生成树 PortFast BPDU 防护增强功能

目录

简介

本文档将介绍 PortFast 网桥协议数据单元 (BPDU) 防护功能。此功能是 Cisco 创建的生成树协议 (STP) 增强功能之一。此功能提高了交换网络的可靠性、可管理性和安全性。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

以下软件版本引入了 STP PortFast BPDU 防护：

- 用于 Catalyst 4500/4000（Supervisor 引擎 II）、5500/5000、6500/6000、2926、2926G、2948G 和 2980G 平台的 Catalyst OS (CatOS) 软件版本 5.4.1
- 用于 Catalyst 6500/6000 平台的 Cisco IOS® 软件版本 12.0(7)XE
- 用于 Catalyst 4500/4000 Supervisor 引擎 III 的 Cisco IOS 软件版本 12.1(8a)EW
- 用于 Catalyst 4500/4000 Supervisor 引擎 IV 的 Cisco IOS 软件版本 12.1(12c)EW
- 用于 Catalyst 2900XL 和 3500XL 系列的 Cisco IOS 软件版本 12.0(5)WC5
- 用于 Catalyst 3750 系列交换机的 Cisco IOS 软件版本 12.1(11)AX
- 用于 Catalyst 3750 Metro 交换机的 Cisco IOS 软件版本 12.1(14)AX
- 用于 Catalyst 3560 系列交换机的 Cisco IOS 软件版本 12.1(19)EA1
- 用于 Catalyst 3550 系列交换机的 Cisco IOS 软件版本 12.1(4)EA1

- 用于 Catalyst 2970 系列交换机的 Cisco IOS 软件版本 12.1(11)AX
- 用于 Catalyst 2955 系列交换机的 Cisco IOS 软件版本 12.1(12c)EA1
- 用于 Catalyst 2950 系列交换机的 Cisco IOS 软件版本 12.1(6)EA2
- 用于 Catalyst 2950 长距离以太网 (LRE) 交换机的 Cisco IOS 软件版本 12.1(11)EA1
- 用于 Catalyst 2940 系列交换机的 Cisco IOS 软件版本 12.1(13)AY

注意： 对于 Catalyst 8500 系列、2948G-L3 或 4908G-L3 交换机*未* 提供 STP PortFast BPDU 防护。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

功能描述

STP 将网状拓扑配置为无环路的树形拓扑。当网桥端口上的链路接通时，会在该端口上进行 STP 计算。计算的结果是将该端口转换为转发或阻塞状态。结果取决于该端口在网络中的位置和 STP 参数。此计算和转换时间通常花费大约 30 到 50 秒。在该时段内，没有任何用户数据通过该端口传递。在该时段内，一些用户应用程序可能会超时。

为了能将端口立即转换为转发状态，请启用 STP PortFast 功能。PortFast 会在接通时立即将端口转换为 STP 转发模式。该端口仍然参与 STP。因此，如果该端口要成为环路的一部分，则该端口最终将转换成 STP 阻塞模式。

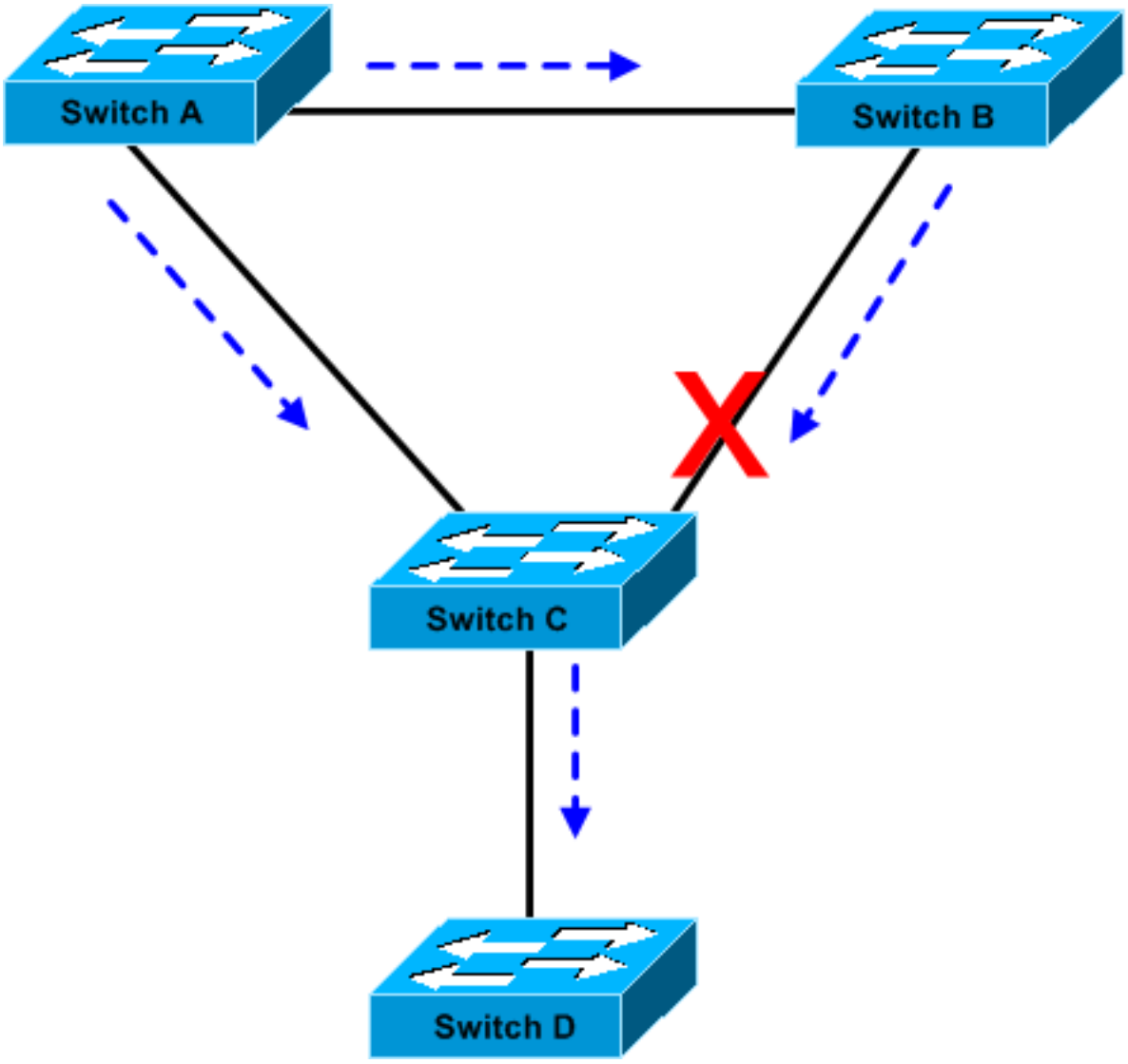
只要该端口参与 STP，一些设备就可以接管根网桥功能，并影响活动 STP 拓扑结构。要接管根网桥功能，该设备必须连接到该端口，并且必须以低于当前根网桥优先级的网桥优先级运行 STP。如果另一个设备以这种方式接管根网桥功能，它将使得网络性能下降。这是网络上的拒绝服务 (DoS) 攻击的简单形式。临时引入并在随后删除具有低 (0) 网桥优先级的 STP 设备将导致永久性 STP 重新计算。

STP PortFast BPDU 防护增强功能使网络设计人员可以强制实施 STP 域边界，并保持活动拓扑的可预测性。启用了 STP PortFast 的端口后面的设备无法影响 STP 拓扑。在收到 BPDU 后，BPDU 防护操作将禁用已配置 PortFast 的端口。BPDU 防护将端口转换为 errdisable 状态，并在控制台上显示一条消息。以下消息是一个示例：

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

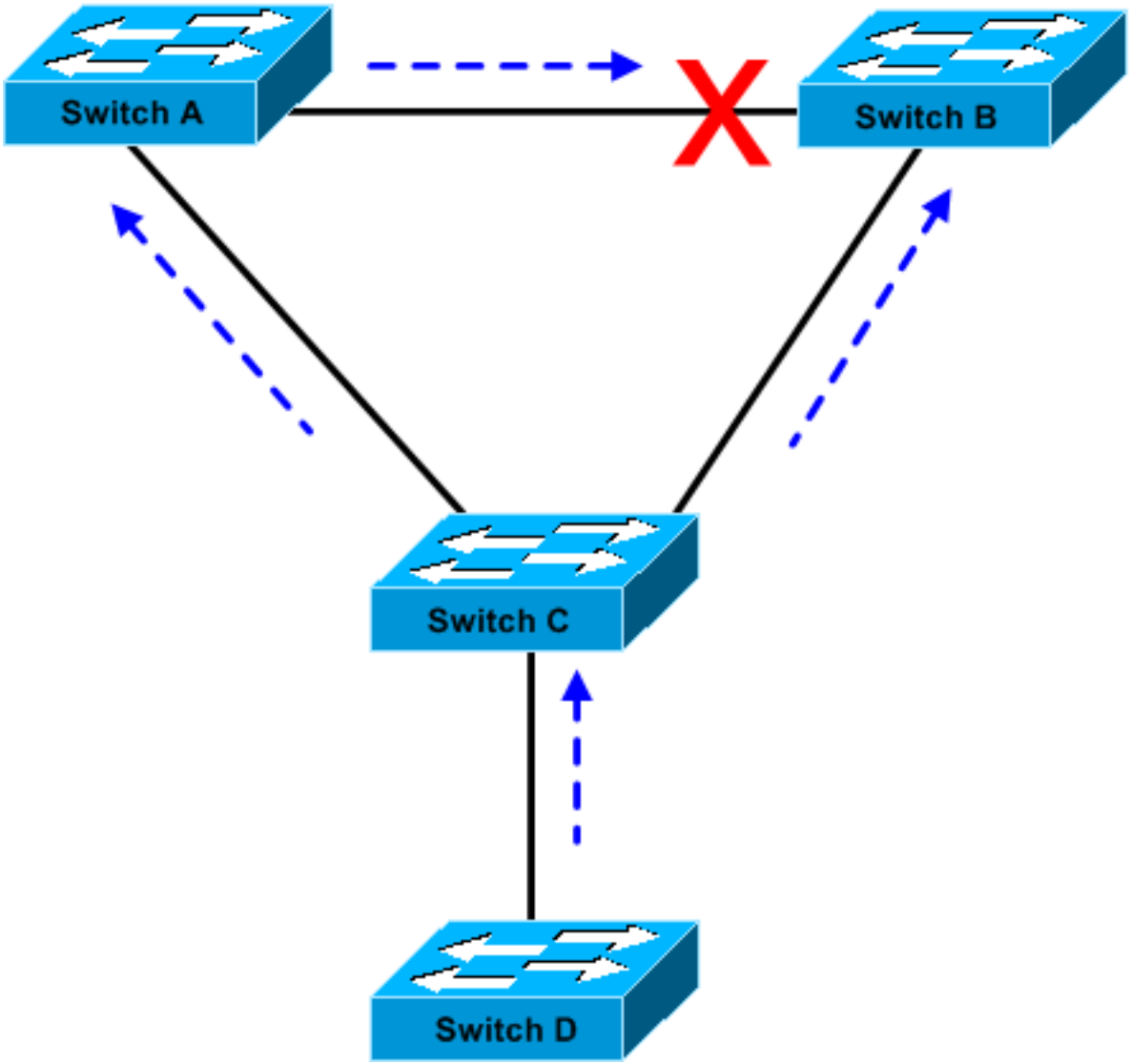
请考虑以下示例：

图 1



网桥 A 具有优先级 8192，并且是 VLAN 的根。网桥 B 具有优先级 16384，并且是同一 VLAN 的备用根网桥。通过千兆以太网链路连接的网桥 A 和网桥 B，构成了网络的核心。网桥 C 是接入交换机，并且已在连接到设备 D 的端口上配置了 PortFast。如果其他 STP 参数都是默认值，则连接到网桥 B 的网桥 C 端口将处于 STP 阻塞状态。设备 D (PC) 不参与 STP。虚线箭头指示 STP BPDU 的流向。

图 2



在图 2 中，设备 D 已开始参与 STP。例如，在 PC 上启动了一个基于 Linux 的网桥应用程序。如果该软件网桥的优先级是 0 或任何低于根网桥优先级的值，则该软件网桥将接管根网桥功能。连接这两个核心交换机的千兆以太网链路将转换为阻塞模式。该转换将导致该 VLAN 中的所有数据都通过 100 Mbps 链路流动。如果流经该 VLAN 核心的数据超出了该链路的容纳能力，则将出现帧丢弃。帧丢弃会导致连接中断。

STP PortFast BPDU 防护功能可防止出现这样的情况。当网桥 C 收到来自设备 D 的 STP BPDU 时，该功能会立即禁用该端口。

配置

可以在全局启用或禁用 STP PortFast BPDU 防护，这将影响所有已配置 PortFast 的端口。默认情况下，STP BPDU 防护处于禁用状态。请发出以下命令以在交换机上启用 STP Portfast BPDU 防护：

CatOS 命令

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

Spantree portfast bpdu-guard enabled on this switch.
```

```
Console> (enable)
```

Cisco IOS 软件命令

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

STP BPDU 防护禁用端口后，除非手动启用该端口，否则该端口将保持处于禁用状态。可以将端口配置为从 errdisable 状态自动重新启用它自己。发出以下命令，以设置 **errdisable-timeout interval** 并启用超时功能：

CatOS 命令

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

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

Cisco IOS 软件命令

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

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

注意： 默认超时间隔是 300 秒，并且在默认情况下禁用超时功能。

监控

为了验证该功能是处于启用状态还是禁用状态，请发出以下命令：

命令输出

CatOS 命令

```
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 软件命令

```
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#
```

相关信息

- LAN 产品支持页
- LAN 交换技术支持页
- 技术支持和文档 - Cisco Systems