通过根防护增强生成树协议(STP)

目录

简介

本文档介绍增强交换网络可靠性、可管理性和安全性的改进STP根防护功能。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

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 Cisco 技术提示规则。

功能描述

标准 STP 并未为网络管理员提供任何安全执行第 2 层 (L2) 交换网络拓扑的方法。执行拓扑的方法对于采用共享管理控制（即不同管理实体或公司控制一个交换网络）的网络特别重要。

交换网络的转发拓扑被计算出来。除其他参数外，该计算还基于根网桥安置。任何交换机都可能是网络中的根网桥。但最优转发拓扑会将根网桥放置在预先确定的特定位置。使用标准 STP，网络中任何网桥 ID 较低的网桥将扮演根网桥的角色。管理员不能强制确定根网桥的位置。

注意：管理员可将根网桥优先级设置为0，以保护根网桥的位置。但是，优先级为 0 的网桥并不能保证具有较低的 MAC 地址。

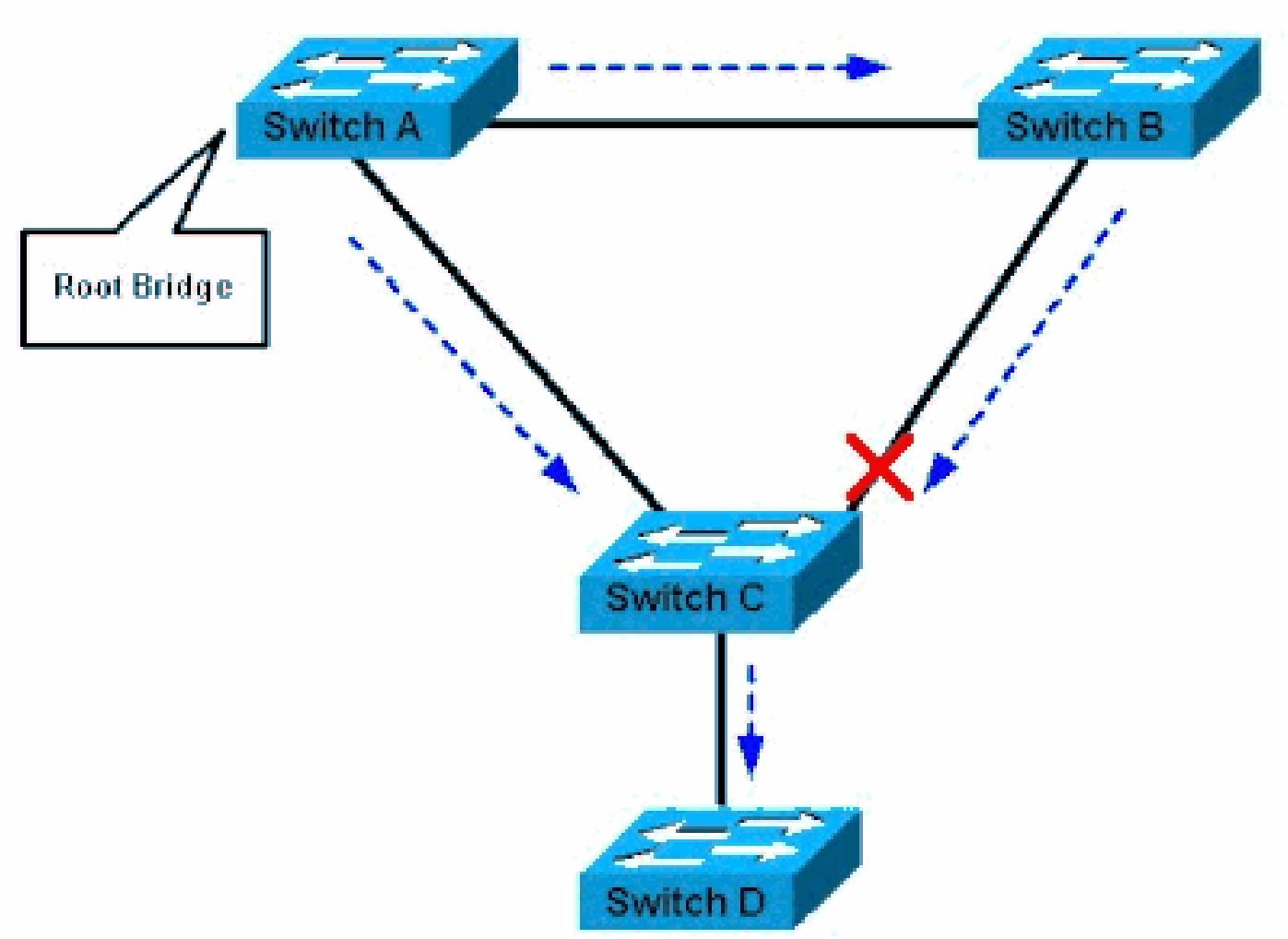
根防护功能提供了在网络中强制执行根网桥安置的方法。

根防护可确保启用了根防护的端口为指定端口。通常，除非根网桥的两个或多个端口连接在一起，否则根网桥端口全部为指定端口。如果网桥在启用了根防护的端口上收到高级 STP 网桥协议数据单元 (BPDU)，根防护会将此端口转换为根不一致 STP 状态。此根不一致状态实际上等效于监听状态。此时不会通过此端口转发任何流量。根防护以这种方式强制确定根网桥的位置。

本部分的示例说明恶意根网桥如何在网络中造成问题，以及根防护如何帮助解决这类问题。

在映像1中，交换机A和B构成了网络的核心，A是VLAN的根网桥。交换机 C 为接入层交换机。B和C之间的链路在C端被阻断。箭头表示 STP BPDU 的流向。

图 1

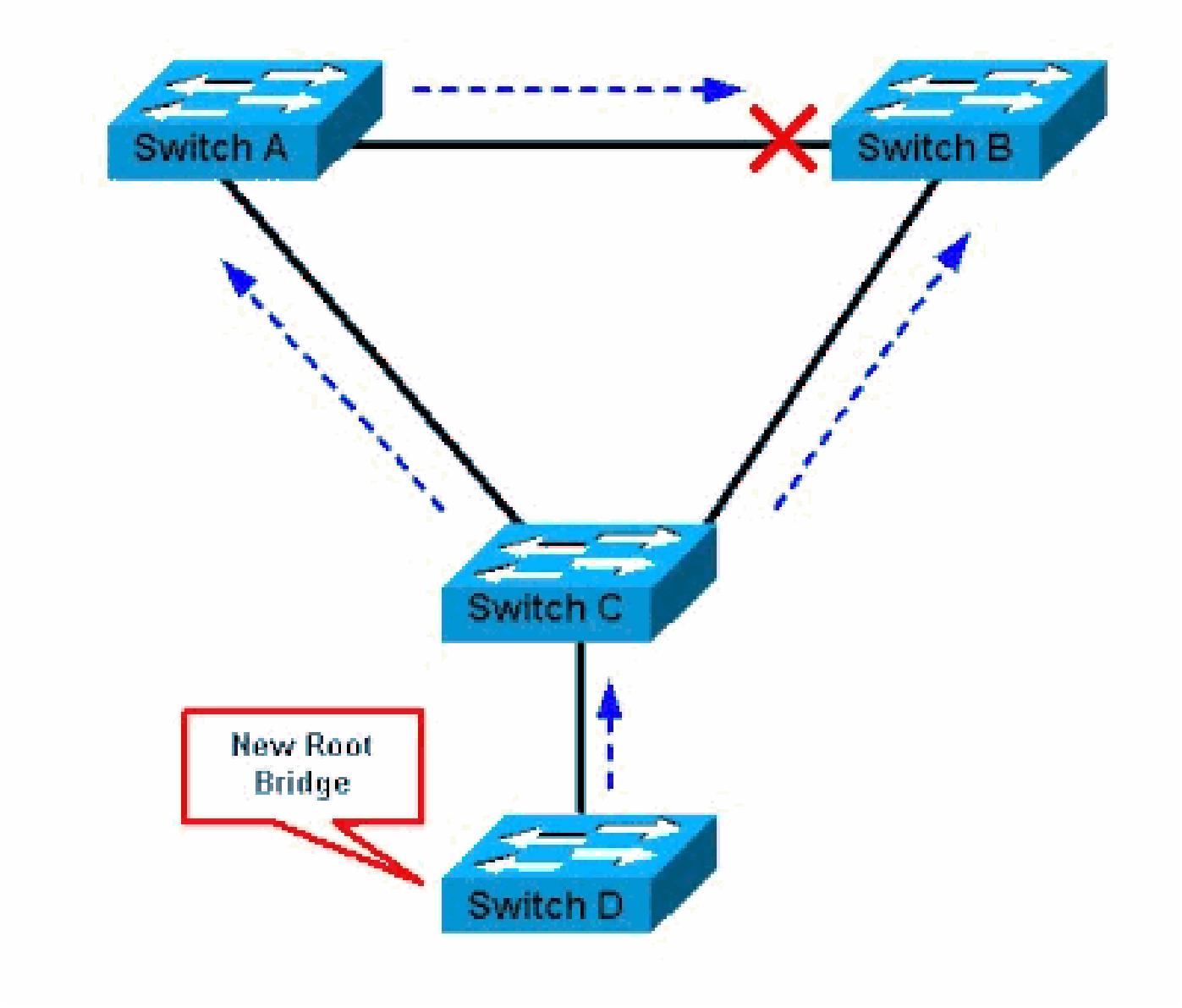


交换机A是根桥

在映像2中，设备D开始参与STP。例如，基于软件的网桥应用程序在连接到服务提供商网络的PC或其他交换机上启动。如果网桥 D 的优先级为 0 或任何低于根网桥优先级的值，则设备 D 将被选为此 VLAN 的根网桥。如果设备 A 与 B 之间的链路为 1 千兆，并且 A 与 C 之间以及 B 与 C 之间的链路为 100 Mbps，则选择 D 作为根网桥将导致连接两个核心交换机的千兆以太网受到阻塞。

此阻塞将使该 VLAN 中的所有数据通过一条 100 Mbps 链路流经接入层。如果通过该VLAN核心的数据流多于此链路可容纳的数据流，则会丢弃一些帧。帧丢弃会导致性能下降或连接中断。

图 2



交换机D是新的根桥

根防护功能可防止网络出现此类问题。

根防护配置针对的是每个端口。根防护不允许端口成为 STP 根端口，因此，端口始终是 STP 指定的。如果一个更好的 BPDU 到达此端口，根防护不会考虑此 BPDU 并选择新的 STP 根。相反，根防护会将该端口置于根不一致 STP 状态。您必须在所有不能出现根网桥的端口上启用根防护。从某

种程度上说，您可以在能够定位 STP 根的网络部分周围配置一个边界。

在Image 2中，在连接到交换机D的交换机C端口上启用根防护。

交换机C inImage 2会在交换机收到上级BPDU后阻塞连接到交换机D的端口。根防护将该端口置于根不一致 STP 状态。在此状态下，没有流量经过该端口。设备 D 停止发送高级 BPDU 之后，该端口再次解除阻塞。通过 STP，该端口从监听状态进入识别状态，并最终转换为转发状态。恢复是自动的；不需要人为干预。

本消息在根防护阻塞端口后出现：

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
Moved to root-inconsistent state
```

可用性

根防护在运行Cisco IOS®系统软件的Catalyst 6500/6000中可用。此功能首先在Cisco IOS软件版本12.0(7)XE中引入。对于运行 Cisco IOS 系统软件的 Catalyst 4500/4000，此功能在所有版本中均可用。

对于 Catalyst 2900XL 和 3500XL 交换机，根防护在 Cisco IOS 软件版本 12.0(5)XU 及更高版本中可用。Catalyst 2950 系列交换机在 Cisco IOS 软件版本 12.0(5.2)WC(1) 及更高版本中支持根防护功能。Catalyst 3550 系列交换机在 Cisco IOS 软件版本 12.1(4)EA1 及更高版本中支持根防护功能。

新型Cisco Catalyst系列交换机也具备此功能。

配置

Catalyst 6500/6000 和 Catalyst 4500/4000 的 Cisco IOS 软件配置

在运行 Cisco IOS 系统软件的 Catalyst 6500/6000 或 Catalyst 4500/4000 交换机上，请发出以下一组命令以配置 STP 根防护：

```
<#root>

Switch#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
!
Switch#(config)#

interface fastethernet 3/1

Switch#(config-if)#
```

```
spanning-tree guard root
!
```

> 注：运行Cisco IOS系统软件的Catalyst 6500/6000的Cisco IOS软件版本12.1(3a)E3将此命令从spanning-tree rootguard更改为spanning-tree guard root。运行 Cisco IOS 系统软件的 Catalyst 4500/4000 在所有版本中使用 spanning-tree guard root 命令。

Catalyst 2900XL/3500XL、2950 和 3550 的 Cisco IOS 软件配置

在 Catalyst 2900XL、3500XL、2950 和 3550 上，请按本例所示，在接口配置模式下为交换机配置根防护：

```
<#root>
Switch#
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
interface fastethernet 0/8
Switch(config-if)#
spanning-tree rootguard
Switch(config-if)#
^Z
*Mar 15 20:15:16: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Rootguard enabled on
port FastEthernet0/8 VLAN 1.
Switch#
```

STP BPDU防护与STP根防护有何区别

BPDU 防护与根防护类似，但它们的作用不同。如果在端口上启用了 PortFast，则 BPDU 防护会在收到 BPDU 时禁用该端口。该禁用有效阻止了位于此类端口之后的设备参与 STP。您必须手动重新启用处入 errDisable 状态的端口或配置 errdisable-timeout。

只要设备不尝试成为根，根防护就允许设备参与 STP。如果根防护阻塞端口，随后的恢复将自动完成。一旦设备停止发送上级BPDU，就会立即进行恢复。

有关BPDU防护的详细信息，请参阅生成树PortFast BPDU防护增强功能。

根防护是否有助于解决两个根的问题

网络中的两个网桥之间可能存在单向链路故障。由于该故障，一个网桥无法从根网桥接收 BPDU。出现此故障时，根交换机可以接收其他交换机发送的帧，但其他交换机无法接收根交换机发送的 BPDU。这可能会导致 STP 循环。由于其他交换机无法接收来自根的任何 BPDU，因此，这些交换机认为自己是根，并开始发送 BPDU。

当真正的根网桥开始接收 BPDU 时，根会丢弃这些 BPDU，因为它们并不是高级 BPDU。根网桥不会发生更改。因此，根防护并不能帮助解决该问题。单向链路检测 (UDLD) 和环路防护功能可解决该问题。

有关STP故障场景及其故障排除方法的详细信息，请参阅生成树协议问题和相关设计注意事项。

相关信息

- 了解和配置 UDLD 协议功能
- 在 Cisco IOS 平台上恢复 errdisable 端口状态
- 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）。