Configuring Spanning Tree Protocol

This chapter descibes how to configure Spanning Tree Protocol (STP) on your access point/bridge.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Access Points and Bridges* of this release.

Note STP is available only when the access point is in bridge mode.

Understanding Spanning Tree Protocol

This section describes how spanning-tree features work. It includes this information:

STP Overview

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

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 Layer 2 network. Infrastructure devices such as wireless access point/bridges and switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The devices do not forward these frames but use them to construct a loop-free path.

Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Infrastructure devices might also learn end-station MAC addresses on multiple Layer 2 interfaces. 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 infrastructure devices in the Layer 2 network.

Note STP discussions use the term *root* to describe two concepts: the bridge on the network that serves as a central point in the spanning tree is called the *root bridge*, and the port on each bridge that provides the most efficient path to the root bridge is called the *root port*. These meanings are separate from the Role in radio network setting that includes root and non-root options. A bridge whose Role in radio network setting is Root Bridge does not necessarily become the root bridge in the spanning tree. In this chapter, the root bridge in the spanning tree is called the *spanning-tree root*.

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.

When two interfaces on a bridge are part of a loop, the spanning-tree port priority and path cost settings determine which interface is put in the forwarding state and which is put in the blocking state. The port priority value represents the location of an interface in the network topology and how well it is located to pass traffic. The path cost value represents media speed.

The access point/bridge supports both per-VLAN spanning tree (PVST) and a single 802.1q spanning tree without VLANs. The access point/bridge cannot run 802.1s MST or 802.1d Common Spanning Tree, which maps multiple VLANs into a one-instance spanning tree.

The access point/bridge maintains a separate spanning-tree instance for each active VLAN configured on it. A bridge ID, consisting of the bridge priority and the access point/bridge MAC address, is associated with each instance. For each VLAN, the access point/bridge with the lowest access point/bridge ID becomes the spanning-tree root for that VLAN.

Access Point/Bridge Protocol Data Units

The stable, active spanning-tree topology of your network is determined by these elements:

- The unique access point/bridge ID (wireless access point/bridge priority and MAC address) associated with each VLAN on each wireless access point/bridge
- The spanning-tree path cost to the spanning-tree root
- The port identifier (port priority and MAC address) associated with each Layer 2 interface

When the access point/bridges in a network are powered up, each access point/bridge functions as the STP root. The access point/bridges send configuration BPDUs through the Ethernet and radio ports. The BPDUs communicate and compute the spanning-tree topology. Each configuration BPDU contains this information:

- The unique access point/bridge ID of the wireless access point/bridge that the sending access point/bridge identifies as the spanning-tree root
- The spanning-tree path cost to the root
- The access point/bridge ID of the sending access point/bridge
- Message age
- The identifier of the sending interface
- Values for the hello, forward delay, and max-age protocol timers

When a access point/bridge receives a configuration BPDU that contains *superior* information (lower access point/bridge ID, lower path cost, and so forth), it stores the information for that port. If this BPDU is received on the root port of the access point/bridge, the access point/bridge also forwards it with an updated message to all attached LANs for which it is the designated access point/bridge.

If a access point/bridge receives a configuration BPDU that contains *inferior* information to that currently stored for that port, it discards the BPDU. If the access point/bridge is a designated access point/bridge for the LAN from which the inferior BPDU was received, it sends that LAN a BPDU containing the up-to-date information stored for that port. In this way, inferior information is discarded, and superior information is propagated on the network.

A BPDU exchange results in these actions:

- One access point/bridge is elected as the spanning-tree root.
- A root port is selected for each access point/bridge (except the spanning-tree root). This port provides the best path (lowest cost) when the access point/bridge forwards packets to the spanning-tree root.
- The shortest distance to the spanning-tree root is calculated for each access point/bridge based on the path cost.
- A designated access point/bridge for each LAN segment is selected. The designated access point/bridge incurs the lowest path cost when forwarding packets from that LAN to the spanning-tree root. The port through which the designated access point/bridge is attached to the LAN is called the *designated port*.

- Interfaces included in the spanning-tree instance are selected. Root ports and designated ports are put in the forwarding state.
- All interfaces not included in the spanning tree are blocked.

Election of the Spanning-Tree Root

All access point/bridges in the Layer 2 network participating in STP gather information about other access point/bridges in the network through an exchange of BPDU data messages. This exchange of messages results in these actions:

- The election of a unique spanning-tree root for each spanning-tree instance
- The election of a designated access point/bridge for every LAN segment
- The removal of loops in the network by blocking Layer 2 interfaces connected to redundant links

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

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

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

BPDUs contain information about the sending access point/bridge and its ports, including access point/bridge and MAC addresses, access point/bridge priority, port priority, and path cost. STP uses this information to elect the spanning-tree root and root port for the network and the root port and designated port for each LAN segment.

Spanning-Tree Timers

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

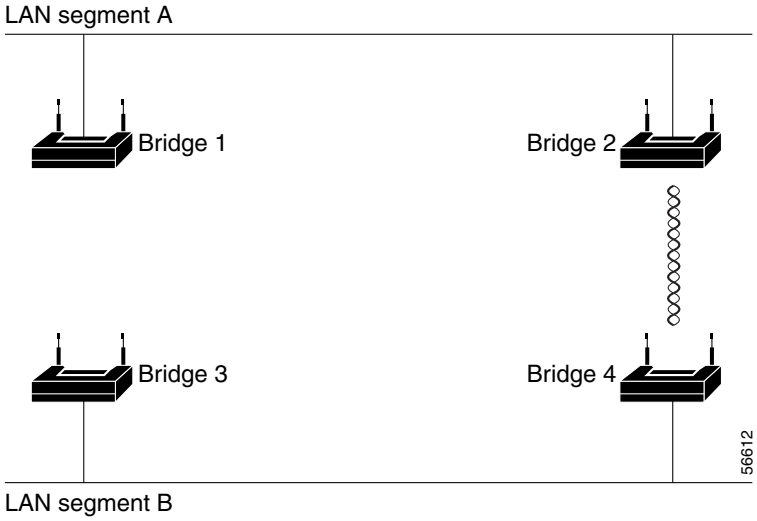
Table 8-1 Spanning-Tree Timers

Variable	Description
Hello timer	Determines how often the access point/bridge broadcasts hello messages to other access point/bridges.
Forward-delay timer	Determines how long each of the listening and learning states last before the interface begins forwarding.
Maximum-age timer	Determines the amount of time the access point/bridge stores protocol information received on an interface.

Creating the Spanning-Tree Topology

In Figure 8-1, bridge 4 is elected as the spanning-tree root because the priority of all the access point/bridges is set to the default (32768) and bridge 4 has the lowest MAC address. However, because of traffic patterns, number of forwarding interfaces, or link types, bridge 4 might not be the ideal spanning-tree root. By increasing the priority (lowering the numerical value) of the ideal bridge so that it becomes the spanning-tree root, you force a spanning-tree recalculation to form a new topology with the ideal bridge as the spanning-tree root.

Figure 8-1 Spanning-Tree Topology



Spanning-Tree Interface States

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

Each interface on a access point/bridge using spanning tree exists in one of these states:

- Blocking—The interface does not participate in frame forwarding.
- Listening—The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.
- Learning—The interface prepares to participate in frame forwarding.
- Forwarding—The interface forwards frames.
- Disabled—The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

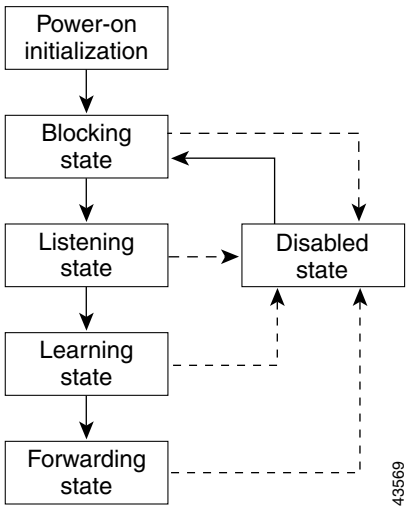
An interface moves through these states:

- 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 an interface moves through the states.

Figure 8-2 Spanning-Tree Interface States



When you enable STP on the access point/bridge, the Ethernet and radio interfaces go through the blocking state and the transitory states of listening and learning. Spanning tree stabilizes each interface at the forwarding or blocking state.

When the spanning-tree algorithm places a Layer 2 interface in the forwarding state, this process occurs:

1. The interface is in the listening state while spanning tree waits for protocol information to transition the interface to the blocking state.
2. While spanning tree waits the forward-delay timer to expire, it moves the interface to the learning state and resets the forward-delay timer.
3. In the learning state, the interface continues to block frame forwarding as the access point/bridge learns end-station location information for the forwarding database.
4. When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, where both learning and frame forwarding are enabled.

Blocking State

An interface in the blocking state does not participate in frame forwarding. After initialization, a BPDU is sent to the access point/bridge's Ethernet and radio ports. A access point/bridge initially functions as the spanning-tree root until it exchanges BPDUs with other access point/bridges. This exchange establishes which access point/bridge in the network is the spanning-tree root. If there is only one access point/bridge in the network, no exchange occurs, the forward-delay timer expires, and the interfaces move to the listening state. An interface always enters the blocking state when you enable STP.

An interface in the blocking state performs as follows:

- Discards frames received on the port
- Does not learn addresses
- Receives BPDUs

Note If a access point/bridge port is blocked, some broadcast or multicast packets can reach a forwarding port on the access point/bridge and cause the bridging logic to switch the blocked port into listening state momentarily before the packets are dropped at the blocked port.

Listening State

The listening state is the first state an interface enters after the blocking state. The interface enters this state when STP determines that the interface should participate in frame forwarding.

An interface in the listening state performs as follows:

- Discards frames received on the port
- Does not learn addresses
- Receives BPDUs

Learning State

An interface in the learning state prepares to participate in frame forwarding. The interface enters the learning state from the listening state.

An interface in the learning state performs as follows:

- Discards frames received on the port
- Learns addresses
- Receives BPDUs

Forwarding State

An interface in the forwarding state forwards frames. The interface enters the forwarding state from the learning state.

An interface in the forwarding state performs as follows:

- Receives and forwards frames received on the port
- Learns addresses
- Receives BPDUs

Disabled State

An interface in the disabled state does not participate in frame forwarding or in the spanning tree. An interface in the disabled state is nonoperational.

A disabled interface performs as follows:

- Discards frames received on the port
- Does not learn addresses

- Does not receive BPDUs

Configuring STP Features

You complete three major steps to configure STP on the access point/bridge:

1. If necessary, assign interfaces and sub-interfaces to bridge groups
2. Enable STP for each bridge group
3. Set the STP priority for each bridge group

These sections include spanning-tree configuration information:

- Default STP Configuration, page 8-8
- Configuring STP Settings, page 8-9
- STP Configuration Examples, page 8-10

Default STP Configuration

STP is disabled by default. Table 8-2 lists the default STP settings when you enable STP.

Table 8-2 Default STP Values When STP is Enabled

Setting	Default Value
Bridge priority	32768
Bridge max age	20
Bridge hello time	2
Bridge forward delay	15
Ethernet port path cost	19
Ethernet port priority	128
Radio port path cost	33
Radio port priority	128

The radio and Ethernet interfaces and the native VLAN on the access point/bridge are assigned to bridge group 1 by default. When you enable STP and assign a priority on bridge group 1, STP is enabled on the radio and Ethernet interfaces and on the primary VLAN, and those interfaces adopt the priority assigned to bridge group 1. You can create bridge groups for sub-interfaces and assign different STP settings to those bridge groups.

Configuring STP Settings

Beginning in privileged EXEC mode, follow these steps to configure STP on the access point/bridge:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface { dot11radio** *number* **| fastethernet** *number* **|** GigabitEthernet *number*}	Enter interface configuration mode for radio or Ethernet interfaces or sub-interfaces. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1. The fast Ethernet interface is 0.
Step 3	**bridge-group** *number*	Assign the interface to a bridge group. You can number your bridge groups from 1 to 255.
Step 4	**no bridge-group** *number* **spanning-disabled**	Counteract the command that automatically disables STP for a bridge group. STP is enabled on the interface when you enter the **bridge** *n* **protocol ieee** command.
Step 5	**exit**	Return to global configuration mode.
Step 6	**bridge** *number* **protocol ieee**	Enable STP for the bridge group. You must enable STP on each bridge group that you create with **bridge-group** commands.
Step 7	**bridge** *number* **priority** *priority*	(Optional) Assign a priority to a bridge group. The lower the priority, the more likely it is that the bridge becomes the spanning-tree root.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show spanning-tree bridge**	Verify your entries.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

STP Configuration Examples

These configuration examples show how to enable STP on root and non-root access point/bridges with and without VLANs:

Root Bridge Without VLANs

This example shows the configuration of a root bridge with no VLANs configured and with STP enabled:

```
hostname master-bridge-south
!
dot11 syslog
!
dot11 ssid visitor
!
dot11 ssid visitor2
!
dot11 guest
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid visitor
 !
 antenna gain 0
 stbc
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 ssid visitor2
 !
 antenna gain 0
 peakdetect
 dfs band 3 block
 stbc
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
```

```
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 9000
bridge 1 protocol ieee
bridge 1 route ip
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```

Non-Root Bridge Without VLANs

This example shows the configuration of a non-root bridge with no VLANs configured with STP enabled:

```
hostname client-bridge-north
!
dot11 syslog
!
dot11 ssid visitor
!
dot11 ssid visitor2
!
dot11 guest
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid visitor
 !
 antenna gain 0
 stbc
 station-role non-root
 bridge-group 1
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 ssid visitor2
 !
```

```
 antenna gain 0
 peakdetect
 stbc
 station-role non-root
 bridge-group 1
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 path-cost 40
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 10000
bridge 1 protocol ieee
bridge 1 route ip
!
line con 0
line vty 0 4
 login local
 transport input all
!
End
```

Root Bridge with VLANs

This example shows the configuration of a root bridge with VLANs configured with STP enabled:

```
hostname master-bridge-hq
!
dot11 syslog
!
dot11 ssid vlan1
   vlan 1
   authentication open
!
dot11 guest
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid vlan1
 !
 antenna gain 0
 stbc
 station-role root
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 no ip route-cache
```

```
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 path-cost 500
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
!
interface Dot11Radio1.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
!
interface Dot11Radio1.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 path-cost 500
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
!
interface GigabitEthernet0
 no ip address
```

```
 no ip route-cache
 duplex auto
 speed auto
!
interface GigabitEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 no bridge-group 2 source-learning
!
interface GigabitEthernet0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 no bridge-group 3 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 9000
bridge 1 protocol ieee
bridge 1 route ip
bridge 2 priority 10000
bridge 2 protocol ieee
bridge 3 priority 3100
bridge 3 protocol ieee
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```

Non-Root Bridge with VLANs

This example shows the configuration of a non-root bridge with VLANs configured with STP enabled:

```
hostname client-bridge-remote
!
dot11 syslog
!
dot11 ssid vlan1
   vlan 1
   authentication open
!
dot11 guest
!
bridge irb
!
interface Dot11Radio0
```

```
 no ip address
 no ip route-cache
 !
 ssid vlan1
 !
 antenna gain 0
 stbc
 station-role non-root
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
!
interface Dot11Radio0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 antenna gain 0
 peakdetect
 station-role non-root
!
interface Dot11Radio1.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
!
interface Dot11Radio1.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
!
interface Dot11Radio1.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 path-cost 500
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface GigabitEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
!
interface GigabitEthernet0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
!
interface GigabitEthernet0.3
```

```
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 path-cost 400
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 10000
bridge 1 protocol ieee
bridge 1 route ip
bridge 2 priority 12000
bridge 2 protocol ieee
bridge 3 priority 2900
bridge 3 protocol ieee
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```

Displaying Spanning-Tree Status

To display the spanning-tree status, use one or more of the privileged EXEC commands in Table 8-3.

Table 8-3 Commands for Displaying Spanning-Tree Status

Command	Purpose
show spanning-tree	Displays information on your network's spanning tree.
show spanning-tree blocked-ports	Displays a list of blocked ports on this bridge.
show spanning-tree bridge	Displays status and configuration of this bridge.
show spanning-tree active	Displays spanning-tree information on active interfaces only.
show spanning-tree root	Displays a detailed summary of information on the spanning-tree root.
show spanning-tree interface *interface-id*	Displays spanning-tree information for the specified interface.
show spanning-tree summary [**totals**]	Displays a summary of port states or displays the total lines of the STP state section.

For information about other keywords for the **show spanning-tree** privileged EXEC command, refer to the *Cisco Aironet IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release.