使用环路防护和BPDU迟滞检测配置STP

目录

简介

本文档介绍用于提高第2层网络稳定性的生成树协议功能。

先决条件

要求

本文档假设读者熟悉 STP 的基本工作原理。有关详细信息，请参阅[了解和配置Catalyst交换机上的生成树协议(STP)](#)。

使用的组件

本文档基于Catalyst交换机，但所描述功能的可用性取决于所使用的软件版本。

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。

背景信息

生成树协议 (STP) 将物理上冗余的拓扑解析为无环路的树形拓扑。STP 的最大问题是一些硬件故障可能导致它出现故障。此故障将导致生成转发环路（或 STP 环路）。STP 环路会引起主网中断。

本文档介绍了旨在提高第 2 层网络的稳定性的环路防护 STP 功能。本文档还介绍了网桥协议数据单元 (BPDU) 迟滞检测。BPDU 迟滞检测是一种诊断功能，用于在未及时收到 BPDU 的情况下生成 syslog 消息。

功能可用性

CatOS

- 在用于 Catalyst 4000 及 Catalyst 5000 平台的 Catalyst 软件的 CatOS 版本 6.2.1 和用于 Catalyst 6000 平台的版本 6.2.2 中引入了 STP 环路防护功能。
- 在用于 Catalyst 4000 及 Catalyst 5000 平台的 Catalyst 软件的 CatOS 版本 6.2.1 和用于 Catalyst 6000 平台的版本 6.2.2 中引入了 BPDU 迟滞检测功能。

思科IOS®

- 在用于 Catalyst 4500 交换机的 Cisco IOS 软件版本 12.1(12c)EW 和用于 Catalyst 6500 的 Cisco IOS 软件版本 12.1(11b)EX 中引入了 STP 环路防护功能。
- 运行Cisco IOS系统软件的Catalyst交换机不支持BPDU迟滞检测功能。

STP端口角色

在内部，STP 分配给每个网桥（或交换机）端口一个角色，该角色基于拓扑中的该端口的配置、拓扑、相对位置以及其他考虑事项。端口角色从 STP 的角度定义了端口的行为。根据端口角色，端口发送或接收 STP BPDU，然后转发或阻塞数据流。此列表提供了每个 STP 端口角色的概要：

- *指定 - 为每个链路（网段）选择一个指定的端口。*指定的端口是最接近根网桥的端口。此端口将 BPDU 发送到链路（网段）上并向根网桥转发数据流。在 STP 收敛网络中，每个指定的端口都处于 STP 转发状态。
- *根 - 网桥只能有一个根端口。*根端口是通向根网桥的端口。在 STP 收敛网络中，根端口处于 STP 转发状态。
- *备用* — 备用端口通向根网桥，但不是根端口。替代端口保持 STP 阻塞状态。
- *备份* — 当同一交换机之间的两个或多个端口直接或通过共享介质连接在一起时，这是一种特殊情况。在这种情况下，一个端口被指定，其余端口被阻塞。此端口的角色是备用端口。

STP 环路防护

功能描述

STP 环路防护功能提供了额外保护，以防出现第 2 层转发环路（STP 环路）。当冗余拓扑中的 STP 阻塞端口错误地转换到转发状态时，会生成 STP 环路。发生这种情况的原因通常是物理冗余拓扑中的某个端口（不一定是 STP 阻塞端口）不再接收 STP BPDU。STP 在其运行过程中依赖于基于端口角色的 BPDU 的连续接收或传送。指定的端口传输 BPDU，非指定的端口接收 BPDU。

当物理冗余拓扑中的某个端口不再接收 BPDU 时，STP 将认为该拓扑无环路。最终，阻塞端口将从备用或备份端口变为指定端口，并转换为转发状态。这种情况将导致生成环路。

环路防护功能会进行额外的检查。如果非指定端口未收到 BPDU，并且已启用环路防护，则该端口将转换为 STP 环路不一致阻塞状态，而非侦听/识别/转发状态。如果不使用环路防护功能，端口将承担指定的端口角色。该端口将转换到 STP 转发状态，并且会生成环路。

当环路防护阻塞了一个不一致的端口时，会将以下消息记录到日志中：

- 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.
```

一旦处于环路不一致 STP 状态的端口收到 BPDU，该端口就会转换到其他 STP 状态。对于收到的 BPDU，这意味着恢复是自动进行的，无需干预。在恢复之后，会将以下消息记录到日志中：

- CatOS

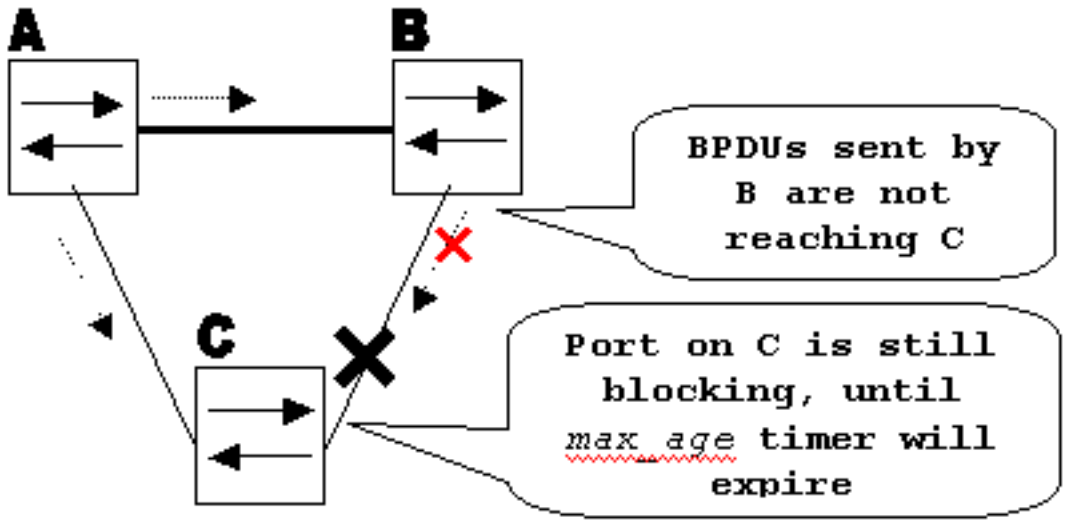
```
%SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

- Cisco IOS

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

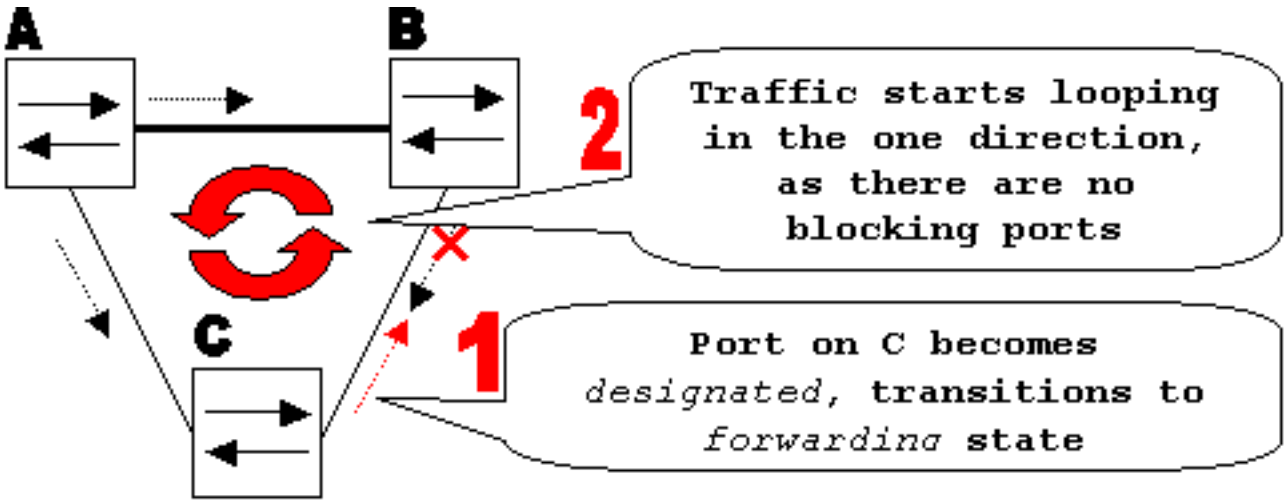
请考虑以下示例来说明此行为：

交换机 A 是根交换机。由于交换机 B 和交换机 C 之间的链路发生单向链路故障，交换机 C 没有接收到来自交换机 B 的 BPDU。



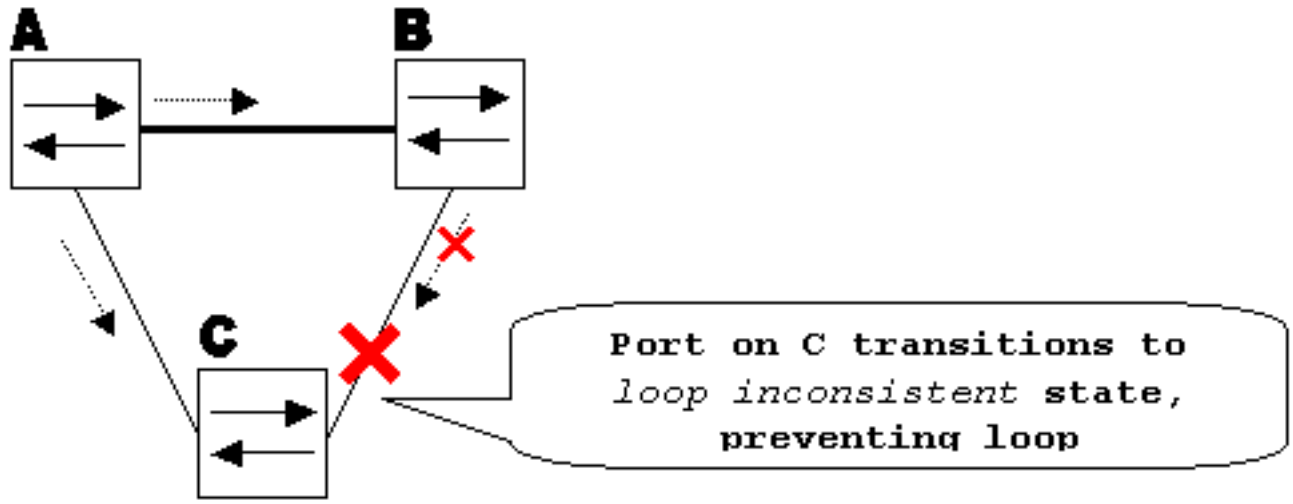
单向链路故障

如果不使用环路防护，当 max_age 定时器到期时，交换机 C 上的 STP 阻塞端口将转换到 STP 侦听状态，然后在 forward_delay 的两倍时间内转换到转发状态。这种情况将导致生成环路。



创建环路

如果启用了环路防护，当 max_age 定时器到期时，交换机 C 上的阻塞端口将转换到 STP 环路不一致状态。处于 STP 环路不一致状态的端口不允许用户数据流通过，因此不会生成环路。（环路不一致状态与阻塞状态的作用相同。）



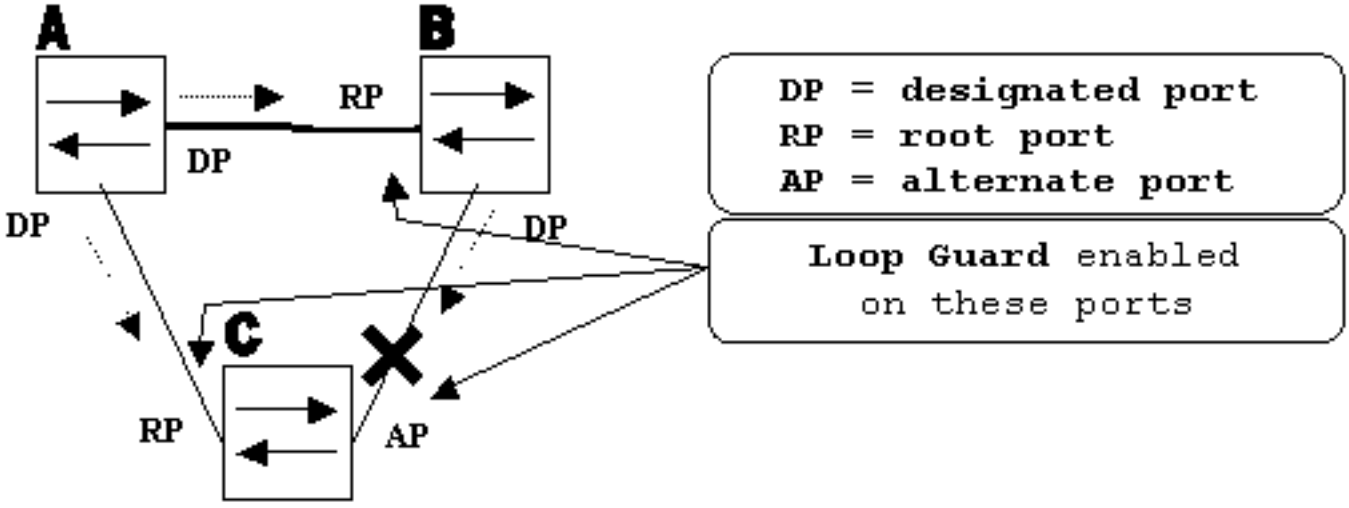
启用环路防护可防止环路

配置注意事项

环路防护功能是基于每个端口启用的。但是，只要它在 STP 级别阻塞端口，环路防护就会基于每个 VLAN 阻塞不一致的端口（因为是每 VLAN STP）。即，如果只在一个特定 VLAN 的中继端口上没有收到 BPDU，则只阻塞该 VLAN（转换到环路不一致 STP 状态）。由于同样的原因，如果在 EtherChannel 接口上启用，则将阻塞特定 VLAN 的整个通道，而不只是阻塞一条链路（因为从 STP 角度看，EtherChannel 被视为一个逻辑端口）。

在哪些端口上启用环路防护？最显而易见的答案是在阻塞端口上。然而，这并不完全正确。对于活动拓扑的所有可能组合，必须在非指定端口上（更准确地讲，在根端口和替代端口上）启用环路防护。只要环路防护不是每个VLAN的功能，就可以为一个VLAN指定同一（中继）端口，为另一个VLAN指定非指定端口。还必须考虑可能的故障切换方案。

示例



启用环路防护的端口

默认情况下，环路防护处于禁用状态。可使用以下命令启用环路防护：

- 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
```

使用 7.1(1) 版本的 Catalyst 软件 (CatOS)，可以对所有端口全局启用环路防护。实际上是对所有点对点链路启用环路防护。可以通过链路的双工状态检测到点对点链路。如果双工是全双工，则认为链路是点对点链路。还可以基于每个端口配置或覆盖全局设置。

要全局启用环路防护，请发出以下命令：

- CatOS

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

- Cisco IOS

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

要禁用环路防护，请发出以下命令：

- CatOS

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

- Cisco IOS

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

要全局禁用环路防护，请发出以下命令：

- CatOS

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

- Cisco IOS

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

要确认环路防护状态，请发出以下命令：

- 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
```

环路防护与 UDLD

就防止由单向链路引起的 STP 故障而言，环路防护和单向链路检测 (UDLD) 有一部分功能重叠。但是，这两种功能在功能上以及它们处理问题的方式上有所不同。此表描述环路防护和 UDLD 功能：

功能	环路防护	UDLD
配置	每个端口	每个端口

操作粒度	每个 VLAN	每个端口
自动恢复	Yes	是，具有 err-disable 超时功能
防止单向链路引起的 STP 故障	是，在冗余拓扑中的所有根端口和替代端口上启用时。	是，在冗余拓扑中的所有链路上启用时
防止软件中的问题导致的 STP 故障（指定的交换机不发送 BPDU）	Yes	无
防止接线错误。	无	Yes

基于各种设计考虑，可以选择 UDLD 或环路防护功能。在STP方面，这两个功能之间最明显的区别是UDLD中缺少针对软件问题引起的STP故障的保护。因此，指定的交换机不发送 BPDU。但是，这种类型的故障（数量级）比单向链路导致的故障更罕见。反过来，在EtherChannel上使用单向链路时，UDLD可以更加灵活。在这种情况下，UDLD仅禁用故障链路，并且信道可以保持正常运行和链路保留。在发生此类故障时，环路防护会将它置于环路不一致状态以阻塞整个通道。

另外，在共用链路上，或者在链路自接通以来已是单向链路的情况下，环路防护不起作用。在最后一种情况下，端口从不接收 BPDU，并会成为指定端口。由于此行为可能是正常的，因此环路防护不涵盖此特定情况。UDLD 可以防止出现这样的情况。

如上所述，当同时启用了 UDLD 和环路防护时，将提供最高级别的保护。

环路防护与其他 STP 功能的互操作性

根防护

根防护与环路防护是互相排斥的。根防护用于指定的端口，并且它不允许端口变为非指定的端口。环路防护用于非指定的端口，并且不允许该端口通过 max_age 的到期变为指定的端口。不能对启用了环路防护的端口启用根防护。如果在端口上配置了环路防护，它会禁用在同一端口上配置的根防护。

Uplink Fast和Backbone Fast

Uplink Fast 和 Backbone Fast 对环路防护都是透明的。如果 Backbone Fast 在重新收敛时跳过 max_age，它不会触发环路防护。有关 Uplink Fast 和 Backbone Fast 的更多信息，请参阅以下文档：

- 了解和配置 Cisco Uplink Fast 功能
- 了解和配置Catalyst交换机上的Backbone Fast

PortFast 和 BPDU 防护以及动态 VLAN

环路防护无法在已启用 PortFast 的端口上启用。因为 BPDU 防护用于启用了 PortFast 的端口，所以一些限制条件适用于 BPDU 防护。因为在动态 VLAN 端口上已启用 PortFast，所以在这些端口上无法启用环路防护。

共用链路

不得在共享链路上启用环路防护。如果在共享链路上启用环路防护，则来自连接到共享网段的主机的流量可能会被阻止。

多生成树 (MST)

环路防护在 MST 环境中可以正常工作。

BPDU 迟滞检测

环路防护可通过BPDU迟滞检测正确运行。

BPDU 迟滞检测

功能描述

STP 的运行严重依赖于 BPDU 的及时接收。在发送每个 hello_time 消息（默认情况下每 2 秒发送一次）时，根网桥会发送 BPDU。非根网桥不为每个 hello_time 消息重新生成 BPDU，但它们从根网桥接收被中继的 BPDU。因此，每个非根网桥必须在每个VLAN上为每个hello_time消息接收 BPDU。在某些情况下，BPDU 丢失，或者网桥 CPU 太忙，不能及时中继 BPDU。这些问题以及其他问题可能导致 BPDU 迟到（如果它们到达）。此问题可能会破坏生成树拓扑的稳定性。

BPDU 迟滞检测允许交换机跟踪迟到的 BPDU，并使用 syslog 消息通知管理员。对于已出现 BPDU 迟到（或迟滞）情况的每个端口，迟滞检测将报告最近一次迟滞和迟滞的持续时间（等待时间）。它还报告在此特定端口上的最长的 BPDU 延迟。

为了防止网桥 CPU 过载，并不会在每次发生 BPDU 迟滞时都生成 syslog 消息。将消息的速率限制为每 60 秒一个消息。但是，BPDU的延迟必须超过max_age除以2（默认情况下等于10秒），消息才会立即显示。

> **注意**:BPDU迟滞检测是一种诊断功能。检测到 BPDU 迟滞时，它会立即发送 syslog 消息。BPDU 迟滞检测不采取任何进一步纠正措施。

> **注：**运行Cisco IOS系统软件的Catalyst交换机不支持BPDU迟滞检测功能

以下是由 BPDU 迟滞检测生成的 syslog 消息的示例：

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

配置注意事项

BPDU 迟滞检测是基于每台交换机进行配置的。默认设置为已禁用。为了启用 BPDU 迟滞检测，请发出以下命令：

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

要查看BPDU倾斜信息，请使用**show spantree bpdu-skewing <vlan>|<mod/port>** 命令，如本示例所示：

```
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
```

相关信息

- 生成树协议根防护增强功能
- 生成树 PortFast BPDU 防护增强功能
- 了解并配置单向链路检测协议功能
- 使用 PortFast 和其他命令解决工作站启动连接延迟问题
- 技术支持和下载 — Cisco Systems

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）。