使用根防護增強生成樹協定(STP)

目錄

簡介

本文檔介紹增強交換網路可靠性、可管理性和安全性的經改進的STP根防護功能。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

功能說明

標準STP沒有為網路管理員提供任何方法來安全實施交換式第2層(L2)網路的拓撲。在具有共用管理控制的網路中，採用強制拓撲的方法尤為重要，因為不同的管理實體或公司會控制一個交換網路。

計算交換網路的轉發拓撲。計算基於根網橋位置，以及其他引數。任何交換機都可以作為網路中的根網橋。但是更最佳化的轉發拓撲將根網橋放置在特定的預定位置。使用標準STP時，網路中網橋ID較低的任何網橋都充當根網橋的角色。管理員無法強制實施根網橋的位置。

注意：管理員可將根網橋優先順序設定為0，以努力保護根網橋位置。但是無法保證優先順序為0且MAC地址較低的網橋不會受到攻擊。

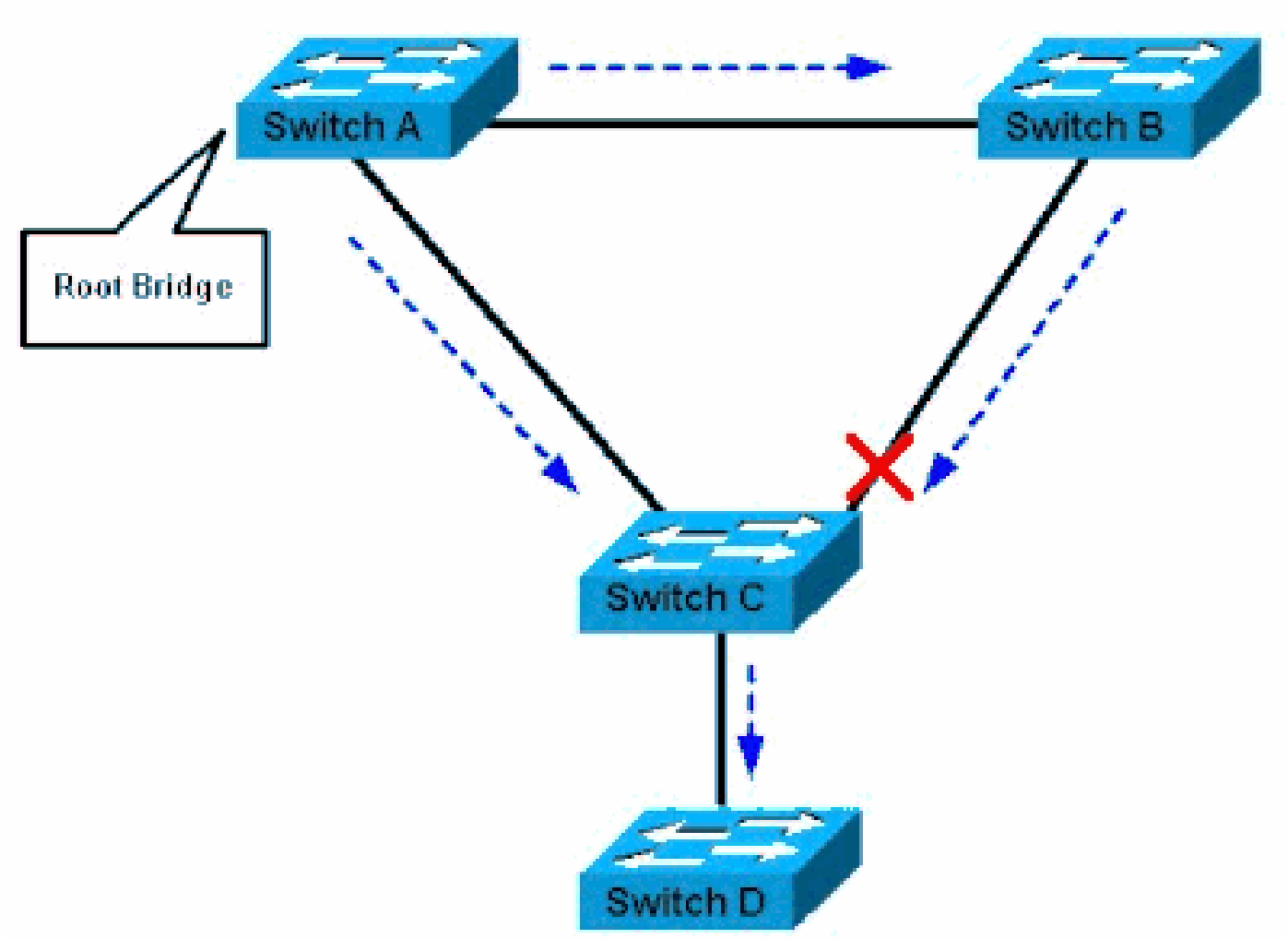
根防護功能提供了一種在網路中實施根網橋放置的方法。

根防護確保啟用根防護的埠是指定埠。通常，根網橋埠都是指定埠，除非根網橋的兩個或多個埠連線在一起。如果網橋在啟用根防護的埠上收到上級STP網橋協定資料單元(BPDU)，則根防護會將此埠移至根不一致STP狀態。這種根不一致狀態實際上等於偵聽狀態。沒有流量通過此連線埠轉送。通過這種方式，根防護將強制實施根網橋的位置。

本節中的示例演示了欺詐根網橋如何導致網路問題，以及根防護如何提供幫助。

在映像1中，交換機A和B構成了網路的核心，A是VLAN的根網橋。交換機C是接入層交換機。B和C之間的鏈路在C端被阻斷。箭頭顯示STP BPDU的流量。

圖1

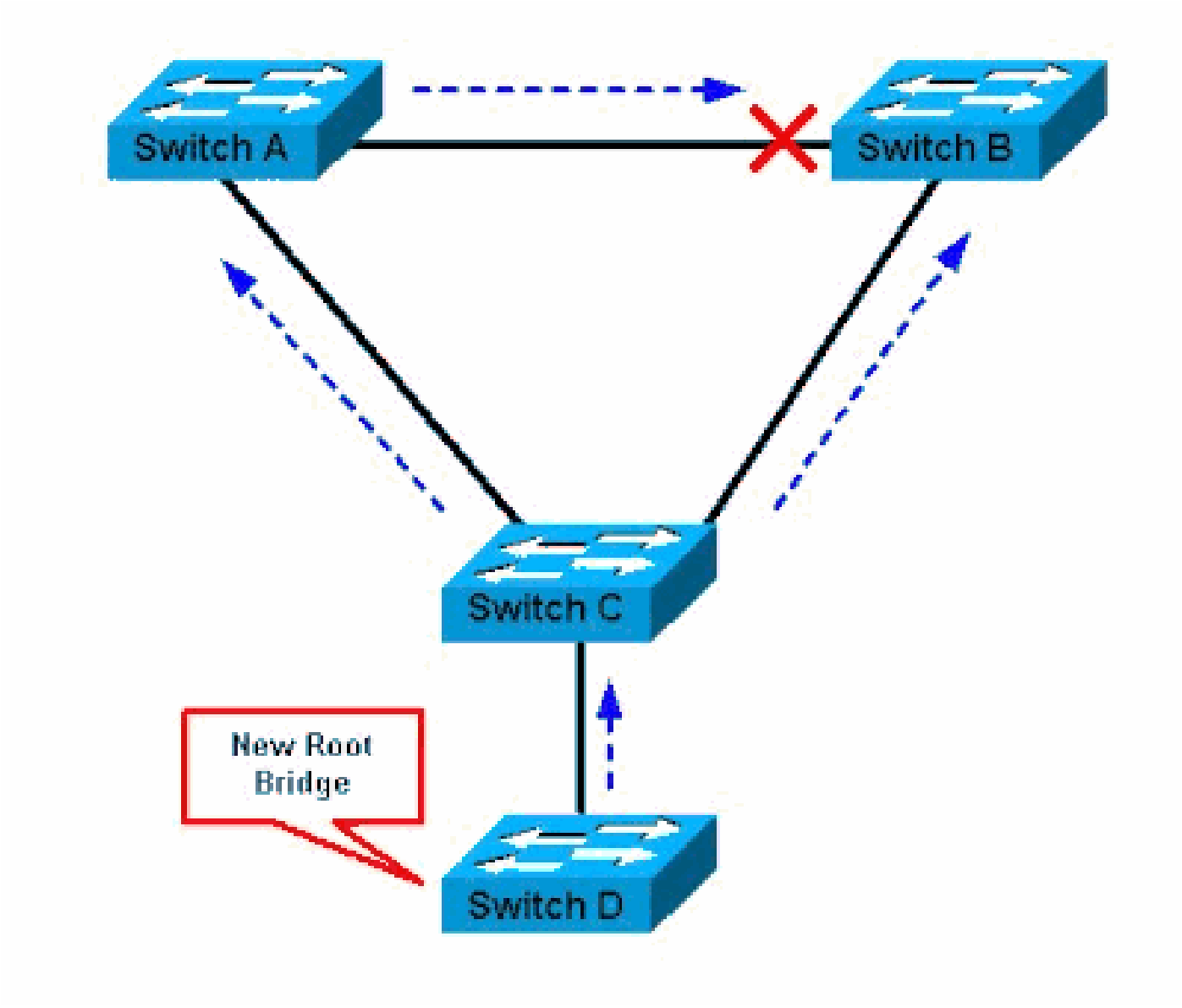


交換機A是根橋

在映像2中，裝置D開始參與STP。例如，基於軟體的橋接應用程式在您連線到服務提供商網路的PC或其他交換機上啟動。如果網橋D的優先順序為0或者任何低於根網橋的優先順序的值，則裝置D被選為此VLAN的根網橋。如果裝置A和B之間的鏈路為1 Gb，並且A和C以及B和C之間的鏈路為100 Mbps，則選擇D作為根會導致連線兩台核心交換機的千兆乙太網鏈路被阻塞。

此阻塞導致該VLAN中的所有資料通過100 Mbps鏈路在接入層流動。如果通過該VLAN中的核心傳輸的資料流量超過此鏈路所能容納的流量，則會丟棄某些幀。幀丟棄會導致效能損失或連線中斷。

圖2



交換機D是新的根橋

根防護功能可保護網路免受此類問題的影響。

根防護的配置基於每個埠。根防護不允許埠成為STP根埠，因此埠始終是STP指定的。如果有更好的BPDU到達此埠，根防護不會考慮BPDU並選擇新的STP根。相反，根防護會將埠置於根不一致STP狀態。必須在根網橋不能出現的所有埠上啟用根防護。在某種方式中，您可以圍繞網路的

STP根可以找到的部分配置邊界。

在Image 2中，在連線到交換機D的交換機C埠上啟用根防護。

交換器C inImage 2會在交換器收到上級BPDU後，封鎖連線到交換器D的連線埠。根防護將埠置於根不一致STP狀態。在此狀態下，沒有流量通過埠。在裝置D停止傳送上級BPDU後，埠將再次解除阻塞。通過STP，埠從偵聽狀態轉換到學習狀態，最終轉換為轉發狀態。恢復是自動的；不需要人工干預。

在根防護阻止埠後，將出現以下消息：

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

可用性

執行Cisco IOS®系統軟體的Catalyst 6500/6000提供根防護。此功能最初是在Cisco IOS軟體版本12.0(7)XE中匯入。對於執行Cisco IOS系統軟體的Catalyst 4500/4000，此功能在所有版本中均可用。

若是Catalyst 2900XL和3500XL交換器，Cisco IOS軟體版本12.0(5)XU和更新版本提供根防護。Catalyst 2950系列交換器支援Cisco IOS軟體版本12.0(5.2)WC(1)和更新版本中的根防護功能。Catalyst 3550系列交換器支援Cisco IOS軟體版本12.1(4)EA1和更新版本的根防護功能。

在較新版本的Cisco Catalyst系列交換器上也可使用此功能。

組態

Catalyst 6500/6000和Catalyst 4500/4000的Cisco IOS軟體組態

在執行Cisco IOS系統軟體的Catalyst 6500/6000或Catalyst 4500/4000交換器上，發出此組命令以設定STP根防護：

```
<#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
```

!

> 註：運行Cisco IOS系統軟體的Catalyst 6500/6000的Cisco IOS軟體版本12.1(3a)E3將此命令從spanning-tree rootguard更改為spanning-tree guard root。執行Cisco IOS系統軟體的Catalyst 4500/4000在所有版本中使用spanning-tree guard root 指令。

Catalyst 2900XL/3500XL、2950和3550的Cisco IOS軟體組態

在Catalyst 2900XL、3500XL、2950和3550上，在介面組態模式中設定具有根防護的交換器，如以下範例所示：

```
<#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防護和STP根防護之間有何差異

BPDU防護和根防護類似，但其影響不同。如果在連線埠上啟用PortFast，則BPDU防護會在BPDU接收時停用連線埠。此停用實際上會拒絕此類連線埠後面的裝置參與STP。您必須手動重新啟用進入錯誤停用狀態的連線埠，或設定錯誤停用逾時。

根防護允許裝置參與STP，只要裝置不嘗試成為根即可。如果根防護阻塞埠，後續恢復將自動進行。只要異常裝置停止傳送上級BPDU，就會立即進行恢復。

有關BPDU防護的詳細資訊，請參閱生成樹埠快速BPDU防護增強功能。

根防護是否有助於解決兩個根問題

網路中兩個網橋之間可能存在單向鏈路故障。由於發生故障，一個網橋無法接收來自根網橋的

BPDU。發生此類故障時，根交換機會收到其他交換機傳送的幀，但其他交換機不會收到根交換機傳送的BPDU。這可以導致STP環路。由於其它交換機沒有從根交換機收到任何BPDU，因此這些交換機認為自己是根交換機，並開始傳送BPDU。

當真正的根網橋開始接收BPDU時，根會丟棄BPDU，因為它們並不優越。根網橋不會改變。因此，根防護不能幫助解決此問題。單向連結偵測(UDLD)和回圈防護功能可解決此問題。

有關STP故障方案以及如何對其進行故障排除的詳細資訊，請參閱生成樹協定問題和相關設計注意事項。

相關資訊

- 瞭解和設定 UDLD 通訊協定功能
- 在 Cisco IOS 平台上復原錯誤停用連接埠狀態
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。