



## CHAPTER 6

# Configuring STP Extensions

---

This chapter describes how to configure Spanning Tree Protocol (STP) extensions on NX-OS devices. For more information about the Data Center Network Manager features, see the *Cisco DCNM Fundamentals Configuration Guide*.

This chapter includes the following sections:

- [Information About STP Extensions, page 6-1](#)
- [Licensing Requirements for STP Extensions, page 6-8](#)
- [Prerequisites for STP Extensions, page 6-9](#)
- [Guidelines and Limitations, page 6-9](#)
- [Configuring STP Extensions, page 6-10](#)
- [Field Descriptions for Configuring STP Extensions, page 6-14](#)
- [Additional References, page 6-16](#)



Note

---

See [Chapter 4, “Configuring Rapid PVST+”](#) for complete information on STP and Rapid PVST+ and [Chapter 5, “Configuring MST”](#) for complete information on MST.

---

## Information About STP Extensions



Note

---

Before using DCNM to configure any Spanning Tree Protocol parameters, you must set the logging level by entering the NX-OS global commands in the command line of your device:

```
--logging-level spanning-tree 6
```

```
--logging logfile messages 6
```

```
--logging event link-status default
```

See the *Cisco NX-OS System Management Configuration Guide* for information on logging levels.

---



Note

---

See the *Cisco DCNM Interfaces Configuration Guide* for information on creating Layer 2 interfaces.

---

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

Cisco has added extensions to STP that enhances loop prevention, protects against some possible user misconfigurations, and provides better control over the protocol parameters. Although, in some cases, similar functionality may be incorporated into the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) standard, we recommend using these extensions. All of these extensions, except PVST Simulation, can be used with both Rapid PVST+ and MST. You use PVST Simulation only with MST.

The available extensions are spanning tree edge ports (which supply the functionality previously known as PortFast), Bridge Assurance, BPDU Guard, BPDU Filtering, Loop Guard, Root Guard, and PVT Simulation. Many of these features can be applied either globally or on specified interfaces.



**Note**

---

Spanning tree is used to refer to IEEE 802.1w and IEEE 802.1s. If the text is discussing the IEEE 802.1D Spanning Tree Protocol, 802.1D is stated specifically.

---

This section discusses the following topics:

- [STP Port Types, page 6-2](#)
- [Bridge Assurance, page 6-3](#)
- [BPDU Guard, page 6-5](#)
- [BPDU Filtering, page 6-5](#)
- [Loop Guard, page 6-6](#)
- [Root Guard, page 6-7](#)
- [Applying STP Extension Features, page 6-7](#)
- [PVST Simulation, page 6-8](#)
- [High Availability, page 6-8](#)
- [Virtualization Support, page 6-8](#)

## STP Port Types

You can configure a spanning tree port as an edge port, a network port, or a normal port. A port can be in only one of these states at a given time. The default spanning tree port type is normal.

Edge ports, which are connected to Layer 2 hosts, can be either an access port or a trunk port.



**Note**

---

If you configure a port connected to a Layer 2 switch or bridge as an edge port, you might create a bridging loop.

---

Network ports are connected only to Layer 2 switches or bridges.



**Note**

---

If you mistakenly configure ports that are connected to Layer 2 hosts, or edge devices, as spanning tree network ports, those ports will automatically move into the blocking state.

---

## STP Edge Ports

You connect STP edge ports only to Layer 2 hosts. The edge port interface immediately transitions to the forwarding state, without moving through the blocking or learning states. (This immediate transition was previously configured as the Cisco- proprietary feature PortFast.)

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).**

Interfaces that are connected to Layer 2 hosts should not receive STP Bridge Protocol Data Units (BPDUs).

## Bridge Assurance

You can use Bridge Assurance to protect against certain problems that can cause bridging loops in the network. Specifically, you use Bridge Assurance to protect against a unidirectional link failure or other software failure and a device that continues to forward data traffic when it is no longer running the spanning tree algorithm.



### Note

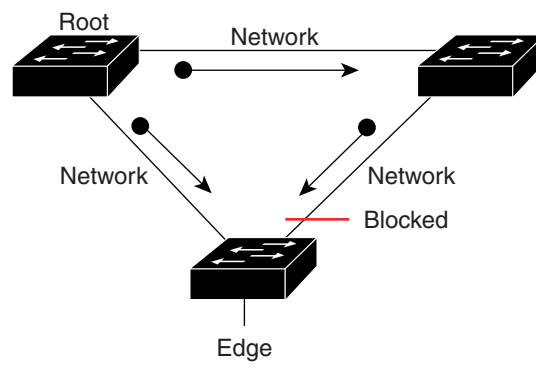
Bridge Assurance is supported only by Rapid PVST+ and MST.

Bridge Assurance is enabled by default and can only be disabled globally. Also, Bridge Assurance can be enabled only on spanning tree network ports that are point-to-point links. Finally, both ends of the link must have Bridge Assurance enabled. If the device on one side of the link has Bridge Assurance enabled and the device on the other side either does not support Bridge Assurance or does not have this feature enabled, the connecting port is blocked.

With Bridge Assurance enabled, BPDUs are sent out on all operational network ports, including alternate and backup ports, for each hello time period. If the port does not receive a BPDU for a specified period, the port moves into the blocking state and is not used in the root port calculation. Once that port receives a BPDU, it resumes the normal spanning tree transitions.

Figure 6-1 shows a normal STP topology, and Figure 6-2 demonstrates a potential network problem when the device fails and you are not running Bridge Assurance.

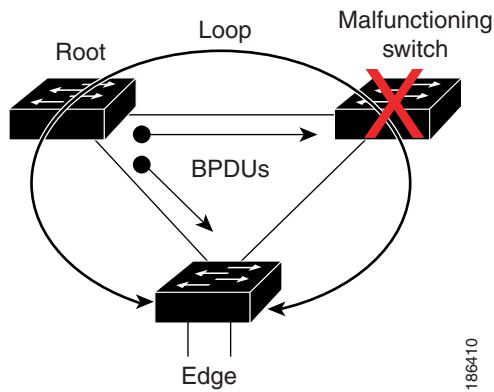
**Figure 6-1 Network with Normal STP Topology**



186525

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).**

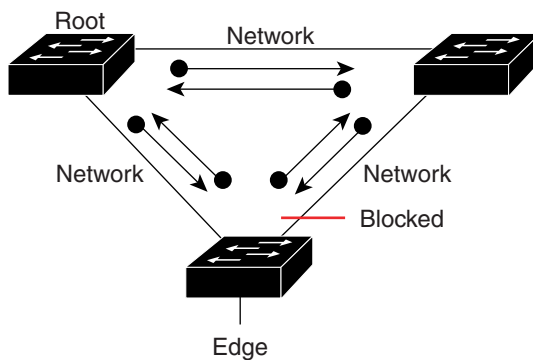
**Figure 6-2 Network Problem without Running Bridge Assurance**



186410

Figure 6-3 shows the network with Bridge Assurance enabled, and the STP topology progressing normally with bidirectional BPDUs issuing from every STP network port. Figure 6-4 shows how the potential network problem shown in Figure 6-2 does not happen when you have Bridge Assurance enabled on your network.

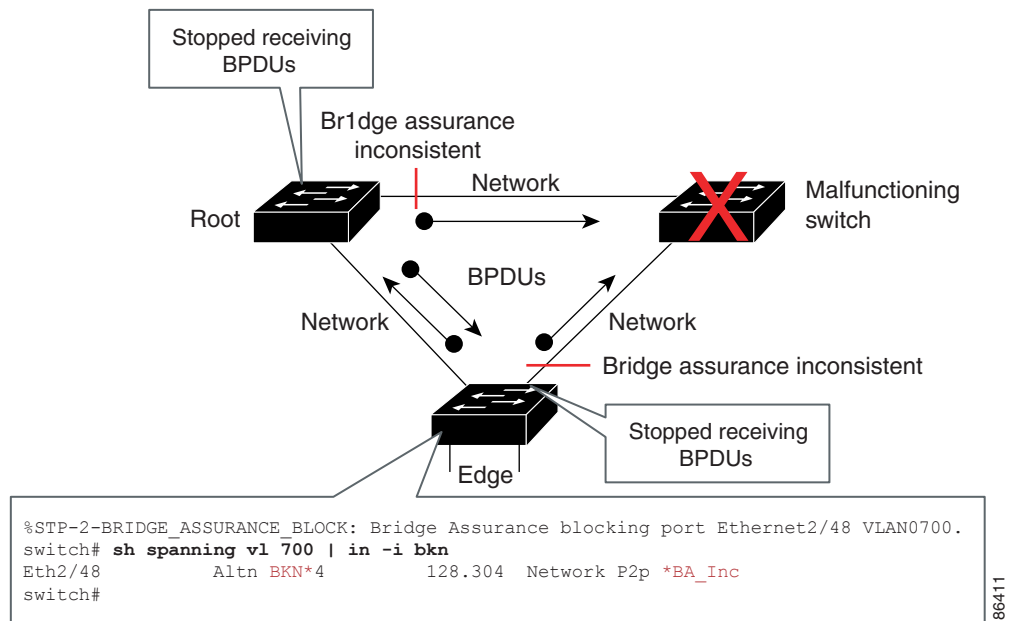
**Figure 6-3 Network STP Topology Running Bridge Assurance**



186526

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

**Figure 6-4** Network Problem Averted with Bridge Assurance Enabled



## BPDU Guard

Enabling BPDU Guard shuts down that interface if a BPDU is received.

You can configure BPDU Guard at the interface level. When configured at the interface level, BPDU Guard shuts the port down as soon as the port receives a BPDU, regardless of the port type configuration.

When you configure BPDU Guard globally, it is effective only on operational spanning tree edge ports. In a valid configuration, Layer 2 LAN edge interfaces do not receive BPDUs. A BPDU that is received by an edge Layer 2 LAN interface signals an invalid configuration, such as the connection of an unauthorized device. BPDU Guard, when enabled globally, shuts down all spanning tree edge ports when they receive a BPDU.

BPDU Guard provides a secure response to invalid configurations, because you must manually put the Layer 2 LAN interface back in service after an invalid configuration.



**Note**

When enabled globally, BPDU Guard applies to all operational spanning tree edge interfaces.

## BPDU Filtering

You can use BPDU Filtering to prevent the device from sending or even receiving BPDUs on specified ports.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).**

When configured globally, BPDU Filtering applies to all operational spanning tree edge ports. You should connect edge ports only to hosts, which typically drop BPDUs. If an operational spanning tree edge port receives a BPDU, it immediately returns to a normal spanning tree port type and moves through the regular transitions. In that case, BPDU Filtering is disabled on this port, and spanning tree resumes sending BPDUs on this port.

In addition, you can configure BPDU Filtering by the individual interface. When you explicitly configure BPDU Filtering on a port, that port does not send any BPDUs and drops all BPDUs that it receives. You can effectively override the global BPDU Filtering setting on individual ports by configuring the specific interface. This BPDU Filtering command on the interface applies to the entire interface, whether the interface is trunking or not.



**Caution**

Use care when configuring BPDU Filtering per interface. If you explicitly configuring BPDU Filtering on a port that is not connected to a host, it can result in bridging loops because the port will ignore any BPDU that it receives and go to forwarding.

Table 6-1 lists all the BPDU Filtering combinations.

**Table 6-1 BPDU Filtering Configurations**

BPDU Filtering Per Port Configuration	BPDU Filtering Global Configuration	STP Edge Port Configuration	BPDU Filtering State
Default <sup>1</sup>	Enable	Enable	Enable <sup>2</sup>
Default	Enable	Disable	Disable
Default	Disable	Not applicable	Disable
Disable	Not applicable	Not applicable	Disable
Enable	Not applicable	Not applicable	Enable

1. No explicit port configuration.
2. The port transmits at least 10 BPDUs. If this port receives any BPDUs, the port returns to the spanning tree normal port state and BPDU Filtering is disabled

## Loop Guard

Loop Guard helps prevent bridging loops that could occur because of a unidirectional link failure on a point-to-point link.

An STP loop occurs when a blocking port in a redundant topology erroneously transitions to the forwarding state. This transition usually happens because one of the ports in a physically redundant topology (not necessarily the blocking port) stops receiving BPDUs.

Loop Guard enabled globally is useful only in switched networks where devices are connected by point-to-point links. On a point-to-point link, a designated bridge cannot disappear unless it sends an inferior BPDU or brings the link down. However, you can enable Loop Guard on shared links per interface,

You can use Loop Guard to determine if a root port or an alternate/backup root port receives BPDUs. If the port that was previously receiving BPDUs is no receiving longer BPDUs, Loop Guard puts the port into an inconsistent state (blocking) until the port starts to receive BPDUs again. If such a port receives BPDUs again, the port—and link—is deemed viable again. The protocol removes the loop-inconsistent condition from the port, and the STP determines the port state because such recovery is automatic.



**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).**

## PVST Simulation

MST interoperates with Rapid PVST+ with no need for user configuration. The PVST simulation feature enables this interoperability.



### Note

PVST simulation is enabled by default when you enable MST. By default, all interfaces on the device interoperate between MST and Rapid PVST+.

However, you may want to control the connection between MST and Rapid PVST+ to protect against accidentally connecting an MST-enabled port to a port enabled to run Rapid PVST+. Because Rapid PVST+ is the default STP mode, you may encounter many Rapid PVST+ connections.

Disabling Rapid PVST+ simulation, which can be done globally for the entire device, moves the MST-enabled port to the blocking state once it detects it is connected to a Rapid PVST+-enabled port. This port remains in the inconsistent state until the port stops receiving Rapid PVST+/SSTP BPDUs, and then the port resumes the normal STP transition process.

The root bridge for all STP instances must all be in either the MST region or the Rapid PVST+ side. If the root bridge for all STP instances are not on one side or the other, the software moves the port into a PVST simulation-inconsistent state.



### Note

We recommend that you put the root bridge for all STP instances in the MST region.

## High Availability

The software supports high availability for STP. However, the statistics and timers are not restored when STP restarts. The timers start again and the statistics begin from 0.



### Note

See the *Cisco NX-OS High Availability and Redundancy Configuration Guide* for complete information on high-availability features.

## Virtualization Support

The system provides support for virtual device contexts (VDCs), and each VDC runs a separate STP. You can run Rapid PVST+ in one VDC and MST in another VDC.



### Note

See the *Cisco DCNM Virtual Device Context Configuration Guide* for complete information on VDCs and assigning resources.

## Licensing Requirements for STP Extensions

The following table shows the licensing requirements for this feature:

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

Product	License Requirement
DCNM	STP extensions require no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the <i>Cisco DCNM Licensing Guide</i> .
NX-OS	STP extensions require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> .

However, using VDCs requires an Advanced Services license.

## Prerequisites for STP Extensions

STP has the following prerequisites:

- You must be logged onto the device.
- Before using DCNM to configure any Spanning Tree Protocol parameters, you must set the logging level by entering the NX-OS global command **logging-level spanning-tree 6** in the command line of your device. See the *Cisco NX-OS System Management Configuration Guide* for information on logging levels.

## Guidelines and Limitations

Follow these guidelines and limitations when configuring STP extensions:

- Connect STP network ports only to switches.
- You should configure host ports as STP edge ports and not as network ports.
- If you enable STP network port types globally, ensure that you manually configure all ports connected to hosts as STP edge ports.
- You should configure all access and trunk ports connected to Layer 2 hosts as edge ports.
- Bridge Assurance runs only on point-to-point spanning tree network ports. You must configure each side of the link for this feature.
- We recommend that you enable Bridge Assurance throughout your network.
- We recommend that you enable BPDU Guard on all edge ports.
- Enabling Loop Guard globally works only on point-to-point links.
- Enabling Loop Guard per interface works on both shared and point-to-point links.
- Root Guard forces a port to always be a designated port; it does not allow a port to become a root port. Loop Guard is effective only if the port is a root port or an alternate port. You cannot enable Loop Guard and Root Guard on a port at the same time.
- Loop Guard has no effect on a disabled spanning tree instance or a VLAN.
- Spanning tree always chooses the first operational port in the channel to send the BPDUs. If that link becomes unidirectional, Loop Guard blocks the channel, even if other links in the channel are functioning properly.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).**

- If you group together a set of ports that are already blocked by Loop Guard to form a channel, spanning tree loses all the state information for those ports and the new channel port may obtain the forwarding state with a designated role.
- If a channel is blocked by Loop Guard and the channel members go back to an individual link status, spanning tree loses all the state information. The individual physical ports may obtain the forwarding state with the designated role, even if one or more of the links that formed the channel are unidirectional.



---

**Note** You can enable UniDirectional Link Detection (UDLD) aggressive mode to isolate the link failure. A loop may occur until UDLD detects the failure, but Loop Guard will not be able to detect it. See the *Cisco NX-OS Interfaces Configuration Guide* for information on UDLD.

---

- You should enable Loop Guard globally on a switch network with physical loops.
- You should enable Root Guard on ports that connect to network devices that are not under direct administrative control.

## Configuring STP Extensions

This section includes the following topics:

- [Setting Default Values for STP Extensions, page 6-10](#)
- [Setting STP Extensions Globally, page 6-11](#)
- [Configuring PVST Simulation Globally, page 6-12](#)
- [Setting STP Extensions Per Interface, page 6-13](#)

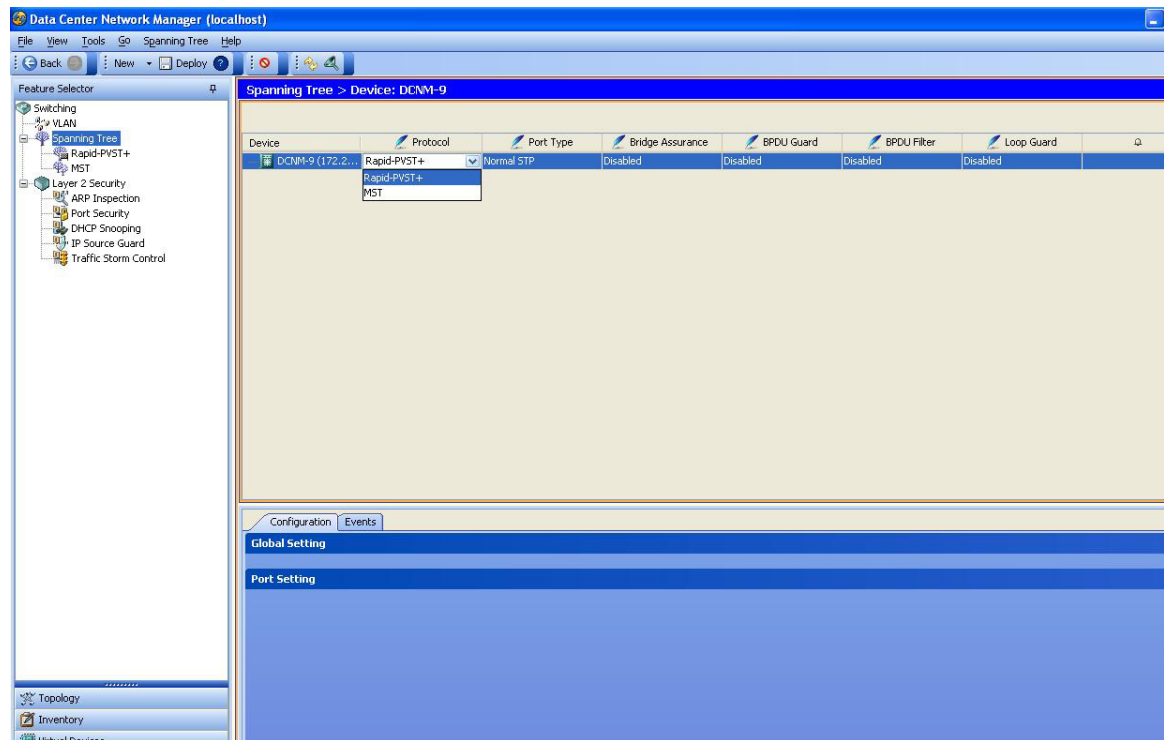
You can enable Loop Guard per interface on either shared or point-to-point links.

## Setting Default Values for STP Extensions

You use the Spanning Tree pane to return to the default settings for these features (see [Figure 6-6](#)).

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

**Figure 6-6** Configuring STP Extensions



## DETAILED STEPS

To set the STP extensions to the default settings either globally or per port, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Switching > Spanning Tree** to open the Spanning Tree pane.
  - Step 2** In the Summary pane, click the device to set the default settings globally for the entire device.
  - Step 3** On the menu bar, choose **Spanning-Tree > Set to default**.
  - Step 4** In the Details pane, click the **Configuration** tab to set the default settings for the port.
  - Step 5** Click the **Port Setting** section.  
The Port Setting section expands and displays the ports.
  - Step 6** In the Port Setting section, choose the interface that you want to configure.
  - Step 7** On the menu bar, choose **Spanning-Tree > Set to default**.
  - Step 8** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Setting STP Extensions Globally

You use the Spanning Tree pane to configure STP extensions globally (see [Figure 6-6](#)).

*Send document comments to [nexus7k-docfeedback@cisisco.com](mailto:nexus7k-docfeedback@cisisco.com).*

## DETAILED STEPS

To set the STP extensions globally, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Switching > Spanning Tree** to open the Spanning Tree pane.
  - Step 2** In the Summary pane, click the device.
  - Step 3** In the Details pane, click the **Configuration** tab.
  - Step 4** In the Details pane, click the **Global Setting** section.  
The Global Setting section expands.
  - Step 5** From the Port Type drop-down list, choose the port type.  
The default port type is Normal STP.
  - Step 6** From the Bridge Assurance drop-down list, choose **Enabled** or **Disabled**.  
Bridge Assurance is enabled by default.
  - Step 7** From the BPDU Guard drop-down list, choose **Enabled** or **Disabled**.  
BPDU Guard is disabled by default.
  - Step 8** From the BPDU Filter drop-down list, choose **Enabled** or **Disabled**.  
BPDU Filter is disabled by default.
  - Step 9** From the Loop Guard drop-down list, choose **Enabled** or **Disabled**.  
Loop Guard is disabled by default.
  - Step 10** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Configuring PVST Simulation Globally



### Note

PVST simulation is enabled by default. By default, all interfaces on the device interoperate between MST and Rapid PVST+.

You configure PVST simulation only when you are running MST on the device (Rapid PVST+ is the default STP mode). MST interoperates with Rapid PVST+. However, to prevent an accidental connection to a device that does not run MST as the default STP mode, you may want to disable this automatic feature. If you disable PVST simulation, the MST-enabled port moves to the blocking state once it detects it is connected to a Rapid PVST+-enabled port. This port remains in the inconsistent state until the port stops receiving BPDUs, and then the port resumes the normal STP transition process.

You use the Spanning Tree pane to configure PVST simulation (see [Figure 6-6](#)).

## DETAILED STEPS

To configure PVST simulation globally, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Switching > Spanning Tree** to open the Spanning Tree pane.
  - Step 2** In the Summary pane, click the device on which you want to specify the MST name and revision number.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

- The system highlights the device in the Summary pane, and tabs appear in the Details pane
- Step 3** In the Details pane, click the **Configuration** tab.
  - Step 4** Click the **Global Setting** section.
  - Step 5** In the MST Setting area, in the Simulate PVST field, click the drop-down list and click **Enabled**.  
The default is Enabled.
  - Step 6** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Setting STP Extensions Per Interface

You use the Spanning Tree pane to configure the STP extensions per interface (see [Figure 6-6](#)).

### DETAILED STEPS

To set the STP extensions per interface, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Switching > Spanning Tree** to open the Spanning Tree pane.
  - Step 2** In the Summary pane, click the device.
  - Step 3** In the Details pane, click the **Configuration** tab.
  - Step 4** In the Details pane, click the **Port Setting** section.  
The Port Setting section expands.
  - Step 5** In the Port Setting section, click the interface that you want to configure.
  - Step 6** In the Port Type column, click the drop-down list and choose the port type.  
By default, the port type for each interface is set to Default, which returns the port type to the globally set port type.
  - Step 7** In the BPDU Guard column, click the drop-down list and choose the BPDU Guard setting.  
By default, the BPDU Guard setting for each interface is set to Default, which returns the interface to the globally set BPDU Guard value.
  - Step 8** In the BPDU Filter column, click the drop-down list and choose the BPDU Filter setting.  
By default, the BPDU Filter setting for each interface is set to Default, which returns the interface to the globally set BPDU Filter value.
  - Step 9** In the Guard column, click the drop-down list and choose the Loop Guard or Root Guard setting.  
By default, the Guard setting for each interface is set to Default, which returns the interface to the globally set Loop Guard value.
  - Step 10** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

## Field Descriptions for Configuring STP Extensions

The following topics describe the fields for setting the type of STP that you want to run, configuring many MST settings, and configuring the STP extension features:

- [Device: Configuration: Global Setting Section, page 6-14](#)
- [Device: Configuration: Port Setting Section, page 6-15](#)

### Device: Configuration: Global Setting Section

**Table 6-2** Device: Configuration: Global Setting Section

Field	Description
<b>STP Setting</b>	
Device	<i>Display only.</i> The name or IP address of the device
Protocol	STP protocol running in the device. The range is PVRST or MST. The default is PVRST.
Port Type	Global STP port type for the device. The range is Edge, Network, or Normal STP. The default port type is Normal STP.
Bridge Assurance	Bridge Assurance feature. The range is enabled or disabled, and the default is Enabled.
BPDU Guard	Bridge Guard feature. The range is enabled or disabled, and the default is Disabled.
BPDU Filter	Bridge Filter feature. The range is enabled or disabled, and the default is Disabled.
Loop Guard	Loop Guard feature. The range is enabled or disabled, and the default is Disabled.
Path Cost	Path-cost feature. The range is short or long, and the default is short.  <b>Note</b> This field applies to Rapid PVST+ only; the path-cost method is always long with MST.
<b>MST Setting</b>	
Name	Name for the MST region. You can enter up to 34 alphanumeric characters. The default is blank.
Hello Time	Hello time for the MST protocol. The valid range is 1 to 10 seconds, and the default value is 2 seconds.
Revision Number	Revision of the current MST configuration. Valid values are from 0 to 65535, and the default value is 0.
Simulate PVST	PVST simulation. The range is enabled or disabled, and the default value is Enabled.
Digest	<i>Display only.</i> MD5 digest of VLAN-to-MST-instance mapping.
Pre-Standard Digest	<i>Display only.</i> MD5 digest of VLAN-to-MST-instance mapping using pre-standard key.
Forward Delay Time	Period that the learning state lasts before the interface begins forwarding. The range is 4 to 30 seconds, and the default value is 15 seconds.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

**Table 6-2**      **Device: Configuration: Global Setting Section (continued)**

Field	Description
Max Age Time	Period that the protocol information received on a port is stored on the device. The range is 6 to 40 seconds, and the default value is 20 seconds.
Max Hop Count	Number of hops permissible within the region before the BPDU is discarded. The range is from 1 to 255 hops, and the default value is 20 hops.

## Device: Configuration: Port Setting Section

**Table 6-3**      **Device: Configuration: Port Setting Section**

Field	Description
Name	<i>Display only.</i> The name of the interface.
Priority	STP port priority for the interface. The range is 0 to 224 in increments of 32. The default value is 128.
Cost	STP port cost for the interface. The range is from 1 to 200,000,000, and the default is derived from the media speed of the interface.
Port Type	STP port type Valid values are as follows: <ul style="list-style-type: none"> <li>• Network—Use only when a connection is to another switch or bridge.</li> <li>• Edge access—Use only when a connection is to a host port.</li> <li>• Edge trunk—Use only when a connection is to a host port and you want to carry traffic for more than one VLAN.</li> <li>• Disable—Sets the port to an STP Normal port.</li> <li>• Default—Returns the port to the global STP port type setting.</li> </ul> The default value is Default.
BPDU Guard	BPDU Guard feature on the specified interface. Valid values are: <ul style="list-style-type: none"> <li>• Enable</li> <li>• Disable</li> <li>• Default—Returns the port to the global BPDU Guard setting.</li> </ul> The default value is Default.
BPDU Filter	BPDU Filter feature on the specified interface. Valid values are as follows: <ul style="list-style-type: none"> <li>• Enable</li> <li>• Disable</li> <li>• Default—Returns the port to the global BPDU Filter setting.</li> </ul> The default value is Default.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

**Table 6-3**      **Device: Configuration: Port Setting Section (continued)**

Field	Description
Guard	<p>Loop Guard or Root Guard. Valid values are as follows:</p> <ul style="list-style-type: none"> <li>• Loop</li> <li>• None</li> <li>• Root</li> </ul> <p>The default value is Default.</p>
Simulate PVST	<p>PVST simulation per interface. Valid values are as follows:</p> <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> <li>• Default—Returns the interface to the global PVST simulation setting for the device.</li> </ul> <p>The default value is Default.</p>
Link Type	<p>Lnk type for this interface. Valid values are as follows:</p> <ul style="list-style-type: none"> <li>• Point-to-point</li> <li>• Shared</li> <li>• Auto—Sets the link type based on the duplex setting of the interface.</li> </ul> <p>The default value for this feature is Auto.</p>

## Additional References

For additional information related to implementing these STP extensions, see the following sections:

- [Related Documents, page 6-17](#)
- [Standards, page 6-17](#)
- [MIBs, page 6-17](#)

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## Related Documents

Related Topic	Document Title
Rapid PVST+	Chapter 4, “Configuring Rapid PVST+”
MST	Chapter 5, “Configuring MST”
NX-OS Layer 2 switching configuration	<i>Cisco NX-OS Layer 2 Switching Configuration Guide</i>
Layer 2 interfaces	<i>Cisco DCNM Interfaces Configuration Guide</i>
DCNM fundamentals	<i>Cisco DCNM Fundamentals Configuration Guide</i>
High availability	<i>Cisco NX-OS High Availability and Redundancy Guide</i>
System management	<i>Cisco NX-OS System Management Configuration Guide</i>
VDCs	<i>Cisco DCNM Virtual Device Context Configuration Guide</i>
Licensing	<i>Cisco DCNM Licensing Guide</i>
Release notes	<i>Cisco DCNM Release Notes, Release 4.0</i>

## Standards

Standards	Title
IEEE 802.1Q-2006 (formerly known as IEEE 802.1s), IEEE 802.1D-2004 (formerly known as IEEE 802.1w), IEEE 802.1D, IEEE 802.1t	—

## MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> <li>CISCO_STP_EXTENSION MIB</li> <li>BRIDGE MIB</li> </ul>	To locate and download MIBs, go to the following URL: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***