

Spanning Tree Protocol

- Spanning Tree Protocol, on page 2
- Establish the STP using BPDUs, on page 2
- BPDU exchange results, on page 3
- STP port roles, on page 4
- Bridge ID and switch priority, on page 4
- Port priority and path cost, on page 5
- Spanning-tree interface states, on page 6
- How a switch becomes the root switch, on page 9
- STP and redundant connectivity, on page 11
- Spanning-Tree address management, on page 11
- Accelerated aging to retain connectivity, on page 12
- Spanning-Tree modes and protocols, on page 12
- Spanning-Tree instances, on page 13
- Spanning-Tree interoperability and backward compatibility, on page 13
- Spanning-Tree interoperability and backward compatibility, on page 13
- Spanning tree and switch stacks, on page 14
- Configuration guidelines, on page 14
- Default configuration, on page 15
- Configure Spanning-Tree mode, on page 16
- Disable Spanning Tree on VLANs, on page 17
- Configure the root switch, on page 18
- Configure the secondary root switch, on page 19
- Configure port priority for an interface, on page 20
- Configure path cost for an interface, on page 21
- Configure VLAN switch priority, on page 22
- Configure VLAN hello time, on page 23
- Configure VLAN forward delay time, on page 24
- Configure maximum-aging time, on page 25
- Configure the transmit hold-count, on page 26
- Monitor Spanning Tree status, on page 27
- Additional references for STP, on page 27
- Feature information for STP, on page 28

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network.

- Ensures only one active path exists between any two stations in a Layer 2 Ethernet network.
- Prevents network loops that can cause duplicate messages and unstable network conditions.
- Operates transparently to end stations, which cannot detect the underlying network topology.

Path redundancy and loop prevention in Ethernet networks

STP is essential for maintaining a stable and loop-free Layer 2 Ethernet network by managing redundant paths and ensuring only one active path exists between any two stations.

Key functions

STP performs these essential functions.

- Prevents loops in the network by blocking redundant paths.
- Provides path redundancy for network reliability.
- Automatically recalculates topology when network segments fail.
- Operates transparently to end stations.

Supported STP modes

This topic identifies the three spanning-tree modes supported by the switch.

The switch supports the following spanning-tree modes:

- **PVST+ (Per-VLAN Spanning Tree Plus)** - Based on IEEE 802.1D standard with Cisco proprietary extensions
- **Rapid PVST+** - Based on IEEE 802.1w standard
- **MSTP (Multiple Spanning Tree Protocol)** - Based on IEEE 802.1s standard

Establish the STP using BPDUs

The STP uses a spanning-tree algorithm to select one switch as the root of the spanning tree in a redundantly connected network. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on its role in the active topology.

Procedure

Step 1 Power up all switches in the network.

When switches are powered up, the spanning-tree topology is established through a series of stages.

Step 2 Allow each switch to function as the root switch and send configuration BPDUs through all ports.

Step 3 Enable switches to communicate and compute the spanning-tree topology using BPDU information.

Step 4 Review the information contained in each configuration BPDU.

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

Step 5 When a switch receives a configuration BPDU with superior information (lower bridge ID, lower path cost), store the information for that port.

Step 6 If this BPDU is received on the root port of the switch, forward it with an updated message to all attached LANs for which it is the designated switch.

Step 7 If a switch receives a configuration BPDU with inferior information to that currently stored for that port, discard the BPDU.

Step 8 If the switch is a designated switch for the LAN from which the inferior BPDU was received, send that LAN a BPDU containing the up-to-date information stored for that port.

BPDU exchange results

A BPDU exchange results in these actions in a switched network.

- One switch in the network is elected as the root switch (the logical center of the spanning-tree topology in a switched network)
- For each VLAN, the switch with the highest switch priority (the lowest numerical priority value) is elected as the root switch. If all switchs are configured with the default priority (32768), the switch with the lowest MAC address in the VLAN becomes the root switch. The switch priority value occupies the most significant bits of the bridge ID
- A root port is selected for each switch (except the root switch). This port provides the best path (lowest cost) when the switch forwards packets to the root switch
- The shortest distance to the root switch is calculated for each switch based on the path cost

- A designated switch for each LAN segment is selected. The designated switch incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port
- All paths that are not needed to reach the root switch from anywhere in the switched network are placed in the spanning-tree blocking mode

STP port roles

The spanning-tree algorithm assigns roles to ports based on their function in the active topology.

- **Root** - Forwarding port elected for the spanning-tree topology.
- **Designated** - Forwarding port elected for every switched LAN segment.
- **Alternate** - Blocked port providing an alternate path to the root bridge.
- **Backup** - Blocked port in a loopback configuration.

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated Switch.

Spanning tree 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.

Switchs send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switchs do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending Switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

Bridge ID and switch priority

The bridge ID is a unique identifier assigned to each switch and VLAN, as required by the IEEE 802.1D standard, and is used to control the selection of the root switch.

- Each switch must have a unique bridge ID for every configured VLAN.
- The bridge ID is 8 bytes long: the first 2 bytes represent the switch priority, and the remaining 6 bytes are derived from the switch MAC address.
- With PVST+ and Rapid PVST+, each VLAN is treated as a separate logical bridge, requiring a distinct bridge ID per VLAN.

Bridge ID components with extended system ID

The 2 bytes previously used for the switch priority are reallocated into a 4-bit priority value and a 12-bit extended system ID value equal to the VLAN ID.

Table 1: Bits and their value

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

The bridge ID comprises:

- **Switch Priority** (2 bytes) - 4-bit priority value
- **Extended System ID** (2 bytes) - 12-bit value equal to the VLAN ID
- **MAC Address** (6 bytes) - Derived from the Switch MAC address

Spanning tree uses the extended system ID, the Switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN.

Support for the extended system ID affects how you manually configure the root Switch, the secondary root Switch, and the Switch priority of a VLAN. For example, when you change the Switch priority value, you change the probability that the Switch will be elected as the root Switch. Configuring a higher value decreases the probability; a lower value increases the probability.

Port priority and path cost

Port priority and path cost are key attributes used by the spanning tree protocol to determine which switch port forwards traffic and which port is blocked in the event of a network loop.

- **Port Priority** : Determines the preference of an interface for forwarding state selection. Lower numerical values have higher priority.
- **Path Cost** : Represents the cost associated with an interface, typically based on media speed. Lower cost values are preferred for forwarding.
- If all interfaces have the same priority or cost, the interface with the lowest interface number is selected for forwarding, and others are blocked.

Port priority and path cost and spanning tree

Port priority and path cost are used by spanning tree to control port states during network loops.

- The spanning-tree port priority value indicates a port's location in the network topology and its suitability for passing traffic.
- The path cost value is derived from the media speed of an interface and influences which interface is selected for forwarding.

1. Assign higher port priority (lower numerical value) to interfaces you want selected first.
2. Assign lower path cost values to interfaces you want selected first.

- Port priority: Assigning higher priority (lower value) increases the likelihood of an interface being selected for forwarding.
- Path cost: Assigning lower cost values increases the likelihood of an interface being selected for forwarding.

Table 2: comparision of port priority and path cost

Attribute	Port Priority	Path Cost
Default Value	128	Based on media speed
Selection Criteria	Lower value preferred	Lower value preferred

Note TIP: The short path cost method is the default STP path cost method.

Note TIP: If your switch is a member of a switch stack, assign lower cost values to interfaces you want selected first, rather than adjusting port priority.

Note TIP: By default, the switch sends keepalive messages only on interfaces without SFP modules. You can change this by entering the **[no] keepalive** interface configuration command.

Example: port priority and path cost selection

For example, if two interfaces have the same port priority and path cost, the interface with the lowest interface number is placed in the forwarding state, and the other is blocked.

Spanning-tree interface states

[Information Type: Reference]

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 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 switched LAN before starting to forward frames. They must allow the frame lifetime to expire for forwarded frames that have used the old topology.

Each layer 2 interface on a switch using spanning tree exists in one of these states:

State	Description
Blocking	Does not participate in frame forwarding
Listening	First transitional state after blocking when spanning tree decides the interface should participate in frame forwarding
Learning	Prepares to participate in frame forwarding
Forwarding	Forwards frames

State	Description
Disabled	Not participating in spanning tree due to shutdown, no link, or no spanning-tree instance

Interface state transitions

These stages describe how an interface transitions through spanning-tree states.

- From initialization to blocking.
- From blocking, the interface to listening or to disabled.
- From listening, the interface to learning or to disabled.
- From learning, the interface to forwarding or to disabled.
- From forwarding, the interface can move to disabled.

When you power up the Switch, spanning tree is enabled by default, and every interface in the Switch, VLAN, or network goes through the blocking state and the transitory states of listening and learning. Spanning tree stabilizes each interface at the forwarding or blocking state.

Forwarding state transitions

When the spanning-tree algorithm places a Layer 2 interface in the forwarding state, a specific sequence of state transitions occurs.

Summary

These actors and components participate in this process:

- Spanning-tree algorithm: Manages the state transitions of Layer 2 interfaces.
- Layer 2 interface: Undergoes state changes as directed by the spanning-tree protocol.
- Forward-delay timer: Controls timing for transitions between states.
- Switch: Learns end-station location information during the learning state.

This process summarizes how a layer 2 interface transitions through listening, learning, and forwarding states under the control of the spanning-tree algorithm.

Workflow

These stages describe the transitions a layer 2 interface undergoes when moving to the forwarding state.

1. The interface enters the listening state while spanning tree waits for protocol information to determine if it should move to the blocking state.
    - The interface is in the listening state.
    - Spanning tree waits for protocol information.

2. Spanning tree moves the interface to the learning state and resets the forward-delay timer while waiting for the timer to expire.
    - The interface transitions to the learning state.
    - The forward-delay timer is reset.
3. In the learning state, the interface continues to block frame forwarding as the Switch learns end-station location information for the forwarding database.
    - Frame forwarding remains blocked.
    - The Switch learns end-station locations for the forwarding database.
4. When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, enabling both learning and frame forwarding.
    - The forward-delay timer expires.
    - The interface enters the forwarding state.
    - Both learning and frame forwarding are enabled.

Interface state functions

This topic describes the functions performed by layer 2 interfaces in each spanning tree state: blocking, listening, learning, forwarding, and disabled.

Blocking state

After initialization, a BPDU is sent to each switch interface. A switch initially functions as the root until it exchanges BPDUs with other switchs. This exchange establishes which switch in the network is the root or root switch. If there is only one switch in the network, no exchange occurs, the forward-delay timer expires, and the interface moves to the listening state.

An interface always enters the blocking state after switch initialization.

An interface in the blocking state performs these functions:

- Discards frames received on the interface.
- Discards frames switched from another interface for forwarding.
- Does not learn addresses.
- Receives BPDUs.

Listening state:

The listening state is the first state a layer 2 interface enters after the blocking state. The interface enters this state when the spanning tree decides that the interface should participate in frame forwarding.

An interface in the listening state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding

- Does not learn addresses
- Receives BPDUs

Learning state:

A layer 2 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 these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Learns addresses
- Receives BPDUs

Forwarding state:

A layer 2 interface in the forwarding state forwards frames. The interface enters the forwarding state from the learning state.

An interface in the forwarding state performs these functions:

- Receives and forwards frames received on the interface
- Forwards frames switched from another interface
- Learns addresses
- Receives BPDUs

Disabled state:

A layer 2 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 these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Does not receive BPDUs

How a switch becomes the root switch

These stages describe how the root switch is elected.

Summary

In a network with multiple switches, the root switch is elected based on spanning-tree protocol settings.

- Switch: Participates in the election process and can become the root switch depending on its priority and MAC address.

The process involves evaluating switch priorities and MAC addresses to determine the root switch, and optionally adjusting priorities to select the ideal root switch.

Workflow

These stages describe how a switch becomes the root switch in a spanning-tree enabled network.

1. If all switches in a network are enabled with default spanning-tree settings, the switch with the lowest MAC address becomes the root switch.
2. The switch priority of all switches is set to the default value (32768).
3. In the example topology, Switch A is elected as the root switch because all switches have the default priority (32768) and Switch A has the lowest MAC address.
4. However, due to traffic patterns, number of forwarding interfaces, or link types, Switch A might not be the ideal root switch.
5. By increasing the priority (lowering the numerical value) of the ideal switch so that it becomes the root switch, you force a spanning-tree recalculation to form a new topology with the ideal switch as the root.

Root port change

A root port change occurs in a spanning-tree topology when a port with a higher-speed link is configured with a higher priority (lower numerical value) than the current root port, causing the faster link to become the new root port.

- Spanning-tree topology may not always select the fastest link as the root port by default.
- Changing the port priority on a higher-speed link can influence which port becomes the root port.
- Optimizing port priorities can improve network efficiency by selecting the best available link as the root port.

Root port change in Spanning-tree topology

When the spanning-tree topology is calculated using default parameters, the selected path between source and destination may not utilize the fastest available link.

Example: Changing the Root Port to a Faster Link

For example, if switch B has both a Gigabit Ethernet link and a 10/100 link, and the 10/100 link is currently the root port, network traffic may be more efficient over the Gigabit Ethernet link. By configuring the spanning-tree port priority on the Gigabit Ethernet port to a higher priority (lower numerical value) than the root port, the Gigabit Ethernet port becomes the new root port.

STP and redundant connectivity

- Spanning tree allows redundant backbone connections between switches by connecting multiple interfaces.
- It automatically disables one interface to prevent network loops, but re-enables it if the active link fails.
- Redundant links can also be created using EtherChannel groups.

Redundant connectivity with STP

STPmanages redundant links between switches to prevent loops and maintain network stability.

- When two switch interfaces are connected to another switch or to two different switches, spanning tree disables one interface to avoid loops.
- If one link is high-speed and the other is low-speed, the low-speed link is always disabled.
- If both links have the same speed, spanning tree uses port priority and port ID to determine which link to disable.

Spanning Tree redundant links

For example, if two switches are connected by two links, one fast and one slow spanning tree disables the slow link. If both links are the same speed, the protocol disables the link with the highest combined port priority and port ID value.

Spanning-Tree address management

Spanning-Tree address management refers to the handling of specific multicast addresses as defined by IEEE 802.1D for bridge protocols, and how switches process these addresses based on spanning-tree state.

- IEEE 802.1D specifies 17 static multicast addresses (0x00180C2000000 to 0x0180C2000010) for bridge protocols.
- These addresses are static and cannot be removed from the switch configuration.
- Switches receive but do not forward packets destined for addresses between 0x0180C2000000 and 0x0180C200000F, regardless of spanning-tree state.

Spanning-Tree address handling and forwarding behavior

Spanning-tree address management involves specific behaviors for packet forwarding and receiving, depending on whether spanning tree is enabled or disabled on the switch.

- If spanning tree is enabled, the CPU on the switch or on each switch in the stack receives packets destined for 0x0180C2000000 and 0x0180C2000010.
- If spanning tree is disabled, the switch or each switch in the stack forwards those packets as unknown multicast addresses.

Accelerated aging to retain connectivity

Accelerated aging is a mechanism that reduces the address-aging time for dynamic MAC addresses during spanning-tree reconfiguration, enabling the network to quickly relearn station locations and maintain connectivity.

- The default aging time for dynamic addresses is 5 minutes, set by the **mac address-table aging-time** global configuration command.
- During a spanning-tree reconfiguration, the address-aging time is accelerated to match the forward-delay parameter value.
- Accelerated aging is applied on a per-VLAN basis, affecting only the VLANs undergoing reconfiguration.

Accelerated aging reconfiguration

Accelerated aging ensures that after a spanning-tree reconfiguration, outdated dynamic MAC addresses are quickly removed and relearned, minimizing the period during which stations may be unreachable.

Accelerated aging in action

For example, if a spanning-tree reconfiguration occurs on VLAN 10, the switch accelerates the aging of dynamic addresses on VLAN 10 to the forward-delay value, allowing the network to promptly relearn the correct station locations and restore connectivity.

Spanning-Tree modes and protocols

The Switch supports these spanning-tree modes and protocols: PVST+, Rapid PVST+, and MSTP.

PVST+ - This spanning-tree mode is based on the IEEE 802.1D standard and Cisco proprietary extensions. PVST+ runs on each VLAN on the Switch up to the maximum supported, ensuring that each has a loop-free path through the network. PVST+ provides Layer 2 load-balancing for the VLAN on which it runs. You can create different logical topologies by using the VLANs on your network to ensure that all of your links are used but that no one link is oversubscribed. Each instance of PVST+ on a VLAN has a single root Switch. This root Switch propagates the spanning-tree information associated with that VLAN to all other Switchs in the network. Because each Switch has the same information about the network, this process ensures that the network topology is maintained.

Rapid PVST+ - This spanning-tree mode is the same as PVST+ except that it uses rapid convergence based on the IEEE 802.1w standard. Rapid PVST+ is the STP default mode. To provide rapid convergence, Rapid PVST+ immediately deletes dynamically learned MAC address entries on a per-port basis upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC address entries. Rapid PVST+ uses the same configuration as PVST+ (except where noted), and the Switch needs only minimal extra configuration. The benefit of Rapid PVST+ is that you can migrate a large PVST+ install base to Rapid PVST+ without having to learn the complexities of the Multiple Spanning Tree Protocol (MSTP) configuration and without having to reprovision your network. In Rapid PVST+ mode, each VLAN runs its own spanning-tree instance up to the maximum supported.

MSTP - This spanning-tree mode is based on the IEEE 802.1s standard. You can map multiple VLANs to the same spanning-tree instance, which reduces the number of spanning-tree instances required to support a

large number of VLANs. MSTP runs on top of RSTP (based on IEEE 802.1w), which provides for rapid convergence of the spanning tree by eliminating the forward delay and by quickly transitioning root ports and designated ports to the forwarding state. In a Switch stack, the cross-stack rapid transition (CSRT) feature performs the same function as RSTP. You cannot run MSTP without RSTP or CSRT.

Spanning-Tree instances

This topic provides reference information about the number of spanning-tree instances supported in different spanning-tree modes.

- In PVST+ or Rapid PVST+ mode, the Switch or Switch stack supports up to 128 spanning-tree instances.
- In MSTP mode, the Switch or Switch stack supports up to 64 MST instances. The number of VLANs that can be mapped to a particular MST instance is 512.

Spanning-Tree interoperability and backward compatibility

In a mixed MSTP and PVST+ network, the common spanning-tree (CST) root must be inside the MST backbone, and a PVST+ switch cannot connect to multiple MST regions.

When a network contains switchs running Rapid PVST+ and switchs running PVST+, we recommend that the Rapid PVST+ switchs and PVST+ switchs be configured for different spanning-tree instances. In the Rapid PVST+ spanning-tree instances, the root switch must be a Rapid PVST+ switch. In the PVST+ instances, the root switch must be a PVST+ switch. The PVST+ switchs should be at the edge of the network.

All stack members run the same version of spanning tree (all PVST+, all Rapid PVST+, or all MSTP).

PVST+, MSTP, and Rapid-PVST+ Interoperability and Compatibility:

PVST+	MSTP	Rapid PVST+	
PVST+	Yes	Yes (with restrictions)	Yes (reverts to PVST+)
MSTP	Yes (with restrictions)	Yes	Yes (reverts to PVST+)
Rapid PVST+	Yes (reverts to PVST+)	Yes (reverts to PVST+)	Yes

Spanning-Tree interoperability and backward compatibility

In a mixed MSTP and PVST+ network, the common spanning-tree (CST) root must be inside the MST backbone, and a PVST+ Switch cannot connect to multiple MST regions.

When a network contains Switchs running Rapid PVST+ and Switchs running PVST+, we recommend that the Rapid PVST+ Switchs and PVST+ Switchs be configured for different spanning-tree instances. In the Rapid PVST+ spanning-tree instances, the root Switch must be a Rapid PVST+ Switch. In the PVST+ instances, the root Switch must be a PVST+ Switch. The PVST+ Switchs should be at the edge of the network.

All stack members run the same version of spanning tree (all PVST+, all Rapid PVST+, or all MSTP).

PVST+, MSTP, and Rapid-PVST+ Interoperability and Compatibility:

Table 3: PVST+, MSTP, and Rapid-PVST+ Interoperability and Compatibility

PVST+	MSTP	Rapid PVST+	
PVST+	Yes	Yes (with restrictions)	Yes (reverts to PVST+)
MSTP	Yes (with restrictions)	Yes	Yes (reverts to PVST+)
Rapid PVST+	Yes (reverts to PVST+)	Yes (reverts to PVST+)	Yes

Spanning tree and switch stacks

- A switch stack operating in PVST+ or Rapid PVST+ mode appears as a single spanning-tree node to the rest of the network, and all stack members use the same bridge ID derived from the MAC address of the active stack.
- When a new switch joins the stack, it adopts the active stack bridge ID; if it has the lowest ID and equal root path cost, it becomes the stack root.
- When a stack member leaves, spanning-tree reconvergence occurs, and the remaining member with the lowest stack port ID becomes the stack root.
- Spanning-tree reconvergence may also occur if a neighboring switch external to the stack fails or is powered down, or if a new external switch is added to the network.

Spanning tree and switch stack reference information

Spanning tree operation in switch stacks involves bridge ID assignment, stack root election, and reconvergence processes during topology changes.

Spanning tree behavior in switch stacks

For example, if a new switch with the lowest ID joins an existing stack, it becomes the stack root if root path costs are equal. If a stack member leaves, the member with the lowest stack port ID becomes the new root.

Configuration guidelines

Configure all system parameters according to the established baseline to prevent unexpected behavior. Always verify settings in a staging environment before applying them to production devices.

Root switch configuration guidelines

Do not configure access Switchs as root: The root Switch for each spanning-tree instance should be a backbone or distribution Switch. Do not configure an access Switch as the spanning-tree primary root.

Consider network topology: Because of traffic patterns, number of forwarding interfaces, or link types, the Switch with the lowest MAC address might not be the ideal root Switch.

Use diameter and hello keywords appropriately: When you specify the network diameter, the Switch automatically sets 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.

Configuration change restrictions

Priority value limitations: An attempt to configure a switch as the root switch fails if the value necessary to be the root switch is less than 1.

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

Root switch placement: The root switch for each spanning-tree instance should be a backbone or distribution switch. Do not configure an access switch as the spanning-tree primary root.

Default configuration

This reference provides the default settings for spanning-tree features on Cisco devices.

Table 4: Default Spanning-Tree configuration settings

Feature	Default Setting
Enable state	Enabled on VLAN 1
Spanning-tree mode	Rapid PVST+ (PVST+ and MSTP are disabled)
Switch priority	32768
Spanning-tree port priority (configurable on a per-interface basis)	128
Spanning-tree port cost (configurable on a per-interface basis)	• 1000 Mb/s: 4 • 100 Mb/s: 19 • 10 Mb/s: 100
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	• 1000 Mb/s: 4 • 100 Mb/s: 19 • 10 Mb/s: 100

Feature	Default Setting
Spanning-tree timers	• Hello time: 2 seconds • Forward-delay time: 15 seconds • Maximum-aging time: 20 seconds • Transmit hold count: 6 BPDUs

Configure Spanning-Tree mode

You can change the spanning-tree mode from the default Rapid PVST+ to PVST+ or MSTP.

This task allows you to select the appropriate spanning-tree protocol for your network based on convergence requirements and VLAN scalability needs.

Perform these steps to change the spanning-tree mode.

Before you begin

If you want to enable a mode that is different from the default mode, this procedure is required.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Switch> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 Use the **spanning-tree mode** command to configure a spanning-tree mode.

Example:

```
Switch(config)# spanning-tree mode {pvst | mst | rapid-pvst}
```

Select **pvst** to enable PVST+

Select **mst** to enable MSTP

Select **rapid-pvst** to enable Rapid PVST+

Step 4 Use the **interface** command to specify an interface to configure and enter interface configuration mode.

Example:

```
Switch(config)# interface interface-id
```

Valid interfaces include physical ports, VLANs, and port channels. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 48.

Step 5 Use the **spanning-tree link-type point-to-point** command to specify that the link type for this port is point-to-point.

Example:

```
Switch(config-if)# spanning-tree link-type point-to-point
```

If you connect this port (local port) to a remote port through a point-to-point link and the local port becomes a designated port, the Switch negotiates with the remote port and rapidly changes the local port to the forwarding state.

Step 6 Use the **end** command to return to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

Step 7 (Optional) Use the **clear spanning-tree detected-protocols** command to restart the protocol migration process on the entire Switch.

Example:

```
Switch# clear spanning-tree detected-protocols
```

If any port on the switch is connected to a port on a legacy IEEE 802.1D switch, this command restarts the protocol migration process on the entire Switch.

This step is optional if the designated switch detects that this switch is running sapid PVST+.

The spanning-tree mode is changed and configured on the switch.

Disable Spanning Tree on VLANs

You can disable spanning tree on specific VLANs when you are certain there are no loops in the network topology.

This task allows you to disable spanning tree protection on VLANs where loops cannot occur, but use extreme caution as disabling spanning tree when loops are present can drastically reduce network performance.



Note When spanning tree is disabled and loops are present in the topology, excessive traffic and indefinite packet duplication can drastically reduce network performance.

Before you begin

Spanning tree is enabled by default on VLAN 1 and on all newly created VLANs up to the spanning-tree limit. Disable spanning tree only if you are sure there are no loops in the network topology.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Switch> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 Use the **no spanning-tree vlan** command to disable spanning tree for the specified VLAN.

Example:

```
Switch(config)# no spanning-tree vlan vlan-id
```

For `vlan-id`, the range is 1 to 4094.

Step 4 Use the **end** command to return to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

Configure the root switch

You can configure a switch as the root for the specified VLAN by modifying the switch priority to a significantly lower value.

This task enables you to control which switch becomes the root bridge for optimal network traffic flow and convergence by automatically setting the switch priority to 24576 if this value will cause the switch to become the root.

Before you begin

To configure a switch as the root for the specified VLAN, use the **spanning-tree vlan vlan-id root** global configuration command to modify the switch priority from the default value (32768) to a significantly lower value.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Switch> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 Use the **spanning-tree vlan** *vlan-id* **root primary** command to configure a switch to become the root for the specified VLAN.

Example:

```
Switch(config)# spanning-tree vlan vlan-id root primary [diameter net-diameter]
```

When you enter this command, the software checks the Switch priority of the root Switchs for each VLAN. Because of the extended system ID support, the Switch sets its own priority for the specified VLAN to 24576 if this value will cause this Switch to become the root for the specified VLAN.

For `vlan-id`, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

(Optional) For `diameter net-diameter`, specify the maximum number of Switchs between any two end stations. The range is 2 to 7.

Use the diameter keyword to specify the Layer 2 network diameter (that is, the maximum number of Switch hops between any two end stations in the Layer 2 network). When you specify the network diameter, the Switch 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.

Step 4 Use the **end** command to return to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

Configure the secondary root switch

You can configure a Switch as the secondary root by modifying the Switch priority from the default value (32768) to 28672.

This task ensures that the Switch is likely to become the root Switch for the specified VLAN if the primary root Switch fails, assuming other network Switchs use the default Switch priority of 32768.

Before you begin

When you configure a Switch as the secondary root, the Switch priority is modified from the default value (32768) to 28672. With this priority, the Switch is likely to become the root Switch for the specified VLAN if the primary root Switch fails. This is assuming that the other network Switchs use the default Switch priority of 32768, and therefore, are unlikely to become the root Switch.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Switch> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 Use the **spanning-tree vlan** *valn-id* **root secondary** command to configure a Switch to become the secondary root for the specified VLAN.

Example:

```
Switch(config)# spanning-tree vlan vlan-id root secondary [diameter net-diameter]
```

For `vlan-id`, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

(Optional) For `diameter net-diameter`, specify the maximum number of Switchs between any two end stations. The range is 2 to 7.

Use the same network diameter value that you used when configuring the primary root Switch.

Step 4 Use the **end** command to return to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

Configure port priority for an interface

You can configure the port priority for an interface to control which interface spanning tree selects when a loop occurs.

This task allows you to 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, with spanning tree putting the interface with the lowest interface number in the forwarding state if all interfaces have the same priority value.

Before you begin

Perform these steps to configure path cost for an interface.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Switch> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 Use the **interface** *interface_id* command to specify an interface to configure and enter interface configuration mode.

Example:

```
Switch(config)# interface 10
```

Valid interfaces include physical ports and port-channel logical interfaces (port-channel port-channel-number).

Step 4 Use the **spanning-tree port-priority** *priority_val* command to configure the port priority for an interface.

Example:

```
Switch(config-if)# spanning-tree port-priority 100
```

For `priority_val`, the range is 0 to 240, in increments of 16; the default is 128. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.

Step 5 Use the **spanning-tree vlan port-priority** *vlan_id* **port-priority** *port-priority_val* command to configure the port priority for a VLAN.

Example:

```
Switch(config-if)# spanning-tree 100 port-priority 1000
```

If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.

For `vlan-id`, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

For `port-priority_val`, the range is 1 to 200000000; the default value is derived from the media speed of the interface.

Step 6 Use the **end** command to return to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

Configure path cost for an interface

You can configure the path cost for an interface to control which interface spanning tree places into the forwarding state when a loop occurs.

This task enables you to assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last, with lower path cost representing higher-speed transmission and spanning tree putting the interface with the lowest interface number in the forwarding state if all interfaces have the same cost value.

Before you begin

Perform these steps to configure path cost for an interface.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Switch> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 Use the **interface** *interface-id* command to specify an interface to configure and enter interface configuration mode.

Example:

```
Switch(config)# interface interface-id
```

Valid interfaces include physical ports and port-channel logical interfaces (port-channel port-channel-number).

Step 4 Use the **spanning-tree cost** *cost* command to configure the cost for an interface.

Example:

```
Switch(config-if)# spanning-tree cost cost
```

If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.

For `cost`, the range is 1 to 200000000; the default value is derived from the media speed of the interface.

Step 5 Use the **spanning-tree vlan** *vlan_id* **cost** *cost* command to configure the cost for a VLAN.

Example:

```
Switch(config-if)# spanning-tree vlan 10 cost 1000
```

If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.

For `vlan-id`, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

For `cost`, the range is 1 to 200000000; the default value is derived from the media speed of the interface.

Step 6 Use the **end** command to return to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

Configure VLAN switch priority

You can configure the Switch priority to make it more likely that a standalone Switch or a Switch in the stack will be chosen as the root Switch.

This task enables you to control root Switch selection by directly setting the Switch priority value for a VLAN, but exercise care when using this command as it directly manipulates priority values rather than using the recommended root primary and root secondary commands.

For most situations, we recommend that you use the **spanning-tree vlan vlan-id root primary** and **spanning-tree vlan vlan-id root secondary** global configuration commands to modify the Switch priority.

Before you begin

Perform these steps to configure switch priority.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Switch> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 Use the **spanning-tree vlan** *vlan_id* **priority** *priority* command to configure the Switch priority of a VLAN.

Example:

```
Switch(config)# spanning-tree vlan 10 priority 1
```

For `vlan-id`, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 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 Switch will be chosen as the root Switch. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Step 4 Use the **end** command to return to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

Configure VLAN hello time

You can configure the hello time of a VLAN to control the time interval between configuration messages generated and sent by the root Switch.

This task enables you to adjust how frequently the root Switch sends messages to indicate that it is alive.

Before you begin

Perform these steps to configure VLAN hello time.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Switch> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 Use the **spanning-tree vlan hello-time** command to configure the hello time of a VLAN.

Example:

```
Switch(config)# spanning-tree vlan vlan-id hello-time seconds
```

The hello time is the time interval between configuration messages generated and sent by the root Switch. These messages mean that the Switch is alive.

For `vlan-id`, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

For `seconds`, the range is 4 to 30 and the default is 2.

Step 4 Use the **end** command to return to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

Configure VLAN forward delay time

You can configure the forward time of a VLAN to control how long an interface waits before changing from its spanning-tree learning and listening states to the forwarding state.

This task enables you to adjust the forwarding delay, which is the number of seconds an interface waits before transitioning states.

Before you begin

Perform these steps to configure forwarding-delay time.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Switch> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 Use the **spanning-tree vlan forward-time** command to configure the forward time of a VLAN.

Example:

```
Switch(config)# spanning-tree vlan vlan-id forward-time seconds
```

The forwarding delay is the number of seconds an interface waits before changing from its spanning-tree learning and listening states to the forwarding state.

For `vlan-id`, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

For `seconds`, the range is 4 to 30 and the default is 15.

Step 4 Use the **end** command to return to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

Configure maximum-aging time

You can configure the maximum-aging time of a VLAN to control how long a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.

This task enables you to adjust the maximum-aging time to determine when the switch should consider configuration information stale and trigger topology recalculation.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Switch> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 Use the **spanning-tree vlan max-age** command to configure the maximum-aging time of a VLAN.

Example:

```
Switch(config)# spanning-tree vlan vlan-id max-age seconds
```

The maximum-aging time is the number of seconds a Switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.

For `vlan-id`, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

For `seconds`, the range is 6 to 40; the default is 20.

Step 4 Use the **end** command to return to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

Configure the transmit hold-count

You can configure the BPDU burst size by changing the transmit hold count value to control the number of BPDUs that can be sent before pausing.

This task enables you to adjust the transmit hold-count. Changing this parameter to a higher value can have a significant impact on CPU utilization, especially in rapid PVST+ mode, so maintain the default setting unless specifically required.



Note Changing this parameter to a higher value can have a significant impact on CPU utilization, especially in Rapid PVST+ mode. Lowering this value can slow down convergence in certain scenarios. We recommend that you maintain the default setting.

Before you begin

Perform these steps to configure transmit hold-count.

Procedure

Step 1 Use the **enable** command to enter privileged EXEC mode.

Example:

```
Switch> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Switch# configure terminal
```

Step 3 Use the **no spanning-tree vlan** command to disable spanning tree for the specified VLAN.

Example:

```
Switch(config)# no spanning-tree vlan vlan-id
```

For `vlan-id`, the range is 1 to 4094.

Step 4 Use the **end** command to return to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

Monitor Spanning Tree status

Use these commands to display spanning-tree status.

Table 5: Spanning-Tree Status Commands

Command	Description
`show spanning-tree active`	Display spanning-tree information on active interfaces only
`show spanning-tree detail`	Display a detailed summary of interface information
`show spanning-tree vlan vlan-id`	Display spanning-tree information for the specified VLAN
`show spanning-tree interface interface-id`	Display spanning-tree information for the specified interface
`show spanning-tree interface interface-id portfast`	Display spanning-tree portfast information for the specified interface
`show spanning-tree summary [totals]`	Display a summary of interface states or display the total lines of the STP state section

To clear spanning-tree counters, use the **clear spanning-tree [interface interface-id]** privileged EXEC command.

Additional references for STP

Related documents

For additional information, see the related documents in this guide.

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All the supported MIBs for this release	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature information for STP

Release	Modification
Cisco IOS XE 17.18.1	This feature was introduced