使用環路防護和BPDU偏差檢測配置STP

目錄

簡介

本檔案介紹旨在提高第2層網路穩定性的生成樹通訊協定功能。

必要條件

需求

本文檔假設讀者熟悉STP的基本操作。如需詳細資訊，請參閱瞭解和設定Catalyst交換器上的跨距樹狀目錄通訊協定(STP)。

採用元件

本檔案是根據Catalyst交換器，但上述功能的可用性取決於使用的軟體版本。

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。

背景資訊

生成樹協定(STP)將物理冗餘拓撲解析為無環樹狀拓撲。STP的最大問題是某些硬體故障會導致其發生故障。此故障會導致轉發環路（或STP環路）。STP環路造成了嚴重的網路故障。

本檔案介紹旨在提高第2層網路穩定性的環路防護STP功能。本檔案也說明橋接通訊協定資料單元(BPDU)歪斜偵測。BPDU傾斜檢測是一種診斷功能，可在未及時收到BPDU時生成系統日誌消息。

功能可用性

CatOS

- STP環路防護功能在適用於Catalyst 4000和Catalyst 5000平台的Catalyst軟體的CatOS版本6.2.1和適用於Catalyst 6000平台的6.2.2版中引入。
- 適用於Catalyst 4000和Catalyst 5000平台的Catalyst軟體的CatOS版本6.2.1和適用於Catalyst 6000平台的6.2.2版引入了BPDU歪斜偵測功能。

Cisco IOS®

- STP環路防護功能在適用於Catalyst 4500交換器的Cisco IOS軟體版本12.1(12c)EW和適用於Catalyst 6500的Cisco IOS軟體版本12.1(11b)EX中匯入。
- 執行Cisco IOS系統軟體的Catalyst交換器不支援BPDU偏差偵測功能。

STP埠角色

在內部，STP根據配置、拓撲、埠在拓撲中的相對位置以及其他考慮因素，為每個網橋（或交換機）埠分配一個角色。埠角色定義從STP角度出發的埠行為。根據埠角色，埠傳送或接收STP BPDU並轉發或阻止資料流量。此清單提供每個STP埠角色的簡短摘要：

- *Designated* — 每個鏈路（網段）選擇一個指定埠。指定的埠是最靠近根網橋的埠。此連線埠在連結（區段）上傳送BPDU，並將流量轉送到根網橋。在STP融合網路中，每個指定埠都處於STP轉發狀態。
- *Root* — 網橋只能有一個根埠。根埠是通向根網橋的埠。在STP融合網路中，根埠處於STP轉發狀態。
- *Alternate* — 備用埠通向根網橋，但不是根埠。備用埠保持STP阻塞狀態。
- *備份* — 當同一交換機之間的兩個或多個埠直接或通過共用介質連線在一起時，這是一個特殊情況。這種情況下，會指定一個連線埠，而其餘連線埠會遭到封鎖。此連線埠的角色為備份。

STP環路防護

功能說明

STP環路防護功能針對第2層轉發環路（STP環路）提供額外的保護。當冗餘拓撲中的STP阻塞埠錯誤地轉換到轉發狀態時，會建立STP環路。發生這種情況通常是因為物理冗餘拓撲的一個埠（不一定是該STP阻塞埠）不再接收STP BPDU。在運行過程中，STP依賴於基於埠角色的BPDU的持續接收或傳輸。指定埠傳輸BPDU，非指定埠接收BPDU。

當物理冗餘拓撲中的一個埠不再接收BPDU時，STP會認為該拓撲沒有環路。最終，來自備用或備

用埠的阻塞埠變為指定狀態並變為轉發狀態。這種情況會形成環路。

環路防護功能會進行其他檢查。如果未在非指定埠上接收BPDU，並且啟用了環路防護，則該埠將進入STP環路不一致的阻塞狀態，而不是偵聽/學習/轉發狀態。如果沒有回圈防護功能，連線埠會承擔指定的連線埠角色。埠將進入STP轉發狀態並建立環路。

當環路防護阻塞不一致的埠時，將記錄以下消息：

- CatOS

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

- Cisco IOS

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

在處於環路不一致STP狀態的埠上收到BPDU後，該埠會轉換到另一個STP狀態。對於收到的BPDU，這意味著恢復是自動進行的，無需干預。恢復後，將記錄以下消息：

- CatOS

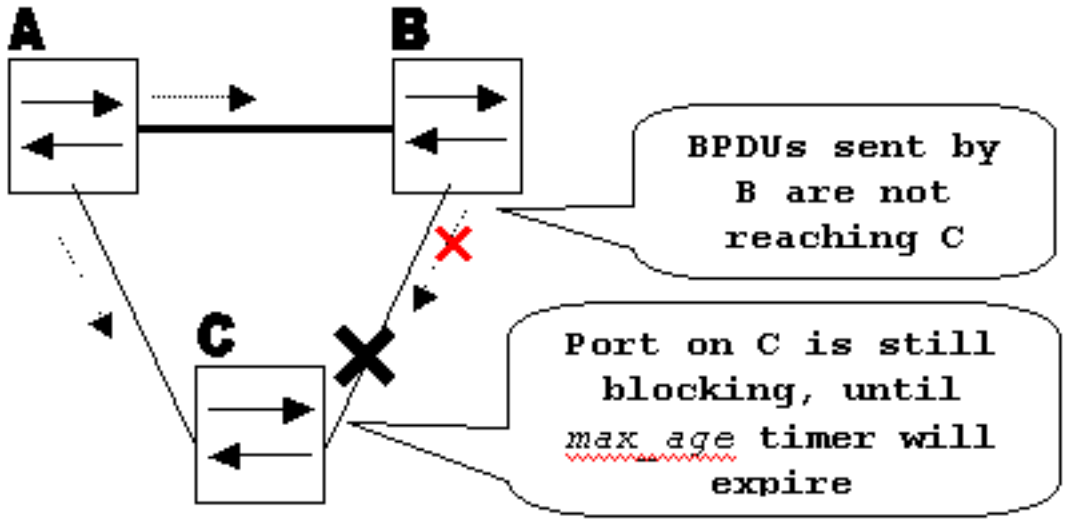
```
%SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

- Cisco IOS

```
%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port FastEthernet0/24 on
VLAN0050.
```

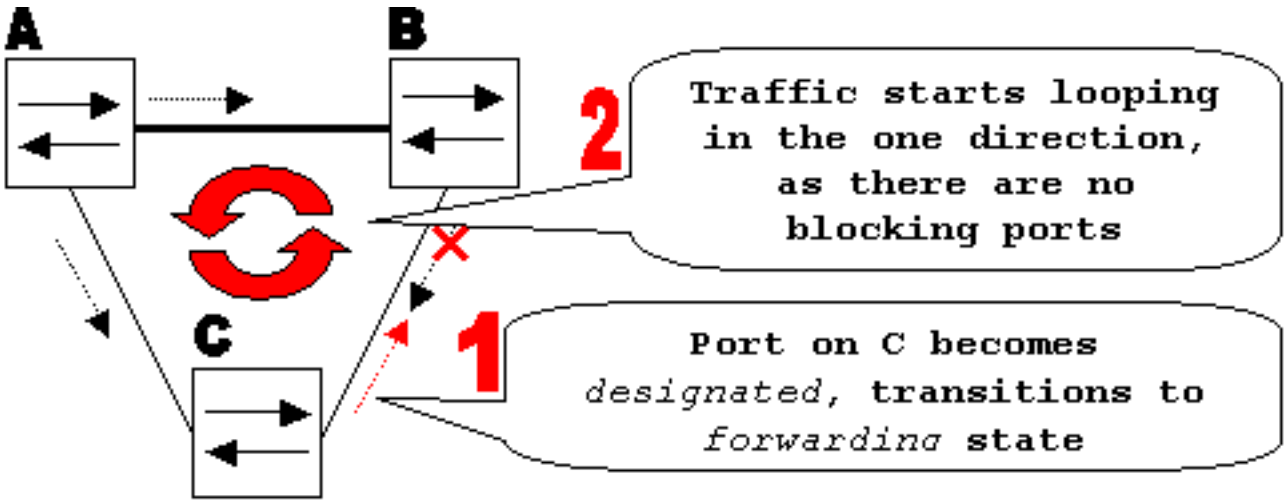
請考慮以下示例來說明此行為：

交換機A是根交換機。由於交換器B和交換器C之間的連結上的單向連結失敗，交換器C沒有收到來自交換器B的BPDU。



單向連結失敗

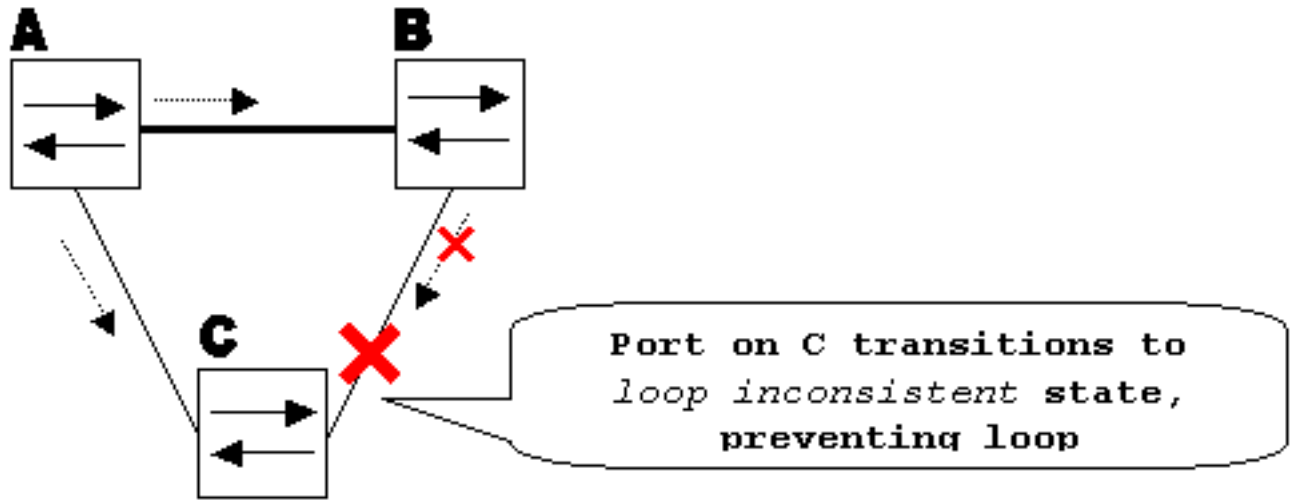
如果沒有環路防護，交換機C上的STP阻塞埠在max_age計時器到期時轉變為STP偵聽狀態，然後在forward_delay時間的兩倍內轉變為forwarding狀態。這種情況會形成環路。



已建立

循環

啟用環路防護後，當max_age計時器到期時，交換機C上的阻塞埠會轉換為STP環路不一致狀態。處於STP環路不一致狀態的埠不會傳遞使用者流量，因此不會建立環路。（環路不一致狀態實際上等於阻塞狀態。）



啟用環

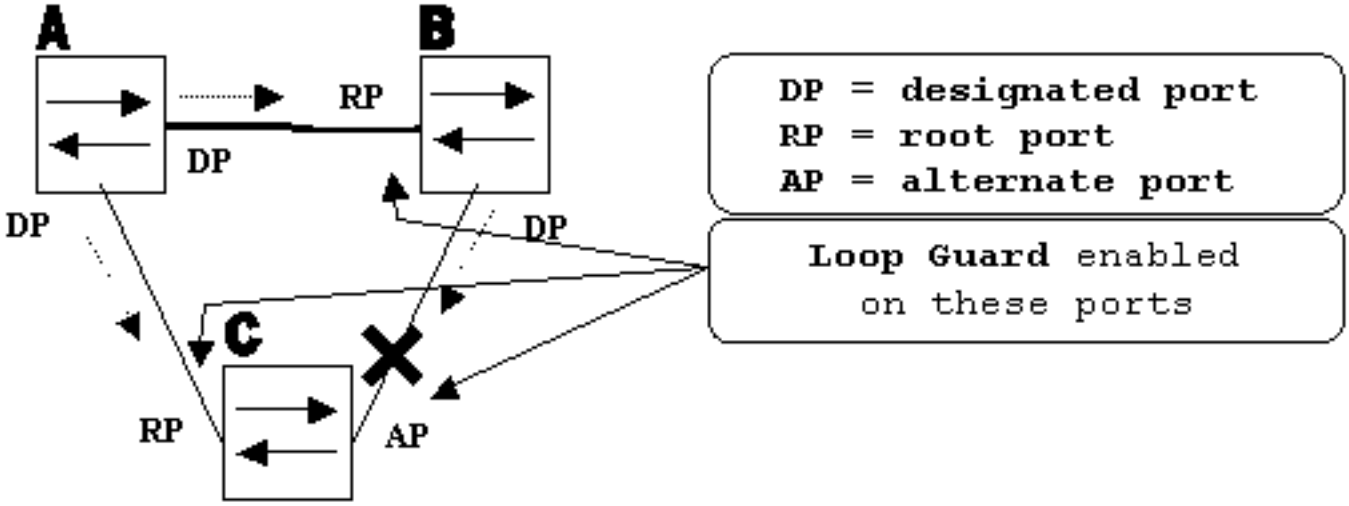
路防護可防止環路

配置注意事項

環路防護功能是基於每個埠啟用的。但是，只要它在STP級別阻塞埠，環路防護就會根據VLAN阻塞不一致的埠（因為每個VLAN STP）。也就是說，如果只在一個特定VLAN的中繼埠上未接收BPDU，則只有該VLAN被阻塞（移至環路不一致STP狀態）。出於相同原因，如果在EtherChannel介面上啟用，則整個通道對於特定VLAN而不是僅針對一條鏈路被阻塞（因為EtherChannel從STP的角度被視為一個邏輯埠）。

在哪些埠上啟用環路防護？最明顯的答案是阻塞埠。但是，這並不完全正確。對於所有可能的活動拓撲組合，必須在非指定埠（更準確地說，在根埠和備用埠）上啟用環路防護。只要環路防護不是每個VLAN的功能，就可以為一個VLAN指定相同（中繼）埠，為另一個VLAN指定非指定埠。還必須考慮可能的故障切換方案。

範例



已

啟用環路防護的連線埠

預設情況下，環路防護處於禁用狀態。以下命令用於啟用環路防護：

- CatOS

```
set spantree guard loop
```

```
Console> (enable) set spantree guard loop 3/13
Enable loopguard will disable rootguard if it's currently enabled on the port(s).
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
```

在Catalyst軟體(CatOS)版本7.1(1)中，可以在所有連線埠上全域啟用回圈防護。實際上，所有點對點鏈路都啟用了環路防護。點對點連結會透過連結的雙工狀態來檢測。如果雙工為全雙工，則鏈路視為點對點。仍可以基於每個埠配置或覆蓋全域性設定。

發出以下命令可全域性啟用環路防護：

- CatOS

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

- Cisco IOS

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

發出以下命令可停用回圈防護：

- CatOS

```
Console> (enable) set spantree guard none
```

- Cisco IOS

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

發出以下命令可全域性禁用環路防護：

- CatOS

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

- Cisco IOS

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

發出以下命令可驗證環路防護狀態：

- CatOS

```
show spantree guard
```

```
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 Active
---------------------- -------- --------- -------- ---------- ----------
Total                         0         0        0          0          0
```

環路防護與UDLD

環路防護和單向鏈路檢測(UDLD)功能重疊，部分原因是兩者都防止單向鏈路導致的STP故障。但是，這兩個功能在功能以及解決問題方式上有所不同。下表介紹環路防護和UDLD功能：

功能	環路防護	UDLD
組態	每個埠	每個埠

操作粒度	每個VLAN	每個埠
自動恢復	是	是，具有錯誤禁用超時功能
針對單向鏈路導致的STP故障提供保護	是，在冗餘拓撲中的所有根埠和備用埠上啟用時	是，在冗餘拓撲中的所有鏈路上啟用時
防止軟體出現問題導致的STP故障（指定交換機不傳送BPDU）	是	否
防止接線錯誤。	否	是

根據各種設計注意事項，您可以選擇UDLD或環路防護功能。在STP方面，這兩個功能之間最明顯的區別是UDLD中缺少針對軟體問題導致的STP故障的保護。因此，指定交換機不傳送BPDU。但是，這種型別的故障（數量級）比單向鏈路導致的故障更為罕見。反過來，在EtherChannel上使用單向連結時，UDLD可能更為靈活。在這種情況下，UDLD只會停用失敗連結，且通道可以透過保留連結保持運作。在這樣的故障中，環路防護使其進入環路不一致狀態，以阻塞整個通道。

此外，自連結啟動後，如果連結是單向的，則回圈防護無法作用在共用連結上，或發生這種情況。在最後一種情況下，埠從不接收BPDU而成為指定埠。由於此行為可能是正常的，因此環路防護不會涵蓋此特定情況。UDLD會針對此類情況提供保護。

如所述，啟用UDLD和環路防護時提供最高級別的保護。

環路防護與其他STP功能的互操作性

根防護

根防護與環路防護互斥。根防護用於指定埠，它不允許埠成為非指定埠。環路防護在非指定埠上工作，不允許埠在max_age到期後成為指定埠。根防護不能在與環路防護相同的埠上啟用。當在埠上配置環路防護時，它會禁用在同一埠上配置的根防護。

Uplink Fast和Backbone Fast

上行鏈路fast和主幹fast對環路防護都是透明的。重新收斂時backbone fast跳過max_age時，不會觸發環路防護。有關uplink fast和backbone fast的詳細資訊，請參閱以下文檔：

- 瞭解和配置思科上行鏈路快速功能
- 瞭解和設定Catalyst交換器上的快速主幹

PortFast和BPDU防護以及動態VLAN

無法為已啟用portfast的連線埠啟用回圈防護。由於BPDU防護在已啟用portfast的埠上工作，因此有些限制適用於BPDU防護。無法在動態VLAN埠上啟用環路防護，因為這些埠已啟用portfast。

共用連結

不能在共用鏈路上啟用環路防護。如果在共用鏈路上啟用環路防護，則來自連線到共用網段的主機的流量可能會被阻止。

多重跨距樹狀目錄(MST)

環路防護在MST環境中正常工作。

BPDU歪斜檢測

通過BPDU偏差檢測，環路防護可以正常運行。

BPDU歪斜檢測

功能說明

STP操作在很大程度上依賴於BPDU的及時接收。在每個hello_time消息（預設情況下為2秒）處，根網橋會傳送BPDU。非根網橋不會為每個hello_time消息重新生成BPDU，但是它們從根網橋接收中繼的BPDU。因此，每個非根網橋必須在每個VLAN上為每個hello_time消息接收BPDU。在某些情況下，BPDU會丟失，或者網橋CPU太忙而無法及時中繼BPDU。這些問題以及其他問題都可能導致BPDU到達延遲（如果它們到達的話）。此問題可能會影響生成樹拓撲的穩定性。

通過BPDU偏差檢測，交換機可以跟蹤到達較晚的BPDU，並使用系統日誌消息通知管理員。對於BPDU到達過延遲（或發生傾斜）的每個埠，歪斜檢測報告最近的歪斜和歪斜的持續時間（延遲）。它也會報告此特定連線埠上最長的BPDU延遲。

為了保護網橋CPU免受過載，每次發生BPDU偏移時，系統不會生成系統日誌消息。消息速率限製為每60秒一條消息。但是，BPDU的延遲必須超過max_age除以2（預設為10秒），消息才會立即顯示。

> **註**:BPDU偏差檢測是一種診斷功能。檢測到BPDU偏移時，它會傳送系統日誌消息。BPDU歪斜檢測無需進一步的糾正操作。

> **註**：運行Cisco IOS系統軟體的Catalyst交換機不支援BPDU偏差檢測功能

以下是BPDU偏差檢測生成的系統日誌消息的示例：

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

配置注意事項

BPDU偏差檢測是針對每台交換機配置的。預設設定已禁用。發出以下命令以啟用BPDU偏差檢測：

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

若要檢視BPDU傾斜資訊，請使用**show spantree bpdu-skewing <vlan>|<mod/port>** 命令，如以下示例所示：

```
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
```

相關資訊

- 跨距樹狀目錄通訊協定根目錄防護增強功能
- 跨距樹狀目錄 PortFast BPDU 防護增強功能

- 瞭解和設定單向連結偵測通訊協定功能
- 使用 PortFast 和其他命令修復工作站啟動連線延遲
- 技術支援與下載 — Cisco Systems

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）。