STP Optional Characteristic Configuration

Table of Contents

Chapter 1Configuring STP Optional Characteristic

1.1 STP Optional Characteristic Introduction

The spanning tree protocol module of the switch supports seven additional features (the so-called optional features). These features are not configured by default. The supported condition of various spanning tree protocol modes towards the optional characteristics is as follows:

Optional Characteristic	Single STP	PVST	RSTP	MSTP
Port Fast	Yes	Yes	No	No
BPDU Guard	Yes	Yes	Yes	Yes
BPDU Filter	Yes	Yes	No	No
Uplink Fast	Yes	Yes	No	No
Backbone Fast	Yes	Yes	No	No
Root Guard	Yes	Yes	Yes	Yes
Loop Guard	Yes	Yes	Yes	Yes

1.1.1 Port Fast

Port Fast immediately brings an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states. You can use Port Fast on interfaces connected to a single workstation or server, to allow those devices to immediately connect to the network, rather than waiting for the spanning tree to converge.

Interfaces connected to a single workstation or server should not receive bridge protocol data units (BPDUs). An interface with Port Fast enabled goes through the normal cycle of spanning-tree status changes when the switch is restarted.

Because the purpose of Port Fast is to minimize the time interfaces must wait for spanning-tree to converge, it is effective only when used on interfaces connected to end stations. If you enable Port Fast on an interface connecting to another switch, you risk creating a spanning-tree loop.

You can enable this feature by using the spanning-tree portfast interface configuration or the spanning-tree portfast default global configuration command.
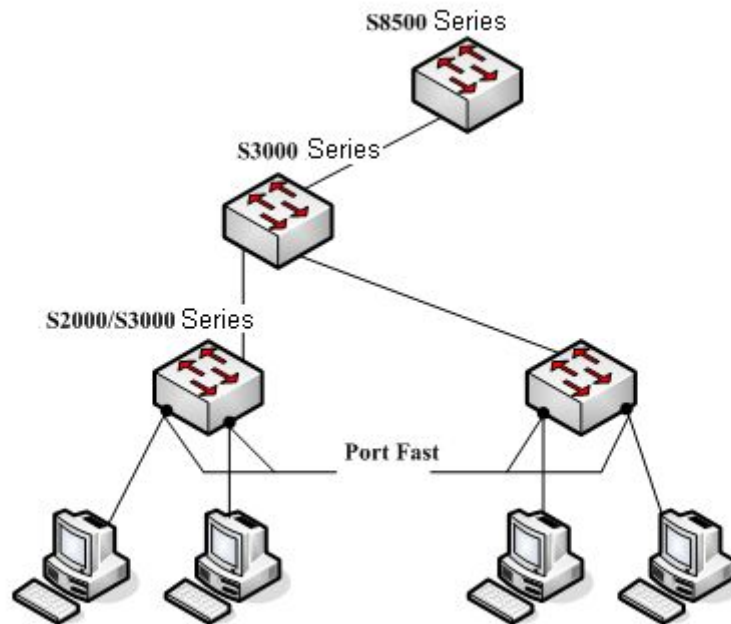
Figure 1.1 Port Fast

Instruction：

For the rapid convergent spanning tree protocol, RSTP and MSTP, can immediately bring an interface to the forwarding state, and therefore there is no need to use Port Fast feature. Series   Series   Series

1.1.2   BPDU Guard

The BPDU guard feature can be globally enabled on the switch or can be enabled per port, but the feature operates with some differences.

At the global level, you enable BPDU guard on Port Fast-enabled ports by using the spanning-tree portfast bpduguard default global configuration command. Spanning tree shuts down ports that are in a Port Fast-operational state if any BPDU is received on them. In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port means an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state. When this happens, the switch shuts down the entire port on which the violation occurred.

To prevent the port from shutting down, you can use the errdisable detect cause bpduguard shutdown vlan global configuration command to shut down just the offending VLAN on the port where the violation occurred.

At the interface level, you enable BPDU guard on any port by using the spanning-tree bpduguard enable interface configuration command without also enabling the Port Fast feature. When the port receives a BPDU, it is put in the error-disabled state.

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard

feature in a service-provider network to prevent an access port from participating in the spanning tree.

1.1.3 BPDU Filter

The BPDU filtering feature can be globally enabled on the switch or can be enabled per interface, but the feature operates with some differences.

In SSTP/PVST mode,.if a **Port Fast** port with BPDU filter configured receives the BPDU, the features BPDU Filter and Port Fast at the port will be automatically disabled, resuming the port as a normal port. Before entering the **Forwarding** state, the port must be in the **Listening** state and **Learning** state.

The BPDU Filter feature can be configured in global configuration mode or in port configuration mode. In global configuratiom mode, run the command **spanning-tree portfast bpdufilter** to block all ports to send BPDU out. The port, howerver, can still receive and process BPDU.

1.1.4 Uplink Fast

The feature **Uplink Fast** enables new root ports to rapidly enter the **Forwarding** state when the connection between the switch and the root bridge is disconnected.

A complex network always contains multilayers of devices, as shown in figure 1.2. Both aggregation layer and the access layer of the switch have redundancy connections with the upper layer. These redundancy connections are normally blocked by the STP to avoid loops.
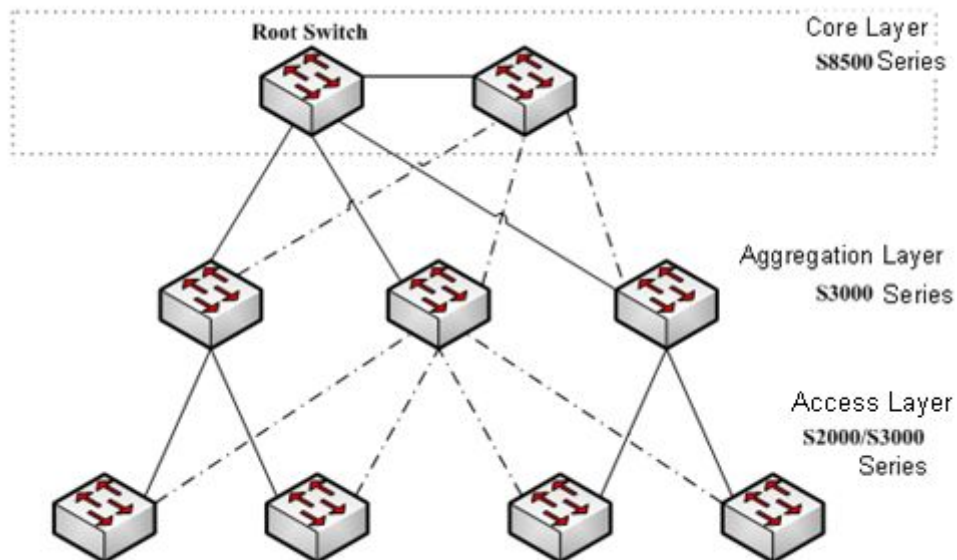
Figure 1.2 switching network topology

Suppose the connection between a switch and the upper layer is disconnected (called as Direct Link Failure), the STP chooses the Alternate port on the redundancy line as the root port. Before entering the **Forwarding** state, the Alternate port must be in the **Listening** state and **Learning** state. If the **Uplink Fast** feature is configured by running the command **spanning-tree uplinkfast** in

global configuration mode, new root port can directly enter the forwarding state, resuming the connection between the switch and the upper layer.

Figure 1.3 shows the working principle of the **Uplink Fast** feature. The port for switch C to connect switch B is the standby port when the port is in the original state. When the connection between switch C and root switch A is disconnected, the previous Alternate port is selected as new root port and immediately start forwarding.

New root port promptly

changes to

the Forwarding state
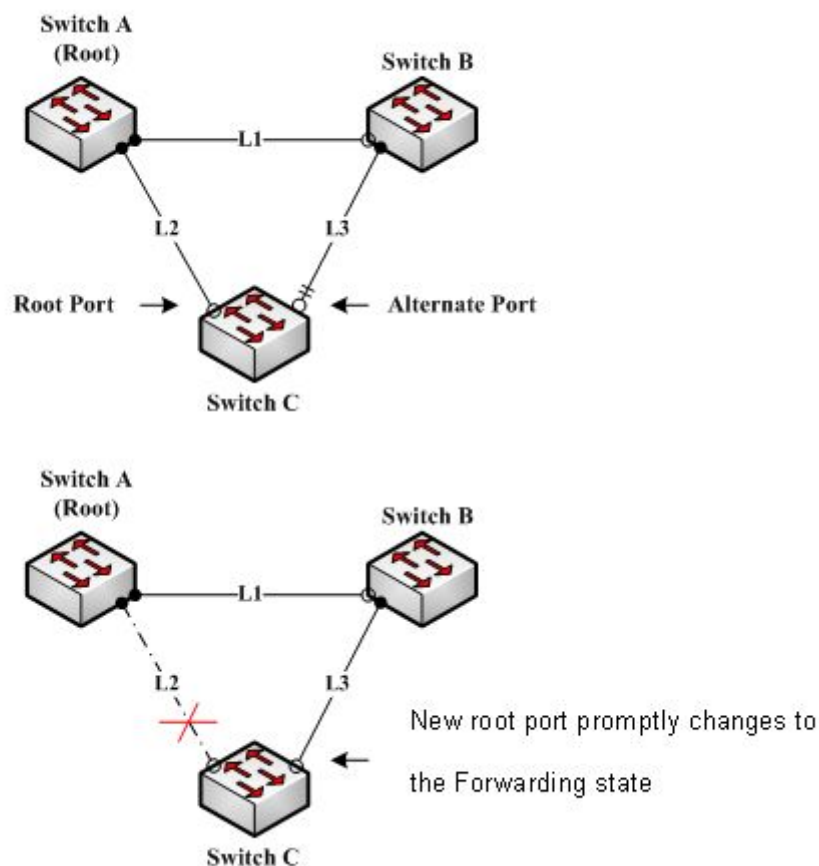
Figure 1.3 Uplink Fast

Note:

The **Uplink Fast** feature adjusts to the slowly convergent SSTP and PVST. In RSTP and MSTP mode, new root port can rapidly enter the Forwarding state without the **Uplink Fast** function.

1.1.5 Backbone Fast

The **Backbone Fast** feature is a supplement of the **Uplink Fast** technology. The **Uplink Fast** technology makes the redundancy line rapidly work in case the direct connection to the designated switch is disconnected, while the **Backbone Fast**

technology detects the indirect-link network blackout in the upper-layer network and boosts the change of the port state.

In figure 1.3, Connection L2 between switch C and switch A is called as the direct link between switch C and root switch A. If the connection is disconnected, the **Uplink Fast** function can solve the problem. Connection L1 between switches A and B is called as the indirect link of switch C. The disconnected indirect link is called as indirect failure, which is handled by the **Backbone Fast** function.

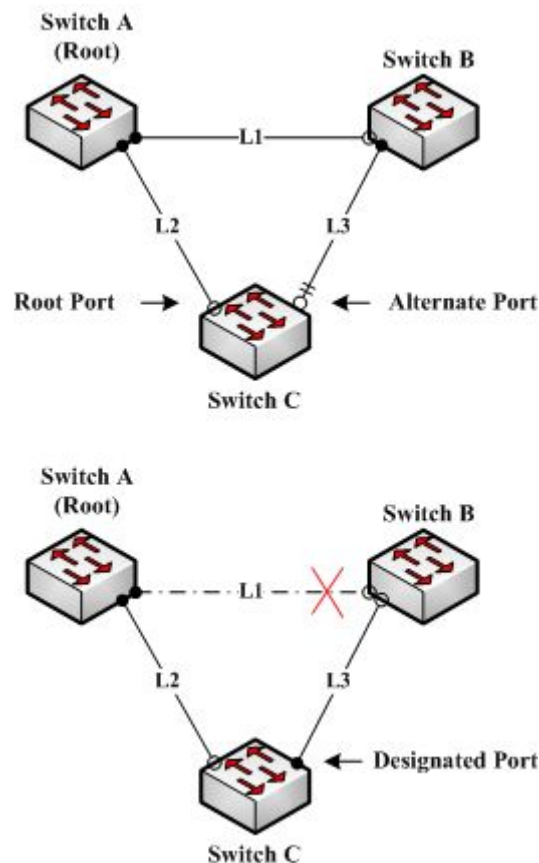The working principle of the Backbone Fast function is shown in Figure 1.4.

Figure 1.4 Backbone Fast

Suppose the bridge priority of switch C is higher than that of switch B. When L1 is disconnected, switch B is selected to send BPDU to switch C because the bridge priority is used as root priority. To switch C, the information contained by BPDU is not prior to information contained by its own. When Backbone Fast is not enabled, the port between switch C and switch B ages when awaiting the bridge information and then turns to be the designated port. The aging normally takes a few seconds. After the function is configured in global configuration mode by running the command **spanning-tree backbonefast**, when the Alternate port of switch C receives a BPDU with lower priority, switch C thinks that an indirect-link and root-switch-reachable connection on the port is disconnected. Switch C then promptly update the port as the designated port without waiting the aging information.

After the Backbone Fast function is enabled, if BPDU with low priority is received at different ports, the switch will perform different actions. If the Alternate port receives the message, the port is updated to the designated port. If the root port

receives the low-priority message and there is no other standby port, the switch turns to be the root switch.

Note that the Backbone Fast feature just omits the time of information aging. New designated port still needs to follow the state change order: the listening state, then the learning state and finally the forwarding state.

Note:

Similar to Uplink Fast, the Backbone Fast feature is effective in SSTP and PVST modes.

1.1.6   Root Guard

The Root Guard feature prevents a port from turning into a root port because of receiving high-priority BPDU.

The Layer 2 network of a service provider (SP) can include many connections to switches that are not owned by the SP. In such a topology, the spanning tree can reconfigure itself and select a customer switch as the root switch, as shown in Figure 17-8. You can avoid this situation by enabling root guard on SP switch interfaces that connect to switches in your customer's network. If spanning-tree calculations cause an interface in the customer network to be selected as the root port, root guard then places the interface in the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root.

If a switch outside the SP network becomes the root switch, the interface is blocked (root-inconsistent state), and spanning tree selects a new root switch. The customer's switch does not become the root switch and is not in the path to the root.

If the switch is operating in multiple spanning-tree (MST) modes, root guard forces the interface to be a designated port. If a boundary port is blocked in an internal spanning-tree (IST) instance because of root guard, the interface also is blocked in all MST instances. A boundary port is an interface that connects to a LAN, the designated switch of which is either an IEEE 802.1D switch or a switch with a different MST region configuration.

Root guard enabled on an interface applies to all the VLANs to which the interface belongs. VLANs can be grouped and mapped to an MST instance.

You can enable this feature by using the spanning-tree guard root interface configuration command.

Note：

Root Guard feature acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, Root port is always blocked by Root Guard. In RSTP/MSTP mode, Root port won't be blocked until receiving higher level BPDU. A port which formerly plays the Root role will not be blocked.

1.1.7   Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is enabled on the entire switched network. Loop

guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

You can enable this feature by using the spanning-tree loopguard default global configuration command.

When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

When the switch is operating in MST mode, BPDUs are not sent on nonboundary ports only if loop guard in all MST instances blocks the interface. On a boundary port, loop guard blocks the interface in all MST instances.

Note：

Loop Guard feature acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, the designated port is always be blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked only when it changes into the designated port because of inaccessibility to receiving BPDU. Loop Guard will not block a port, which is provided with the designated role due to receiving the lower level BPDU.

1.2   Configuring STP Optional Characteristic

1.2.1   STP Optional Characteristic Configuration Task

- Configuring Port Fast

- Configuring BPDU Guard

- Configuring BPDU Filter

- Configuring Uplink Fast

- Configuring Backbone Fast

- Configuring Root Guard

- Configuring Loop Guard

1.2.2   Configuring Port Fast

An interface with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without waiting for the standard forward-time delay.

Use the following command to configure the port fast feature in the global configuration mode：

command	purpose
spanning-tree port fast default	Globally enables port fast feature. It is valid to all interfaces.

no spanning-tree portfast default	Globally disables port fast feature. It has no effect on the interface configuration.

Note：

The port fast feature only applies to the interface that connects to the host. The BPDU Guard or BPDU Filter must be configured at the same time when the port fast feature is configured globally.

Use the following command to configure the port fast feature in the interface configuration mode：

command	purpose
spanning-tree portfast	Enables port fast feature on the interface.
no spanning-tree portfast	Disables port fast feature on the interface. It has no effect on the global configuration.

1.2.3   Configuring BPDU Guard

When you globally enable BPDU guard on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state), spanning tree shuts down Port Fast-enabled ports that receive BPDUs.

In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port means an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state. When this happens, the switch shuts down the entire port on which the violation occurred.

To prevent the port from shutting down, you can use the errdisable detect cause bpduguard shutdown vlan global configuration command to shut down just the offending VLAN on the port where the violation occurred.

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

Follow these steps to globally enable the BPDU guard feature：

command	purpose
spanning-tree portfast bpduguard	Globally enables bpdu guard feature. It is valid to all interfaces.
no spanning-tree portfast bpduguard	Globally disables bpdu guard feature.

Instruction：

Globally enabling port fast feature may result in broadcast storm. The BPDU Guard or BPDU Filter should be configured for protection sake.

Follow these steps to enable the BPDU guard feature in interface configuration mode：

command	purpose
spanning-tree bpduguard enable	Enables bpdu guard feature on the interface.
spanning-tree bpduguard disable	Disables bpdu guard feature on the interface. It has no effect on the global configuration.
no spanning-tree bpduguard	Disable bpdu guard feature on the interface. It has no effect on the global configuration.

1.2.4 Configuring BPDU Filter

When you globally enable BPDU filtering on Port Fast-enabled interfaces, it prevents interfaces that are in a Port Fast-operational state from sending or receiving BPDUs. The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to these interfaces do not receive BPDUs. If a BPDU is received on a Port Fast-enabled interface, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

Follow these steps to globally enable the BPDU filter feature.：

command	purpose
spanning-tree portfast bpdufilter	Globally enables bpdu filter feature. It is valid to all interfaces.
no spanning-tree portfast bpdufilter	Globally disables bpdu filter feature.

Instruction：

Globally enabling port fast feature may result in broadcast storm. The BPDU Guard or BPDU Filter should be configured for protection sake.

Follow these steps to enable the BPDU filter feature in the interface configuration mode ：

command	purpose
spanning-tree bpdufilter enable	Enables bpdu filter feature on the interface.
spanning-tree bpdufilter disable	Disables bpdu filter feature. It has no effect on the global configuration.
no spanning-tree bpdufilter	Disables bpdu filter feature. It has no influence on the global configuration.

1.2.5 Configuring Uplink Fast

If a switch loses connectivity, it begins using the alternate paths as soon as the spanning tree selects a new root port. By enabling UplinkFast with the spanning-tree uplinkfast global configuration command, you can accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. The root port transitions to the forwarding state immediately

without going through the listening and learning states, as it would with the normal spanning-tree procedures.

Uplink Fast feature is only valid in SSTP/PVST mode.

Follow these steps to globally enable UplinkFast.：

command	purpose
spanning-tree uplinkfast	Enables uplink fast feature.
no spanning-tree uplinkfast	Disables uplink fast feature.

1.2.6   Configuring Backbone Fast

BackboneFast is a complementary technology to the UplinkFast feature, which responds to failures on links directly connected to access switches. BackboneFast optimizes the maximum-age timer, which controls the amount of time the switch stores protocol information received on an interface. When a switch receives an inferior BPDU from the designated port of another switch, the BPDU is a signal that the other switch might have lost its path to the root, and BackboneFast tries to find an alternate path to the root.

Backbone fast feature is only valid in SSTP/PVST mode.

Follow these steps to globally enable BackboneFast.：

command	purpose
spanning-tree backbonefast	Enables backbone fast feature.
no spanning-tree backbonefast	Disables backbone fast feature.

1.2.7   Configuring Root Guard

Root guard enabled on an interface applies to all the VLANs to which the interface belongs. Do not enable the root guard on interfaces to be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and are prevented from reaching the forwarding state.

Root Guard feature acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, Root port is always blocked by Root Guard. In RSTP/MSTP mode, Root port won't be blocked until receiving higher level BPDU. A port which formerly plays the Root role will not be blocked.

Follow these steps to enable root guard on an interface.：

command	purpose
spanning-tree guard root	Enables root guard feature on the interface.

no spanning-tree guard	Disables root guard and loop guard features on the interface.
spanning-tree guard none	Disables root guard and loop guard features on the interface.

1.2.8   Configuring Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is configured on the entire switched network. Loop guard operates only on interfaces that are considered point-to-point by the spanning tree.

Loop Guard feature acts differently somehow in SSTP/PVST. In SSTP/PVST mode,, the designated port is always blocked by Loop Guard. In RSTP/MSTP, the designated port is always blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked only when it changes into the designated port because of inaccessibility to receiving BPDU. A port which is provided with the designated role due to receiving the lower level BPDU will not be blocked by Loop Guard.

Follow these steps to enable loop guard in global configuration mode.：

command	purpose
spanning-tree loopguard default	Globally enables loop guard feature. It is valid to all interfaces.
no spanning-tree loopguard default	Globally disables loop guard.

Follow these steps to enable loop guard in the interface configuration mode.：

Command	Purpose
spanning-tree guard loop	Enables loop guard feature on the interface.
no spanning-tree guard	Disables root guard and loop guard feature on the interface.
spanning-tree guard none	Disables root guard and loop guard on the interface.