-time** *hello_time*	Configures the hello time of a VLAN. The *hello_time* value can be from 1 to 10 seconds. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **hello-time**	Reverts to the default hello time.
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show spanning-tree vlan** *vlan_ID* **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** *vlan_ID* **forward-time** *forward_time*	Configures the forward time of a VLAN. The *forward_time* value can be from 4 to 30 seconds. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **forward-time**	Reverts to the default forward time.
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show spanning-tree vlan** *vlan_ID* **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
                                Hello Max  Fwd
Vlan               Bridge ID    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** *vlan_ID* **max-age** *max_age*	Configures the maximum aging time of a VLAN. The *max_age* value can be from 6 to 40 seconds. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 14-1 on page 14-2).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **max-age**	Reverts to the default maximum aging time.
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show spanning-tree vlan** *vlan_ID* **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
                                Hello Max  Fwd
Vlan                Bridge ID   Time Age  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 19-25.

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 MST

These sections describe how to configure MST:

Default MST Configuration

Table 19-7 shows the default MST configuration.

Table 19-7   Default MST Configuration

Feature	Default Setting
spanning tree mode	PVST+ (Rapid PVST+ and MST are disabled)
Switch priority (configurable on a per-CIST port basis)	32768
spanning tree port priority (configurable on a per-CIST port basis)	128
spanning tree port cost (configurable on a per-CIST port basis)	1000 Mbps: 4 100 Mbps: 19 10 Mbps: 100
Hello time	2 seconds
Forward-delay time	15 seconds
Maximum-aging time	20 seconds
Maximum hop count	20 hops

MST Configuration Guidelines and Restrictions

When configuring MST, follow these guidelines and restrictions:

- The 802.1s MST standard allows up to 65 MST instances. You can map an unlimited number of VLANs to an MST instance.

- PVST+, rapid PVST+, and MST are supported, but only one version can be active at any time.

- VTP does not propagate the MST configuration. You must manually configure the MST configuration (region name, revision number, and VLAN-to-instance mapping) on each router within the MST region through the command-line interface (CLI) or SNMP.

- For load balancing across redundant paths in the network to work, all VLAN-to-instance mapping assignments must match; otherwise, all traffic flows on a single link.

- All MST boundary ports must be forwarding for load balancing between a PVST+ and an MST cloud or between a rapid-PVST+ and an MST cloud. For this to occur, the CIST regional root of the MST cloud must be the root of the CST. If the MST cloud consists of multiple MST regions, one of the MST regions must contain the CST root, and all of the other MST regions must have a better path to the root contained within the MST cloud than a path through the PVST+ or rapid-PVST+ cloud.

- Partitioning the network into a large number of regions is not recommended. However, if this situation is unavoidable, we recommend that you partition the switched LAN into smaller LANs interconnected by non-Layer 2 devices.

Specifying the MST Region Configuration and Enabling MST

For two or more routers to be in the same MST region, they must have the same VLAN-to-instance mapping, the same configuration revision number, and the same MST name.

A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, but each region can only support up to 65 spanning tree instances. You can assign a VLAN to only one spanning tree instance at a time.

To specify the MST region configuration and enable MST, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **spanning-tree mst configuration**	Enters MST configuration mode.
Step 3	Router(config-mst)# **instance** *instance_id* **vlan** *vlan_range*	Maps VLANs to an MST instance. • For *instance_id*, the range is 0 to 4094. • For **vlan** *vlan_range*, the range is 1 to 4094. When you map VLANs to an MST instance, the mapping is incremental, and the VLANs specified in the command are added to or removed from the VLANs that were previously mapped. To specify a VLAN range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 through 63 to MST instance 1. To specify a VLAN series, use a comma; for example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.
Step 4	Router(config-mst)# **name** *instance_name*	Specifies the instance name. The *name* string has a maximum length of 32 characters and is case sensitive.
Step 5	Router(config-mst)# **revision** *version*	Specifies the configuration revision number. The range is 0 to 65535.
Step 6	Router(config-mst)# **show pending**	Verifies your configuration by displaying the pending configuration.
Step 7	Router(config)# **exit**	Applies all changes, and return to global configuration mode.
Step 8	Router(config)# **spanning-tree mode mst**	Enables MST and RSTP. ⚠ **Caution** Changing the spanning tree mode can disrupt traffic because all spanning tree instances are stopped for the previous mode and restarted in the new mode. You cannot run both MST and PVST+ or both MST and rapid PVST+ at the same time.
Step 9	Router(config)# **end**	Returns to privileged EXEC mode.

…

Command	Purpose
Step 10 Router# **show running-config**	Verifies your entries.
Step 11 Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return to defaults, do the following:

- To return to the default MST region configuration, use the **no spanning-tree mst configuration** global configuration command.

- To return to the default VLAN-to-instance map, use the **no instance** *instance_id* [**vlan** *vlan_range*] MST configuration command.

- To return to the default name, use the **no name** MST configuration command.

- To return to the default revision number, use the **no revision** MST configuration command.

- To reenable PVST+, use the **no spanning-tree mode** or the **spanning-tree mode pvst** global configuration command.

This example shows how to enter MST configuration mode, map VLANs 10 to 20 to MST instance 1, name the region *region1*, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 10-20
Router(config-mst)# name region1
Router(config-mst)# revision 1
Router(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instances configured 2
Instance  Vlans Mapped
--------  --------------------
0         1-9,21-4094
1         10-20
-------------------------------

Router(config-mst)# exit
Router(config)#
```

Configuring the Root Bridge

The router maintains a spanning tree instance for the group of VLANs mapped to it. A switch ID, consisting of the switch priority and the router MAC address, is associated with each instance. For a group of VLANs, the router with the lowest switch ID becomes the root bridge.

To configure a router to become the root bridge, use the **spanning-tree mst** *instance_id* **root** global configuration command to modify the switch priority from the default value (32768) to a significantly lower value so that the router becomes the root bridge for the specified spanning tree instance. When you enter this command, the router checks the switch priorities of the root bridges. Because of extended system ID support, the router sets its own priority for the specified instance to 24576 if this value will cause this router to become the root bridge for the specified spanning tree instance.

If any root bridge for the specified instance has a switch priority lower than 24576, the router sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value as shown in .)

If your network consists of routers that both do and do not support the extended system ID, it is unlikely that the router with the extended system ID support will become the root bridge. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected routers running older software.

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

Use the **diameter** keyword, which is available only for MST instance 0, to specify the Layer 2 network diameter (that is, the maximum number of Layer 2 hops between any two end stations in the Layer 2 network). When you specify the network diameter, the router automatically sets an optimal hello time, forward-delay time, and maximum-age time for a network of that diameter, which can significantly reduce the convergence time. You can use the **hello** keyword to override the automatically calculated hello time.

> **Note** With the router configured as the root bridge, do not manually configure the hello time, forward-delay time, and maximum-age time with the **spanning-tree mst hello-time**, **spanning-tree mst forward-time**, and **spanning-tree mst max-age** global configuration commands.

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

	Command	**Purpose**
Step 1	Router(config)# **configure terminal**	Enters global configuration mode.
Step 2	Router(config-config)# **spanning-tree mst** *instance_id* **root primary** [**diameter** *net_diameter* [**hello-time** *seconds*]]	(Optional) Configures a router as the root bridge. • For *instance_id*, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. • (Optional) For **diameter** *net_diameter*, specify the maximum number of Layer 2 hops between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0. • (Optional) For **hello-time** *seconds*, specify the interval in seconds between the generation of configuration messages by the root bridge. The range is 1 to 10 seconds; the default is 2 seconds.
Step 3	Router(config-config)# **end**	Returns to privileged EXEC mode.
Step 4	Router# **show spanning-tree mst** *instance_id*	Verifies your entries.
Step 5	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return the router to its default setting, use the **no spanning-tree mst** *instance_id* **root** global configuration command.

Configuring a Secondary Root Bridge

When you configure a router with the extended system ID support as the secondary root, the switch priority is modified from the default value (32768) to 28672. The router is then likely to become the root bridge for the specified instance if the primary root bridge fails. This is assuming that the other network routers use the default switch priority of 32768 and therefore are unlikely to become the root bridge.

You can execute this command on more than one router to configure multiple backup root bridges. Use the same network diameter and hello-time values that you used when you configured the primary root bridge with the **spanning-tree mst** *instance_id* **root primary** global configuration command.

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

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **spanning-tree mst** *instance_id* **root secondary** [**diameter** *net_diameter* [**hello-time** *seconds*]]	(Optional) Configures a router as the secondary root bridge. • For *instance_id*, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. • (Optional) For **diameter** *net_diameter*, specify the maximum number of routers between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0. • (Optional) For **hello-time** *seconds*, specify the interval in seconds between the generation of configuration messages by the root bridge. The range is 1 to 10 seconds; the default is 2 seconds. Use the same network diameter and hello-time values that you used when configuring the primary root bridge. See the "Configuring the Root Bridge" section on page 19-40.
Step 3	Router(config)# **end**	Returns to privileged EXEC mode.
Step 4	Router# **show spanning-tree mst** *instance_id*	Verifies your entries.
Step 5	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return the router to its default setting, use the **no spanning-tree mst** *instance_id* **root** global configuration command.

Configuring Port Priority

If a loop occurs, MST uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, MST puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

To configure the MST port priority of an interface, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **interface** {{**gigabitethernet 1**/*port*} | {**port-channel** *number*}}	(Optional) Specifies an interface to configure, and enters interface configuration mode.
Step 3	Router(config-if)# **spanning-tree mst** *instance_id* **port-priority** *priority*	Configures the port priority. • For *instance_id*, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. • For *priority*, the range is 0 to 240 in increments of 16. The default is 128. The lower the number, the higher the priority. The priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected.
Step 4	Router(config-if)# **end**	Returns to privileged EXEC mode.
Step 5	Router# **show spanning-tree mst interface** *interface_id* or Router# **show spanning-tree mst** *instance_id*	Verifies your entries.
Step 6	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

> **Note** The **show spanning-tree mst interface** *interface_id* privileged EXEC command displays information only if the port is in a link-up operative state. Otherwise, you can use the **show running-config interface** privileged EXEC command to confirm the configuration.

To return the interface to its default setting, use the **no spanning-tree mst** *instance_id* **port-priority** interface configuration command.

Configuring Path Cost

The MST path cost default value is derived from the media speed of an interface. If a loop occurs, MST uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, MST puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

To configure the MST cost of an interface, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **interface** {{**gigabitethernet 1**/*port*}	{**port-channel** *number*}}	(Optional) Specifies an interface to configure, and enters interface configuration mode.
Step 3	Router(config-if)# **spanning-tree mst** *instance_id* **cost** *cost*	Configures the cost. If a loop occurs, MST uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission. • For *instance_id*, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. • For *cost*, the range is 1 to 200000000; the default value is derived from the media speed of the interface.
Step 4	Router(config-if)# **end**	Returns to privileged EXEC mode.
Step 5	Router# **show spanning-tree mst interface** *interface_id* or Router# **show spanning-tree mst** *instance_id*	Verifies your entries.
Step 6	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

> **Note** The **show spanning-tree mst interface** *interface_id* privileged EXEC command displays information only for ports that are in a link-up operative state. Otherwise, you can use the **show running-config** privileged EXEC command to confirm the configuration.

To return the interface to its default setting, use the **no spanning-tree mst** *instance_id* **cost** interface configuration command.

Configuring the Switch Priority

You can configure the switch priority so that it is more likely that a router is chosen as the root bridge.

> **Note** Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree mst** *instance_id* **root primary** and the **spanning-tree mst** *instance_id* **root secondary** global configuration commands to modify the switch priority.

To configure the switch priority, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **spanning-tree mst** *instance_id* **priority** *priority*	(Optional) Configures the switch priority. • For *instance_id*, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. • For *priority*, the range is 0 to 61440 in increments of 4096; the default is 32768. The lower the number, the more likely the router will be chosen as the root bridge. Priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
Step 3	Router(config)# **end**	Returns to privileged EXEC mode.
Step 4	Router# **show spanning-tree mst** *instance_id*	Verifies your entries.
Step 5	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return the router to its default setting, use the **no spanning-tree mst** *instance_id* **priority** global configuration command.

Configuring the Hello Time

You can configure the interval between the generation of configuration messages by the root bridge by changing the hello time.

> **Note** Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree mst** *instance_id* **root primary** and the **spanning-tree mst** *instance_id* **root secondary** global configuration commands to modify the hello time.

To configure the hello time for all MST instances, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **spanning-tree mst hello-time** *seconds*	(Optional) Configures the hello time for all MST instances. The hello time is the interval between the generation of configuration messages by the root bridge. These messages mean that the router is alive. For *seconds*, the range is 1 to 10; the default is 2.
Step 3	**end**	Returns to privileged EXEC mode.

	Command	Purpose
Step 4	Router# **show spanning-tree mst**	Verifies your entries.
Step 5	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return the router to its default setting, use the **no spanning-tree mst hello-time** global configuration command.

Configuring the Forwarding-Delay Time

To configure the forwarding-delay time for all MST instances, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **spanning-tree mst forward-time** *seconds*	(Optional) Configures the forward time for all MST instances. The forward delay is the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state. For *seconds*, the range is 4 to 30; the default is 15.
Step 3	Router(config)# **end**	Returns to privileged EXEC mode.
Step 4	Router# **show spanning-tree mst**	Verifies your entries.
Step 5	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return the router to its default setting, use the **no spanning-tree mst forward-time** global configuration command.

Configuring the Transmit Hold Count

To configure the transmit hold count for all MST instances, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **spanning-tree transmit hold-count** *hold_count_value*	Configures the transmit hold count for all MST instances. For *hold_count_value*, the range is 1 to 20; the default is 6.
Step 3	Router(config)# **end**	Returns to privileged EXEC mode.
Step 4	Router# **show spanning-tree mst**	Verifies your entries.
Step 5	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return the router to its default setting, use the **no spanning-tree transmit hold-count** global configuration command.

Configuring the Maximum-Aging Time

To configure the maximum-aging time for all MST instances, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **spanning-tree mst max-age** *seconds*	(Optional) Configures the maximum-aging time for all MST instances. The maximum-aging time is the number of seconds a router waits without receiving spanning-tree configuration messages before attempting a reconfiguration.
		For *seconds*, the range is 6 to 40; the default is 20.
Step 3	Router(config)# **end**	Returns to privileged EXEC mode.
Step 4	Router# **show spanning-tree mst**	Verifies your entries.
Step 5	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return the router to its default setting, use the **no spanning-tree mst max-age** global configuration command.

Configuring the Maximum-Hop Count

To configure the maximum-hop count for all MST instances, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **spanning-tree mst max-hops** *hop_count*	(Optional) Specifies the number of hops in a region before the BPDU is discarded, and the information held for a port is aged.
		For *hop_count*, the range is 1 to 255; the default is 20.
Step 3	Router(config)# **end**	Returns to privileged EXEC mode.
Step 4	Router# **show spanning-tree mst**	Verifies your entries.
Step 5	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return the router to its default setting, use the **no spanning-tree mst max-hops** global configuration command.

Specifying the Link Type to Ensure Rapid Transitions

If you connect a port to another port through a point-to-point link and the local port becomes a designated port, the RSTP negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology as described in the "Rapid Convergence" section on page 19-13.

By default, the link type is controlled from the duplex mode of the interface: a full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection. If you have a half-duplex link physically connected point-to-point to a single port on a remote router running MST, you can override the default setting of the link type and enable rapid transitions to the forwarding state.

To override the default link-type setting, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **interface** {{**gigabitethernet 1**/*port*}	{**port-channel** *number*}}	(Optional) Specifies an interface to configure, and enters interface configuration mode.
Step 3	Router(config)# **spanning-tree link-type point-to-point**	Specifies that the link type of a port is point-to-point.
Step 4	Router(config)# **end**	Returns to privileged EXEC mode.
Step 5	Router# **show spanning-tree mst interface** *interface_id*	Verifies your entries.
Step 6	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return the port to its default setting, use the **no spanning-tree link-type** interface configuration command.

Designating the Neighbor Type

A topology could contain both prestandard and 802.1s standard compliant devices. By default, ports can automatically detect prestandard devices, but they can still receive both standard and prestandard BPDUs. When there is a mismatch between a device and its neighbor, only the CIST runs on the interface.

You can choose to set a port to send only prestandard BPDUs. The prestandard flag appears in all the **show** commands, even if the port is in STP compatibility mode.

To override the default link-type setting, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **interface** {{**gigabitethernet 1**/*port*}	{**port-channel** *number*}}	(Optional) Specifies an interface to configure, and enters interface configuration mode.
Step 3	Router(config)# **spanning-tree mst pre-standard**	Specifies that the port can send only prestandard BPDUs.
Step 4	Router(config)# **end**	Returns to privileged EXEC mode.
Step 5	Router# **show spanning-tree mst interface** *interface_id*	Verifies your entries.
Step 6	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return the port to its default setting, use the **no spanning-tree mst prestandard** interface configuration command.

Restarting the Protocol Migration Process

A router running MST supports a built-in protocol migration feature that enables it to interoperate with 802.1D routers. If this router receives an 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MST router also can detect that a port is at the boundary of a region when it receives an 802.1D 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 MST mode if it no longer receives 802.1D BPDUs because it cannot detect whether the 802.1D router has been removed from the link unless the 802.1D 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 routers) on the router, use the **clear spanning-tree detected-protocols** privileged EXEC command.

To restart the protocol migration process on a specific interface, use the **clear spanning-tree detected-protocols interface** *interface_id* privileged EXEC command.

Displaying the MST Configuration and Status

To display the spanning-tree status, use one or more of the privileged EXEC commands that are described in Table 19-8.

Table 19-8   Commands for Displaying MST Status

Command	Purpose
`show spanning-tree mst configuration`	Displays the MST region configuration.
`show spanning-tree mst configuration digest`	Displays the MD5 digest included in the current MSTCI.
`show spanning-tree mst` *instance_id*	Displays MST information for the specified instance.
`show spanning-tree mst interface` *interface_id*	Displays MST information for the specified interface.