31 Days Before Your CCNA Exam (200-301)

A Day-By-Day Review Guide for the CCNA 200-301 Certification Exam

2nd Edition

ciscopress.com

Allan Johnson

31 Days Before Your CCNA Exam

A Day-by-Day Review Guide for the CCNA 200-301 Certification Exam

Second Edition

Allan Johnson

Cisco Press
Hoboken, NJ

```
S1(config)# spanning-tree vlan 1 root primary
!---------
S2(config)# spanning-tree vlan 1 root secondary
```

The **primary** keyword automatically sets the priority to 24576 or to the next 4096 increment value below the lowest bridge priority detected on the network.

The **secondary** keyword automatically sets the priority to 28672, assuming that the rest of the network is set to the default priority of 32768.

Alternatively, the network administrator can explicitly configure the priority value in increments of 4096 between 0 and 65536 using the following command:

```
S1(config)# spanning-tree vlan 1 priority 24576
!---------
S2(config)# spanning-tree vlan 1 priority 28672
```

NOTE: In this example, these commands changed the priority values only for VLAN 1. Additional commands must be entered for each VLAN to take advantage of load balancing.

To verify the current spanning tree instances and root bridges, use the **show spanning-tree** command (see Example 25-2).

Example 25-2 Verifying Spanning Tree Configurations

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     001b.5302.4e80
             This bridge is the root
             Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    24577 (priority 24576 sys-id-ext 1)
             Address     001b.5302.4e80
             Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time  300

Interface            Role  Sts  Cost       Prio.Nbr  Type
----------------     ----- ---- --------- --------   --------
Fa0/1                Desg  FWD  19         128.1     P2p
Fa0/2                Desg  FWD  19         128.2     P2p
```

Notice in Example 25-2 that the BID is not the default 24576 that was configured on S1 with the **spanning-tree vlan 1 priority 24576** command. This is because the value of the priority is extended to include the VLAN ID. Therefore, a priority of 24576 plus a VLAN of 1 results in a priority output of 24577.

Configuring PortFast and BPDU Guard

To speed convergence for access ports when they become active, you can use Cisco's proprietary PortFast technology. After PortFast is configured and a port is activated, the port immediately transitions from the blocking state to the forwarding state. This immediate transition is useful for devices that do not participate in STP and helps to minimize network disruption during device startups or reconnections.

In a valid PortFast configuration, BPDUs should never be received because receipt of a BPDU indicates that another bridge or switch is connected to the port, potentially causing a spanning tree loop. When it is enabled, BPDU Guard puts the port in an errdisabled (error-disabled) state upon receipt of a BPDU. This effectively shuts down the port. The BPDU Guard feature provides a secure response to invalid configurations because you must manually put the interface back into service.

Example 25-3 shows the interface commands to configure PortFast and BPDU Guard on S2 in Figure 25-8.

Example 25-3 Configuring PortFast and BPDU Guard

```
S2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)# interface range f0/11 - f0/13
S2(config-if-range)# switchport mode access
S2(config-if-range)# spanning-tree portfast
S2(config-if-range)# spanning-tree bpduguard enable
```

Alternatively, you can skip the **interface range** command and directly configure the global commands **spanning-tree portfast default** and **spanning-tree bpduguard default**, which enable PortFast and BPDU Guard on all access ports.

Configuring BPDU Filter

Instead of using BPDU Guard, you can use a feature called BPDU Filter to suppress the sending and receiving of BPDUs on a port. When enabled globally, BPDU Filter prevents a PortFast-enabled port from sending BPDUs. If a BPDU is received, PortFast is disabled, and the port starts participating in STP. When configured at the interface level, BPDU Filter prevents the port from both sending and receiving BPDUs, regardless of PortFast.

In general, use BPDU Guard on ports where you want to ensure that no BPDUs are received and where immediate shutdown of the port upon receipt of a BPDU is desired. This is typically used on access ports connected to end devices. Use BPDU Filter when you need to suppress BPDU traffic entirely. This might be necessary in more controlled environments or specific topologies where you know that BPDU traffic should not exist. For example, in data centers administrators might use BPDU Filter to suppress BPDU traffic. This helps simplify the network topology and prevent unintended participation in STP by devices that do not need to be involved. BPDU Filter ensures that specific ports neither send nor receive BPDUs, maintaining a streamlined and optimized network.

NOTE: BPDU Guard and BPDU Filter should not be used on the same interface because their functionalities can overlap and potentially cause confusion or unexpected behavior in your network.

To configure BPDU Filter globally for all PortFast interfaces, reverse the default **no spanning-tree portfast bpdufilter default** command by entering **spanning-tree portfast bpdufilter default**. To disable BDPU Filter on an interface, enter the command **spanning-tree bpdufilter disable**. This interface will participate in normal STP operations. To disable STP on an interface, use the command **spanning-tree bpdufilter enable**. Be sure to exercise great care when enabling BPDU Filter on an interface because you are effectively shutting down STP. That one command can create a loop on a LAN that will make it unusable in another switch that is attached to that interface.

Configuring Root Guard

To avoid the potential of suboptimal paths, Root Guard is used on ports that are connected to switches that should never become root. It is configured on the interface with the **spanning-tree guard root** command. This feature ensures that a designated switch remains the root bridge, preventing topology changes that could occur if an unauthorized or misconfigured switch tries to become the root bridge.

When Root Guard is enabled on a port, it monitors incoming BPDUs. As shown in Example 25-4, if a superior BPDU (indicating a switch that has a lower bridge ID and is trying to become the root bridge) is received on a Root Guard-enabled port, the port is placed into a "root-inconsistent" state. This state prevents the port from forwarding traffic but allows it to receive BPDUs. Once the superior BPDU ceases, the port automatically recovers and returns to its normal state.

Example 25-4 Configuring and Verifying Root Guard

```
S1(config)# interface g1/0/1
S1(config-if)# spanning-tree guard root
S1(config-if)# end

S1# show spanning-tree vlan 1 int g1/0/1

Vlan           Role Sts Cost    Prio.Nbr  Type
-------------- ---- --- ------- --------  ------------
VLAN0001       Desg FWD 20000   128.1     P2p

S1#! A rogue switch is attached to G1/0/1 and sends a superior BPDU

*May 23 18:39:20.418: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port
  GigabitEthernet1/0/1 on VLAN0001.

S1# show spanning-tree vlan 1 int g1/0/1
```

```
Vlan              Role Sts    Cost       Prio.Nbr   Type
-------------- ---- ---    --------- --------   ---------
VLAN0001          Desg BKN*   20000      128.1      P2p *ROOT_Inc

S1#! The rogue switch in disconnected from G1/0/1

*May 23 19:43:25.452: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port
   GigabitEthernet1/0/1 on VLAN0001.

S1# show spanning-tree vlan 1 int g1/0/1

Vlan             Role  Sts Cost     Prio.Nbr    Type
------------- ----  --- ------- ---------- ------
VLAN0001         Desg  FWD 20000    128.1       P2p
S1#
```

Configuring Loop Guard

Loop Guard is used to prevent network loops in situations where a blocking port erroneously transitions to the forwarding state, potentially due to the absence of BPDUs. Loop Guard ensures that if a port should be receiving BPDUs and it suddenly stops receiving them, the port does not transition to the forwarding state. In this way, Loop Guard prevents possible loops.

By ensuring that designated and root ports remain in the blocking state when BPDUs are not received, Loop Guard enhances the redundancy and reliability of the network. It complements other STP features like Root Guard, providing additional protection in complex network topologies with redundant links.

When Loop Guard is enabled on a switch port, it monitors the receipt of BPDUs. If a port configured to receive BPDUs stops receiving them, the port is placed into a "loop-inconsistent" state instead of transitioning to the forwarding state. This state prevents the port from forwarding traffic, thus avoiding a potential loop. The port will remain in this state until BPDUs are detected again, at which point it will automatically recover.

You can enable Loop Guard globally with the **spanning-tree loopguard default** command. You can also configure it on an interface with the **spanning-tree guard loop** command.

Verifying STP

Several commands enable you to verify the state of the current STP implementation. Table 25-9 summarizes commands most likely to appear on the CCNA exam.

Table 25-9 STP Verification Commands

Description	Command
Displays STP information	`Switch#` **`show spanning-tree`**
Displays STP information for active interfaces only	`Switch#` **`show spanning-tree active`**

Description	Command
Displays abbreviated information for all STP instances	`Switch# show spanning-tree bridge`
Displays detailed information for all STP instances	`Switch# show spanning-tree detail`
Displays STP information for the specified interface	`Switch# show spanning-tree interface interface-id`
Displays STP information for the specified VLAN	`Switch# show spanning-tree vlan vlan-id`
Displays a summary of STP port states	`Switch# show spanning-tree summary`

NOTE: Ideally, you should review the output of these commands today on lab equipment or a simulator. At the very least, refer to the examples in your study resources.

Study Resources

For today's exam topics, refer to the following resources for more study.

Resource	Module or Chapter
Cisco Network Academy: Switching, Routing, and Wireless Essentials v7	5
CCNA 200-301 Official Cert Guide, Volume 1, 2nd edition	5
	9–10
Portable Command Guide	11

This page intentionally left blank