生成树协议问题及相关设计注意事项

目录

简介

本文档提出了一系列建议，有助于在运行 Catalyst OS (CatOS) 和 Cisco IOS 软件的 Cisco Catalyst 交换机的桥接过程中实施安全网络。本文档讨论生成树协议 (STP) 可能失效的一些常见原因以及为查明问题来源而要寻找的信息。本文档也显示可最大限度地减小与生成树相关的问题且易于排除故障的设计类型。

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。

背景信息

本文档不讨论 STP 的基本运行。要了解 STP 的工作方式，请参考此文档：

- 了解和配置 Catalyst 交换机上的生成树协议 (STP)

本文档不讨论 IEEE 802.1w 中定义的快速 STP (RSTP)。此外，本文档也不讨论 IEEE 802.1s 中定义的多生成树 (MST) 协议。有关 RSTP 和 MST 的详细信息，请参阅以下文档：

- 了解多生成树协议 (802.1s)
- 了解快速生成树协议 (802.1w)

有关适用于运行 Cisco IOS 软件的 Catalyst 交换机的更具体的 STP 故障排除文档，请参考文档在运行 Cisco 集成 IOS（本地模式）的 Catalyst 交换机上排除 STP 的故障。

生成树协议失效

生成树算法（STA）的主要功能是减少在桥接网络中冗余链路所产生的环路。STP 运行在开放式系统互联 (OSI) 模型的第二层。通过在网桥之间交换的网桥协议数据单元 (BPDU)，STP 选择最终转发或阻止数据流的端口。此协议在某些特定情况下可能会失效，并且对产生的情况进行故障排除可能非常困难，具体取决于网络的设计。在此特定区域中，在问题发生之前，请执行故障排除的最重要部分。

STA 失效一般会导致桥接环路。致电 Cisco 技术支持询问生成树问题的大多数客户都怀疑有 Bug，但原因从来都不是 Bug。即使软件是问题所在，STP 环境中的桥接环路也仍来自应阻止流量的端口，而非转发流量的端口。

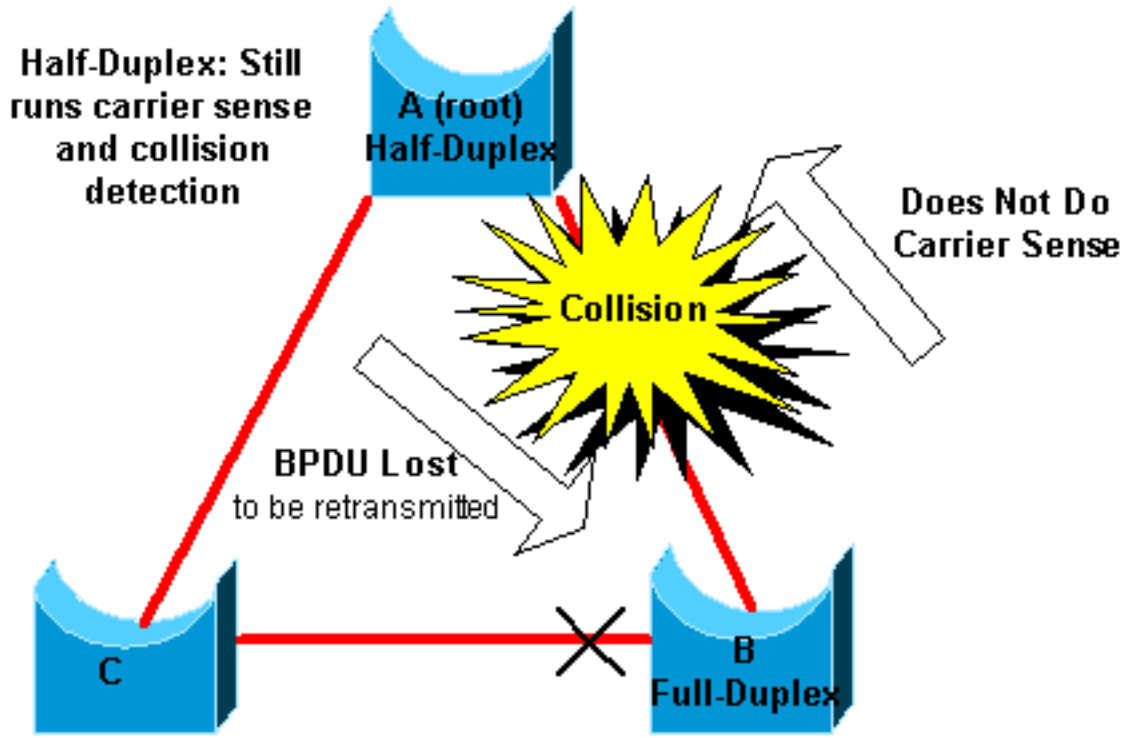
生成树收敛

参考生成树视频 参见解释的示例生成树如何最初聚合。该示例还解释为何由于丢失 BPDU 过多，受阻端口会进入转发模式，从而造成 STA 失效。

本文档的其余部分列出了导致 STA 失效的不同情况。这些失效中的大多数都与丢失 BPDU 过多有关。此项丢失将导致受阻端口过渡到转发模式。

双工不匹配

点对点链路上双工不匹配是很常见的配置错误。如果在链路的一端手动将双工模式设置为全双工，而使另一端保持为自动协商模式，则链路最终会采用半双工。（双工模式设置为全双工的端口不再进行协商。）



最坏的局面是发送 BPDU 的网桥中某个端口的双工模式设置为半双工，而链路另一端对等端口的双工模式设置为全双工。在上述示例中，网桥 A 和 B 之间链路上双工不匹配的情况很容易产生桥接环路。由于网桥 B 的配置为全双工，因此它在访问该链路之前不执行载波侦听。即使网桥 A 已在使用该链路，网桥 B 也会开始发送帧。这种情况对 A 形成了一个问题；网桥 A 将检测冲突并运行补偿算法，然后再尝试再次传输该帧。如果从 B 到 A 有足够的流量，则 A 发送的每个数据包（包含 BPDU）都会遭遇延迟或冲突，并最终被丢弃。从 STP 的角度来看，由于网桥 B 不再从 A 接收 BPDU，因此网桥 B 已丢失根网桥。这种情况使 B 取消阻止与网桥 C 相连的端口，而这会产生环路。

每当双工不匹配时，运行 CatOS 和 Cisco IOS 软件的 Catalyst 交换机的控制台上将出现以下错误消息：

CatOS

```
CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port [mod]/[port]
```

Cisco IOS 软件

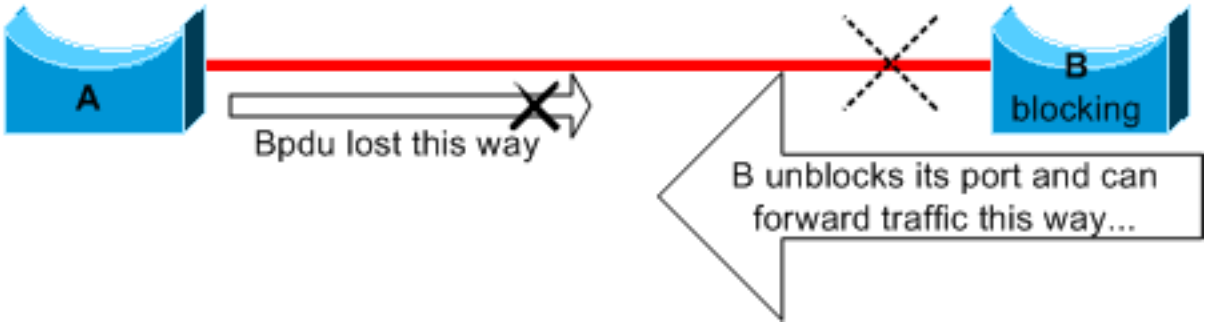
```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

请检查双工设置，如果双工配置不匹配，请设置适当的配置。

有关如何排除双工不匹配故障的详细信息，请参考文档配置以太网 10/100/1000Mb 半/全双工自动协商和排除其故障。

单向链路

单向链路是桥接环路的常见原因。在光纤链路上，检测不到的故障常常会导致单向链路。另一个原因是收发器有问题。可导致链路保持 up 状态和提供单向通信的任何情况对 STP 都非常危险。此示例可解释清楚：



此处，假设 A 与 B 之间的链路是单向的。链路从A降低流量到B，当链路传送从B的流量给A.桥接B阻塞的Assume时，在链路变得单向前。但是，只有从优先级更高的网桥接收 BPDU 的端口才能阻止。由于在这种情况下丢失了来自 A 的所有 BPDU，因此网桥 B 最终将其面向 A 的端口过渡到转发状态并转发流量。这会产生一个环路。如果启动时就有这种失效情况，则 STP 无法正确收敛。在双工不匹配的情况下，重新启动暂时有所帮助；但在这种情况下，重新启动网桥完全无效。

为了在产生转发环路之前检测到单向链路，Cisco 设计并实现了单向链路检测 (UDLD) 协议。 此功能可检测不正确的接线或第二层的单向链路，并且通过禁用某些端口自动切断产生的环路。在桥接环境中，只要有可能，就请运行 UDLD。

有关使用 UDLD 的详细信息，请参考文档了解和配置单向链路检测协议 (UDLD) 功能。

数据包损坏

数据包损坏也会导致同类失效。如果链路的物理错误率很高，则可能会丢失一定量的连续 BPDU。此项丢失可能会导致阻塞端口过渡到转发状态。由于 STP 默认参数非常保守，因此不会经常看到这种情况。阻塞端口需要保持丢失 BPDU 的状态 50 秒，然后才会过渡到转发。成功传输一个 BPDU 即可切断环路。草率地调整 STP 参数时通常会发生这种情况。减小 max-age 就是调整的一个示例。

双工不匹配、电缆有缺陷或电缆长度不正确可能会导致数据包损坏。请参考文档排除交换机端口和接口问题，其中解释了 CatOS 和 Cisco IOS 软件错误计数器输出。

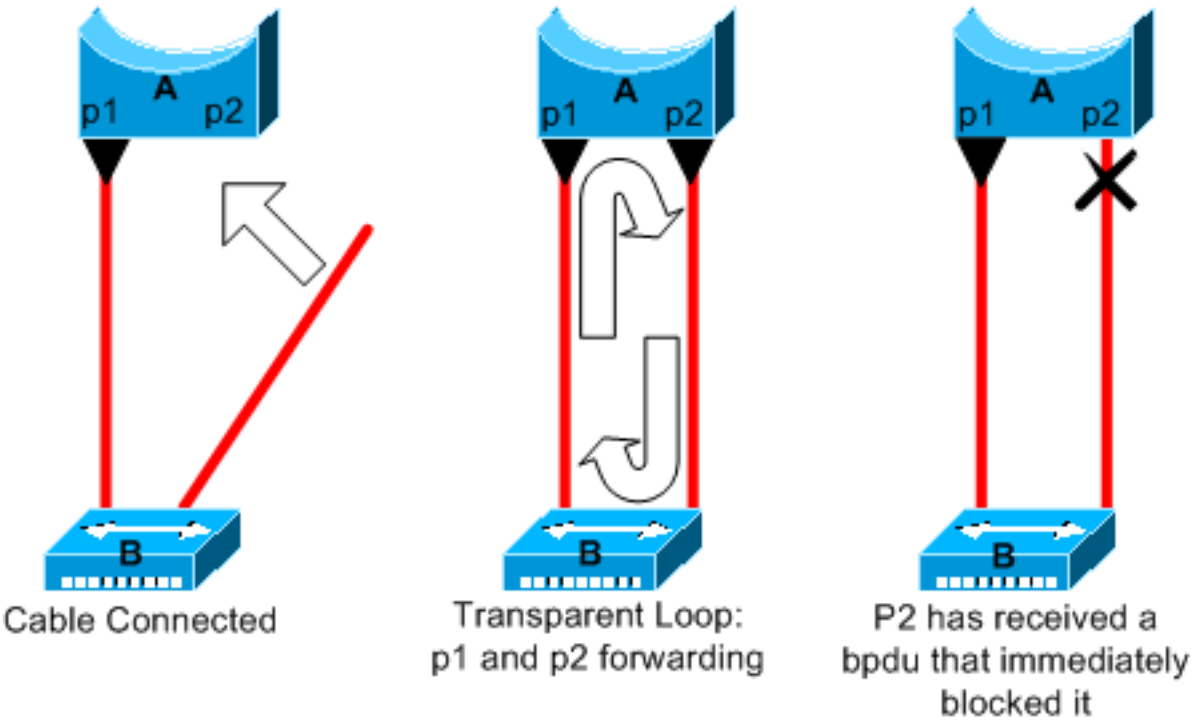
资源错误

STP 以软件方式实现，即使是在以含有专门的应用专用集成电路 (ASIC) 的硬件执行大部分交换功能的高端交换机上也是如此。如果因故过度使用了网桥的 CPU，则资源可能不足以进行 BPDU 的传输。STA 一般不大量占用处理器，并且优先级高于其他进程。本文档的查找资源错误部分中罗列了某个特定平台可处理的 STP 实例数。

Portfast 配置错误

PortFast 是通常只为连接到主机的端口或接口启用的一种功能。此端口上链路变为 up 状态后，网桥会跳过 STA 的第一个阶段，直接过渡到转发模式。

警告：请勿在连接到其他交换机、集线器或路由器的交换机端口或接口上使用 Portfast 功能。否则可能会产生网络环路。



在本示例中，设备 A 是端口 p1 已成为转发模式的网桥。端口 p2 具有 PortFast 配置。设备 B 是集线器。将第二根电缆插入 A 后，端口 p2 就会变为转发模式，从而在 p1 与 p2 之间产生一个环路。p1 或 p2 收到将其中一个端口置于阻塞模式的 BPDU 后，此环路就会终止。但是，这种临时环路存在一个问题。如果循环的流量非常密集，则网桥可能难以成功地传输终止环路的 BPDU。此问题可能会显著推迟收敛过程，在极端情况下甚至会使网络瘫痪。

有关如何在运行 CatOS 和 Cisco IOS 软件的交换机上正确使用 PortFast 的详细信息，请参考文档使用 PortFast 和其他命令解决工作站启动连接延迟问题。

即使配置了 PortFast，端口或接口仍可参与 STP。如果网桥优先级低于当前活动根桥优先级的交换机连接到配置了 PortFast 的端口或接口，则可以将该交换机选为根桥。由于根桥发生改变，活动 STP 拓扑也会受到影响，致使网络性能下降。为防止发生这种情况，大多数运行 CatOS 和 Cisco IOS 软件的 Catalyst 交换机都具有一种名为 BPDU 防护的功能。BPDU 防护可在配置了 PortFast 的端口或接口接收 BPDU 时将其禁用。

有关在运行 CatOS 和 Cisco IOS 软件的交换机上使用 BPDU 防护功能的详细信息，请参考文档生成树 Portfast BPDU 防护增强。

不适当的 STP 参数调整和直径问题

max-age 参数的值过于积极和转发延迟可能会导致 STP 拓扑很不稳定。在此类情况下，丢失某些 BPDU 可能会产生环路。另一个不太为人所知的问题与桥接网络的直径有关。STP 计时器的默认值将最大网络直径保守的限制为 7。这个最大网络直径限制了网络中网桥相互之间可以相距多远。这种情况下，二个不同的网桥彼此相距不得超过 7 跳。造成此限制的部分原因来源于 BPDU 所具有的 age 字段。

当 BPDU 从根桥向树叶传播时，BPDU 每经过一个网桥，age 字段都会递增。最后，当 age 字段超过最大 age 值时，网桥即丢弃该 BPDU。如果根与网络的某些网桥距离过远，则可能出现此问题。此问题影响生成树的收敛。

如果要将 STP 计时器从默认值更改为其他值，请格外谨慎。尝试以此方式获得更快的再收敛速度时存在风险。STP 计时器变动会影响网络的直径以及 STP 的稳定性。可以更改网桥优先级以选择根桥，还可以更改端口开销或优先级参数以控制冗余性和负载平衡。

Cisco Catalyst 软件为您提供可精细调整最重要的 STP 参数的各种宏：

- set spantree root [secondary] 宏命令降低网桥的优先级，以使该网桥成为根（或备用根）。此命令还有另一个选项，可通过指定网络直径调整 STP 计时器。即使正确完成后，调整计时器也不会显著改善收敛时间，反而会在网络中引入某些不稳定性的风险。此外，每当向网络中添加设备时，都必须更新这种调整。保留保守的默认值，网络工程师熟知这些值。
- CatOS 的 set spantree uplinkfast 命令或 Cisco IOS 软件的 spanning-tree uplinkfast 命令将提高交换机的优先级，以使该交换机不能成为根。在上行链路发生失效的情况下，该命令将增加 STP 收敛时间。 请在与某些核心交换机具有双重连接的分发层交换机上使用此命令。请参考文档了解和配置 Cisco UplinkFast 功能。
- CatOS 的 spantree backbonefast enable 命令和 Cisco IOS 软件的 spanning-tree backbonefast 命令可以在间接链路故障的情况下增加交换机的 STP 聚合时间。BackboneFast 是 Cisco 的专有功能。请参考文档了解和配置 Catalyst 交换机上的 Backbone Fast。

有关 STP 计时器和在确实必要时调整这些计数器的规则的详细信息，请参考文档了解和调整生成树协议计时器。

软件错误

正如简介中所提及，STP 是 Cisco 产品中实现的首批功能之一。此功能可望非常稳定。只有与较新功能（如 EtherChannel）的交互会导致 STP 在某些非常特殊的情况下失效，现已解决这些情况下失效的问题。多种不同的因素会导致软件 Bug，并且会造成多种不同的影响。无法详细介绍 Bug 可能会引入的问题。软件错误所能引起的最危险情况是如果忽略某些 BPDU，一般来说，即某个阻塞端口过渡到转发。

排除故障

遗憾的是，没有系统化的过程可用于解决 STP 问题。但是，本部分总结了一些可供您使用的操作。本部分中的大多数步骤一般都适用于排除桥接环路故障。对于导致丢失连接的 STP 的其他故障，可使用更为常规的方法进行排查。例如，可以探查遇到问题的流量所采用的路径。

注意： 大多数这些故障排除步骤都假设与桥接网络的不同设备具有连接。这种连接意味着您可以进行控制台访问。例如，在有桥接环路期间，您可能无法建立 Telnet 连接。

如果有输出一**show-tech support命令**从您的Cisco设备，您能使用Cisco CLI分析器 (仅限注册用户)显示潜在问题和修正。

使用网络图

在排除桥接环路故障之前，您至少需要了解以下各项：

- 桥接网络的拓扑
- 根桥的位置
- 受阻端口和冗余链路的位置

至少有以下两个原因决定必须了解上述内容：

- 要了解网络中需要修复什么，必须了解网络正常工作时的情况。
- 大多数故障排除步骤都仅仅使用 **show** 命令尝试找出错误情况。对网络的了解有助于重点专注关键设备的重要端口。

识别桥接环路

过去，广播风暴可能会对网络造成灾难性影响。如今，有了高速链路和在硬件级别提供交换的设备，一台主机（如服务器）不太可能通过广播使网络瘫痪。识别桥接环路的最佳方法是在已饱和的链路上捕获流量，并检查是否多次发现相似的数据包。但实际上，如果某个网桥域中的所有用户同时遇到连接问题，则可以怀疑出现了桥接环路。

检查设备上的端口使用率，并查找异常值。请参考本文档的检查端口使用率部分。

在运行 CatOS 的 Catalyst 交换机上，可以用 show system 命令轻松地检查背板的总体使用情况。该命令提供交换机背板的当前使用情况，还可指出使用高峰和使用高峰的日期。异常的峰值使用率可说明此设备上是否曾有桥接环路。

快速恢复连接并为下次做好准备

禁用端口以断开环路

桥接环路会对网桥网络造成极为严重的后果。管理员一般没有时间寻找产生环路的原因，因此更愿意尽快恢复连接。这种情况下解决问题的简单方法是手动禁用在网络中提供冗余的每个端口。如果能确定网络中受影响最大的部分，则请开始禁用该区域中的端口。或者，如果可能，开始禁用应为阻塞状态的端口。每次禁用端口时，都请检查是否已恢复了网络中的连接。 通过识别哪个被禁用的端口终止了环路，还可以识别此端口所处的冗余路径。如果此端口应该被阻拦，您能够正确查找出现故障的链路。

在托管受阻端口的设备上记录 STP 事件

如果无法准确地查明问题的来源，或如果问题只是暂时现象，则请在出现故障的网络的网桥和交换机上启用 STP 事件的日志记录。如果要限制所配置的设备数，请在托管受阻端口的设备上至少启用此日志记录；受阻端口的过渡即产生环路。

- Cisco IOS软件问题启用STP调试信息的exec命令**debug spanning-tree events**。发出常规配置模式命令 logging buffered，在设备缓冲区中捕获该调试信息。
- CatOS **set logging level spantree 7 default命令**增加与STP关连与调试级别的默认级别事件。请确保使用 set logging buffer 500 命令，在交换机缓冲区中记录尽可能多的消息。

也可尝试将调试输出发送到 syslog 设备。遗憾的是，出现桥接环路时，很难与 syslog 服务器保持连接。

检查端口

首先调查的重要端口是阻塞端口。本部分提供在不同端口上要寻找的内容的列表，同时简要介绍对运行 CatOS 和 Cisco IOS 软件的交换机发出的命令。

检查受阻端口是否收到 BPDU

尤其是对受阻端口和根端口，检查是否能定期收到 BPDU。有多种问题会导致端口故障，从而无法接收数据包或 BPDU。

- 软件在Cisco IOS软件版本12.0的Cisco IOS或以后，输出**show spanning-tree bridge-group -命令**有一BPDU。该字段向您显示每个接口收到的 BPDU 数。再发出一两次该命令，确定设备能否

收到 BPDU。如果 show spanning-tree 命令的输出中没有 BPDU 字段，则可以用 debug spanning-tree 命令启用 STP 调试以确认收到 BPDU。
- **show mac module/port命令的**CatOS这告诉您组播信息包的数量一个特定端口接收。但是，所使用的最简单命令是 show spantree statisticsmodule#/port#vlan 命令。此命令显示特定 VLAN 中特定端口收到的配置 BPDU 的确切数量。一个端口可属于多个 VLAN（如果有中继）。请参阅本文档的其他 CatOS 命令部分。

检查是否有双工不匹配的情况

要查找双工不匹配的情况，必须检查点对点链路的每一端。

- Cisco IOS软件问题**show interfaces [interface interface-number] status命令**检查特定端口的速度和双工状态。
- 输出的CatOS这首先线路**show port module-/port-命令**根据端口配置给您速度和双工。

检查端口使用率

流量过载的接口可能无法传输重要的 BPDU。链路过载也表示可能有桥接环路。

- Cisco IOS软件使用show interfaces命令**确定在接口的利用率。**有几个字段可帮助您做出判断，例如 load 和 packets input 或 packets output。请参考文档排除交换机端口和接口问题，以获得 **show interfaces** 命令输出的解释。
- 关于端口收到并且发送的数据包的CatOS这**show mac module-/port-命令**显示统计信息。show top 命令自动计算 30 秒内端口的使用率并显示结果。该命令按百分比带宽利用率将结果分类，但还可以按其他条件将结果分类。此外，show system 命令可指示背板利用率，但该命令并不指某个具体的端口。

检查数据包损坏

- 错误的Cisco IOS软件查看在计数器增加**show interfaces命令**。错误计数器包括 runts、giants、no buffer、CRC、frame、overrun 和 ignored 数量。请参考文档排除交换机端口和接口问题，以获得 **show interfaces** 命令输出的解释。
- CatOS这show port module-/port-命令**给予您与**一些详细信息 `fcs-err Xmit-ErrRcv-Err`和字段。show counters module#/port# 命令提供更详细的统计信息。

其他 CatOS 命令

命令 show spantree statistics module#/port# vlan# 提供有关某个特定端口的非常准确的信息。请在您怀疑的端口上发出此命令，并特别注意以下这些字段：

- `trans`计数器记住多少时期端口从学习过渡了到转发。在稳定的拓扑中，此计数器总是显示 1。当端口变为 down 或 up 状态时，此计数器重置为 0。因此，此值高于 1 表明端口所经历的过渡是 STP 重新计算的结果。过渡不是直接链路故障的结果。
- 计数器跟踪该的次数在此链路超时的最大老化时间。大体而言，期待 BPDU 的端口等待 max age 所指的时间，然后将指定网桥视为丢失。max age 默认值为 20 秒。每次发生此事件时，计数器就会递增。当值不为 0 时，该计数器表明此 LAN 的指定网桥不稳定或在传输 BPDU 方面有问题。

查找资源错误

CPU 使用率过高对运行 STA 的系统可能很危险。请使用下面这个方法检查设备的 CPU 资源是否充足：

- Cisco IOS软件问题**show processes cpu命令**。检查 CPU 使用率是否不太高。有关运行 CatOS 或 Cisco IOS 软件的 Catalyst 4500/4000 系列交换机，请参考文档 Catalyst 4500/4000、2948G、2980G 和 4912G 交换机上的 CPU 使用率。
- CatOS问题**show proc cpu命令**显示CPU利用率信息。检查 CPU 使用率是否不太高。

Supervisor 引擎能处理的各种 STP 实例的数量有一定限制。确保不同 VLAN 的所有 STP 实例中逻辑端口的总数不超过每个 Supervisor 引擎类型和内存配置支持的最大数量。

对运行 CatOS 的交换机发出 **show spantree summary** 命令，或对运行 Cisco IOS 软件的交换机发出 show spantree summary 命令。这些命令在 STP Active列中显示每个 VLAN 的逻辑端口或接口的数量。此列的底部显示总数。总数表示不同 VLAN 的所有 STP 实例中所有逻辑端口之和。 请确保此数字不超出对每种 Supervisor 引擎支持的最大数量。

注意： 计算交换机上逻辑端口之和的公式为：

```
(number of non-ATM trunks * number of active Vlans on that trunk)
+ 2*(number of ATM trunks * number of active Vlans on that trunk)
+ number of non-trunking ports
```

有关适用于 Catalyst 交换机的 STP 限制的汇总，请参考以下这些文档：

平台	CatOS STP 限制	Cisco IOS 软件 STP 限制
Catalyst 6500/6000 Supervisor 引擎 I 和 II	STP 故障排除	
Catalyst 6500/6000 Supervisor 引擎 720	STP 故障排除	生成树故障排除
Catalyst 4500/4000	**生成树**	排除生成树故障
Catalyst 3750		配置 STP

禁用不必要的功能

故障排除是关于识别网络中哪些内容当前错误的问题。请禁用尽可能多的功能。禁用有助于简化网络结构，并且便于发现问题。例如，EtherChanneling 是要求 STP 将几条不同的链路在逻辑上捆绑为一条链路的功能；在故障排除期间禁用此功能很有意义。一般而言，使配置尽可能简单可以更容易地排除故障。

有用的命令

Cisco IOS 软件命令

- **show interfaces**
- **show spanning-tree**
- **show bridge**
- **show processes cpu**
- **debug spanning-tree**
- **logging buffered**

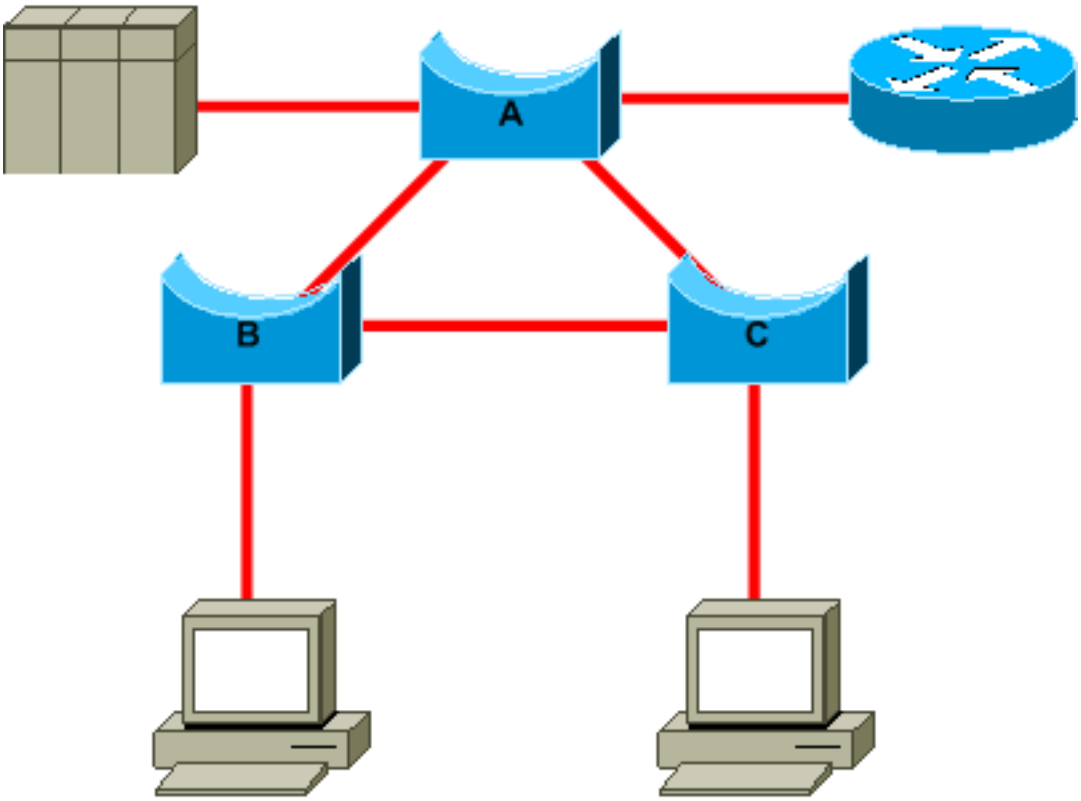
CatOS 命令

- show port
- show mac
- show spantree
- show spantree statistics
- show spantree blockedports
- show spantree summary
- show top
- show proc cpu
- show system
- show counters
- set spantree root [secondary]
- set spantree uplinkfast
- set logging level
- set logging buffered

设计 STP 以避免出现问题

了解根桥的位置

排除故障时经常会不了解根桥的位置。不要让 STP 决定哪个网桥是根桥。对于每个 VLAN，您通常都可以确定哪台交换机最适合作为根桥。这取决于网络的设计。一般情况下，选择位于网络中央位置、而且功能较强的网桥。如果将根桥放在网络中央，直接连接到服务器和路由器，通常能缩短客户端到服务器和路由器的平均距离。



此图显示：

- 如果网桥 B 是根桥，则在网桥 A 或网桥 C 上将阻止链路 A 到 C。在这种情况下，连接到交换机 B 的主机通过 2 跳可以访问服务器和路由器。连接到网桥 C 的主机通过 3 跳可以访问服务

器和路由器。因此平均距离是两跳半。
- 如果网桥 A 是根桥，则 B 和 C 上连接的两台主机通过 2 跳即可到达路由器和服务器。现在的平均距离为两跳。

这个简单例子所揭示的逻辑同样适用于更为复杂的拓扑。

重要说明：对于每个 VLAN，对根桥和备用根桥进行硬编码，其中对于备用根桥减小 STP priority 参数的值。或者，可以使用 set spantree root 宏。

了解冗余的位置

规划冗余链路的组织结构。请忘记 STP 的即插即用功能。调整 STP cost 参数以决定哪些端口进行阻止。如果采用分层设计而且根桥所在的位置恰当，那么一般不需要调整该参数。

重要说明：对于每个 VLAN，了解在稳定的网络中应有哪些端口进行阻止。得到一张网络图，其中应清晰地显示网络中的每个物理环路以及哪些受阻端口可打破这些环路。

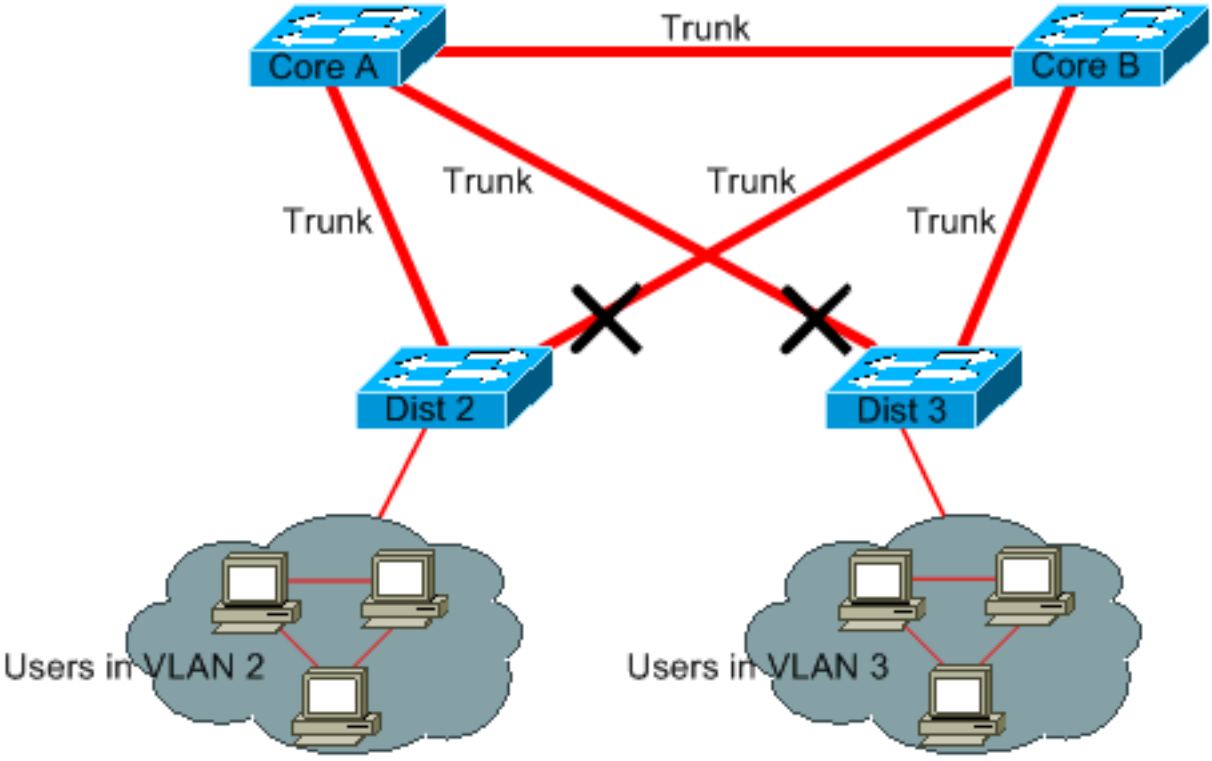
了解冗余链路的位置有助于发现偶然产生的桥接环路及其原因。此外，了解受阻端口的位置可确定错误的位置。

将阻塞端口的数量减到最小

STP 采取的唯一一项重要举措就是阻塞端口。只要有一个阻塞端口错误地过渡到转发状态，就可能使大部分网络瘫痪。避免产生使用 STP 的内在风险的一个好办法就是尽量减少受阻端口的数量。

修剪不使用的 VLAN

在桥接网络中，两个节点之间不需要二条以上的冗余链路。但是，此类配置很常见：



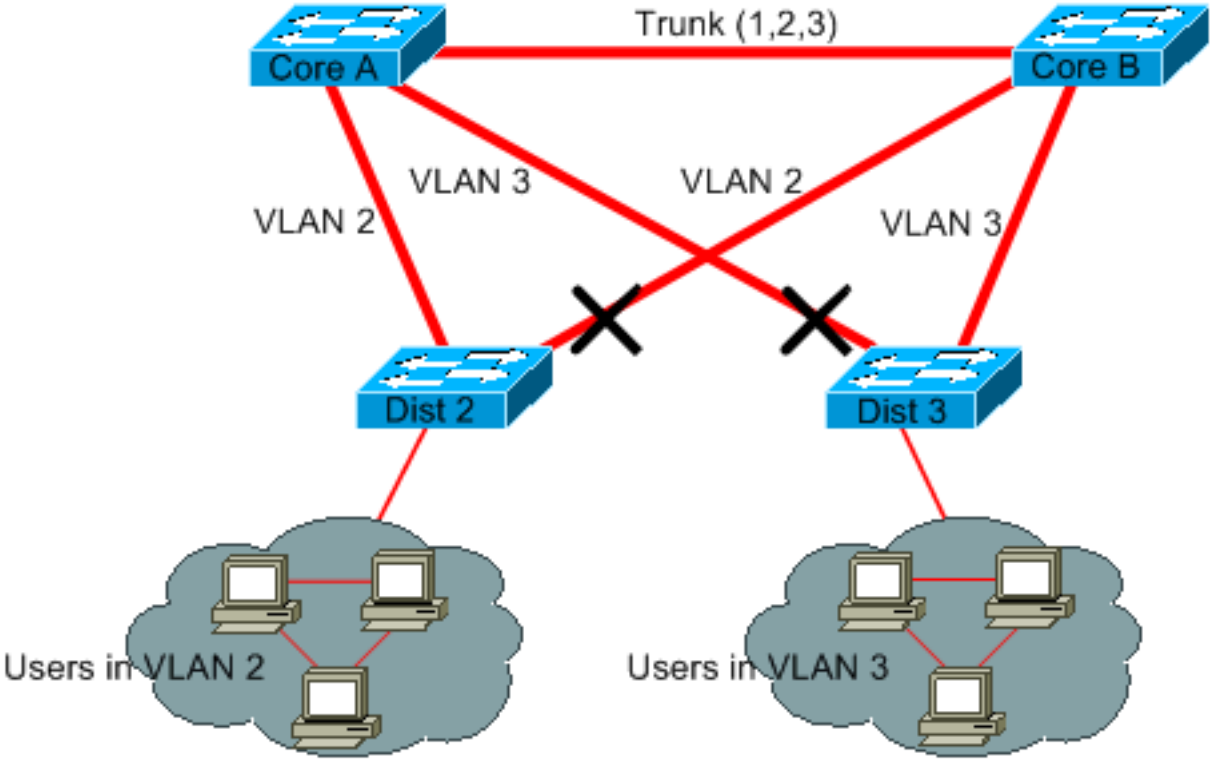
每台分发层交换机分别连接到两台核心层交换机。分发层交换机上连接的用户都只位于网络中可用 VLAN 的子集中。在本示例中，Dist 2 上连接的用户都位于 VLAN 2 中；Dist 3 仅连接 VLAN 3 中的

用户。默认情况下，中继承载 VLAN 中继协议 (VTP) 域中定义的所有 VLAN。只有 Dist2 接收 VLAN3 中不必要的广播和多播流量，但是 Dist2 也正在阻止其用于 VLAN3 的端口之一。结果是 Core A 与 Core B 之间有三条冗余路径。这种冗余设置会导致许多端口被阻塞，形成环路的机率也更高。

重要说明：请从中继修剪掉任何不需要的 VLAN。

VTP 修剪可起到一定作用，但在网络的核心层中没有必要使用此类即插即用功能。

在本示例中，只使用了一个接入层 VLAN 将分发层交换机连接到核心层：



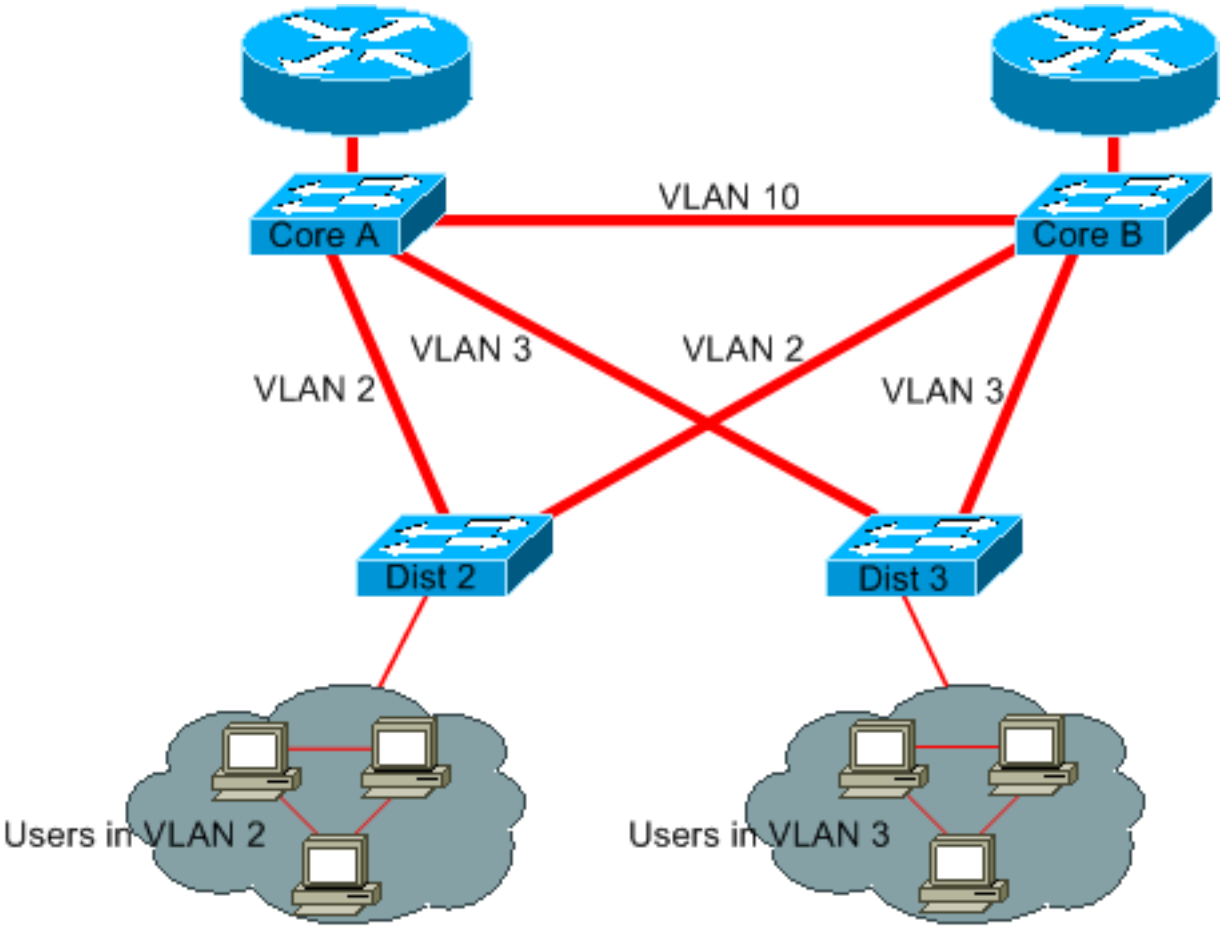
在此设计中，每个 VLAN 只阻塞了一个端口。此外，对于此设计，如果关闭 Core A 或 Core B，那么只需一步即可消除所有冗余链路。

使用第 3 层交换

第 3 层交换表示以接近交换的速度进行路由。路由器执行两项基本工作：

- 路由器构建转发表。路由器一般通过路由协议与对等点交换信息。
- 路由器接收数据包，并根据目标地址将其转发到正确的接口。

高端的 Cisco 第 3 层交换机现在能够使用与第 2 层交换功能相同的速度执行这第二项功能。如果引入路由跳跃，并创建网络的另一个分段，则不会损失速度。此图使用修剪不使用的 VLAN 部分中的示例作为基础：



Core A 和 Core B 现在是第 3 层交换机。Core A 和 Core B 之间不再桥接 VLAN 2 和 VLAN 3，因此不可能形成 STP 环路。

- 冗余仍然存在，但现在依靠第 3 层路由协议。此设计确保再收敛比 STP 的再收敛还快。
- STP 不会再阻塞任何单个端口。因此，不可能再产生桥接环路。
- 速度没有损失，因为 VLAN 由第 3 层交换处理时与 VLAN 内的桥接一样快。

此设计只有一个缺点。迁移到此类设计一般表示要重新制作寻址方案。

即使不必要也保留 STP

即使成功地从网络消除了所有受阻端口，并且没有任何物理冗余，也不要禁用 STP。STP 一般不会大量占用处理器；数据包交换在大多数 Cisco 交换机中不会牵扯到 CPU。此外，每条链路发送的 BPDU 极少，不会显著降低可用带宽。但是，例如如果操作员在配线面板上操作错误，没有 STP 的桥接网络在几分之一秒内就可能瘫痪。通常，不值得冒此风险禁用桥接网络中的 STP。

使流量远离管理 VLAN，不要用单个 VLAN 覆盖整个网络

Cisco 交换机通常有一个 VLAN 绑定有 IP 地址，此 VLAN 即是管理 VLAN。在此 VLAN 中，交换机像普通的 IP 主机一样运行。具体而言，即每个广播或多播数据包都会转发到 CPU。管理 VLAN 中广播或多播流量的速率太高会对 CPU 造成不利影响，从而削弱 CPU 处理重要的 BPDU 的能力。因此，用户流量不应在管理 VLAN 上传输。

直到不久前，Cisco 实现才有办法从中继内去除 VLAN 1。VLAN 1 一般用作管理 VLAN，其中在同一 IP 子网内可以访问所有交换机。尽管此设置很有用，但也非常危险，因为 VLAN 1 上的桥接环路会影响所有中继，从而可能导致整个网络瘫痪。当然，无论您使用哪个 VLAN 都存在同样的问题。请尝试使用高速第 3 层交换机将桥接域分段。

从 CatOS 版本 5.4 和 Cisco IOS 软件版本 12.1(11b)E 起，可以从中继内去除 VLAN 1。VLAN 1 依然存在，但它会阻塞流量，以免形成环路。

相关信息

- 工具和资源 - 技术支持和文档
- 技术支持和文档 - Cisco Systems