Spanning Tree Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches

Cisco Catalyst IE9300 Rugged Series
Updated March 2, 2026

Full Cisco Trademarks with Software License

Topics included

1 Spanning Tree Protocol

Topics:

Spanning Tree Protocol

This topic explains the Spanning Tree Protocol (STP), a Layer 2 link management protocol that provides path redundancy and prevents loops in Ethernet networks, ensuring network stability and proper operation.

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 manages redundant paths and ensures only one active path exists between any two stations to maintain a stable and loop-free Layer 2 Ethernet network.

Key functions

This topic explains the essential functions performed by STP, including loop prevention, path redundancy, and network topology recalculation.

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

Describes the spanning-tree modes supported by the switch to ensure network loop prevention and redundancy. These modes provide compatibility with various IEEE standards and Cisco proprietary extensions.

This topic identifies the three Spanning Tree modes supported by the switch.

The switch supports these 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

Learn how to establish the Spanning Tree topology in a Layer 2 network using Bridge Protocol Data Units (BPDUs) to ensure a loop-free path and assign port roles.

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

1. Power on all switches in the network.

   When switches are powered on, the Spanning Tree topology establishes itself in multiple stages.

2. Allow each switch to function as the root switch and send configuration BPDUs through all ports.
3. Enable switches to exchange BPDU information in order to compute the Spanning Tree topology.
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.
5. When a switch receives a configuration BPDU with superior information (lower bridge ID, lower path cost), store the information for that port.
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.
7. If a switch receives a configuration BPDU with information less preferable than the information currently stored for that port, discard the BPDU.
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

This topic explains the actions that result from a BPDU exchange in a switched network, including root switch election, port selection, and path blocking in the Spanning Tree topology.

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 switches 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 is stored in 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 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 that connects the designated switch 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

This topic explains the roles assigned to ports by the Spanning Tree algorithm and how these roles affect network topology and redundancy.

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.

Switches send and receive Spanning Tree frames, known as bridge protocol data units (BPDUs), at regular intervals. Switches do not forward these frames; instead, they use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including the switch MAC address, switch priority, port priority, and path cost. Spanning Tree 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.

Bridge ID and switch priority

This topic explains the concept of Bridge ID and Switch Priority in IEEE 802.1D, describing how each switch and VLAN is uniquely identified and how the bridge ID is constructed.

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

- Each switch must have a unique bridge ID for every configured VLAN.
- The bridge ID is eight bytes long. The first two bytes represent the switch priority, and the remaining six 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

This topic explains how the bridge ID is constructed using the switch priority, extended system ID, and MAC address, and describes the impact of the extended system ID on spanning tree configuration.

The two bytes previously used for the switch priority are reallocated into a four-bit priority value and a twelve-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 includes these components:

- **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

The extended system ID, switch priority, and Spanning Tree MAC address together make each bridge ID unique for each VLAN.

Support for the extended system ID affects how you configure the root switch, secondary root switch, and VLAN switch priority. If you set a higher priority value, your switch is less likely to become the root switch. If you set a lower value, your switch is more likely to become the root switch.

Port priority and path cost

This topic explains how Spanning Tree port priority and path cost settings determine which switch port is placed in the forwarding or blocking state when a loop occurs, and describes how these values influence interface selection.

Port priority and path cost help the STP determine the forwarding and blocking state of switch ports during 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 interface cost, usually based on media speed. Lower values are preferred for forwarding.
- If all interfaces have the same priority or cost, Spanning Tree selects the interface with the lowest interface number for forwarding. The remaining interfaces are blocked.

Port priority, path cost, and Spanning Tree

Spanning tree uses port priority and path cost to control port states during network loops.

- The spanning-tree port priority value shows where the port is in the network and whether it should pass traffic.
- The path cost value is based on the interface's media speed and affects which interface is chosen for forwarding.

1. Assign a higher port priority (lower 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) makes it more likely the interface will be selected for forwarding.
- **Path cost**: Assigning lower cost values increases the likelihood of an interface being selected for forwarding.

Table 2: Comparison 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

The short path cost method is the default STP path cost method.

Note

If your switch is a member of a switch stack, assign lower cost values to interfaces you want selected first. Avoid adjusting port priority in this situation.

Note

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.

Port priority and path cost selection

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

Spanning Tree interface states

Lists the five states that layer 2 interfaces can exist in when using Spanning Tree protocol.

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can occur at varying times and locations within a switched network. An interface that transitions directly from nonparticipation in Spanning Tree topology to the forwarding state 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 frames forwarded using the old topology.

Each layer 2 interface on a switch using Spanning Tree exists in one of these states:

State	Description
Blocking	The interface does not participate in forwarding frames.
Listening	This is the first transitional state after blocking, when Spanning Tree determines that the interface should participate in forwarding frames.
Learning	The interface prepares to participate in forwarding frames.
Forwarding	The interface forwards frames.
Disabled	The interface is not participating in Spanning Tree because it is shut down, there is no link, or no Spanning Tree instance exists.

Interface state transitions

This topic explains how an interface transitions through spanning-tree states, including the sequence of state changes and the default behavior when a switch is powered up.

These stages describe how an interface transitions through Spanning Tree states.

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

When you power up the switch, the spanning tree feature is enabled by default. Every interface in the switch, VLAN, or network goes through the blocking state, then transitions through the intermediate listening and learning states. The Spanning Tree protocol stabilizes each interface in either the forwarding or blocking state.

How forwarding state transitions work

This process describes the sequence of state transitions that a layer 2 interface undergoes when the Spanning Tree algorithm places it in the forwarding state.

The Spanning Tree algorithm places a layer 2 interface in the forwarding state. When this occurs, the interface goes through a specific sequence of state transitions.

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 explains the functions and behaviors of layer 2 interface states, including blocking, listening, learning, forwarding, and disabled states in a switching environment.

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. It remains in this role until it exchanges BPDUs with other switches. 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

When a layer 2 interface enters the learning state from the listening state, it prepares to participate in frame forwarding.

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

When a layer 2 interface enters the forwarding state from the learning state, it begins forwarding frames.

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

When a layer 2 interface enters the disabled state, it does not participate in frame forwarding or the Spanning Tree and becomes 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

This process describes how a switch is elected as the root switch in a network using default spanning-tree settings and how the root switch can be changed by adjusting switch priority.

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 (32,768).
3. In the example topology, switch A is elected as the root switch because all switches have the default priority (32,768) 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. Increase the priority (lower the numerical value) of the ideal switch to make it the root switch. This action triggers a Spanning Tree recalculation and forms a new topology with the ideal switch as the root.

Root port change

This topic explains how a root port change can occur in a spanning-tree topology when higher-speed links are present, and how adjusting port priorities can optimize network traffic flow.

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. As a result, the faster link becomes 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 STP 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.

Change the root port to a faster link

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. Configure the Spanning Tree port priority on the Gigabit Ethernet port to a higher priority (lower numerical value) than the root port. After configuration, the Gigabit Ethernet port becomes the new root port.

STP and redundant connectivity

This topic explains how spanning tree protocol enables redundant connectivity between switches by automatically managing link states to prevent loops and ensure network reliability.

- 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

STP manages 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

If two switches are connected by two links, one fast and one slow, Spanning Tree disables the slow link. If both links have the same speed, Spanning Tree uses the port priority and port ID to determine which link to disable.

Spanning Tree address management

This topic explains how IEEE 802.1D defines and manages multicast addresses for Spanning Tree protocols, including address handling and forwarding behavior on switches depending on the spanning-tree state.

Spanning Tree address management explains how switches handle specific multicast addresses, as defined by IEEE 802.1D, based on their Spanning Tree state.

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

Spanning Tree address handling and forwarding behavior

Spanning Tree address management determines how your switch forwards and receives packets, depending on whether spanning tree is enabled or disabled.

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

Accelerated aging to retain connectivity

This topic explains how accelerated aging is used to retain network connectivity by reducing the address-aging time during spanning-tree reconfiguration events, allowing dynamic addresses to be quickly relearned and minimizing connectivity loss.

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

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

This topic explains the spanning-tree modes and protocols supported by the switch, including PVST+, Rapid PVST+, and MSTP, and describes their key features and differences.

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. This architecture ensures that each VLAN 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 configuring VLANs on your network. This approach ensures that all links are utilized while preventing any single link from being 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 switches 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. In 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 serves the same function as RSTP. You cannot run MSTP without RSTP or CSRT.

Spanning Tree instances

This topic explains the supported spanning-tree instances for PVST+, Rapid PVST+, and MSTP modes on the Switch or Switch stack.

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

This topic explains interoperability and backward compatibility considerations for Spanning Tree Protocols (PVST+, MSTP, and Rapid PVST+) in mixed network environments.

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 switches running Rapid PVST+ and switches running PVST+, configure the Rapid PVST+ switches and PVST+ switches for different Spanning Tree instances. In Rapid PVST+ spanning-tree instances, use a Rapid PVST+

switch as the root. In PVST+ instances, use a PVST+ switch as the root. The PVST+ switches 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+	Interoperability and Compatibility
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

This topic explains how Spanning Tree operates in switch stacks, including the behavior of bridge IDs, stack root election, and reconvergence scenarios when switches join or leave the stack or network.

- 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, which is 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

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

Provides guidelines for configuring system parameters to ensure optimal performance and stability. These standards help administrators maintain consistent settings across the network infrastructure.

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

Use these guidelines when configuring root switches in a spanning-tree topology to ensure optimal network performance and stability.

Do not configure access switches 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

Use these guidelines when configuring Spanning Tree root switches to avoid issues with priority values, extended system ID compatibility, and root switch placement in your network.

Priority value limitations: You cannot configure a switch as the root switch if the required value is less than 1.

Extended system ID impact: If your network includes switches both with and without extended system ID support, a switch that supports the extended system ID is unlikely to become the root switch. The extended system ID increases the switch priority value when the VLAN number exceeds the priority value of connected switches running older software.

Root switch placement: Assign a backbone or distribution switch as the root switch for each Spanning Tree instance. Do not make an access switch the Spanning Tree primary root.

Default configuration

This topic explains the default configuration settings for Spanning Tree features, including enable state, mode, priorities, port costs, and timers on Cisco devices.

This reference provides the default settings for Spanning Tree features on Cisco devices.

Table 3: 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

Learn how to change the spanning-tree mode from the default Rapid PVST+ to PVST+ or MSTP to meet your network's convergence and VLAN scalability requirements.

You can change the Spanning Tree mode from the default rapid PVST+ to PVST+ or MSTP.

This task allows you to select the appropriate STP 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

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

   Example

   ```
   Switch> enable
   ```

   Enter your password if prompted.

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

   Example

   ```
   Switch# configure terminal
   ```

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+

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 values range from 1 to 4094. The port channel values range from 1 to 48.

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.

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

Example

```
Switch(config)# end
```

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 connects to a port on a legacy IEEE 802.1D switch, this command restarts the protocol migration process for the switch.

This step is optional if the designated switch detects that this switch is running rapid PVST+. The switch changes and configures the Spanning Tree mode.

Disable Spanning Tree on VLANs

Learn how to disable spanning tree on specific VLANs when you are certain there are no loops in the network topology. Use this procedure to prevent Spanning Tree protection where it is not needed, but exercise caution to avoid network issues.

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. Use extreme caution, because 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. Only disable spanning tree if you are sure there are no loops in the network topology.

Procedure

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

   Example

   ```
   Switch> enable
   ```

   Enter your password if prompted.

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

   Example

   ```
   Switch# configure terminal
   ```

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

   Example

   ```
   Switch(config)# no spanning-tree vlan 20
   ```

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

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

   Example

   ```
   Switch(config)# end
   ```

Configure the root switch

Learn how to configure a switch as the root for a specified VLAN by modifying its priority to ensure optimal network traffic flow and convergence.

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

This task lets you control which switch becomes the root bridge for optimal network traffic flow and convergence. The switch priority is automatically set to 24576 if this value will make the switch 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

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

   Example

   ```
   Switch> enable
   ```

   Enter your password if prompted.

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

   Example

   ```
   Switch# configure terminal
   ```

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

   Example

   ```
   Switch(config)# spanning-tree vlan 20 root primary diameter 4
   ```

   When you enter this command, the software checks the switch priority of the root switches for each VLAN. With extended system ID support, the switch sets its own priority for the specified VLAN to 24576 if this value will make the switch 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 commas. The range is 1 to 4094.

   (Optional) For `diameter net-diameter`, specify the maximum number of switches 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.

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

   Example

   ```
   Switch(config)# end
   ```

Configure the secondary root switch

Learn how to configure a switch as the secondary root by modifying its priority, ensuring it becomes the root switch if the primary fails and other switches use the default priority.

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. This is based on the assumption that other network switches use the default switch priority of 32768.

Before you begin

When you configure a switch as the secondary root, the switch priority changes 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 based on the assumption that the other network switches use the default switch priority of 32768 and are, therefore, unlikely to become the root switch.

Procedure

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

   Example

   ```
   Switch> enable
   ```

   Enter your password if prompted.

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

   Example

   ```
   Switch# configure terminal
   ```

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

   Example

   ```
   Switch(config)# spanning-tree vlan 20 root secondary diameter 4
   ```

   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 valid range is 1 to 4094.

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

   Use the same network diameter value as that configured for the primary root switch.

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

   Example

   ```
   Switch(config)# end
   ```

Configure port priority for an interface

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

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 you want selected first and lower priority values (higher numerical values) to interfaces you want selected last. If all interfaces have the same priority value, spanning tree places the interface with the lowest interface number into the forwarding state.

Before you begin

Perform these steps to configure port priority for an interface.

Procedure

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

   Example

   ```
   Switch> enable
   ```

   Enter your password if prompted.

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

   Example

   ```
   Switch# configure terminal
   ```

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

   Example

   ```
   Switch(config)# interface gigabitethernet 1/0/10
   ```

   Valid interfaces include physical ports and port-channel logical interfaces such as port-channel followed by the port channel number.

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

   Example

   ```
   Switch(config-if)# spanning-tree port-priority 96
   ```

   For `priority`, 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. Other values are not accepted. A lower value indicates a higher priority.

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

   Example

   ```
   Switch(config-if)# spanning-tree vlan 100 port-priority 96
   ```

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 valid range is 1 to 4094.

For `priority`, the range is 0 to 240, in increments of 16. The default is 128.

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

   Example

   ```
   Switch(config)# end
   ```

Configure path cost for an interface

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

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 to those you want selected last. A lower path cost represents higher-speed transmission. If all interfaces have the same cost value, spanning tree places the interface with the lowest interface number in the forwarding state.

Before you begin

Perform these steps to configure path cost for an interface.

Procedure

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

   Example

   ```
   Switch> enable
   ```

   Enter your password if prompted.

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

   Example

   ```
   Switch# configure terminal
   ```

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

   Example

   ```
   Switch(config)# interface gigabitethernet 1/0/10
   ```

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

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

Example

```
Switch(config-if)# spanning-tree cost 4
```

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

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

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 values range from 1 to 4094.

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

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

Example

```
Switch(config)# end
```

Configure VLAN switch priority

Learn how to configure the switch priority to influence root switch selection in a stand-alone or stacked environment.

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. This command manipulates priority values directly rather than using the recommended root primary and root secondary commands, so exercise care when using it.

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

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

Example

```
Switch> enable
```

Enter your password if prompted.

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

   Example

```
Switch# configure terminal
```

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

   Example

```
Switch(config)# spanning-tree vlan 20 priority 24576
```

   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. Switches with lower priority numbers are more likely to be chosen as the root switch. Valid priority values include 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. Other values are rejected.

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

   Example

```
Switch(config)# end
```

Configure VLAN hello time

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

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

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

   Example

```
Switch> enable
```

Enter your password if prompted.

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

Example

```
Switch# configure terminal
```

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

Example

```
Switch(config)# spanning-tree vlan 20 hello-time 3
```

The hello time is the time interval between configuration messages generated and sent by the root switch. These messages indicate that the switch is active.

For `vlan-id`, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a list of VLANs separated by commas. The values range from 1 to 4094.

For `seconds`, the values range from 1 to 10 and the default is 2.

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

Example

```
Switch(config)# end
```

Configure VLAN forward delay time

Learn how to 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.

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

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

Example

```
Switch> enable
```

Enter your password if prompted.

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

Example

```
Switch# configure terminal
```

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

   Example

   ```
   Switch(config)# spanning-tree vlan 20 forward-time 10
   ```

   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 values range from 1 to 4094.

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

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

   Example

   ```
   Switch(config)# end
   ```

Configure the maximum-aging time for a VLAN

Learn how to configure the maximum-aging time of a VLAN to control how long a switch waits without receiving Spanning Tree configuration messages before reconfiguration.

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

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

   Example

   ```
   Switch> enable
   ```

   Enter your password if prompted.

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

   Example

   ```
   Switch# configure terminal
   ```

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

Example

```
Switch(config)# spanning-tree vlan 20 max-age 20
```

The maximum-aging time specifies how many seconds a switch waits without receiving Spanning Tree configuration messages before it attempts 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 values range from 1 to 4094.

For `seconds`, the values range from 6 to 40 and the default is 20.

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

Example

```
Switch(config)# end
```

Configure the transmit hold-count

Learn how to configure the transmit hold-count to control the BPDU burst size and manage the number of BPDUs sent before pausing.

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 increases CPU utilization, especially in rapid PVST+ mode. Use the default value unless you need a different setting.

Before you begin

Perform these steps to configure transmit hold-count.

Procedure

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

Example

```
Switch> enable
```

Enter your password if prompted.

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

Example

```
Switch# configure terminal
```

3. Use the **spanning-tree transmit hold-count value** command to configure the transmit hold-count.

   Example

   ```
   Switch(config)# spanning-tree transmit hold-count 6
   ```

   For `hold-count`, the values range from 1 to 10 seconds. The default value is 6.

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

   Example

   ```
   Switch(config)# end
   ```

Monitor Spanning Tree status

This topic explains how to display and clear Spanning Tree status using various show and clear commands on active interfaces, VLANs, and portfast configurations.

Use these commands to display Spanning Tree status.

Table 4: Spanning Tree status commands

Command	Description
show spanning-tree active	Displays Spanning Tree information on active interfaces only.
show spanning-tree detail	Displays a detailed summary of interface information.
show spanning-tree vlan *vlan-id*	Displays Spanning Tree information for the specified VLAN.
show spanning-tree interface *interface-id*	Displays Spanning Tree information for the specified interface.
show spanning-tree interface interface-id portfast	Displays Spanning Tree portfast information for the specified interface.
show spanning-tree summary [totals]	Displays a summary of interface states or displays the total number of lines in the STP state section.

Use the **clear spanning-tree [interface interface-id]** command to clear Spanning Tree counters.

Additional references for STP

Describes supplementary documentation and resources that provide further information about Spanning Tree Protocol (STP) configuration, troubleshooting, and best practices beyond the scope of this guide.

Related documents

Describes the availability of related documents that provide additional information relevant to the current topic within this guide.

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

Standards and RFCs

Describes the absence of applicable standards or RFCs for the current topic or feature implementation.

Standard/RFC	Title
None	–

MIBs

Provides information about supported MIBs for this release and location for downloading them.

This reference provides access to all supported MIBs for this release through the Cisco MIB Locator.

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 the Cisco MIB Locator.

Technical assistance

Provides extensive online resources for troubleshooting and resolving technical issues with Cisco products and technologies.

This reference provides information about technical assistance resources available through the Cisco Support website, including access requirements and subscription services for security and technical information.

Description	Link
Use the Cisco Support website to access 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. Use your Cisco.com user ID and password to access most tools on the Cisco Support website.	http://www.cisco.com/support

Feature information for STP

Describes the introduction of STP (Spanning Tree Protocol) feature modifications in Cisco IOS XE Release 17.18.1, providing enhanced network loop prevention and topology management capabilities.

Release	Modification
Cisco IOS XE 17.18.1	This feature was introduced.