

Spanning Tree PortFast BPDU Guard Enhancement

Document ID: 10586

Introduction

Prerequisites

Requirements

Components Used

Conventions

Feature Description

Figure 1

Figure 2

Configuration

Monitoring

Command Output

Related Information

Introduction

This document explains the PortFast Bridge Protocol Data Unit (BPDU) guard feature. This feature is one of the Spanning Tree Protocol (STP) enhancements that Cisco created. This feature enhances switch network reliability, manageability, and security.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

These software versions introduced the STP PortFast BPDU guard:

- Catalyst OS (CatOS) software version 5.4.1 for the Catalyst 4500/4000 (Supervisor Engine II), 5500/5000, 6500/6000, 2926, 2926G, 2948G, and 2980G platforms
- Cisco IOS® Software Release 12.0(7)XE for the Catalyst 6500/6000 platforms
- Cisco IOS Software Release 12.1(8a)EW for the Catalyst 4500/4000 Supervisor Engine III
- Cisco IOS Software Release 12.1(12c)EW for the Catalyst 4500/4000 Supervisor Engine IV
- Cisco IOS Software Release 12.0(5)WC5 for the Catalyst 2900XL and 3500XL series
- Cisco IOS Software Release 12.1(11)AX for the Catalyst 3750 series switches
- Cisco IOS Software Release 12.1(14)AX for the Catalyst 3750 Metro switches
- Cisco IOS Software Release 12.1(19)EA1 for the Catalyst 3560 series switches
- Cisco IOS Software Release 12.1(4)EA1 for the Catalyst 3550 series switches
- Cisco IOS Software Release 12.1(11)AX for the Catalyst 2970 series switches
- Cisco IOS Software Release 12.1(12c)EA1 for the Catalyst 2955 series switches
- Cisco IOS Software Release 12.1(6)EA2 for the Catalyst 2950 series switches
- Cisco IOS Software Release 12.1(11)EA1 for the Catalyst 2950 Long-Reach Ethernet (LRE) switches
- Cisco IOS Software Release 12.1(13)AY for the Catalyst 2940 series switches

Note: STP PortFast BPDUs guard is *not* available for the Catalyst 8500 series, 2948G-L3, or 4908G-L3 switches.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Feature Description

STP configures meshed topology into a loop-free, tree-like topology. When the link on a bridge port goes up, STP calculation occurs on that port. The result of the calculation is the transition of the port into forwarding or blocking state. The result depends on the position of the port in the network and the STP parameters. This calculation and transition period usually takes about 30 to 50 seconds. At that time, no user data pass via the port. Some user applications can time out during the period.

In order to allow immediate transition of the port into forwarding state, enable the STP PortFast feature. PortFast immediately transitions the port into STP forwarding mode upon linkup. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode.

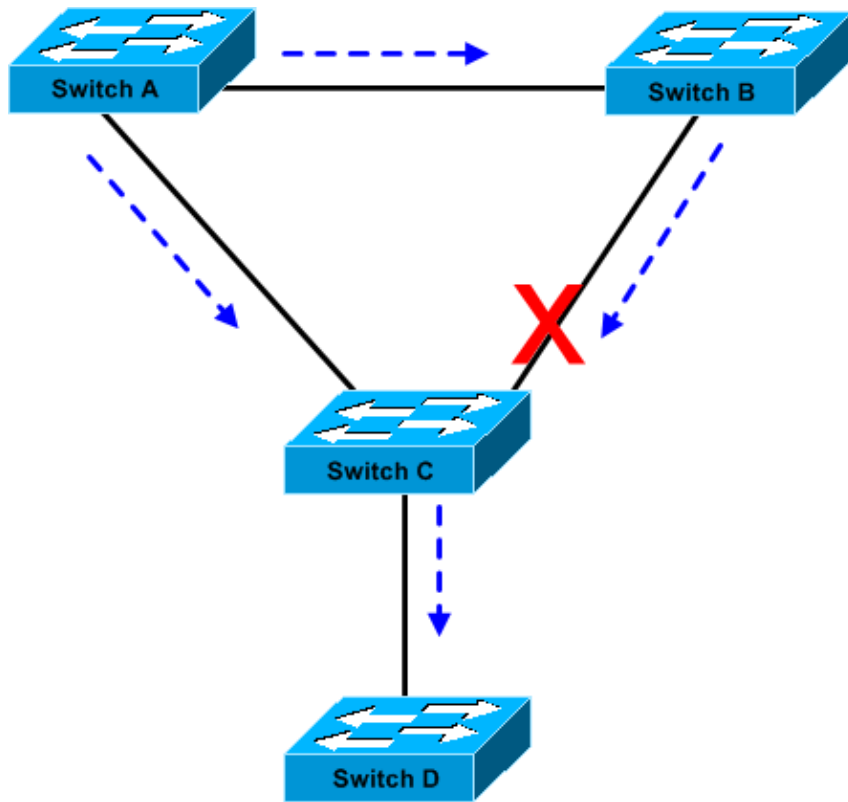
As long as the port participates in STP, some device can assume the root bridge function and affect active STP topology. To assume the root bridge function, the device would be attached to the port and would run STP with a lower bridge priority than that of the current root bridge. If another device assumes the root bridge function in this way, it renders the network suboptimal. This is a simple form of a denial of service (DoS) attack on the network. The temporary introduction and subsequent removal of STP devices with low (0) bridge priority cause a permanent STP recalculation.

The STP PortFast BPDUs guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs, the BPDUs guard operation disables the port that has PortFast configured. The BPDUs guard transitions the port into errdisable state, and a message appears on the console. This message is an example:

```
2000 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received BPDUs on PortFast enable port.  
Disabling 2/1  
2000 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
```

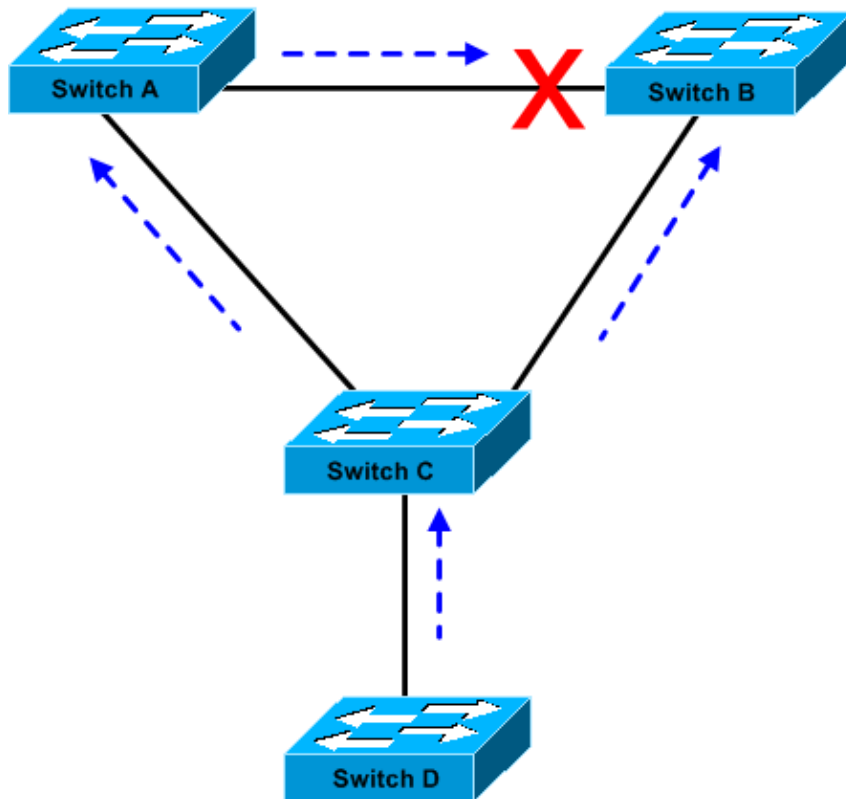
Consider this example:

Figure 1



Bridge A has priority 8192 and is the root for the VLAN. Bridge B has priority 16384 and is the backup root bridge for the same VLAN. Bridges A and B, which a Gigabit Ethernet link connects, make up a core of the network. Bridge C is an access switch and has PortFast configured on the port that connects to device D. If the other STP parameters are default, the bridge C port that connects to bridge B is in STP blocking state. Device D (PC) does not participate in STP. The dashed arrows indicate the flow of STP BPDUs.

Figure 2



In Figure 2, device D has started to participate in STP. For example, a Linux-based bridge application is launched on a PC. If the priority of the software bridge is 0 or any value below the priority of the root bridge, the software bridge takes over the root bridge function. The Gigabit Ethernet link that connects the two core switches transitions into blocking mode. The transition causes all the data in that VLAN to flow via the 100-Mbps link. If more data flow via the core in the VLAN than the link can accommodate, the drop of frames occurs. The frame drop leads to a connectivity outage.

The STP PortFast BPDU guard feature prevents such a situation. The feature disables the port as soon as bridge C receives the STP BPDU from device D.

Configuration

You can enable or disable STP PortFast BPDU guard on a global basis, which affects all ports that have PortFast configured. By default, STP BPDU guard is disabled. Issue this command in order to enable STP PortFast BPDU guard on the switch:

CatOS Command

```
Console> (enable) set spantree portfast bpdu-guard enable

Spantree portfast bpdu-guard enabled on this switch.

Console> (enable)
```

Cisco IOS Software Command

```
CatSwitch-IOS(config)# spanning-tree portfast bpduguard
CatSwitch-IOS(config)
```

When STP BPDU guard disables the port, the port remains in the disabled state unless the port is enabled manually. You can configure a port to reenable itself automatically from the errdisable state. Issue these commands, which set the **errdisable-timeout interval** and enable the **timeout** feature:

CatOS Commands

```
Console> (enable) set errdisable-timeout interval 400  
Console> (enable) set errdisable-timeout enable bpdu-guard
```

Cisco IOS Software Commands

```
CatSwitch-IOS(config)# errdisable recovery cause bpduguard  
CatSwitch-IOS(config)# errdisable recovery interval 400
```

Note: The default timeout interval is 300 seconds and, by default, the timeout feature is disabled.

Monitoring

In order to verify whether the feature is enabled or disabled, issue this command:

Command Output

CatOS Command

```
Console> (enable) show spantree summary  
Root switch for vlans: 3-4.  
Portfast bpdu-guard enabled for bridge.  
Uplinkfast disabled for bridge.  
Backbonefast disabled for bridge.  
  
Summary of Connected Spanning Tree Ports By VLAN:  
  
Vlan  Blocking Listening Learning Forwarding STP Active  
-----  
1      0      0      0      1      1  
3      0      0      0      1      1  
4      0      0      0      1      1  
20     0      0      0      1      1  
  
Blocking Listening Learning Forwarding STP Active  
-----  
Total      0      0      0      4      4  
  
Console> (enable)
```

Cisco IOS Software Command

```
CatSwitch-IOS# show spanning-tree summary totals  
Root bridge for: none.  
PortFast BPDU Guard is enabled
```

UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short

Name	Blocking	Listening	Learning	Forwarding	STP Active
1 VLAN	0	0	0	1	1

CatSwitch-IOS#

Related Information

- [LAN Product Support Pages](#)
- [LAN Switching Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 01, 2005

Document ID: 10586
