了解生成树PortFast和BPDU防护功能

目录

简介

先决条件

- 要求
- 使用的组件
- 规则

背景信息

PortFast和BPDU防护

- 示例1 — 正常STP操作
- 示例2 — 非法网桥导致中断

配置

- 每个接口启用PortFast和BPDU防护
- 全局启用BPDU防护
- 配置自动恢复errdisable状态

确认

相关信息

简介

本文档介绍生成树协议(STP)的PortFast和网桥协议数据单元(BPDU)防护增强功能。

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：

- 适用于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
- 适用于Catalyst 2900XL和3500XL系列的Cisco IOS软件版本12.0(5)WC5
- 适用于Catalyst 3750系列交换机的思科IOS软件版本12.1(11)AX
- 适用于Catalyst 3750 Metro交换机的思科IOS软件版本12.1(14)AX
- 适用于Catalyst 3560系列交换机的思科IOS软件版本12.1(19)EA1
- 适用于Catalyst 3550系列交换机的Cisco IOS软件版本12.1(4)EA1
- 适用于Catalyst 2970系列交换机的思科IOS软件版本12.1(11)AX
- 适用于Catalyst 2955系列交换机的思科IOS软件版本12.1(12c)EA1
- 适用于Catalyst 2950系列交换机的Cisco IOS软件版本12.1(6)EA2
- 适用于Catalyst 2950长距以太网(LRE)交换机的思科IOS软件版本12.1(11)EA1
- 适用于Catalyst 2940系列交换机的思科IOS软件版本12.1(13)AY

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅思科技术提示规则。

背景信息

在正确设计的交换网络中，生成树协议(STP)通过将冗余路径置于阻塞状态来防止第2层环路。每个端口在传递用户流量之前通常都会经过STP状态（侦听、学习和最终转发）。这种融合延迟（传统802.1D大约为30秒）适用于交换机到交换机的链路，但对于连接到终端主机（例如PC、服务器或打印机）的端口而言则不需要，因为后者无法自行创建交换环路。

挑战在于连接到终端主机的端口根本不能接收STP网桥协议数据单元(BPDU)。如果BPDU到达此类端口，通常表示存在以下两个问题之一：有人连接了未授权的交换机，或者设备运行了模拟网桥的软件。这两种情况都会破坏拓扑的稳定，尤其是当非法设备通告上级网桥ID并强制进行根网桥选举时，它永远不能参与。

一个真实案例说明了风险。运行基于Linux的桥接应用程序的用户PC连接到接入端口。由于应用程序发送的BPDU声明网桥优先级较低，因此网络选择该PC作为根网桥。这会将整个生成树拓扑转移

到用电不足的主机，导致链路拥塞并导致网络中断。BPDU防护的存在正是为了防止此类故障。

PortFast和BPDU防护

PortFast会立即将接入端口或中继端口从阻塞状态直接转换为转发状态，跳过侦听和学习阶段。这消除了连接到终端设备的端口的启动延迟，这对于需要立即访问网络的主机（例如，在启动时使用DHCP的工作站）来说非常重要。

PortFast仅用于连接到单个终端站的端口。在链接到另一台交换机的端口上启用此功能，会重新引入STP用来防止的环路风险，因为该端口在STP有机会检测冗余路径之前开始转发。

BPDU防护通过强制假定启用PortFast的端口永远不能看到BPDU来补充PortFast功能。当启用BPDU防护且端口收到BPDU时，交换机将端口置于errdisable状态立即将其关闭。这可以通过两种方式保护拓扑：

- 它可以防止未授权或配置错误的交换机将自身注入生成树。
- 它会阻止设备（如早期场景中的Linux网桥）劫持根角色。

由于端口是管理性禁用而非简单阻止的，因此网络操作员会注意到该事件，并且违规设备会完全隔离，直到问题解决。

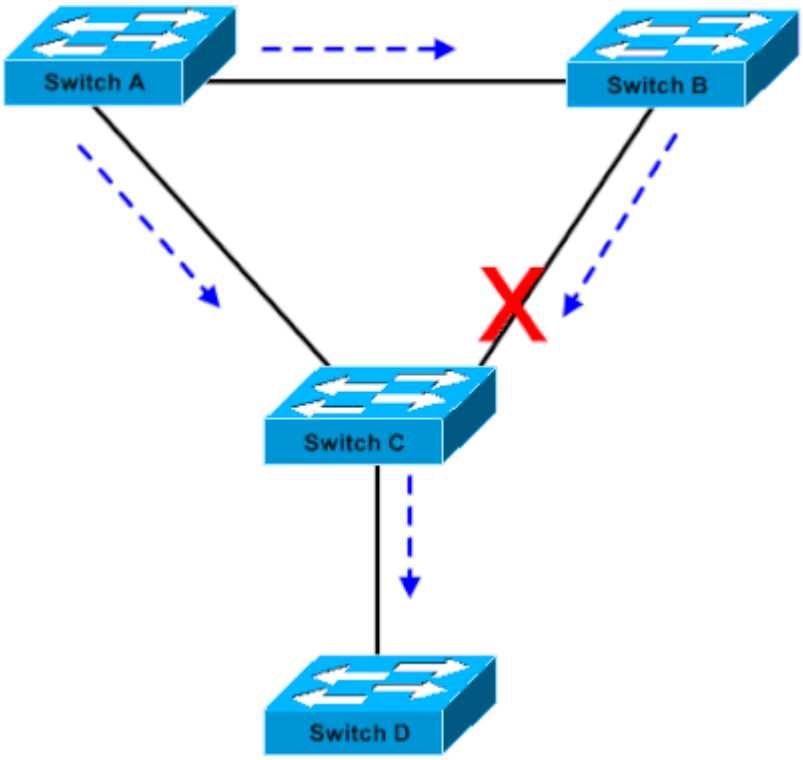
除非配置了errdisable恢复，否则errdisable中的端口不会自行恢复。您可以手动重新启用接口(shutdown后跟no shutdown)，也可以为BPDU防护原因配置自动恢复。

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
```

考虑下一个示例：

示例1 — 正常STP操作



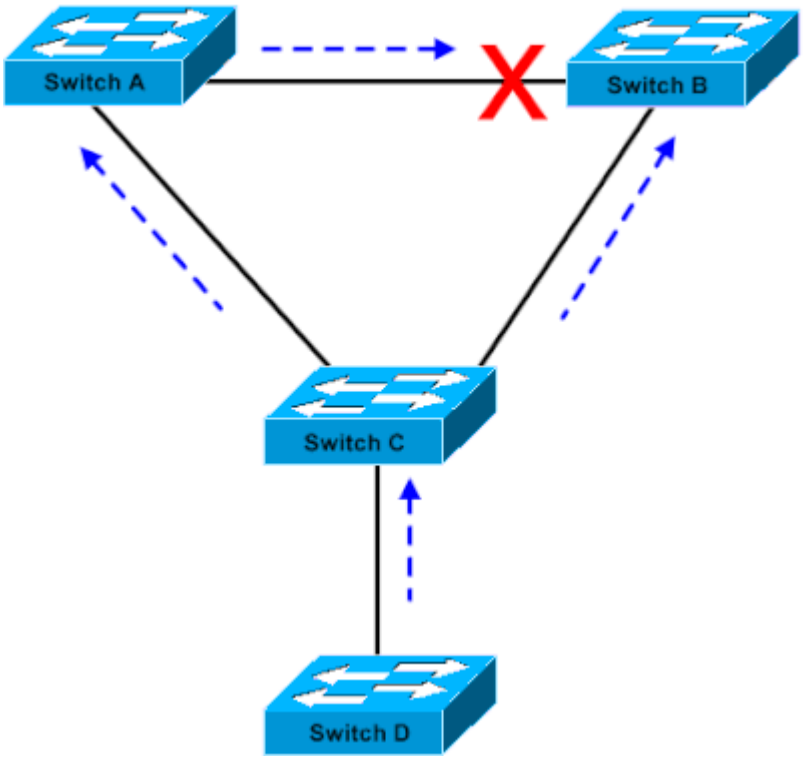
网桥连接

该拓扑包括构成核心层和接入层的三台交换机，以及一台终端设备：

- 交换机网桥优先级为8192，是VLAN的根网桥。
- 交换机B的网桥优先级为16384，使其成为同一VLAN的备用根网桥。
- 交换机A和Bare通过千兆Ethernet链路连接，它们共同构成了网络的核心。
- 交换机Cis是接入交换机。在连接到设备D的端口上配置了PortFaststst。
- 设备是PC，不参与STP。

所有其他STP参数保留为默认值时，STP会按预期收敛。交换机A被选为根桥，冗余路径被阻塞以中断环路，具体而言，面向交换机B的交换机C端口被置于阻塞状态下（在该链路上显示为红色“X”）。 虚线箭头用于跟踪通过拓扑的STP BPDU的正常流量。这可以视为一个稳定的网络，其中PortFast为设备D提供即时连接，而STP则静默地管理冗余核心链路。

示例2 — 非法网桥导致中断



基于Linux的网桥应用程序在PC上启动

此示例显示当设备D停止像简单终端主机一样行为并开始参与STP时会发生什么情况，与BPDU防护设计停止的场景完全相同。在PC（设备D）上启动基于Linux的网桥应用程序。 应用将通告网桥优先级0（或低于当前根优先级的任意值）。 由于STP始终支持最低网桥ID，因此基于Linux的网桥赢得根选举，并从交换机A接管根网桥角色。

这次重新选举将重塑整个拓扑。两个核心交换机（A和B）之间的高速千兆以太网链路转换为阻塞状态（向核心链路移动时显示红色“X”）。 因此，以前使用千兆核心的所有VLAN流量都强制进入较慢的100 Mbps路径。当流量需求超过该链路的传输能力时，交换机开始丢弃帧，结果导致连接中断。

BPDU防护如何防止此问题？由于交换机C在到设备D的端口上启用了PortFast，因此该端口绝不能接收BPDU。当设备D发送STP BPDU时，BPDU防护将端口置于errdisable状态将其关闭。设备D在影响根选举之前被隔离，并且核心拓扑保持不变。

配置

建议的方法是在面向接入端口的主机上同时启用PortFast和BPDU防护。您可以全局或按接口启用或禁用STP PortFast BPDU防护。默认情况下，STP BPDU防护处于禁用状态。

每个接口启用PortFast和BPDU防护

<#root>

CatSwitch-IOS(config-if)#

spanning-tree portfast

CatSwitch-IOS(config-if)#

spanning-tree bpduguard enable

全局启用BPDU防护

<#root>

CatSwitch-IOS(config)#

spanning-tree portfast bpduguard default

使用全局命令时，每个配置了PortFast的端口都会自动继承BPDU防护，因此您不需要在每个接口上单独设置它。

配置自动恢复errdisable状态

当STP BPDU防护禁用端口时，除非手动启用端口，否则端口将保持禁用状态。可以将端口配置为从errdisable状态自动重新启用自身。发出以下命令，以设置 errdisable-timeout interval 并启用超时功能：

<#root>

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。

确认

要验证功能是启用还是禁用，请运行下一个适用的命令：

<#root>

```
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

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。