排除STP问题及相关设计注意事项

目录

- 简介
- 先决条件
  - 要求
  - 使用的组件
- 背景信息
- 生成树协议失效
  - 生成树收敛
  - 双工不匹配
    - Cisco IOS 软件
  - 单向链路
  - 数据包损坏
  - 资源错误
  - Portfast 配置错误
  - 不适当的 STP 参数调整和直径问题
  - 软件错误
- 排除故障
  - 使用网络图
  - 识别桥接环路
  - 快速恢复连接并为下次做好准备
    - 禁用端口以断开环路
    - 在托管受阻端口的设备上记录 STP 事件
  - 检查端口
    - 检查受阻端口是否收到 BPDU
    - 检查是否有双工不匹配的情况
    - 检查端口使用率
    - 检查数据包损坏
  - 查找资源错误
  - 有用的命令
    - Cisco IOS 软件命令
- 设计 STP 以避免出现问题
  - 了解根桥的位置
  - 了解冗余的位置
  - 将阻塞端口的数量减到最小
    - 修剪不使用的 VLAN
    - 使用第 3 层交换
  - 即使不必要也保留 STP
  - 使流量远离管理 VLAN，不要用单个 VLAN 覆盖整个网络
- 相关信息

简介

本文档介绍如何对桥接Cisco Catalyst网络中的生成树协议(STP)故障进行故障排除并防止其发生。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档重点介绍传统STP行为和Cisco IOS软件命令。

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。

背景信息

本文档讨论STP可能失败的一些常见原因，以及查找以确定问题来源的信息。它还显示了可最大限度地减少生成树相关问题并易于故障排除的设计。

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 STP

本文档不讨论 IEEE 802.1w 中定义的快速 STP (RSTP)。此外，本文档不讨论IEEE 802.1s中定义的多生成树(MST)协议。除非另有说明，否则本文档中的计时器和收敛说明适用于传统IEEE 802.1D STP行为。

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，请参阅排除Catalyst交换机上的STP问题文档。



注意：本文档保留传统STP信息，以提供传统IEEE 802.1D STP行为的基础知识。建议不要将传统STP用于生产环境。对于生产网络，请使用第3层路由设计，根据平台支持和网络设计要求部署较新的生成树协议或模式，例如快速生成树协议(RSTP)、快速PVST+或多生成树(MST)

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在开放式系统互联(OSI)模型的第2层运行。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败，并且排查结果可能会非常困难的情况，具体取决于网络的设计。在此特定区域中，在问题发生之前，您需要执行故障排除过程的最重要部分。

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。即使软件存在问题，STP环境中的桥接环路仍然来自可以阻塞（而是转发流量）的端口。

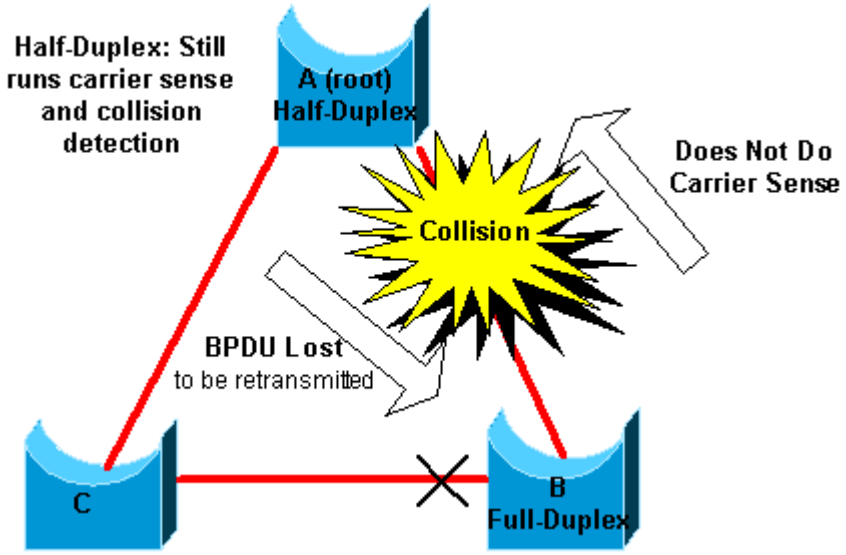
生成树收敛

请参阅生成树视频 中的举例说明，了解生成树最初如何收敛。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。在传统10/100 Mbps以太网链路上，如果您在链路的一端将双工模式手动设置为“全”，而将另一端保留为自动协商模式，则该链路最终将处于半双工模式。（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。在前面的示例中，网桥A和B之间的链路上的双工不匹配很容易导致桥接环路。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。

当出现双工不匹配时，在运行Cisco IOS软件的Catalyst交换机的交换机控制台上可以看到以下错误消息：

Cisco IOS 软件

```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half duplex), with TBA050714
```

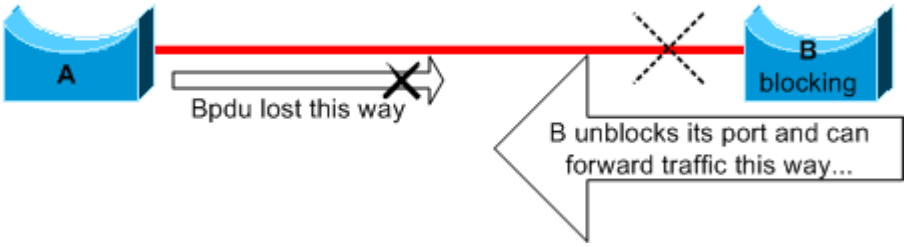
请检查双工设置，如果双工配置不匹配，请设置适当的配置。

有关如何排除双工不匹配问题的详细信息，请参阅文档配置和验证以太网10/100/1000Mb半双工/全双工自动协商。

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。链路会丢弃从 A 到 B 的流量，同时链路会传输从 B 到 A 的流量。假设网桥 B 处于阻塞状态，然后链路成为单向链路。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。UDLD检测受支持的第2层链路上的单向情况。在受支持的点对点链路上配置UDLD主动模式，在检测到单向条件后需要自动禁用端口。

有关使用UDLD的详细信息，请参阅文档配置UDLD协议功能。

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。使用传统IEEE 802.1D默认计时器时，阻塞端口可能需要50秒才能达到转发状态，因为最后一个BPDU会丢失：最长时间为20秒，倾听15秒，学习15秒。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。有关Cisco IOS软件错误计数器输出的说明，请参阅排除交换机端口和接口故障。

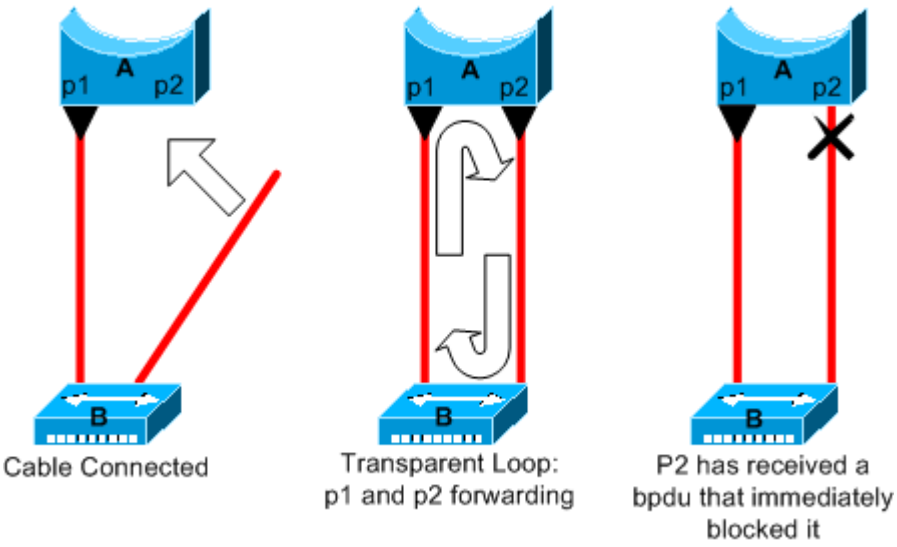
资源错误

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。 如果由于任何原因导致网桥的CPU使用过度，则资源可能不足以传输 BPDU。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：仅在未连接到第2层桥接设备的边缘接口上启用PortFast。请勿在可以接收BPDU的接口上启用PortFast或创建第2层环路。



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。只要将第二根电缆插入A，端口p2就会进入转发模式，并在p1和p2之间形成环路。当p1或p2收到将这两个端口之一置于阻塞模式的BPDU时，此环路就会停止。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。

有关在运行Cisco IOS软件的交换机上正确使用PortFast的详细信息，请参阅文档使用PortFast和其他命令解决工作站启动连接延迟。

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。为防止出现这种情况，大多数运行Cisco IOS软件的Catalyst交换机都具有名为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Cisco IOS软件的交换机上使用BPDU防护功能的详细信息，请参阅了解生成树PortFast BPDU防护增强功能文档。

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。如果您尝试以这种方式实现更快的重新融合，则存在危险。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：

- spanning-tree vlan number root { primary | secondary }命令降低网桥优先级，使其成为根（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。
- Cisco IOS软件的spanning-tree uplinkfast命令会增加交换机优先级，以便交换机不会成为根网桥。该命令可在直接上行链路发生故障后缩短STP收敛时间。当平台和STP模式支持接入层交换机时，在接入层交换机上使用此旧功能，该交换机具有到分布层的冗余上行链路。请参考文档了解和配置 Cisco UplinkFast 功能。
- 用于Cisco IOS软件的spanning-tree backbonefast命令可以在出现间接链路故障时缩短交换机的STP收敛时间。BackboneFast 是 Cisco 的专有功能。请参阅文档了解和配置Catalyst交换机上的Backbone Fast。

有关STP计时器以及在绝对必要时对其进行调整的规则的详细信息，请参阅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 是思科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。如果忽略某些BPDU或者将阻塞端口转换为转发状态，则软件错误最危险的情形就是这种情况。

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：排除故障所需的大部分步骤假设连接了网桥网络的不同设备。这种连接意味着您可以进行控制台访问。例如，在桥接环路期间，您可能无法建立远程连接。

如果从Cisco设备获得命**show tech-support**令的输出，可以使用Cisco CLI分析器。

注意：只有思科注册用户才能访问思科内部工具和信息。

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。
- 进行故障排除的大部分步骤只是使用show命令尝试识别错误情况。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。

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。为了停止活动环路，请使用控制台或带外访问一次禁用一条可疑的冗余路径，并在每次更改后验证连接。避免禁用为网段提供唯一管理或转发路径的链路。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，首先禁用可以阻塞的端口。每次禁用端口时，请检查网络中是否已恢复连接。通过标识哪个禁用的端口可停止环路，还可以标识此端口所在的冗余路径。如果此端口被阻塞，您可能已经找到了出现故障的链路。

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。

⚠ 警告：Debug命令可以在桥接环路期间添加控制平面负载。仅通过控制台或带外访问运行它们，监控CPU使用率，并在数据收集后禁用调试。

- 运行debug spanning-tree events EXEC命令以启用STP事件调试。配置logging buffered以捕获日志记录缓冲区中的消息。

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。本部分提供了在不同端口上查找内容的列表，以及针对运行Cisco IOS软件的交换机发出的命令的简要说明。

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。

- Cisco IOS软件 — 在Cisco IOS软件版本12.0或更高版本中，show spanning-tree vlan <vlan-id> detail命令的输出有一个BPDU字段。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。另一种方法是使用debug spanning-tree bpdu命令启用STP调试，以验证是否收到BPDU。

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 — 发出**show interfaces [interface-number] status**命令检查特定端口的速度和双工状态。

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 — 使用命**show interfaces**令确定接口的利用率。有几个字段可帮助您做出判断，例如 load 和 packets input 或 packets output。有关命令输出的说明，请参阅排除交换机端口和接口问题**show interfaces**文档。

检查数据包损坏

- Cisco IOS 软件 - 在 show interface 命令的输入错误计数器中查找增加的错误数。错误计数器包括 runts、giants、no buffer、CRC、frame、overrun 和 ignored 数量。

  请参阅文档排除交换机端口和接口问题，了解以下内容的说明 **show interfaces** command output.

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 - 发出 show processes cpu 命令。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。

对交换**show spanning-tree summary totals**机发出命令，此命令在`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：

Platform	Cisco IOS 软件 STP 限制
Catalyst 6500/6000 Supervisor 引擎 720	Cisco IOS版本12.2SXF和重建版本说明
Catalyst 4500/4000	Catalyst 4500系列交换机、Cisco IOS、12.1EW的版本说明
Catalyst 3750	Catalyst 3750交换机软件配置指南，版本12.1(19)EA1

有用的命令

Cisco IOS 软件命令

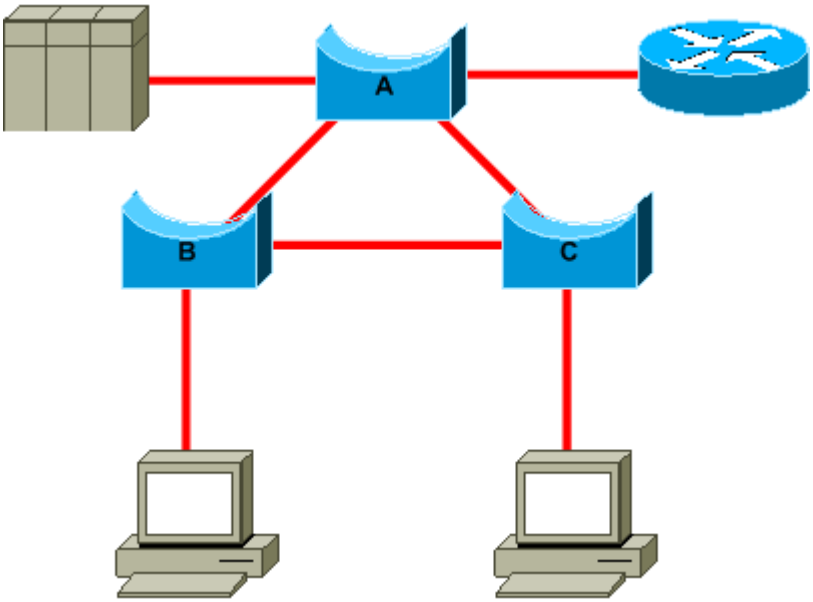
- **show interfaces**
- **show spanning-tree**
- **show processes cpu**
- **debug spanning-tree**
- **logging buffered**

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，则连接到B和C的两个主机均可通过两跳到达路由器和服务器。现在平均距离为两跳。

这个简单例子所揭示的逻辑同样适用于更为复杂的拓扑。

注意：对于每个VLAN，通过减少STP网桥优先级值来配置根网桥和备用根网桥。或者使用spanning-tree vlan <vlan-id> root primary和spanning-tree vlan <vlan-id> root secondary命令。

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。

注意：对于每个VLAN，了解稳定网络中哪些端口会阻塞。绘制网络图，清楚地显示网络中阻止端口中断环路的每条物理环路。

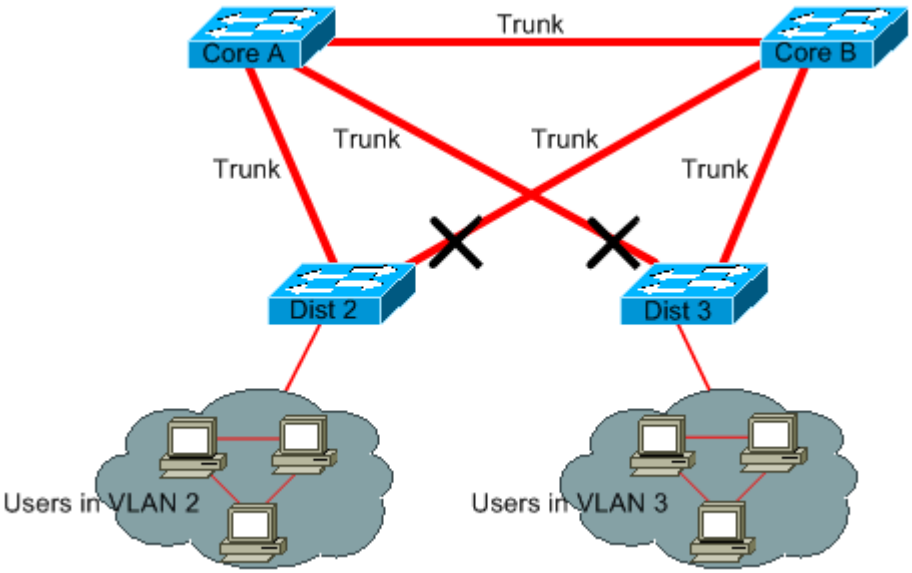
了解冗余链路的位置有助于发现偶然产生的桥接环路及其原因。此外，了解受阻端口的位置可确定错误的位置。

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

避免两个交换节点之间不必要的独立第2层路径。当设计和平台支持EtherChannel时，将并行链路捆绑到其中：

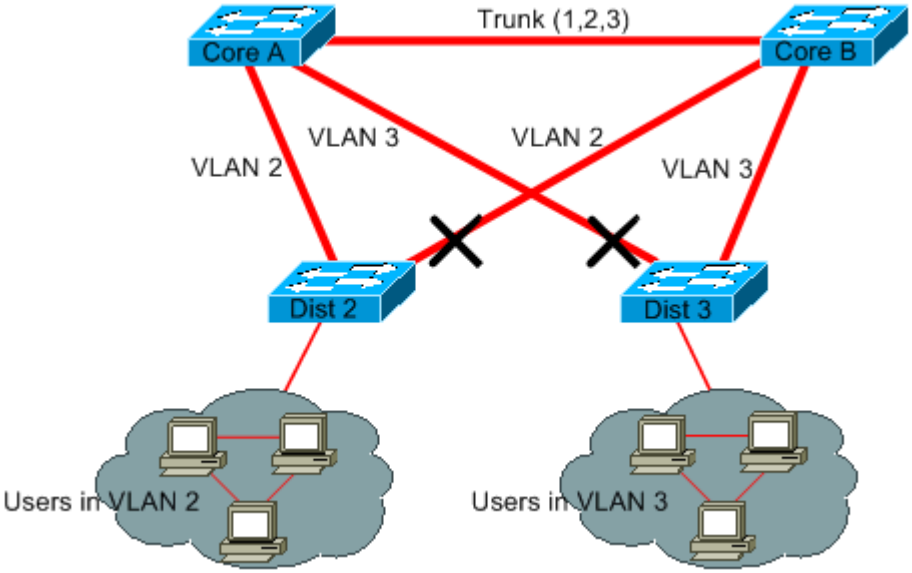


每台分发层交换机分别连接到两台核心层交换机。分发层交换机上连接的用户都只位于网络中可用 VLAN 的子集中。在本示例中，Dist 2 上连接的用户都位于 VLAN 2 中；Dist 3 仅连接 VLAN 3 中的用户。默认情况下，中继承载 VLAN 中继协议 (VTP) 域中定义的所有 VLAN。只有Dist 2接收到VLAN 3的不必要广播和组播流量，但它也阻塞了VLAN 3的一个端口。结果是核心A和核心B之间有三个冗余路径。这种冗余设置会导致许多端口被阻塞，形成环路的机率也更高。

注意：请从中继修剪掉任何不需要的 VLAN。

VTP修剪会为符合条件的VLAN减少不必要的泛洪流量，但是明确的中继允许的VLAN配置提供确定的VLAN位置。请勿将VTP修剪视为从中继允许列表中删除未使用的VLAN的替代方法。

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：



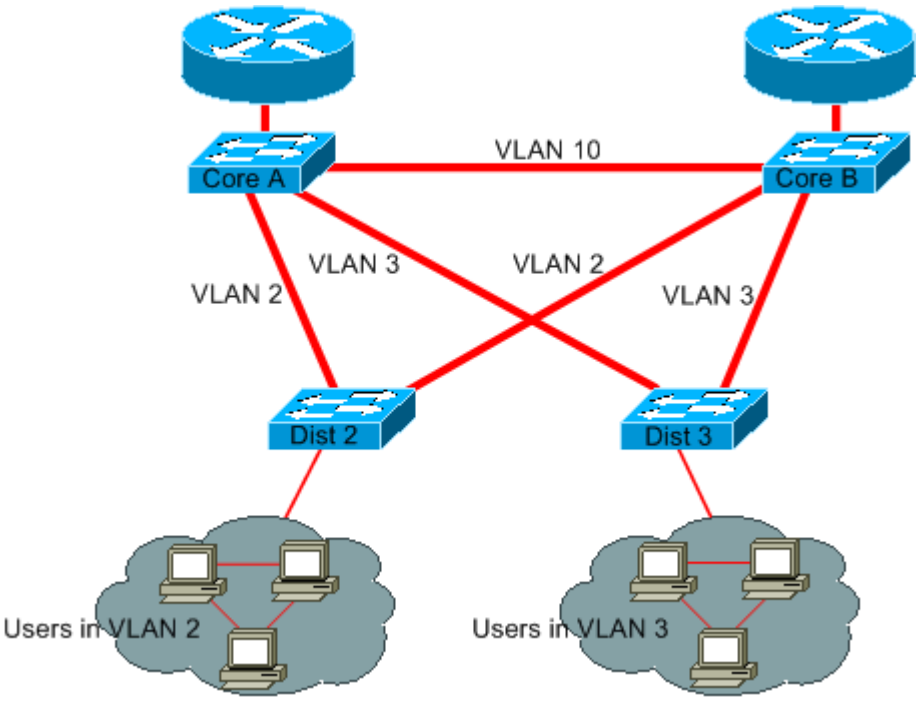
在此设计中，每个 VLAN 只阻塞了一个端口。此外，对于此设计，如果关闭 Core A 或 Core B，那么只需一步即可消除所有冗余链路。

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Cisco第3层交换机能够以与第2层交换功能相同的速度执行该功能。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。VLAN 2和VLAN 3不再桥接在核心A和核心B之间，因此STP环路无法穿过该路由边界。每个桥接VLAN内仍可能存在第2层环路。

- 冗余仍然存在，但现在依靠第 3 层路由协议。该设计使用第3层路由实现路径冗余。收敛时间取决于路由协议、故障检测机制、计时器、拓扑和平台。
- STP 不会再阻塞任何单个端口。因此，不可能再产生桥接环路。
- 没有速度损失，因为第3层交换离开VLAN的速度与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。管理VLAN中的广播、组播和控制平面流量可能会消耗CPU资源，具体取决于流量类型、平台、软件版本和控制平面配置。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。

在较早的版本中，思科实施中无法将VLAN 1从中继中删除。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Cisco IOS软件版本12.1(11b)E开始，您可以将VLAN 1从中继移除。VLAN 1仍然存在，但它可以提高安全性并减少不必要的第2层流量。

相关信息

- 思科支持工具目录
- 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）。