Spanning-Tree Protocol Enhancements with Loop Guard and BPDU Skew Detection Features

TAC Notice: What's Changing on TAC Web

Contents

Introduction

Spanning Tree Protocol (STP) resolves physically redundant topologies into loop-free, tree-like topologies. The biggest issue with STP is that some hardware failures can cause it to fail. This failure creates forwarding loops (or STP loops). Major network outages are caused by STP loops.

This document describes the loop guard STP feature that is intended to improve the stability of the Layer 2 networks. This document also describes Bridge Protocol Data Unit (BPDU) skew detection. BPDU skew detection is a diagnostic feature that generates syslog messages when BPDUs are not received in time.

Prerequisites

Requirements

This document assumes that the reader is familiar with the basic operation of STP. Refer to

Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches in order to learn how STP works.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

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

Feature Availability

CatOS

- The STP loop guard feature was introduced in CatOS version 6.2.1 of the Catalyst software for Catalyst 4000 and Catalyst 5000 platforms and in version 6.2.2 for the Catalyst 6000 platform.
- The BPDU skew detection feature was introduced in CatOS version 6.2.1 of the Catalyst software for Catalyst 4000 and Catalyst 5000 platforms and in version 6.2.2 for the Catalyst 6000 platform.

Cisco IOS®

- The STP loop guard feature was introduced in Cisco IOS Software Release 12.1(12c)EW for Catalyst 4500 switches and Cisco IOS Software Release 12.1(11b)EX for Catalyst 6500.
- The BPDU skew detection feature is not supported in Catalyst switches running Cisco IOS system software.

Brief Summary of STP Port Roles

Internally, STP assigns to each bridge (or switch) port a role that is based on configuration, topology, relative position of the port in the topology, and other considerations. The port role defines the behavior of the port from the STP point of view. Based on the port role, the port either sends or receives STP BPDUs and forwards or blocks the data traffic. This list provides a brief summary of each STP port role:

- *Designated*—One designated port is elected per link (segment). The designated port is the port closest to the root bridge. This port sends BPDUs on the link (segment) and forwards traffic towards the root bridge. In an STP converged network, each designated port is in the STP forwarding state.
- *Root*—The bridge can have only one root port. The root port is the port that leads to the root bridge. In an STP converged network, the root port is in the STP forwarding state.
- *Alternate*—Alternate ports lead to the root bridge, but are not root ports. The alternate ports maintain the STP blocking state.
- *Backup*—This is a special case when two or more ports of the same bridge (switch) are connected together, directly or through shared media. In this case, one port is designated, and the remaining ports block. The role for this port is backup.

STP Loop Guard

Feature Description

The STP loop guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. In its operation, STP relies on continuous reception or transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs.

When one of the ports in a physically redundant topology no longer receives BPDUs, the STP conceives that the topology is loop free. Eventually, the blocking port from the alternate or backup port becomes designated and moves to a forwarding state. This situation creates a loop.

The loop guard feature makes additional checks. If BPDUs are not received on a non-designated port, and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state. Without the loop guard feature, the port assumes the designated port role. The port moves to the STP forwarding state and creates a loop.

When the loop guard blocks an inconsistent port, this message is logged:

- **CatOS**

```
%SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2 in vlan
 loop-inconsistent state.
```

- **Cisco IOS**

```
%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port FastEthernet0/24
VLAN0050.
```

Once the BPDU is received on a port in a loop-inconsistent STP state, the port transitions into another STP state. According to the received BPDU, this means that the recovery is automatic and intervention is not necessary. After recovery, this message is logged:

- **CatOS**

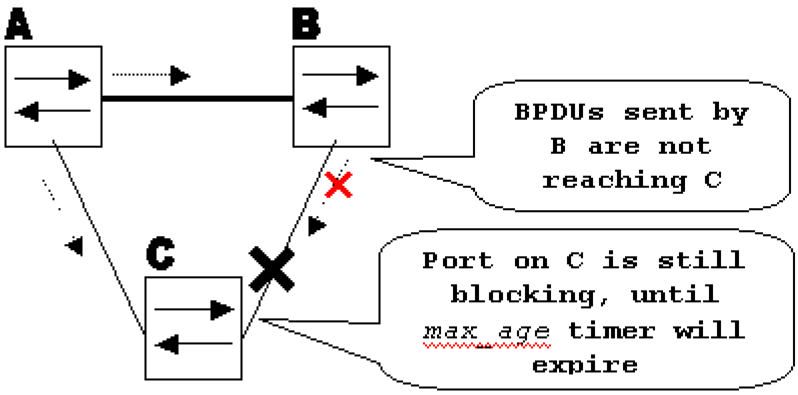
```
%SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

- **Cisco IOS**

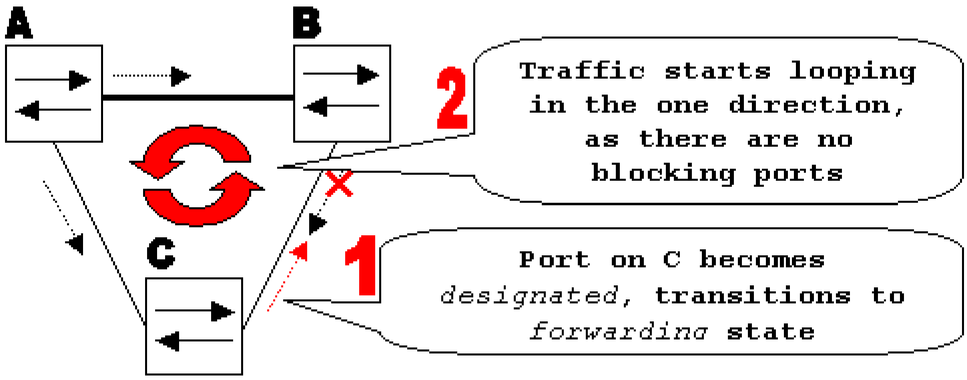
```
%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port FastEthernet0
VLAN0050.
```

Consider this example in order to illustrate this behavior:

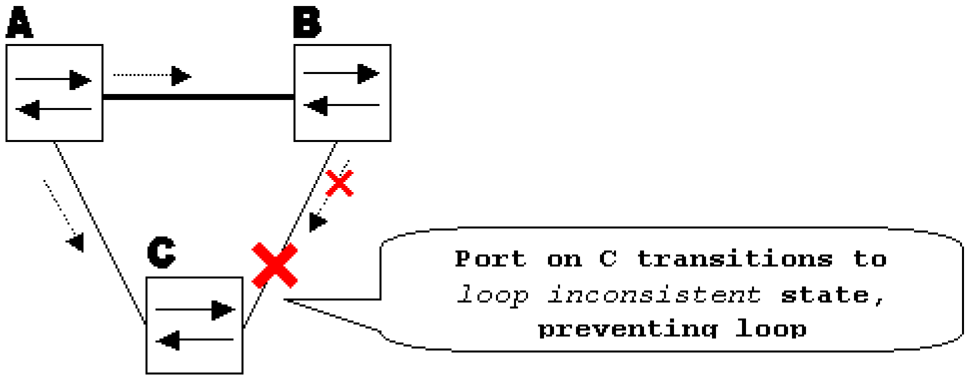
Switch A is the root switch. Switch C does not receive BPDUs from switch B due to unidirectional link failure on the link between switch B and switch C.


A
B
C
BPDUs sent by B are not reaching C
Port on C is still blocking, until max_age timer will expire

Without loop guard, the STP blocking port on switch C transitions to the STP listening state when the max_age timer expires, and then it transitions to the forwarding state in two times the forward_delay time. This situation creates a loop.


A
B
C
2
Traffic starts looping in the one direction, as there are no blocking ports
1
Port on C becomes designated, transitions to forwarding state

With loop guard enabled, the blocking port on switch C transitions into STP loop-inconsistent state when the max_age timer expires. A port in STP loop-inconsistent state does not pass user traffic, so a loop is not created. (The loop-inconsistent state is effectively equal to blocking state.)

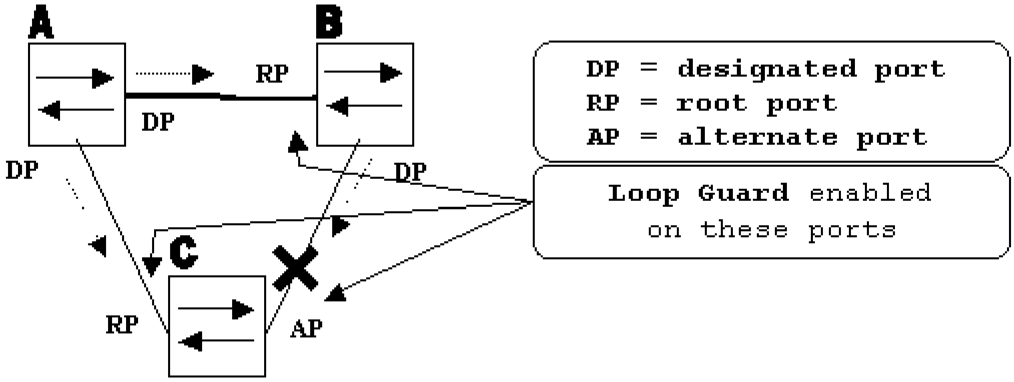

A
B
C
Port on C transitions to loop inconsistent state, preventing loop

Configuration Considerations

The loop guard feature is enabled on a per-port basis. However, as long as it blocks the port on the STP level, loop guard blocks inconsistent ports on a per-VLAN basis (because of per-VLAN STP). That is, if BPDUs are not received on the trunk port for only one particular VLAN, only that VLAN is blocked (moved to loop-inconsistent STP state). For the same reason, if enabled on an EtherChannel interface, the entire channel is blocked for a particular VLAN, not just one link (because EtherChannel is regarded as one logical port from the STP point of view).

On which ports should the loop guard be enabled? The most obvious answer is on the blocking ports. However, this is not totally correct. Loop guard must be enabled on the non-designated ports (more precisely, on root and alternate ports) for all possible combinations of active topologies. As long as the loop guard is not a per-VLAN feature, the same (trunk) port might be designated for one VLAN and non-designated for the other. The possible failover scenarios should also be taken into account.

Consider this example:



By default, loop guard is disabled. This command is used to enable loop guard:

- **CatOS**

```
set spantree guard loop <mod/port>

Console> (enable) set spantree guard loop 3/13
Enable loopguard will disable rootguard if it's currently enabled on th
Do you want to continue (y/n) [n]? y
Loopguard on port 3/13 is enabled.
```

- **Cisco IOS**

```
spanning-tree guard loop

Router(config)#interface gigabitEthernet 1/1
Router(config-if)#spanning-tree guard loop
```

With version 7.1(1) of the Catalyst software (CatOS), loop guard can be enabled globally on all ports. Effectively, loop guard is enabled on all point-to-point links. The point-to-point link is detected by the duplex status of the link. If duplex is full, the link is considered point-to-point. It is still possible to configure, or override, global settings on a per-port basis.

Issue this command in order to enable loop guard globally:

- **CatOS**

```
Console> (enable) set spantree global-default loopguard enable
```

- **Cisco IOS**

```
Router(config)#spanning-tree loopguard default
```

Issue this command in order to disable loop guard:

- **CatOS**

```
Console> (enable) set spantree guard none <mod/port>
```

- **Cisco IOS**

```
Router(config-if)#no spanning-tree guard loop
```

Issue this command in order to globally disable loop guard:

- **CatOS**

```
Console> (enable) set spantree global-default loopguard disable
```

- **Cisco IOS**

```
Router(config)#no spanning-tree loopguard default
```

Issue this command in order to verify loop guard status:

- **CatOS**

```
show spantree guard <mod/port>

Console> (enable) show spantree guard 3/13
Port                     VLAN Port-State    Guard Type
------------------------ ---- ------------- ----------
3/13                     2    forwarding          loop
Console> (enable)
```

- **Cisco IOS**

```
show spanning-tree

Router#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID           is disabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Pathcost method used         is short

Name                   Blocking Listening Learning Forwarding STP Activ
---------------------- -------- --------- -------- ---------- ---------
Total                         0         0        0          0         0
```

Loop Guard versus UDLD

Loop guard and Unidirectional Link Detection (UDLD) functionality overlap, partly in the sense that both protect against STP failures caused by unidirectional links. However, these two features differ in functionality and how they approach the problem. This table describes loop guard and UDLD functionality:

Functionality	Loop Guard	UDLD
Configuration	Per-port	Per-port
Action granularity	Per-VLAN	Per-port
Autorecover	Yes	Yes, with err-disable timeout feature
Protection against STP failures caused by unidirectional links	Yes, when enabled on all root and alternate ports in redundant topology	Yes, when enabled on all links in redundant topology
Protection against STP failures caused by problems in the software (designated switch does not send BPDU)	Yes	No
Protection against miswiring.	No	Yes

Based on the various design considerations, you can choose either UDLD or the loop guard feature. In regards to STP, the most noticeable difference between the two features is the absence of protection in UDLD against STP failures caused by problems in software. As a result, the designated switch does not send BPDUs. However, this type of failure is (by an order of magnitude) more rare than failures caused by unidirectional links. In return, UDLD might be more flexible in the case of unidirectional links on EtherChannel. In this case, UDLD disables only failed links, and the channel should remain functional with the links that remain. In such a failure, the loop guard puts it into loop-inconsistent state in order to block the whole channel.

Additionally, loop guard does not work on shared links or in situations where the link has been unidirectional since the link-up. In the last case, the port never receives BPDU and becomes designated. Because this behaviour could be normal, this particular case is not covered by loop guard. UDLD provides protection against such a scenario.

As described, the highest level of protection is provided when you enable UDLD and loop guard.

Interoperability of Loop Guard with Other STP Features

Root Guard

The root guard is mutually exclusive with the loop guard. The root guard is used on designated ports, and it does not allow the port to become non-designated. The loop guard works on non-designated ports and does not allow the port to become designated through the expiration of max_age. The root guard cannot be enabled on the same port as the loop guard. When the loop guard is configured on the port, it disables the root guard configured on the same port.

Uplink Fast and Backbone Fast

Both uplink fast and backbone fast are transparent to the loop guard. When max_age is skipped by backbone fast at the time of reconvergence, it does not trigger the loop guard. For more information on uplink fast and backbone fast, refer to these documents:

- Understanding and Configuring the Cisco Uplink Fast Feature
- Understanding and Configuring Backbone Fast on Catalyst Switches

PortFast and BPDU Guard and Dynamic VLAN

Loop guard cannot be enabled for ports on which portfast is enabled. Since BPDU guard works on portfast-enabled ports, some restrictions apply to BPDU guard. Loop guard cannot be enabled on dynamic VLAN ports since these ports have portfast enabled.

Shared Links

Loop guard should not be enabled on shared links. If you enable loop guard on shared links, traffic from hosts connected to shared segments might be blocked.

Multiple Spanning Tree (MST)

Loop guard functions correctly in the MST environment.

BPDU Skew Detection

Loop guard should operate correctly with BPDU skew detection.

BPDU Skew Detection

Feature Description

STP operation relies heavily on the timely reception of BPDUs. At every hello_time message (2 seconds by default), the root bridge sends BPDUs. Non-root bridges do not regenerate BPDUs for each hello_time message, but they receive relayed BPDUs from the root bridge. Therefore, every non-root bridge should receive BPDUs on every VLAN for each hello_time message. In some cases, BPDUs are lost, or the bridge CPU is too busy to relay BPDU in a timely manner. These issues, as well as other issues, can cause BPDUs to arrive late (if they arrive at all). This issue potentially compromises the stability of the spanning tree topology.

BPDU skew detection allows the switch to keep track of BPDUs that arrive late and to notify the administrator with syslog messages. For every port on which a BPDU has ever arrived late (or has skewed), skew detection reports the most recent skew and the duration of the skew (latency). It also reports the longest BPDU delay on this particular port.

In order to protect the bridge CPU from overload, a syslog message is not generated every time BPDU skewing occurs. Messages are rate-limited to one message every 60 seconds. However, should the delay of BPDU exceed max_age divided by 2 (which equals 10 seconds by default), the message is immediately printed.

Note: BPDU skew detection is a diagnostic feature. Upon detection of BPDU skewing, it sends a syslog message. BPDU skew detection takes no further corrective action.

This is an example of a syslog message generated by BPDU skew detection:

```
%SPANTREE-2-BPDU_SKEWING: BPDU skewed with a delay of 10 secs (max_age/2)
```

Configuration Considerations

BPDU skew detection is configured on a per-switch basis. The default setting is disabled. Issue this command in order to enable BPDU skew detection:

```
Cat6k> (enable) set spantree bpdu-skewing enable
   Spantree bpdu-skewing enabled on this switch.
```

In order to see BPDU skewing information, use the **show spantree bpdu-skewing** <*vlan*>|<*mod/port*> command as demonstrated in this example:

```
Cat6k> (enable) show spantree bpdu-skewing 1
Bpdu skewing statistics for vlan 1
Port Last Skew (ms) Worst Skew (ms) Worst Skew Time
-------------- --------------- --------------- -------------------------
3/12 4000 4100 Mon Nov 19 2001, 16:36:04
```

NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums - Featured Conversations for LAN
Network Infrastructure: LAN Routing and Switching
Limit switch port bandwidth - Dec 19, 2008 upgrade 3550 smi to emi? - Dec 19, 2008 HWIC-4ESW not recognized by 2821 router - Dec 19, 2008 NAT on a stick problem - Dec 19, 2008 Access Server IOS help - Dec 19, 2008
Network Infrastructure: Getting Started with LANs
Assigning a second external IP address to ASA 5505 - Dec 19, 2008 ISSUES: c2950G-24-EI - Dec 18, 2008 Username in Console of 3750 Switch - Dec 18, 2008 Aging Time - Dec 18, 2008 Ether Channel Configuration Help - Dec 17, 2008

Related Information

- **Spanning Tree Protocol Root Guard Enhancement**
- **Spanning Tree Portfast BPDU Guard Enhancement**
- **Understanding and Configuring the Unidirectional Link Detection Protocol Feature**
- **Using PortFast and Other Commands to Fix Workstation Startup Connectivity Delays**
- **LAN Product Support**
- **LAN Switching Technology Support**
- **Technical Support & Documentation - Cisco Systems**