



## Configuring Spanning Tree

---

This chapter describes how to configure spanning tree on the Catalyst enterprise LAN switches.



**Note**

---

For information on configuring the PortFast, UplinkFast, and BackboneFast spanning tree enhancements, see [Chapter 9, “Configuring Spanning Tree PortFast, UplinkFast, and BackboneFast.”](#)

---



**Note**

---

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 5000 Family Command Reference*.

---

This chapter consists of these sections:

- [Understanding How Spanning Tree Works, page 8-1](#)
- [Default Spanning Tree Configuration, page 8-12](#)
- [Configuring Spanning Tree, page 8-12](#)
- [Understanding How BPDU Skewing Works, page 8-23](#)
- [Configuring Spanning Tree BPDU Skewing, page 8-24](#)

## Understanding How Spanning Tree Works

These sections describe how spanning tree works:

- [Spanning Tree Overview, page 8-2](#)
- [Election of the Root Switch, page 8-2](#)
- [Determining the Spanning Tree Topology with BPDUs, page 8-3](#)
- [Spanning Tree Timers, page 8-4](#)
- [Creating the Spanning Tree Topology, page 8-4](#)
- [STP Port States, page 8-5](#)
- [MAC Address Allocation, page 8-10](#)
- [Spanning Tree and IEEE 802.1Q Trunks, page 8-11](#)
- [Understanding How Spanning Tree for Token Ring Works, page 8-11](#)

## Spanning Tree Overview

The Spanning Tree Protocol (STP) uses a distributed algorithm that selects one bridge on a redundantly connected network as the root of a spanning-tree-connected active topology. STP assigns roles to each port depending on what the port's function is in the active topology. Port roles are as follows:

- Root—A unique forwarding port elected for the spanning tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root port in the spanning tree
- Backup—A blocked port in a loopback configuration

Switches that have ports with these assigned roles are called root or designated switches. For more information, see the [“Election of the Root Switch” section on page 8-2](#).

In Ethernet networks, only one active path may exist between any two stations. Multiple active paths between stations can cause loops in the network. When loops occur, some switches recognize stations on both sides of the switch. This situation causes the forwarding algorithm to malfunction allowing duplicate frames to be forwarded.

Spanning tree is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet or Token Ring network to function properly, one active path must exist between two stations. Spanning tree 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.

The Catalyst enterprise LAN switches use the Spanning Tree Protocol on all Ethernet, Fast Ethernet, Gigabit Ethernet, and Token Ring port-based VLANs. By default, a single instance of STP runs on each configured VLAN (provided you do not manually disable STP). Depending on your hardware, you can enable and disable STP on a per-VLAN or a global basis.



### Note

On a Catalyst 5000 family switch with Supervisor Engine II G or III G, or Supervisor Engine III with a NetFlow Feature Card (NFFC) or NFFC II, you cannot enable or disable STP on a per-VLAN basis. STP must be enabled or disabled for all VLANs on the switch using the `set spantree {enable | disable} all` command.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The spanning tree algorithm calculates the best loop-free path throughout a switched network. Switches send and receive spanning tree frames at regular intervals. The switches do not forward these frames, but use the frames to construct a loop-free path.

Multiple active paths between stations cause loops in the network. If a loop exists in the network, hosts might receive duplicate messages. In addition, switches might learn host Media Access Control (MAC) addresses on multiple switch ports. These conditions result in an unstable network.

Spanning tree defines a tree with a root switch and a loop-free path from the root to all switches in the extended 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 spanning tree algorithm recalculates the spanning tree topology and activates the standby path.

## Election of the Root Switch

All switches in the Layer 2 network participating in spanning tree obtain information about other switches in the network through an exchange of data messages called Bridge Protocol Data Units (BPDUs).

BPDUs contain information about the transmitting switch and its ports, including switch and port MAC addresses, switch priority, port priority, and port cost. The STP uses this information to elect the root switch and root port for the switched network, as well as the root port and designated port for each switched segment.

The exchange of BPDUs results in the following actions:

- The election of a unique root switch for each instance of spanning tree
- The election of a designated switch for every switched LAN segment
- The removal of loops in the switched network by blocking switch ports connected to redundant links

The switch with the highest bridge priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC address in the Layer 2 network becomes the root switch.

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

## Determining the Spanning Tree Topology with BPDUs

The active and active spanning tree topology of a switched network is determined by the following:

- The unique bridge ID (MAC address) associated with each switch
- The path cost to the root associated with each switch port
- The port identifier (MAC address) associated with each switch port

The switch sends configuration BPDUs to compute and communicate the spanning tree topology. Each configuration BPDU contains the following minimal information:

- The unique bridge ID of the switch that the transmitting switch believes to be the root switch
- The cost of the path to the root from the transmitting port
- The identifier of the transmitting port

When a switch transmits a BPDU frame, all switches connected to the LAN on which the frame is transmitted receive the BPDU. When a switch 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 switch is elected as the root switch.
- The shortest distance to the root switch is calculated for each switch.
- A designated switch is selected. This is the switch closest to the root switch through which frames will be forwarded to the root.
- A root port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the spanning tree are selected.

# Spanning Tree Timers

Table 8-1 describes the spanning tree timers that affect the entire spanning tree performance.

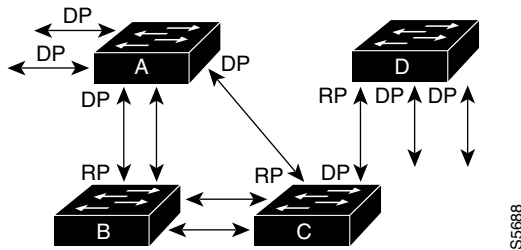
**Table 8-1 Spanning Tree Timers**

Variable	Description
Hello timer	Determines how often the switch broadcasts Hello messages to other switches.
Forward delay timer	Determines the amount of time a port will remain in the listening and learning states before entering the forwarding state.
Maximum age timer	Determines the amount of time protocol information received on a port is stored by the switch.

## Creating the Spanning Tree Topology

In Figure 8-1, Switch A is elected as the root switch because the bridge priority of all the switches is set to the default (32768) and Switch A has the lowest MAC address. However, because of traffic patterns, the number of forwarding ports, or link types, Switch A might not be the best root switch. By increasing the priority (lowering the numerical priority value) of the best switch so that it becomes the root switch, you force an STP recalculation to form a new spanning tree topology with the best switch as the root.

**Figure 8-1 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 stations in a switched network might not be the best route. 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 port 2 on Switch B is a fiber-optic link, and that port 1 on Switch B (an UTP link) is the root port. Network traffic might be more efficient over the high-speed fiber-optic link. By changing the spanning tree port priority or port cost for port 2 to a higher priority (lower numerical value) than port 1, port 2 becomes the root port.

## STP Port States

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 switch 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. The ports must allow the frame lifetime to expire for frames that have been forwarded using the old topology.

Each port on a switch using STP exists in one of the following five states:

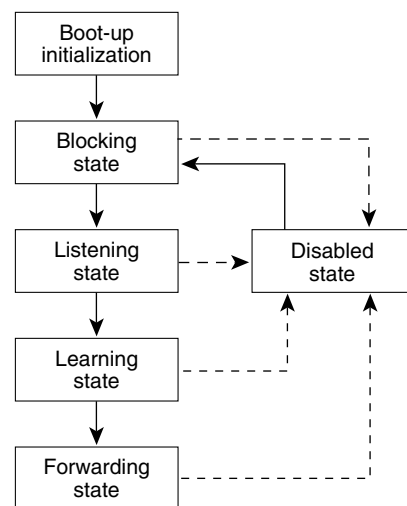
- Blocking
- Listening
- Learning
- Forwarding
- Disabled

A 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 8-2 illustrates how a port moves through the five states.

**Figure 8-2 STP Port States**



When you enable spanning tree, every switch in the network goes through the blocking state and the transitory states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state.

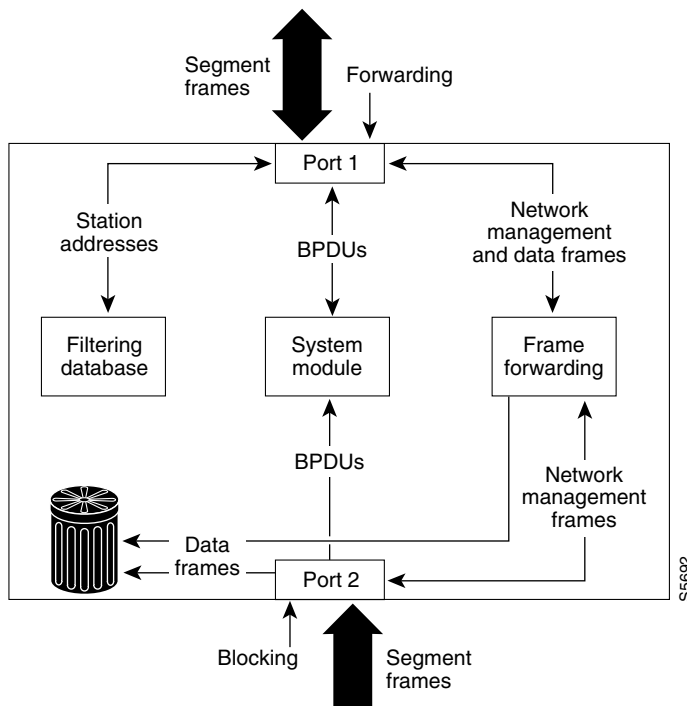
When the spanning tree algorithm places a port in the forwarding state, the following process occurs:

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

## Blocking State

A port in the blocking state does not participate in frame forwarding, as shown in [Figure 8-3](#). After initialization, a BPDU is sent to each port in the switch. A switch initially assumes it is the root until it exchanges BPDUs with other switches. This exchange establishes which switch in the network is the root. If there is only one switch in the network, no exchange occurs, the forward delay timer expires, and the ports move to the listening state. A switch always enters the blocking state following switch initialization.

**Figure 8-3 Port 2 in Blocking State**



A port in the blocking state performs as follows:

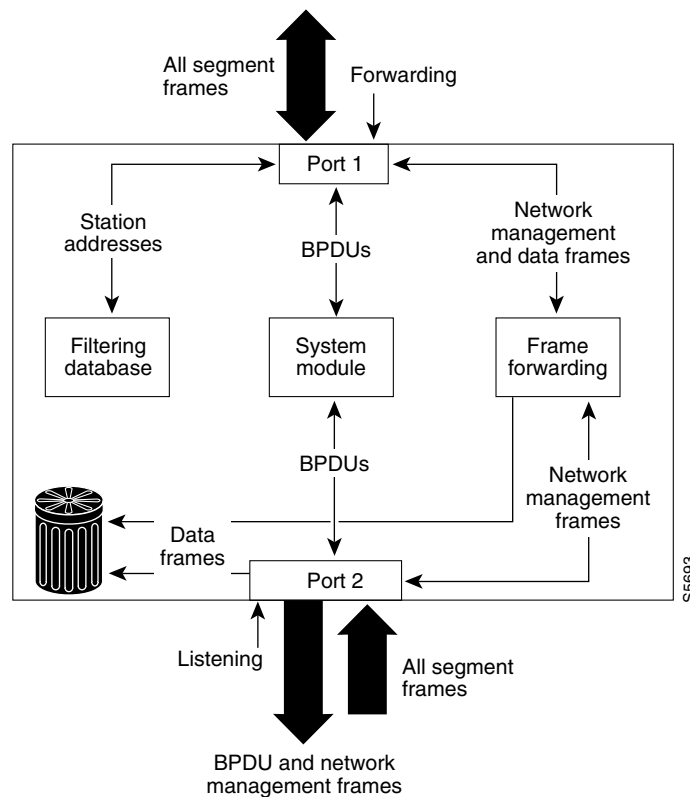
- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate station location into its address database. (There is no learning on a blocking port, so there is no address database update.)

- 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 port enters after the blocking state. The port enters this state when STP determines that the port should participate in frame forwarding. Figure 8-4 shows a port in the listening state.

**Figure 8-4 Port 2 in Listening State**



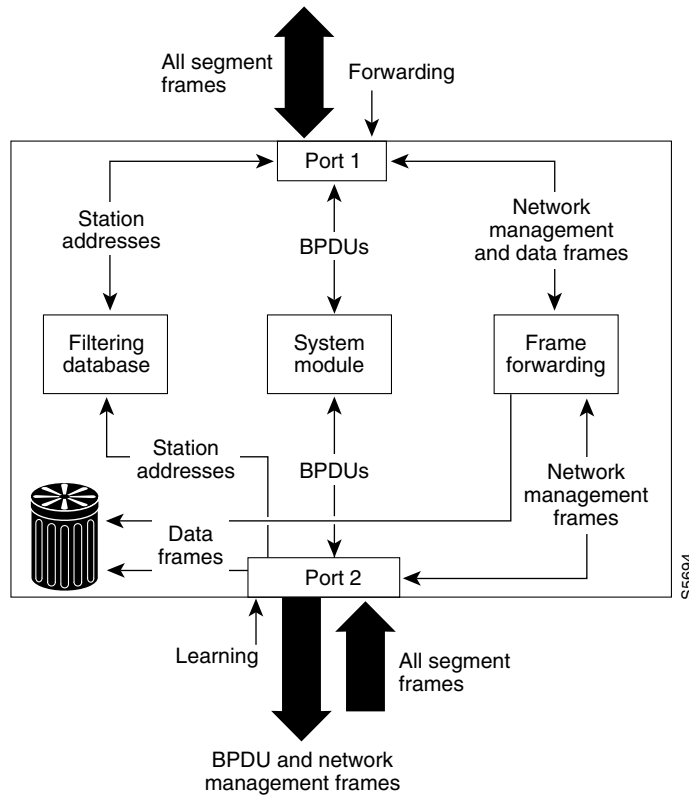
A port in the listening state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate 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.
- Processes BPDUs received from the system module.
- Receives and responds to network management messages.

## Learning State

A port in the learning state prepares to participate in frame forwarding. The port enters the learning state from the listening state. [Figure 8-5](#) shows a port in the learning state.

**Figure 8-5** Port 2 in Learning State



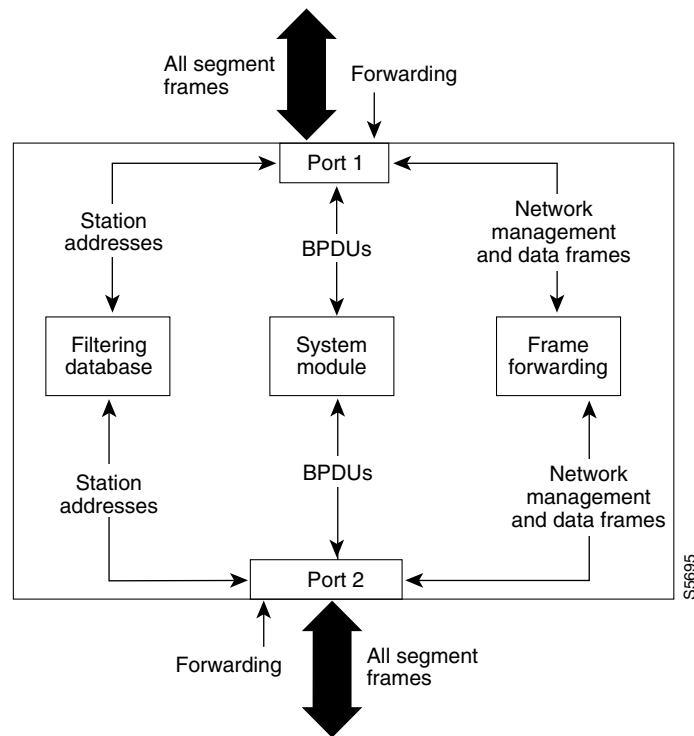
A port in the learning state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Incorporates 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 port in the forwarding state forwards frames, as shown in [Figure 8-6](#). The port enters the forwarding state from the learning state.

**Figure 8-6** Port 2 in Forwarding State



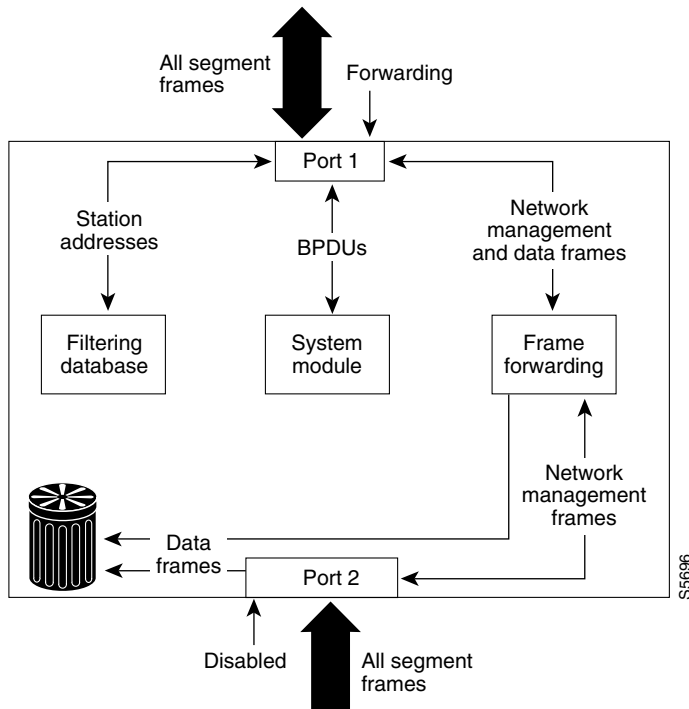
A port in the forwarding state performs as follows:

- Forwards frames received from the attached segment.
- Forwards frames switched from another port for forwarding.
- Incorporates 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 port in the disabled state does not participate in frame forwarding or STP, as shown in [Figure 8-7](#). A port in the disabled state is virtually nonoperational.

**Figure 8-7** Port 2 in Disabled State



A disabled port performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate station location into its address database. (There is no learning, so there is no address database update.)
- Receives BPDUs, but does not direct them to the system module.
- Does not receive BPDUs for transmission from the system module.
- Receives and responds to network management messages.

## MAC Address Allocation

The supervisor engine has a pool of 1024 MAC addresses that are used as the bridge IDs for the VLAN spanning trees. You can use the **show module** command to view the MAC address range for the supervisor engine.

MAC addresses are allocated sequentially, with the first MAC address in the range assigned to VLAN 1, the second MAC address in the range assigned to VLAN 2, and so forth. The last MAC address in the range is assigned to the supervisor engine in-band (sc0) management interface.

For example, if the MAC address range for the supervisor engine is 00-e0-1e-9b-2e-00 to 00-e0-1e-9b-31-ff, the VLAN 1 bridge ID is 00-e0-1e-9b-2e-00, the VLAN 2 bridge ID is 00-e0-1e-9b-2e-01, the VLAN 3 bridge ID is 00-e0-1e-9b-2e-02, and so forth. The in-band (sc0) interface MAC address is 00-e0-1e-9b-31-ff.

## MAC Address Reduction

The MAC address reduction feature is used on Catalyst 6000 family switches to enable extended-range VLAN identification. If you have a Catalyst 6000 switch in your network and you have MAC address reduction enabled on it, you should also enable it on all of your Catalyst 5000 family switches to avoid problems in the spanning tree topology. For detailed information on the MAC address reduction feature, refer to the *Catalyst 6000 Software Configuration Guide*.

## Spanning Tree and IEEE 802.1Q Trunks

IEEE 802.1Q VLAN trunks impose some limitations on the spanning tree feature in a network. In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one instance of spanning tree for each VLAN allowed on the trunks. However, non-Cisco 802.1Q switches maintain only one instance of spanning tree for all VLANs allowed on the trunks.

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



### Note

For more information on IEEE 802.1Q trunks, see [Chapter 12, “Configuring VLAN Trunks on Fast Ethernet and Gigabit Ethernet Ports.”](#)

## Understanding How Spanning Tree for Token Ring Works

Token Ring runs spanning tree both at the Token Ring Concentrator Relay Function (TrCRF) level and the Token Ring Bridge Relay Function (TrBRF) level. The TrCRF spanning tree removes loops in the logical ring. The TrBRF spanning tree, like the Ethernet spanning tree, interacts with other switches to remove loops from the spanning tree topology.

The Catalyst 5000 family Token Ring modules support these STPs:

- IEEE 802.1D STP
- IBM STP
- Cisco STP

The Catalyst 5000 family switches use the IEEE 802.1D and IBM STPs on TrBRFs. The STP that runs on the TrCRF is either the Cisco STP or the IEEE STP, depending on the bridging mode you configured for the TrCRF with the **set vlan** command.



### Caution

Some TrBRF STP and TrCRF bridge mode configurations are incompatible and can place the TrCRFs in a blocked state. For more information about these configurations, see the [“Setting the Spanning Tree Port State”](#) section on page 8-22.

# Default Spanning Tree Configuration

Table 8-2 shows the default spanning tree configuration.

**Table 8-2 Spanning Tree Default Configuration**

Feature	Default Value
Enable state	Spanning tree enabled for all VLANs
Bridge priority	32768
Port priority	32 (global)
Port-VLAN priority	Same as port priority but configurable on a per-VLAN basis
Port cost	<ul style="list-style-type: none"> <li>• Gigabit Ethernet: 4</li> <li>• Fast Ethernet: 10</li> <li>• FDDI/CDDI: 10</li> <li>• Ethernet: 100</li> <li>• Token Ring: 250</li> </ul>
Port-VLAN cost	Same as port cost but configurable on a per-VLAN basis
Hello time	2 seconds
Forward delay time	12 seconds
Maximum aging time	20 seconds

## Configuring Spanning Tree

These sections describe how to configure STP on any Ethernet, Fast Ethernet, Gigabit Ethernet, and Token Ring port-based VLANs:

- [Enabling Spanning Tree, page 8-13](#)
- [Enabling MAC Address Reduction, page 8-13](#)
- [Configuring the Root Switch, page 8-14](#)
- [Configuring a Secondary Root Switch, page 8-15](#)
- [Preventing Switches from Becoming the Root Switch, page 8-17](#)
- [Configuring the Global Port Priority, page 8-17](#)
- [Configuring the Port-VLAN Priority, page 8-18](#)
- [Configuring Global Port Cost, page 8-18](#)
- [Configuring Port-VLAN Cost, page 8-19](#)
- [Configuring the Bridge Priority, page 8-19](#)
- [Configuring the Hello Time, page 8-20](#)
- [Configuring the Forward Delay Time, page 8-20](#)
- [Configuring the Maximum Aging Time, page 8-21](#)
- [Setting the STP Type for a TrBRF, page 8-21](#)

- [Setting the Spanning Tree Port State](#), page 8-22
- [Specifying the STP Functional Address for a TrBRF](#), page 8-22
- [Disabling STP](#), page 8-23

## Enabling Spanning Tree



### Note

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

Depending on your hardware, you can enable spanning tree on a per-VLAN or a global basis. In either case, the switch maintains a separate instance of spanning tree for each VLAN (except on VLANs on which you disable spanning tree).

On Catalyst 5000 family switches with Supervisor Engine II G or III G, or with Supervisor Engine III or III F with NFFC or NFFC II, you must enable spanning tree globally for all VLANs using the **all** keyword.

If you do not specify the *vlan* value, VLAN 1 is assumed.

To enable spanning tree on a per-VLAN or global basis, perform this task in privileged mode:

	Task	Command
Step 1	Enable spanning tree on a per-VLAN or global basis.	<b>set spantree enable</b> [ <i>vlan</i> ] <b>set spantree enable all</b>
Step 2	Verify that spanning tree is enabled.	<b>show spantree</b> [ <i>vlan</i> ]

This example shows how to enable spanning tree globally for all VLANs on a Catalyst 5000 family switch with Supervisor Engine III G:

```
Console> (enable) set spantree enable all
Spanntree enabled.
Console> (enable)
```

This example shows how to enable spanning tree on VLAN 100:

```
Console> (enable) set spantree enable 100
Spanntree 100 enabled.
Console> (enable)
```

## Enabling MAC Address Reduction

To enable MAC address reduction, perform this task in privileged mode:

Task	Command
Enable MAC address reduction.	<b>set spantree macreduction</b> {enable   disable}

This example shows how to enable MAC address reduction:

```
Console> (enable) set spantree macreduction enable
MAC address reduction enabled
Console> (enable)
```

## Configuring the Root Switch

The Catalyst enterprise LAN switches maintain a separate instance of the spanning tree for each active VLAN configured on the switch. A bridge ID (MAC address) and bridge priority are associated with each instance of spanning tree. The switch with the lowest bridge priority becomes the root switch for that instance of spanning tree.

When you configure a switch as the root, the spanning tree bridge priority is modified from the default value (32768) to a significantly lower value so that the switch becomes the root for the specified VLANs.

The switch checks the bridge priority of the current root switches for each VLAN. The bridge priority for the specified VLANs is set to 8192 if this value will cause the switch to become the root for the specified VLANs.

If any root switch for the specified VLANs has a bridge priority lower than 8192, the switch sets the bridge priority for the specified VLANs to 1 less than the lowest bridge priority.

For example, if all switches in the network have the bridge priority for VLANs 100 through 200 set to the default value of 32768, entering the **set spantree root 100-200** command on a switch will set the bridge priority for VLANs 100 through 200 to 8192, causing the switch to become the root switch for those VLANs.

However, if the bridge priority for VLAN 150 on one of the other switches in the network is set to 4000, entering the **set spantree root 100-200** command on another switch will set the bridge priority for VLANs 100 through 200 to 3999, causing the switch to become the root switch for those VLANs.

If reducing the bridge priority to 1 still does not make the switch the root switch for the specified VLANs, the system displays a message.



### Note

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

Use the **dia network\_diameter** keywords to specify the Layer 2 network diameter (that is, the maximum number of bridge hops between any two hosts in the Layer 2 network). When you specify the network diameter, the switch automatically picks an optimal Hello time, forward delay time, and maximum age time for a network of that diameter, which can significantly reduce the spanning tree convergence time. You can use the **hello hello\_time** keywords to override the automatically calculated Hello time.



### Note

We recommend that you avoid configuring the Hello time, forward delay time, and maximum age time manually after configuring the switch as the root.

To configure a switch as the root switch, perform this task in privileged mode:

Task	Command
Configure a switch as the root switch.	<b>set spantree root vlans [dia network_diameter] [hello hello_time]</b>

This example shows how to configure the switch as the root switch for VLANs 1–10 with a network diameter of 4:

```
Console> (enable) set spantree root 1-10 dia 4
VLANs 1-10 bridge priority set to 8192
VLANs 1-10 bridge max aging time set to 14 seconds.
```

```
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 9 seconds.
Switch is now the root switch for active VLANs 1-6.
Console> (enable)
```

## Configuring a Secondary Root Switch

When you configure a switch as the secondary root switch, the spanning tree bridge priority is modified from the default value (32768) to 16384 so that the switch will become the root for the specified VLANs if the primary root switch fails (assuming the other switches in the network use the default bridge priority of 32768).

You can run this command on more than one switch to configure multiple backup root switches. Use the same network diameter and Hello time values as you used when configuring the primary root switch.

To configure a switch as the secondary root switch, perform this task in privileged mode:

Task	Command
Configure a switch as the secondary root switch.	<b>set spantree root secondary</b> <i>vlan</i> [ <b>dia</b> <i>network_diameter</i> ] [ <b>hello</b> <i>hello_time</i> ]

This example shows how to configure a switch as the secondary root switch for VLANs 22 and 24:

```
Console> (enable) set spantree root secondary 22,24 dia 5 hello 1
VLANs 22,24 bridge priority set to 16384.
VLANs 22,24 bridge max aging time set to 10 seconds.
VLANs 22,24 bridge hello time set to 1 second.
VLANs 22,24 bridge forward delay set to 7 seconds.
Console> (enable)
```

## Configuring a Root Switch to Improve Convergence

You can configure the root switch to reduce the STP convergence time. To accomplish this task, you must reduce the values of the Hello Time, Forward Delay Timer, and Maximum Age Timer parameters. For information on configuring timers, see the following sections:

- [Configuring the Hello Time, page 8-20](#)
- [Configuring the Forward Delay Time, page 8-20](#)
- [Configuring the Maximum Aging Time, page 8-21](#)



### Note

You can reduce the value of the timer parameters only if all of the links are LAN links of 10 megabits per second or faster. In this case, the network diameter can reach the maximum value of 7. With WAN connections, the parameters cannot be reduced.

When a link failure occurs in a bridged network, the network reconfiguration does not occur immediately. Hello Time, Forward Delay timer, and Maximum Age timer reconfiguration takes 50 seconds with the default parameters (specified by IEEE 802.1D). The reconfiguration delay depends on the network diameter, which is the maximum number of bridges between any two end stations attachments.

To reduce convergence time, use the non-default parameter values that are permitted by the IEEE 802.1D standard. To set a reconvergence of 14 seconds, use the following non-default parameters:

Parameter	Time
Network diameter (dia)	2
Hello time	2 seconds
Forward Delay timer	4 seconds
Maximum Age timer	6 seconds

These parameters can be set on the Catalyst 5000 family switches without any modification to the switches.



**Note** Switch ports can be set for improved convergence in PortFast mode. This setting only affects the transition from disable (link down) to enable (link up), which moves the port immediately to the forwarding state. If a port in the PortFast mode begins blocking, then it goes through listening and learning before reaching the forwarding state.

To configure the spanning tree bridge to improve convergence time, perform these tasks in privileged mode:

	Task	Command
<b>Step 1</b>	Configure the Hello Time for a VLAN or MISTP instance.	<b>set spantree hello</b> <i>interval</i> [ <i>vlan</i> ] <b>mistp-instance</b> [ <i>instances</i> ]
<b>Step 2</b>	Verify the configuration.	<b>show spantree</b> [ <i>vlan</i>   <b>mistp-instance</b> <i>instances</i> ]
<b>Step 3</b>	Configure the Forward Delay time for a VLAN or MISTP instance.	<b>set spantree fwddelay</b> <i>delay</i> [ <i>vlan</i> ] <b>mistp-instance</b> [ <i>instances</i> ]
<b>Step 4</b>	Verify the configuration.	<b>show spantree</b> [ <i>mod/port</i> ] <b>mistp-instance</b> [ <i>instances</i> ] [ <b>active</b> ]
<b>Step 5</b>	Configure the Maximum Aging time for a VLAN or MISTP instance.	<b>set spantree maxage</b> <i>agingtime</i> [ <i>vlangs</i> ] <b>mistp-instance</b> [ <i>instances</i> ]
<b>Step 6</b>	Verify the configuration.	<b>show spantree</b> [ <i>mod/port</i> ] <b>mistp-instance</b> [ <i>instances</i> ] [ <b>active</b> ]

This example shows how to configure the spanning tree Hello Time, Forward Delay timer, and Maximum Age timer to 2, 4, and 4 seconds respectively:

```

Console> (enable) set spantree hello 2 100
Spantree 100 hello time set to 7 seconds.
Console> (enable)
Console> (enable) set spantree fwddelay 4 100
Spantree 100 forward delay set to 21 seconds.
Console> (enable)
Console> (enable) set spantree maxage 6 100
Spantree 100 max aging time set to 36 seconds.
Console> (enable)
Console> (enable) set spantree root 1-10 dia 4
VLANs 1-10 bridge priority set to 8192
VLANs 1-10 bridge max aging time set to 14 seconds.

```

```
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 9 seconds.
Switch is now the root switch for active VLANs 1-6.
Console> (enable)
```

## Preventing Switches from Becoming the Root Switch

You can prevent switches from becoming the root switch by using the root guard feature. The root guard feature forces a port to become a designated port so that no switch on the other end of the link can become a root switch.

When you enable root guard on a per-port basis, it automatically applies to all of the active VLANs to which that port belongs. When you disable root guard, it is disabled for the specified port. If a port goes into the root-inconsistent state, it automatically goes into the listening state.

To prevent switches from becoming root, perform this task in privileged mode.

	Task	Command
Step 1	Enable root guard on a port.	<b>set spantree guard {root   none} {mod/port}</b>
Step 2	Verify that root guard is enabled.	<b>show spantree guard {root   none} {mod/port   vlan}</b>

## Configuring the Global Port Priority

You can change the global port priority of switch ports. The port with the lowest priority value forwards frames for all VLANs. The possible *priority* value range is 0 through 63. If all ports have the same priority value, the port with the lowest port number forwards frames.

To change the global port priority for a port, perform this task in privileged mode:

	Task	Command
Step 1	Change the global port priority for a switch port.	<b>set spantree portpri mod/port priority</b>
Step 2	Verify the port priority setting.	<b>show spantree [mod/port]</b>

This example shows how to change the global port priority for a port and verify the configuration:

```
Console> (enable) set spantree portpri 1/2 20
Bridge port 1/2 port priority set to 20.
Console> (enable) show spantree 1/2
Port      Vlan  Port-State    Cost   Priority  Fast-Start  Group-method
-----
1/2      1     blocking      19     20     disabled
1/2     100   forwarding    19     20     disabled
1/2     521   blocking      19     20     disabled
1/2     522   blocking      19     20     disabled
1/2     523   blocking      19     20     disabled
1/2     524   blocking      19     20     disabled
1/2    1003   not-connected  19     20     disabled
1/2    1005   not-connected  19     4     disabled
Console> (enable)
```

## Configuring the Port-VLAN Priority

You can set the port priority for a port on a per-VLAN basis. The port with the lowest priority value for a specific VLAN forwards frames for that VLAN. The possible *priority* value range is 0 through 63. If all ports have the same priority value for a particular VLAN, the port with the lowest port number forwards frames for that VLAN. If you do not specify the *vlan* value, VLAN 1 is assumed as the value.

To change the port-VLAN priority for a port, perform this task in privileged mode:

	Task	Command
Step 1	Change the port-VLAN priority for a VLAN on a switch port.	<b>set spantree portvlanpri</b> <i>mod/port priority [vlans]</i>
Step 2	Verify the port-VLAN priority setting.	<b>show spantree</b> [ <i>mod/port</i> ]

This example shows how to change the port-VLAN priority on a port and verify the configuration:

```

Console> (enable) set spantree portvlanpri 1/2 1 100
Port 1/2 vlans 1-99,101-1004 using portpri 32.
Port 1/2 vlans 100 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Console> (enable) show spantree 1/2
Port      Vlan  Port-State  Cost  Priority  Fast-Start  Group-method
-----
1/2      1     blocking    19    32       disabled
1/2      100   forwarding  19    1        disabled
1/2      521   blocking    19    32       disabled
1/2      522   blocking    19    32       disabled
1/2      523   blocking    19    32       disabled
1/2      524   blocking    19    32       disabled
1/2      1003  not-connected 19    32       disabled
1/2      1005  not-connected 19    4        disabled
Console> (enable)

```

## Configuring Global Port Cost

You can change the global port cost of switch ports. Ports with lower port costs are more likely to be used to forward frames for all VLANs. Assign lower numbers to ports attached to faster media (such as full-duplex Fast Ethernet) and higher numbers to ports attached to slower media (such as half-duplex Ethernet). The possible range of the *cost* value is 1 to 65535.

To change the global port cost for a port, perform this task in privileged mode:

	Task	Command
Step 1	Change the global port cost for a switch port.	<b>set spantree portcost</b> <i>mod/port cost</i>
Step 2	Verify the port cost setting.	<b>show spantree</b> [ <i>mod/port</i> ]

This example shows how to change the global port cost on a port and verify the configuration:

```

Console> (enable) set spantree portcost 1/2 10
Spantree port 1/2 path cost set to 10.
Console> (enable) show spantree 1/2
Port      Vlan  Port-State  Cost  Priority  Fast-Start  Group-method
-----
1/2      1     forwarding  10    20       disabled

```

```

1/2    100    forwarding    10        20    disabled
1/2    521    forwarding    10        20    disabled
1/2    522    forwarding    10        20    disabled
1/2    523    forwarding    10        20    disabled
1/2    524    forwarding    10        20    disabled
1/2    1003   not-connected  10        20    disabled
1/2    1005   not-connected  10        4     disabled
Console> (enable)

```

## Configuring Port-VLAN Cost

You can change the port cost for a port on a per-VLAN basis. Ports with lower port-VLAN costs are more likely to be used to forward frames for those VLANs. You should assign lower numbers to ports attached to faster media (such as full-duplex Fast Ethernet) and higher numbers to ports attached to slower media (such as half-duplex Ethernet). The possible range of the *cost* value is 1 to 65535. If you do not specify the *vlan* value, VLAN 1 is assumed as the value.

To change the port-VLAN cost for a port, perform this task in privileged mode:

	Task	Command
Step 1	Change the port-VLAN cost for a VLAN on a switch port.	<b>set spantree portvlancost</b> <i>mod/port cost cost [vlans]</i>
Step 2	Verify the port-VLAN cost setting.	<b>show spantree</b> [ <i>mod/port</i> ]

This example shows how to change the port-VLAN cost on a port and verify the configuration:

```

Console> (enable) set spantree portvlancost 1/2 cost 10 100
Port 1/2 VLANs 1-99,101-1005 have path cost 19.
Port 1/2 VLANs 100 have path cost 10.
Console> (enable) show spantree 1/2
Port      Vlan  Port-State      Cost    Priority  Fast-Start  Group-method
-----
1/2      1     blocking        19      20       disabled
1/2     100    forwarding       10      20       disabled
1/2     521    blocking        19      20       disabled
1/2     522    blocking        19      20       disabled
1/2     523    blocking        19      20       disabled
1/2     524    blocking        19      20       disabled
1/2    1003   not-connected   19      20       disabled
1/2    1005   not-connected   19      4        disabled
Console> (enable)

```

## Configuring the Bridge Priority

Use the **set spantree priority** command to manually change the spanning tree bridge priority for a VLAN. The possible range of the *bridge\_priority* value is 0 to 65535. If you do not specify the *vlan* value, VLAN 1 is assumed as the value.



### Note

Be careful when using this command. For most situations, we recommend that you use the **set spantree root** and **set spantree root secondary** commands to modify the bridge priority and related parameters.

To configure the spanning tree bridge priority for a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Set the bridge priority for a VLAN.	<b>set spantree priority</b> <i>bridge_priority</i> [ <i>vlan</i> ]
Step 2	Verify the configuration.	<b>show spantree</b> [ <i>vlan</i> ]

This example shows how to change the spanning tree bridge priority for VLAN 100 to 8192:

```
Console> (enable) set spantree priority 8192 100
Spantree 100 bridge priority set to 8192.
Console> (enable)
```

## Configuring the Hello Time

Use the **set spantree hello** command to manually change the spanning tree Hello time for a VLAN. The possible range of the *interval* value is 1 to 10 seconds. If you do not specify the *vlan*, VLAN 1 is assumed as the value.



### Note

Be careful when using this command. For most situations, we recommend that you use the **set spantree root** and **set spantree root secondary** commands to modify the Hello time and related parameters.

To configure the spanning tree bridge Hello time for a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Set the Hello time for a VLAN.	<b>set spantree hello</b> <i>interval</i> [ <i>vlan</i> ]
Step 2	Verify the configuration.	<b>show spantree</b> [ <i>vlan</i> ]

This example shows how to change the spanning tree Hello time for VLAN 100 to 7 seconds:

```
Console> (enable) set spantree hello 7 100
Spantree 100 hello time set to 7 seconds.
Console> (enable)
```

## Configuring the Forward Delay Time

Use the **set spantree fwddelay** command to manually change the spanning tree forward delay time for a VLAN. The possible range of the *delay* value is 4 to 30 seconds. If you do not specify the *vlan* value, VLAN 1 is assumed as the value.



### Note

Be careful when using this command. For most situations, we recommend that you use the **set spantree root** and **set spantree root secondary** commands to modify the forward delay time and related parameters.

To configure the spanning tree forward delay time for a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Set the forward delay time for a VLAN.	<b>set spantree fwddelay</b> <i>delay_time</i> [ <i>vlan</i> ]
Step 2	Verify the configuration.	<b>show spantree</b> [ <i>vlan</i> ]

This example shows how to change the spanning tree forward delay time for VLAN 100 to 21 seconds:

```
Console> (enable) set spantree fwddelay 21 100
Spanntree 100 forward delay set to 21 seconds.
Console> (enable)
```

## Configuring the Maximum Aging Time

Use the **set spantree maxage** command to manually change the spanning tree maximum aging time for a VLAN. The possible range of the *agingtime* value is 6 to 40 seconds. If you do not specify the *vlan* value, VLAN 1 is assumed as the value.



### Note

Be careful when using this command. For most situations, we recommend that you use the **set spantree root** and **set spantree root secondary** commands to modify the maximum aging time and related parameters.

To configure the spanning tree maximum aging time for a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Set the maximum aging time for a VLAN.	<b>set spantree maxage</b> <i>agingtime</i> [ <i>vlan</i> ]
Step 2	Verify the configuration.	<b>show spantree</b> [ <i>vlan</i> ]

This example shows how to change the spanning tree maximum aging time for VLAN 100 to 36 seconds:

```
Console> (enable) set spantree maxage 36 100
Spanntree 100 max aging time set to 36 seconds.
Console> (enable)
```

## Setting the STP Type for a TrBRF

You can configure the STP type to be used by a TrBRF. The following STP and bridge mode configurations are incompatible and can place logical ports in a blocked state:

- TrBRF is running the IBM STP and the TrCRF is in SRT mode.
- TrBRF is running the IEEE STP and the TrCRF is in SRB mode.

For more information, see the [“Setting the Spanning Tree Port State”](#) section on page 8-22.

To specify the STP type for a TrBRF, perform this task in privileged mode:

Task	Command
Specify the STP type for a TrBRF.	<b>set vlan</b> <i>vlan_num</i> <b>stp</b> { <i>ieee</i>   <i>ibm</i> }

This example shows how to specify the STP type for a TrBRF:

```
Console> (enable) set vlan 950 stp ieee
Vlan 950 configuration successful
Console> (enable)
```

## Setting the Spanning Tree Port State

When you enable STP, every switch in the network goes through the transitory listening and learning states at power up. If properly configured, the logical ports will stabilize to the forwarding or blocking state. However, with TrBRFs and TrCRFs, if the following situations occur, you need to manually set the state of a logical port of a TrBRF:

- TrBRF is running the IBM STP and the TrCRF is in SRT mode.
- TrBRF is running the IEEE STP and the TrCRF is in SRB mode.



### Note

If one of these configurations occurs, the logical ports are put in a blocked state and STP does not run.

You can use the **set spantree portstate** command to manually set the state of a logical port to blocked or forwarding mode.

To set the state of a logical port manually, perform this task in privileged mode:

Task	Command
Manually set the state of a logical port.	<b>set spantree portstate</b> <i>trcrf</i> { <b>auto</b>   <b>block</b>   <b>forward</b> } [ <i>trbrf</i> ]



### Note

If you disable spanning tree for a TrBRF using the **set spantree disable** command, the logical ports of the TrBRF are placed in the forwarding state regardless of the state you configured using the **set spantree portstate** command.

This example shows how to manually set the STP state of a logical port:

```
Console> (enable) set spantree portstate 950 forward
Portstate successfully set for tokenring crf 950
Console> (enable)
```

## Specifying the STP Functional Address for a TrBRF

To configure a TrBRF running IEEE STP to use the bridge functional address instead of the IEEE STP address, perform this task in privileged mode:

Task	Command
Specify that a TrBRF running IEEE STP uses the bridge functional address instead of the IEEE STP address.	<b>set spantree multicast-address</b> <i>vlan_num</i> <b>ibm</b>

## Disabling STP

Depending on your hardware, you can disable spanning tree on a per-VLAN or a global basis.



### 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.



### Caution

Do not disable spanning tree on a VLAN unless all switches or routers in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches or routers in a VLAN and leave spanning tree enabled on other switches or routers in the VLAN. If spanning tree remains enabled on the switches and routers, they will have incomplete information about the physical topology of the network, which may cause unexpected results.

On Catalyst 5000 family switches with Supervisor Engine II G or III G, or with Supervisor Engine III or III F with NFFC or NFFC II, you must disable spanning tree globally for all VLANs using the **all** keyword.



### Note

In a Token Ring environment, if you disable STP for a TrBRF, then all ports in TrCRFs with that TrBRF as a parent are set to the forwarding state.

If you do not specify the *vlan* value, VLAN 1 is assumed as the value.

To disable spanning tree on a per-VLAN or global basis, perform this task in privileged mode:

Task	Command
Disable spanning tree on a per-VLAN or global basis.	<b>set spantree disable</b> [ <i>vlan</i> ] <b>set spantree disable all</b>

## Understanding How BPDU Skewing Works

The root switch advertises its presence by sending out BPDUs for the configured Hello time interval. The non-root switches receive and process one BPDU during each configured time period. A VLAN may not receive the BPDU as scheduled. If the BPDU is not received on a VLAN at the configured time interval, the BPDU is skewed.

BPDU skewing is the difference between when the BPDUs are expected to be received and the time BPDUs are actually received. Skewing occurs when the following occurs:

- Spanning tree timers lapse
- Expected BPDUs are not received
- Spanning tree detects topology changes.

Skewing causes BPDUs to relood the network to keep the spanning tree topology database current.

Spanning tree uses the Hello Time (see [“Configuring the Hello Time” section on page 20](#)) to detect when a connection to the root switch exists through a port and when that connection is lost. This feature applies to both PVST+ and MISTP. In MISTP, the skewing detection is on a per-instance basis.

BPDU skewing detects BPDUs that are not processed in a regular time frame on the non-root switches in the network. If BPDU skewing occurs, a syslog message is displayed. The syslog applies to both PVST+ and MISTP.

The number of syslog messages that are generated may impact the convergence of the network and the CPU utilization of the switch. New syslog messages are not generated as individual messages for every VLAN because the higher the number of syslog messages that are reported, the slower the switching process will be. To reduce the impact on the switch, the syslog messages are:

- Generated 50 percent of the maximum age time (see [“Configuring the Maximum Aging Time” section on page 21](#))
- Rate limited at one for every 60 seconds

## Configuring Spanning Tree BPDU Skewing

Commands that support the spanning tree BPDU skewing feature perform these functions:

- Allow you to enable or disable BPDU skewing. The default is disabled.
- Modify the **show spantree summary** output to show if the skewing detection is enabled and for which VLANs or PVST+ or MISTP instances the skew was detected.
- Provide a display of the VLAN or PVST+ or MISTP instance and the port affected by the skewing including this information:
  - The last skew duration (in absolute time)
  - The worst skew duration (in absolute time)
  - The date and time of the worst duration

To change how spanning tree performs BPDU skewing statistics gathering, enter the **set spantree bpdus-skewing** command. The **bpdus-skewing** command is disabled by default.

To configure the BPDU skewing statistics-gathering for a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Configure BPDU skewing.	<b>set spantree bpdus-skewing [enable   disable]</b>
Step 2	Verify the configuration.	<b>show spantree bpdus-skewing vlan [mod/port]</b> <b>show spantree bpdus-skewing mistp-instance [instance] [mod/port]</b>

This example shows how to configure BPDU skewing and view the skewing statistics:

```

Console> (debug-eng) set spantree bpdus-skewing
Usage:set spantree bpdus-skewing <enable|disable>
Console> (debug-eng)
Console> (debug-eng)
Console> (debug-eng) set spantree bpdus-skewing enable
Spantree bpdus-skewing enabled on this switch.
Console> (debug-eng)
Console> (enable)

Console> (enable) show spantree bpdus-skewing 1
Bpdu skewing statistics for vlan 1
Port      Last Skew ms   Worst Skew ms   Worst Skew Time
-----

```

```

8/2          5869          108370 Tue Nov 21 2000, 06:25:59
8/4          4050          113198 Tue Nov 21 2000, 06:26:04
8/6          113363         113363 Tue Nov 21 2000, 06:26:05
8/8          4111          113441 Tue Nov 21 2000, 06:26:05
8/10         113522         113522 Tue Nov 21 2000, 06:26:05
8/12         4111          113600 Tue Nov 21 2000, 06:26:05
8/14         113678         113678 Tue Nov 21 2000, 06:26:05
8/16         4111          113755 Tue Nov 21 2000, 06:26:05
8/18         113833         113833 Tue Nov 21 2000, 06:26:05
8/20         4111          113913 Tue Nov 21 2000, 06:26:05
8/22         113917         113917 Tue Nov 21 2000, 06:26:05
8/24         4110          113922 Tue Nov 21 2000, 06:26:05
8/26         113926         113926 Tue Nov 21 2000, 06:26:05
8/28         4111          113931 Tue Nov 21 2000, 06:26:05
Console> (enable)

```

This example shows how to configure BPDU skewing for VLAN 1 on module 8, port 2 and view the skewing statistics:

```

Console> (enable) show spantree bpdu-skewing 1 8/4
Bpdu skewing statistics for vlan 1
Port      Last Skew ms   Worst Skew ms   Worst Skew Time
-----
8/4          5869          108370 Tue Nov 21 2000, 06:25:59

```

You will receive a similar output when MISTP is running.

Use the **show spantree summary** command to display whether BPDU skew detection is enabled and list the VLANs or PVST+ or MISTP instances affected in the skew. This example shows the output when you enter the **show spantree summary** command:

```

Console> (enable) show spantree summary
Root switch for vlans: 1
BPDU skewing detection enabled for the bridge
BPDU skewed for vlans: 1
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of connected spanning tree ports by vlan

VLAN  Blocking Listening Learning Forwarding STP Active
-----
      1         6         4         2         0         12

      Blocking Listening Learning Forwarding STP Active
      -----
Total      6         4         2         0         12
Console> (enable)

```

