运行 Cisco IOS 软件的 Catalyst 6500/6000 系列和 Catalyst 4500/4000 系列交换机的最佳实践

目录

简介
开始使用前
背景
参考
基本配置
Catalyst 控制层面协议
VLAN 1
标准功能
VLAN 中继协议
快速以太网自动协商
千兆以太网自动协商
动态中继协议 (DTP)
生成树协议
EtherChannel
单向链路检测 (UDLD)
多层交换
巨型帧
Cisco IOS 软件安全功能
基本安全功能
AAA 安全服务
TACACS+
管理配置
网络图
交换机管理接口和本地 VLAN
带外管理
系统日志记录
SNMP
网络时间协议 (NTP)
Cisco 发现协议
配置清单
全局命令
接口命令
相关信息

简介

本文档提供在 Supervisor 引擎上运行 Cisco IOS® 软件的 Catalyst 6500/6000 和 4500/4000 系列交换机的最佳实践。

Catalyst 6500/6000 和 Catalyst 4500/4000 系列交换机支持在 Supervisor 引擎上运行的以下两个操作系统之一：

- Catalyst OS (CatOS)
- Cisco IOS 软件

对于 CatOS，可以选择在路由器子卡或模块上运行 Cisco IOS 软件，如：

- Catalyst 6500/6000 中的 Multilayer Switch Feature Card (MSFC)
- Catalyst 4500/4000 中的 4232 第 3 层 (L3) 模块

在此模式下，有以下两种配置命令行：

- 用于交换的 CatOS 命令行
- 用于路由的 Cisco IOS 软件命令行

CatOS 为系统软件，在 Supervisor 引擎上运行。如果选择在路由模块上运行 Cisco IOS 软件，则需要 CatOS 系统软件。

对于 Cisco IOS 软件来说，只有一种配置命令行。在此模式下，已将 CatOS 的功能集成到 Cisco IOS 软件中。通过该集成，能生成同时用于交换和路由配置的单个命令行。在此模式下，Cisco IOS 软件成为系统软件，它会替换 CatOS。

在重要网络中会同时部署 CatOS 和 Cisco IOS 软件操作系统。以下这些交换机系列支持 CatOS 以及针对路由器子卡和模块的 Cisco IOS 软件选项：

- Catalyst 6500/6000
- Catalyst 5500/5000
- Catalyst 4500/4000

以下这些交换机系列支持 Cisco IOS 系统软件：

- Catalyst 6500/6000
- Catalyst 4500/4000

有关 CatOS 的信息，请参阅文档运行 CatOS 配置和管理的 Catalyst 4500/4000、5500/5000 和 6500/6000 系列交换机的最佳实践，因为该文档涵盖了 Cisco IOS 系统软件。

Cisco IOS 系统软件向用户提供了以下一些优点：

- 单个用户接口
- 一个统一的网络管理平台
- 增强的 QoS 功能
- 分布式交换支持

本文档提供模块化配置指导。所以，您可以单独阅读每个部分，并采用分阶段方式进行更改。本文档假设读者基本理解和熟悉 Cisco IOS 软件用户界面。本文档未涉及总体园区网络设计。

开始使用前

背景

本文档提供的解决方案体现了多年来 Cisco 工程师在复杂网络领域以及与许多大型客户合作方面的实际工作经验。因此，本文档重点介绍实现网络成功运行的实际配置。本文档提供以下解决方案：

- 在统计上覆盖面最广因而风险最低的解决方案
- 通过牺牲一定程度的灵活性换取确定性结果的简单解决方案
- 易于管理的解决方案以及网络运营团队配置的解决方案
- 促进高可用性和高稳定性的解决方案

参考

在 Cisco.com 上，有很多有关 Catalyst 6500/6000 和 Catalyst 4500/4000 产品系列的参考网站。此部分列出的参考资料更深入地介绍了本文档所讨论的主题。

有关本文档所涵盖的任何主题的详细信息，请参阅LAN交换技术支持。该技术支持页提供产品文档以及有关故障排除和配置的文档。

本文档提供了公共联机参考材料以便您进一步阅读。不过，其他较好的基础和教育参考资料有：

- Cisco ISP 基本要素
- 比较 Cisco Catalyst 6500 系列交换机的 Cisco Catalyst 和 Cisco IOS 操作系统
- Cisco LAN 交换（CCIE 职业发展系列）
- 组建 Cisco 多层交换网络
- 性能和故障管理
- 安全:企业网络的安全蓝图
- Cisco 现场手册：Catalyst 交换机配置

基本配置

本部分讨论了当您使用大多数 Catalyst 网络时所部署的功能。

Catalyst 控制层面协议

本部分介绍正常操作情况下在交换机之间运行的协议。当您处理每个部分时，能够基本理解协议是很有帮助的。

Supervisor 引擎数据流

在 Catalyst 网络中启用的多数功能均需要两个或多个交换机进行协作。因此，必须能够控制保持连接消息、配置参数和管理更改的交换。无论这些协议是 Cisco 专用协议（如 Cisco 发现协议 (CDP)），还是基于标准的协议（如 IEEE 802.1D（生成树协议 [STP]）），在 Catalyst 系列上实施这些协议时都会存在一些共同因素。

在基本帧转发过程中，用户数据帧源自终端系统。该数据帧的源地址 (SA) 和目标地址 (DA) 在整个第二层 (L2) 交换域中不会更改。在每个交换机 Supervisor 引擎上的内容可寻址存储器 (CAM) 查找表由 SA 识别过程填充。这些表会指示哪个输出端口会转发所接收的每个帧。如果目标未知或帧被发往某个广播或多播地址，则不能完成地址识别过程。如果该过程未完成，帧将被转发（泛洪）到该 VLAN 中的所有端口。交换机也必须识别将通过系统对哪些帧进行交换，以及要将哪些帧定向到交换机 CPU 本身。交换机 CPU 也称为网络管理处理器 (NMP)。

将使用 CAM 表中的特殊条目来创建 Catalyst 控制层面。这些特殊条目称作系统条目。控制层面会

接收数据流，并将其定向到内部交换机端口上的 NMP 中。这样，通过结合使用协议与熟知的目标 MAC 地址，可从数据流中分离控制层面数据流。

正如本部分中的表所示，Cisco 具有保留的以太网 MAC 和协议地址范围。本文档详细介绍了每个保留地址，但是为方便起见，此表提供了一个概要：

功能	SNAP[1] HDLC[2] 协议类型	目标多播 MAC
PAgP[3]	0x0104	01-00-0c-cc-cc-cc
PVST+、RPVST+[4]	0x010b	01-00-0c-cc-cc-cd
VLAN 网桥	0x010c	01-00-0c-cd-cd-ce
UDLD [5]	0x0111	01-00-0c-cc-cc-cc
CDP	0x2000	01-00-0c-cc-cc-cc
DTP[6]	0x2004	01-00-0c-cc-cc-cc
STP UplinkFast	0x200a	01-00-0c-cd-cd-cd
IEEE 生成树 802.1D	N/A - DSAP[7] 42 SSAP[8] 42	01-80-c2-00-00-00
ISL[9]	不适用	01-00-0c-00-00-00
VTP[10]	0x2003	01-00-0c-cc-cc-cc
IEEE 暂停 802.3x	N/A - DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

[1] SNAP =子网访问协议。

[2] HDLC =高级数据链路控制。

[3] PAgP =端口聚合协议。

[4]个PVST+ =每VLAN生成树+,RPVST+ =快速PVST+。

[5] UDLD =单向链路检测。

[6] DTP =动态中继协议。

[7] DSAP =目的服务接入点。

[8] SSAP =源服务接入点。

[9] ISL =交换机间链路。

10 VTP = VLAN中继协议。

多数 Cisco 控制协议使用 IEEE 802.3 SNAP 封装，它包括逻辑链路控制 (LLC) 0xAAAA03 和组织唯一标识符 (OUI) 0x00000C。您可以在 LAN 分析器跟踪中看到此封装。

这些协议假定具有点对点连接。请注意，故意使用多播目标地址会使两台 Catalyst 交换机能够通过非 Cisco 交换机实现透明通信。不识别和拦截帧的设备只对其进行泛洪。然而，通过多供应商环境的点对多点连接可能导致不一致的行为。一般来说，应避免通过多供应商环境的点对多点连接。这些协议会在第三层路由器上终止，并仅在交换机域内运行。这些协议通过入口专用集成电路 (ASIC) 处理和计划接收高于用户数据的优先级。

现在让我们来了解一下 SA。交换机协议使用从可用地址段中取得的 MAC 地址。机箱上的 EPROM 提供该可用地址段。发出 **show module 命令，以显示每个模块在发送数据流（如 STP 网桥协议数据单元 (BPDU) 或 ISL 帧）时可以使用的地址范围。**下面是一个命令输出示例：

```
>show module
…

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------  -----------------
1   00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)      6.1(1d)
    00-01-c9-da-0c-1c to 00-01-c9-da-0c-1
    00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff
!--- These are the MACs for sourcing traffic.
```

VLAN 1

VLAN 1 在 Catalyst 网络中具有特殊意义。

当建立中继时，Catalyst Supervisor 引擎总是使用默认的 VLAN 即 VLAN 1，以便标记一定数量的控制和管理协议。此类协议包括 CDP、VTP 和 PAgP。默认情况下，包括内部sc0接口的所有交换机端口都配置为VLAN 1的成员。默认情况下，所有中继都承载VLAN 1。

为帮助明确 Catalyst 网络连接中常用的一些术语，需要了解以下定义：

- 管理 VLAN 是 sc0 针对 CatOS 和低端交换机所驻留的位置。您可以更改此 VLAN。当您同时将 CatOS 和 Cisco IOS 交换机互联时，请记住这一点。
- 本地 VLAN 是不建立中继时端口返回到的 VLAN。此外，本地 VLAN 也是 IEEE 802.1Q 中继上未标记的 VLAN。

有几个很有说服力的理由可以调整网络，并更改 VLAN 1 中的端口行为：

- 与所有其他 VLAN 一样，当 VLAN 1 的范围大得足以影响稳定性时（特别是从 STP 角度而言），便需要对该 VLAN 进行修剪。有关详细信息，请参阅交换机管理接口和本地 VLAN 部分。
- 您需要将 VLAN 1 上的控制层面数据与用户数据分开，以便简化故障排除并最大限度地使用 CPU 周期。当您设计不使用 STP 的多层园区网络时，请避免在 VLAN 1 中形成第二层环路。为了避免形成第二层环路，请手动从中继端口清除 VLAN 1。

总之，请注意有关中继的以下信息：

- CDP、VTP 和 PAgP 更新总是在带有 VLAN 1 标记的中继上转发。即使已将 VLAN 1 从中继清除，且它并非本地 VLAN，也是如此。如果清除用户数据的 VLAN 1，则该操作对仍使用 VLAN 1 发送的控制层面数据流没有影响。
- 在ISL中继上，DTP数据包在VLAN1上发送。即使VLAN 1已从中继中清除，并且不再是本征

VLAN，也是如此。在 802.1Q 中继上，DTP 数据包在本地 VLAN 中发送。即使本地 VLAN 已经从中继清除，也会出现这种情况。
- 在 PVST+ 中，除非 VLAN 1 已经从中继清除，否则会在通用生成树 VLAN 1 上以无标记的格式转发 802.1Q IEEE BPDU，以便与其他供应商互操作。无论本地 VLAN 配置如何，都是如此。对于所有其他 VLAN，将发送 Cisco PVST+ BPDU 并对其进行标记。有关详细信息，请参阅生成树协议部分。
- 802.1s 多生成树 (MST) BPDU 始终在 ISL 和 802.1Q 中继上的 VLAN 1 中发送。即使 VLAN 1 已经从中继清除，也会出现这种情况。
- 不要在 MST 网桥和 PVST+ 网桥之间的中继上清除或禁用 VLAN 1。但是，在已禁用 VLAN 1 的情况下，MST 网桥必须成为根，以便所有 VLAN 避免在根不一致状态下其边界端口的 MST 网桥安置。有关详细信息，请参阅了解多生成树协议 (802.1s)。

标准功能

本文档的此部分重点介绍所有环境都通用的基本交换功能。应当在客户网络中的所有 Cisco IOS 软件 Catalyst 交换设备上配置这些功能。

VLAN 中继协议

目的

VTP 域（也称为 VLAN 管理域）由通过中继互联的共享同一 VTP 域名的一个或多个交换机组成。VTP 旨在允许用户在一个或多个交换机上集中进行 VLAN 配置更改。VTP 会自动将这些更改传递到（网络）VTP 域中的所有其他交换机。您可以将交换机配置为仅在一个 VTP 域中。创建 VLAN 之前，请确定将在网络中使用的 VTP 模式。

操作概述

VTP 是第 2 层消息传递协议。VTP 在整个网络范围内管理 VLAN 的添加、删除和重命名，以维护 VLAN 配置的一致性。VTP 最大程度地减少了可能导致大量问题的配置错误和配置不一致。这些问题包括重复的 VLAN 名称、不正确的 VLAN 类型规范以及安全违规。

默认情况下，交换机处于 VTP 服务器模式以及无管理域状态。在交换机通过中继链路收到域的通告时，或者在配置管理域时，这些默认设置会发生更改。

VTP协议使用公认的以太网目的组播MAC(01-00-0c-cc-cc-cc)和SNAP HDLC协议类型0x2003在交换机之间通信。与其他固有协议类似，VTP也使用IEEE 802.3 SNAP封装，包括LLC 0xAAAA03和OUI0x00000C。您可以在 LAN 分析器跟踪中看到此封装。VTP 无法在非中继端口上工作。因此，在 DTP 将中继开启之前，不会发送消息。换句话说，VTP 是 ISL 或 802.1Q 的有效负载。

消息类型包括：

- 每 300 秒发送一次的概要通告
- 发生更改时的子集通告和请求通告
- 启用 VTP 修剪时的联结

服务器上每发生一次更改，VTP 配置修订号就加一，然后该表将在整个域中传播。

删除 VLAN 时，曾经是 VLAN 成员的端口进入 `inactive` 同样，如果处于客户端模式下的交换机无法在启动时从 VTP 服务器或另一个 VTP 客户端接收 VTP VLAN 表，将停用 VLAN 中除默认 VLAN

1 以外的所有端口。

您可以将大多数 Catalyst 交换机配置为在下列任一 VTP 模式下运行：

- 服务器 - 在 VTP 服务器模式下，您可以：创建 VLAN修改 VLAN删除 VLAN为整个 VTP 域指定其他配置参数，例如 VTP 版本和 VTP 修剪VTP 服务器向同一个 VTP 域中的其他交换机通告其 VLAN 配置。VTP 服务器还根据通过中继链路收到的通告，将其 VLAN 配置与其他交换机同步。VTP 服务器为默认模式。
- 客户端 - VTP 客户端与 VTP 服务器的行为方式相同。但是，您无法在 VTP 客户端上创建、更改或删除 VLAN。此外，重新启动后，客户端不会记住 VLAN，因为没有任何 VLAN 信息写入 NVRAM。
- 透明 — VTP 透明交换机不参加 VTP。VTP 透明交换机不通告其 VLAN 配置，并且不根据收到的通告同步其 VLAN 配置。但是，在 VTP 版本 2 中，透明交换机会转发它们在中继接口上收到的 VTP 通告。

功能	服务器	客户端	透明	关[1]
源 VTP 消息	Yes	Yes	无	—
监听 VTP 消息	Yes	Yes	无	—
创建 VLAN	Yes	无	是（仅在本地有意义）	—
记住 VLAN	Yes	无	是（仅在本地有意义）	—

[1] Cisco IOS软件没有使用关闭模式禁用VTP项。

下表是初始配置的概要：

功能	默认值
vtp domain name	Null
VTP 模式	服务器
VTP 版本	版本 1 已启用
VTP 修剪	禁用

在 VTP 透明模式下，仅忽略 VTP 更新。已知的 VTP 多播 MAC 地址从系统 CAM 中删除，系统 CAM 通常用于拾取控制帧并将它们发送到 Supervisor 引擎。由于协议使用多播地址，因此处于透明模式的交换机或其他供应商的交换机只是将帧泛洪到域中的其他 Cisco 交换机。

VTP 版本 2 (VTPv2) 包括此列表所描述的功能灵活性。但是，VTPv2 无法与 VTP 版本 1 (VTPv1) 互操作：

- 令牌环支持
- 未识别的 VTP 信息支持 - 现在，交换机传播它们无法解析的值。
- 与版本相关的透明模式 - 透明模式不再检查域名。这会启用在一个透明域中对多个域的支持。
- 版本号传播 — 如果所有交换机上都可以使用VTPv2，则只需配置一台交换机即可启用所有交换机。

有详细信息，请参阅[了解 VLAN 中继协议 (VTP)。]

Cisco IOS 软件中的 VTP 操作

在 CatOS 中进行配置更改后，这些更改会立即写入 NVRAM。相反，除非发出 **copy run start 命令，否则 Cisco IOS 软件不会将配置更改保存到 NVRAM。**VTP 客户端和服务器系统要求在没有用户干预的情况下，立即将来自其他 VTP 服务器的 VTP 更新保存到 NVRAM 中。默认 CatOS 操作符合 VTP 更新要求，但是 Cisco IOS 软件更新模型要求不同的更新操作。

为了满足这一变更，已作为一种立即保存 VTP 客户端和服务器的 VTP 更新的方法，将 VLAN 数据库引入用于 Catalyst 6500 的 Cisco IOS 软件中。在某些软件的版本中，此 VLAN 数据库在 NVRAM 中以单独文件的形式出现，称为 vlan.dat 文件。请检查您的软件版本，以确定是否需要 VLAN 数据库的备份。如果发出 **show vtp status 命令，则可以查看存储在 VTP 客户端或 VTP 服务器的 vlan.dat 文件中的 VTP/VLAN 信息。**

当您在这些系统中发出 **copy run start 命令时，整个 VTP/VLAN 配置没有保存到 NVRAM 中的启动配置文件。**这不适用于以 VTP 透明模式运行的系统。当您发出 **copy run start 命令时，VTP 透明系统将整个 VTP/VLAN 配置保存到 NVRAM 中的启动配置文件。**

在低于 Cisco IOS 软件版本 12.1(11b)E 的 Cisco IOS 软件版本中，只能通过 VLAN 数据库模式配置 VTP 和 VLAN。VLAN 数据库模式是不同于全局配置模式的一种模式。此配置要求的原因是，当您配置处于 VTP 服务器模式或 VTP 客户端模式的设备时，VTP 邻居可以通过 VTP 通告动态更新 VLAN 数据库。您不希望这些更新自动传播到配置。因此，VLAN 数据库和 VTP 信息没有存储到主配置中，而是存储到 NVRAM 中一个名为 vlan.dat 的文件中。

此示例演示如何在 VLAN 数据库模式下创建以太网 VLAN：

```
Switch#vlan database
Switch(vlan)#vlan 3
VLAN 3 added:
Name: VLAN0003
Switch(vlan)#exit
APPLY completed.
Exiting....
```

在 Cisco IOS 软件版本 12.1(11b)E 及更高版本中，可以通过 VLAN 数据库模式或全局配置模式配置 VTP 和 VLAN。在 VTP 服务器模式或 VTP 透明模式下，VLAN 的配置仍会更新 NVRAM 中的 vlan.dat 文件。但是，这些命令没有保存到配置中。因此，在运行配置中不显示这些命令。

有关详细信息，请参阅配置 VLAN[文档的全局配置模式下的 VLAN 配置部分。]

此示例演示如何在全局配置模式下创建以太网 VLAN 以及如何验证配置：

```
Switch#configure terminal
Switch(config#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config#vlan 3
Switch(config-vlan)#end
Switch#
OR
Switch#vlan database
Switch(vlan#vtp server
Switch device to VTP SERVER mode.
Switch(vlan#vlan 3
```

```
Switch(vlan#exit
APPLY completed.
Exiting....
Switch#
```

注意：VLAN配置存储在vlan.dat文件中，该文件存储在非易失性存储器中。要对配置执行完全备份，需要将 vlan.dat 文件与配置一起包含在备份中。之后，如果整个交换机或 Supervisor 引擎模块需要更换，网络管理员必须上载以下两个文件才能恢复完整配置：

- vlan.dat 文件
- 配置文件

VTP 和扩展 VLAN

扩展系统 ID 功能用于启用扩展范围 VLAN 标识。当扩展系统 ID 启用时，它会禁止将 MAC 地址池用于 VLAN 生成树，并保留单个 MAC 地址来标识交换机。Catalyst IOS 软件版本 12.1(11b)EX 和 12.1(13)E 为 Catalyst 6000/6500 引入扩展系统 ID 支持，以支持符合 IEEE 802.1Q 标准的 4096 个 VLAN。此功能是在用于 Catalyst 4000/4500 交换机的 Cisco IOS 软件版本 12.1(12c)EW 中引入的。这些 VLAN 分成了几个范围，每个范围可以有不同的用途。当您使用 VTP 时，其中一些 VLAN 会传播到网络中的其他交换机。扩展范围 VLAN 不传播，因此，您必须在每个网络设备上手动配置扩展范围 VLAN。在 Catalyst 操作系统中，此扩展系统 ID 功能与 MAC 地址缩减功能是等效的。

下表描述了 VLAN 范围：

VLAN	范围	使用率	是否通过 VTP 传播？
0、4095	预留	仅供系统使用。您看不到或无法使用这些 VLAN。	—
1	正常	Cisco 默认值。您可以使用此 VLAN，但是不能删除它。	Yes
2–1001	正常	适用于以太网 VLAN。可以创建、使用和删除这些 VLAN。	Yes
1002–1005	正常	FDDI 和令牌环的 Cisco 默认值。不能删除VLAN 1002-1005。	Yes
1006–4094	预留	仅适用于以太网 VLAN。	无

交换机协议使用从机箱上的 EPROM 提供的一系列可用地址中获取的 MAC 地址，作为在 PVST+ 和 RPVST+ 下运行的 VLAN 的网桥标识符的一部分。Catalyst 6000/6500 和 Catalyst 4000/4500 交换机支持 1024 个或 64 个 MAC 地址，具体取决于机箱类型。

默认情况下，具有 1024 个 MAC 地址的 Catalyst 交换机不启用扩展系统 ID。MAC 地址按顺序分配，范围中的第一个 MAC 地址分配给 VLAN 1，范围中的第二个 MAC 地址分配给 VLAN 2，等等。这使交换机可以支持 1024 个 VLAN，每个 VLAN 使用唯一的网桥标识符。

机箱类型	机箱地址
WS-C4003-S1、WS-C4006-S2	1024

WS-C4503、WS-C4506	64 1
WS-C6509-E、WS-C6509、WS-C6509-NEB、WS-C6506-E、WS-C6506、WS-C6009、WS-C6006、OSR-7609-AC、OSR-7609-DC	10 24
WS-C6513、WS-C6509-NEB-A、WS-C6504-E、WS-C6503-E、WS-C6503、CISCO7603、CISCO7606、CISCO7609、CISCO7613	64 1

[1]具有64个MAC地址的机箱默认启用扩展系统ID，且无法禁用该功能。

有关详细信息，*请参阅配*置STP和IEEE 802.1s MST的了解网桥ID部分。

对于具有 1024 个 MAC 地址的 Catalyst 系列交换机，启用扩展系统 ID 能够支持在 PVST+ 下运行的 4096 个 VLAN 或 16 个 MISTP 实例具有唯一标识符，而不增加交换机上所需的 MAC 地址的数量。扩展系统 ID 将 STP 需要的 MAC 地址数量从每个 VLAN 或 MISTP 实例一个减少到每台交换机一个。

下图显示了未启用扩展系统 ID 时的网桥标识符。该网桥标识符包括 2 字节的网桥优先级和 6 字节的 MAC 地址。

扩展系统 ID 修改网桥协议数据单元 (BPDU) 的生成树协议 (STP) 网桥标识符部分。 原始的 2 字节优先级字段拆分成 2 个字段；4 位网桥优先级字段和允许 VLAN 编号范围为 0-4095 的 12 位系统 ID 扩展。

当在 Catalyst 交换机上启用扩展系统 ID 以有效利用扩展范围 VLAN 时，需要在同一个 STP 域内的所有交换机上启用该功能。为了保持 STP 根计算在所有交换机上一致，这是必需的设置。启用扩展系统 ID 后，根网桥优先级就变为 4096 的倍数与 VLAN ID 之和。因为没有扩展系统 ID 的交换机对其网桥 ID 的选择更加精细，所以这些交换机可能会在无意中声明根。

虽然建议在同一个 STP 域内维护一致的扩展系统 ID 配置，但是将具有 64 个 MAC 地址的新机箱引入 STP 域时，在所有网络设备上强制扩展系统 ID 是不切实际的。但是，请务必了解当两个系统配置为相同的生成树优先级时，没有扩展系统 ID 的系统的生成树优先级更高。要启用扩展系统 ID 配置，请发出以下命令：

spanning-tree extend system-id

内部 VLAN 从 VLAN 1006 开始，按升序顺序分配。为了避免在用户 VLAN 和内部 VLAN 之间发生冲突，建议在分配用户 VLAN 时尽可能接近 VLAN 4094。要显示内部分配的 VLAN，请在交换机上发出命令 **show vlan internal usage。**

```
Switch#show vlan internal usage
```

```
VLAN Usage
---- --------------------
1006 online diag vlan0
1007 online diag vlan1
1008 online diag vlan2
1009 online diag vlan3
1010 online diag vlan4
1011 online diag vlan5
1012 PM vlan process (trunk tagging)
1013 Port-channel100
1014 Control Plane Protection
1015 L3 multicast partial shortcuts for VPN 0
1016 vrf_0_vlan0
1017 Egress internal vlan
1018 Multicast VPN 0 QOS vlan
1019 IPv6 Multicast Egress multicast
1020 GigabitEthernet5/1
1021 ATM7/0/0
1022 ATM7/0/0.1
1023 FastEthernet3/1
1024 FastEthernet3/2
------deleted------
```

在本地 IOS 中，可以配置 **vlan internal allocation policy descending，以便内部 VLAN 按降序分配**。CatOS 软件的等效 CLI 不受官方支持。

vlan internal allocation policy descending

Cisco 配置建议

当 Catalyst 6500/6000 处于 VTP 服务器模式时，即使没有 VTP 域名，也可以创建 VLAN。在运行 Cisco IOS 系统软件的 Catalyst 6500/6000 交换机上配置 VLAN 之前，请先配置 VTP 域名。按此顺序进行配置可以维护与运行 CatOS 的其他 Catalyst 交换机的一致性。

对于使用 VTP client/server 模式，还是使用 VTP transparent 模式，没有具体的建议。尽管本部分中说明了一些注意事项，某些用户还是更喜欢 VTP 客户端/服务器模式管理的方便性。建议在每个域中放置两个 server 模式交换机以实现冗余，一般为两个分布层交换机。将域中的其余交换机设置为客户端模式。在使用 VTPv2 实现客户端/服务器模式时，请记住在同一个 VTP 域中始终接受较高的修订版号。如果在 VTP 客户端或服务器模式下配置的交换机引入 VTP 域且具有高于现有 VTP 服务器的修订版号，则这会覆盖 VTP 域中的 VLAN 数据库。如果配置更改是无意的且已删除 VLAN，则此覆盖可能会导致网络发生严重中断。为了确保客户端或服务器交换机始终具有低于服务器的配置修订版号，请将客户端 VTP 域名更改为除标准名称之外的某个名称，然后再恢复为标准名称。此操作会将客户端上的配置修订版号设置为 0。

可以方便地在网络上更改 VTP，这一点有利也有弊。出于以下这些原因，许多企业更喜欢谨慎的方法并使用 VTP 透明模式：

- 这种做法支持良好的更改控制，因为修改交换机或中继端口上的 VLAN 的要求每次只能考虑一台交换机。
- VTP 透明模式限制发生管理员错误（例如意外删除 VLAN）的风险。此类错误会影响整个域。
- VLAN可以从中继修剪到不含有属于该VLAN 端口的交换机上。这会使帧泛洪更为高效地利用带宽。手动修剪还会减小生成树直径。有关详细信息，请参阅动态中继协议部分。每台交换机 VLAN 配置也鼓励采用这种做法。
- 不存在将具有较高 VTP 修订版号的新交换机引入网络中会覆盖整个域 VLAN 配置的风险。
- 园区管理器3.2支持Cisco IOS软件VTP透明模式，该模式是CiscoWorks2000的一部分。之前要

求您在VTP域中至少拥有一台服务器的限制已被删除。

VTP 命令	备注
vtp domain name	CDP 检查名称，以帮助防止在域之间布线错误。域名区分大小写。
vtp mode {server |客户端 |透明	VTP 以三种模式中的一种运行。
vlan *vlan_number*	这会使用提供的 ID 创建 VLAN。
switchport trunk allowed *vlan_range*	这是一个接口命令，它使中继可以根据需要传输 VLAN。默认为所有 VLAN。
switchport trunk pruning *vlan_range*	这是一个接口命令，它通过手动修剪（例如在中继上从分布层修剪到 VLAN 不存在的接入层）来限制 STP 直径。默认情况下，所有 VLAN 都适合修剪。

其他选项

VTPv2 是实现令牌环环境的一个要求，在该环境中强烈建议使用 client/server 模式。

本文档的 Cisco 配置建议部分将介绍为减少不必要的帧泛洪而修剪 VLAN 的好处。**vtp pruning 命令会自动修剪 VLAN，从而在不需要帧的情况下停止帧的无效泛洪。**

注意：与手动VLAN修剪不同，自动修剪不会限制生成树直径。

IEEE 产生了一个基于标准的体系结构，以实现类似于 VTP 的结果。作为 802.1Q 通用属性注册协议 (GARP) 的成员，通用 VLAN 注册协议 (GVRP) 允许供应商之间的 VLAN 管理互操作性。不过，GVRP 超出了本文档的讨论范围。

注意：Cisco IOS软件没有VTP关闭模式功能，它仅支持VTPv1和VTPv2修剪功能。

快速以太网自动协商

目的

自动协商是 IEEE 802.3u 快速以太网 (FE) 标准的可选功能。自动协商使设备能够通过链路自动交换有关速度和双工功能的信息。自动协商运行在第 1 层 (L1)。 该功能面向分配给临时用户或设备所连接到的网络区域的端口。示例包括接入层交换机和集线器。

操作概述

自动协商使用改进版链路完整性测试，可由 10BASE-T 设备用来协商速度以及交换其他自动协商参

数。原始的 10BASE-T 链路完整性测试称为正常链路脉冲 (NLP)。 10/100 Mbps 自动协商所使用的改进版链路完整性测试称为快速链路脉冲 (FLP)。 10BASE-T 设备期望在链路完整性测试中每 16 (+/-8) 毫秒发送一次突发脉冲。10/100 Mbps 自动协商的 FLP 每 16 (+/-8) 毫秒发送一次突发脉冲，每 62.5 (+/-7) 微秒发送一次其他脉冲。突发序列中的脉冲会生成代码字，用于链路伙伴之间的兼容性交换。

在 10BASE-T 中，每当一个站点开启，就会发出一个链路脉冲。这是每 16 毫秒发送一次的单个脉冲。10BASE-T 设备还在链路空闲时每 16 毫秒发送一次链路脉冲。这些链路脉冲也称为检测信号或 NLP。

100BASE-T 设备发出 FLP。此脉冲作为突发而不是一个脉冲发出。突发在2毫秒内完成，每16毫秒重复一次。在初始化时，设备将16位FLP消息传输到链路伙伴，以协商速度、双工和流量控制。将重复发送该 16 位消息，直到伙伴确认该消息为止。

注意：根据IEEE 802.3u规范，您不能手动配置一个链路伙伴以实现100-Mbps全双工，并且仍然可以与另一个链路伙伴自动协商到全双工。尝试配置一个链路伙伴进行 100 Mbps 全双工通信而与其他链路伙伴进行自动协商会导致双工不匹配。导致双工不匹配的原因是，一个链路伙伴进行自动协商而看不到来自其他链路伙伴的任何自动协商参数。第一个链路伙伴于是默认为半双工。

所有 Catalyst 6500 以太网交换模块都支持 10/100 Mbps 和半双工或全双工。要在其他 Catalyst 交换机上验证此功能，请发出 **show interface capabilities 命令。**

10/100 Mbps 以太网链路上产生性能问题的最常见原因之一是链路上的一个端口在半双工状态下运行，而另一个端口在全双工状态下运行。当您重置链路上的一个或全部两个端口而自动协商过程不会使两个链路伙伴都使用相同配置时，会偶尔发生这种情况。当您重新配置链路的一端而忘记重新配置另一端时，也会发生这种情况。通过以下操作，可避免发出有关性能的支持呼叫：

- 创建一个策略，该策略需要为所有非临时设备的必要行为配置端口
- 使用适当的更改控制方法强制实施该策略

性能问题的典型症状是增加交换机上的帧校验序列 (FCS)、循环冗余校验 (CRC)、校准或残帧计数器。

在半双工模式下，您有一条接收线和一条传输线。不能同时使用这两条线。当接收端有一个数据包时，设备不能进行传输。

在全双工模式下，接收和传输使用同一条线。但是，可以同时使用这两条线，因为已禁用载波监听和冲突检测功能。设备可以同时进行传输和接收。

因此，半双工与全双工的连接可以正常工作，但是在半双工一端会有大量冲突，导致性能下降。冲突发生的原因是配置为全双工的设备可以在接收数据的同时进行传输。

此列表中的文档详细讨论了自动协商。这些文档说明了自动协商的工作原理并讨论了各种配置选项：

- 对以太网 10/100/1000 Mb 半双工/全双工自动协商进行配置和故障排除
- 排除 Cisco Catalyst 交换机的 NIC 兼容性问题

对自动协商的一种常见误解是：可以手动配置一个链路伙伴进行 100 Mbps 全双工通信，并与其他链路伙伴自动协商进行全双工通信。实际上，尝试执行此操作会导致双工不匹配。这是因为，一个链路伙伴进行自动协商而看不到来自其他链路伙伴的任何自动协商参数，便会默认设置为半双工。

大多数 Catalyst 以太网模块支持 10/100 Mbps 和半双工/全双工。不过，可以通过发出 **show interface *mod/port* capabilities *命令来确认这一点。***

FEFI

远端故障指示 (FEFI) 可防止 100BASE-FX（光纤）和千兆接口出现与物理层/信令相关的故障，而自动协商则防止 100BASE-TX（铜缆）出现与物理层/信令相关的故障。

远端故障是一个站点可以检测而另一个站点无法检测的链路中的错误。断开的传输线就是一个示例。在本示例中，发送站点仍接收有效数据，并通过链路完整性监视器检测链路是否良好。但是，发送站点不能检测到另一个站点无法接收传输。检测到这样一个远程故障的 100BASE-FX 站点可以修改其传输的 IDLE 流，以发送特殊的位模式，从而将该远程故障通告邻居。该特殊位模式称为 `FEFI-IDLE` `FEFI-IDLE (errDisable)` 有关防止故障的详细信息，请参阅本文档的单向链路检测 (UDLD) 部分。

以下模块/硬件支持 FEFI：

- Catalyst 6500/6000 和 4500/4000：所有 100BASE-FX 模块和 GE 模块

Cisco 基础架构端口建议

无论是在 10/100 Mbps 链路上配置自动协商，还是对速度和双工进行硬编码，最终都取决于链路伙伴的类型或您已连接到 Catalyst 交换机端口的终端设备的类型。终端设备和 Catalyst 交换机之间的自动协商一般都进行得很好，并且 Catalyst 交换机符合 IEEE 802.3u 规范。但是，当网络接口卡 (NIC) 或供应商交换机不完全符合规范时，会出现问题。另外，在适用于 10/100 Mbps 自动协商的 IEEE 802.3u 规范中未描述的特定于供应商的高级功能会导致硬件不兼容以及其他问题。这些高级功能类型包括自动极性变换和布线完整性。本文档提供一个示例：

- 现场警报：Intel Pro/1000T NIC 连接到 CAT4K/6K 时的性能问题

在某些情况下，需要设置主机、端口速度和双工。一般来说，请完成下列基本故障排除步骤：

- 确保链路两端都配置了自动协商，或者链路两端都配置了硬编码。
- 查看发行版本注释了解一般注意事项。
- 验证您运行的 NIC 驱动程序或操作系统的版本。通常需要最新的驱动程序或修补程序。

通常，首先将自动协商用于任意一种类型的链路伙伴。为临时设备（如便携式计算机）配置自动协商有显而易见的好处。自动协商还适用于其他设备，例如：

- 适用于非临时设备，例如服务器和固定工作站
- 交换机之间
- 从交换机到路由器

但是，出于本部分所提及的一些原因，可能出现协商问题。有关这些情况的基本故障排除步骤，请参阅对以太网 10/100/1000 Mb 半双工/全双工自动协商进行配置和故障排除。

针对以下对象禁用自动协商：

- 支持网络基础架构设备（如交换机和路由器）的端口
- 其他非临时终端系统，例如服务器和打印机

始终对这些端口的速度和双工设置进行硬编码。

为速度和双工（通常是 100 Mbps 全双工）手动配置下列 10/100 Mbps 链路配置：

- 交换机到交换机
- 交换机到服务器

- 交换机到路由器

如果 10/100 Mbps 以太网端口上的端口速度设置为自动，则会自动协商速度和双工。要将端口设置为自动，请发出以下接口命令：

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
!--- This is the default.
```

要配置速度和双工，请发出下列接口命令：

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed {10 | 100 | auto}
Switch(config-if)#duplex {full | half}
```

Cisco 接入端口建议

终端用户、移动工作者和临时主机需要自动协商，以便最大程度地减少对这些主机的管理。您可以使自动协商同样适用于 Catalyst 交换机。通常需要最新的 NIC 驱动程序。

要启用端口速度的自动协商，请发出下列全局命令：

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
```

注意：如果在10/100-Mbps以太网端口上将端口速度设置为auto，则速度和双工都会自动协商。您无法更改自动协商端口的双工模式。

当 NIC 或供应商的交换机不完全符合 IEEE 规范 802.3u 时，会出现问题。另外，在适用于 10/100 Mbps 自动协商的 IEEE 802.3u 规范中未描述的特定于供应商的高级功能会导致硬件不兼容以及其他问题。此类高级功能包括自动极性变换和布线完整性。

其他选项

当禁用交换机之间的自动协商时，某些问题的第 1 层故障指示也可能丢失。请使用第 2 层协议（如主动 UDLD）来加强故障检测。

即使在启用了自动协商时，自动协商也不会检测下列情况：

- 端口阻塞，不接收，也不传输
- 线路的一端开启，但另一端关闭
- 光缆连线错误

因为这些问题不发生在物理层，所以自动协商无法检测到这些问题。这些问题可能导致 STP 环路或流量黑洞。

如果在链路两端都配置了 UDLD，则 UDLD 可以检测到所有这些情况，并对链路的两个端口执行 errdisable 命令。这样，UDLD 可防止 STP 环路和流量黑洞。

千兆以太网自动协商

目的

千兆以太网 (GE) 有一个自动协商过程，该过程比用于 10/100 Mbps 以太网 (IEEE 802.3z) 的过程应用更为广泛。 对于 GE 端口，自动协商用于交换：

- 流控制参数
- 远程故障信息
- 双工信息**注意**：Catalyst系列GE端口仅支持全双工模式。

IEEE 802.3z 已被 IEEE 802.3:2000 规范取代。有关详细信息，请参阅本地和城域网+草案(LAN/MAN 802s)标准订用 。

操作概述

与 10/100 Mbps FE 的自动协商不同的是，GE 自动协商不涉及协商端口速度。另外，您不能通过发出 **set port speed 命令禁用自动协商。**默认情况下会启用 GE 端口协商，GE 链路两端的端口必须具有相同设置。如果链路各端的端口设置不一致（这表示交换的参数不同），那么该链路不会接通。

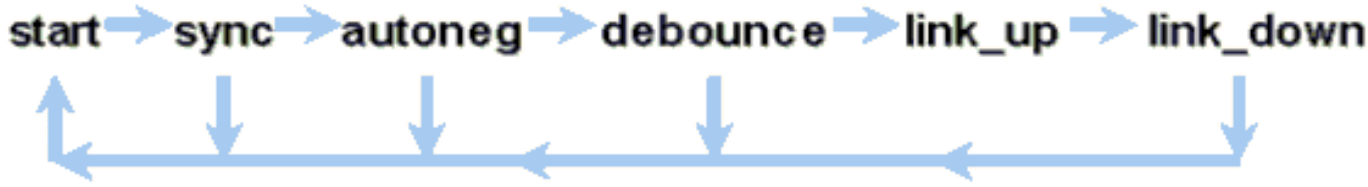
例如，假设有两台设备，A和B。每台设备都可以启用或禁用自动协商。下表列出了可能的配置及其各自的链路状态：

协商	B 启用	B 禁用
A 启用	up	A 为 down，B 为 up
A 禁用	A 为 up，B 为 down	up

在 GE 中，在通过使用特殊的保留链路代码字序列启动链路时，将执行同步和自动协商（如果它们已启用）。

注意：有一个有效单词的词典，并非所有可能的单词在GE中都有效。

可以用以下方式描述 GE 连接的生存期特征：



丢失同步操作意味着 MAC 检测到链路断开。不管是启用还是禁用自动协商，都可能丢失同步操作。在某些出现故障的情况下，例如连续收到三个无效字，将丢失同步操作。如果此情况持续 10 毫秒，则会断定发生了同步失败情况，并且链路更改为 link_down 在丢失同步操作后，需要另外三个连续的有效空闲才能再次执行同步。其他灾难性事件（例如无法收到 (Rx) 信号）会导致链路断开事件。

自动协商是链路连通过程的一部分。当链路连通时，将结束自动协商。但是，交换机仍将监视链路的状态。如果端口上禁用自动协商，则不可能存在“autoneg”阶段。

GE 铜缆规范 (1000BASE-T) 支持通过“下页交换”进行自动协商。“下页交换”允许对铜缆端口上的 10/100/1000 Mbps 速度进行自动协商。

注意：但是，GE光纤规范仅对双工、流量控制和远程故障检测的协商进行了规定。GE 光纤端口不会对端口速度进行协商。有关自动协商的详细信息，请参阅IEEE 802.3-2002规 范的第28和37节。

同步重启延迟是一项软件功能，用来控制自动协商的总时间。如果自动协商在此时间内不成功，固件会重新启动自动协商，以防出现死锁。**sync-restart-delay 命令仅在自动协商设置为启用时有效。**

Cisco 基础架构端口建议

在 GE 环境中配置自动协商比在 10/100 Mbps 环境中配置自动协商重要得多。仅在以下情况下禁用自动协商：

- 在与不支持协商的设备连接的交换机端口上
- 因为互操作性问题导致连接问题时

在所有交换机到交换机的链路中以及通常所有 GE 设备中启用千兆协商。千兆接口上的默认值是自动协商。但是，仍请发出以下命令确保启用自动协商：

```
switch(config)#interface type slot/port
switch(config-If)#no speed
!--- This command sets the port to autonegotiate Gigabit parameters.
```

一个已知的例外情况是：当连接到运行低于 Cisco IOS 软件版本 12.0(10)S、且已添加流控制和自动协商功能的 Cisco IOS 软件的千兆交换路由器 (GSR) 时。在此情况下，请关闭这两个功能。如果不关闭这两个功能，交换机端口将报告没有连接，GSR 将报告错误。以下是示例接口命令序列：

```
flowcontrol receive off
flowcontrol send off
speed nonegotiate
```

Cisco 接入端口建议

因为 FLP 可能因供应商的不同而有所不同，您必须根据具体情况分别查看交换机到服务器的连接。Cisco 客户在 Sun、HP 和 IBM 服务器上遇到过一些与千兆协商有关的问题。如果 NIC 供应商没有特别另行规定，则所有设备将使用千兆自动协商功能。

其他选项

流控制是 802.3x 规范的可选部分。如果使用流控制，则必须对其进行协商。设备可能能够，也可能不能够发送和/或响应 PAUSE 帧（众所周知的 MAC 01-80-C2-00-00-00 0F）。 并且设备可能不同意远端邻居的流控制请求。如果端口的输入缓冲区即将填满，它将向链路伙伴发送一个 PAUSE 帧。链路伙伴将停止传输，并将任何其他帧保存到链路伙伴输出缓冲区中。此功能不能解决任何状态稳定的超额订阅问题。但是，该功能可以在整个突发传输过程中有效增大输入缓冲区，增大幅度为伙伴的输出缓冲区的一部分。

PAUSE 功能旨在防止设备（交换机、路由器或者终端站）由于短期瞬时数据流超载导致的缓冲区溢出情形，而不必要地丢弃收到的帧。对于已出现数据流超载情形的设备，当设备发送一个 PAUSE 帧时，可防止内部缓冲区溢出。PAUSE 帧包含表示全双工伙伴在发送更多数据帧之前应等待的时长的参数。接收 PAUSE 帧的伙伴在指定的时间段内停止发送数据。在此计时器到期时，站点将从刚才停止的地方重新开始发送数据帧。

发出 PAUSE 的站点可以发出包含零时间参数的另一个 PAUSE 帧。此操作可以取消剩余的暂停时

间。因此，一个最近接收的 PAUSE 帧可覆盖当前正在进行的所有 PAUSE 操作。并且，发出 PAUSE 帧的站点可以延长 PAUSE 周期。该站点可在第一个 PAUSE 周期到期之前，发出包含非零时间参数的另一个 PAUSE 帧。

此 PAUSE 操作不是基于速率的流控制。该操作是一种简单的开始-停止机制，允许传输数据流的设备（即发送 PAUSE 帧的设备）有机会缓解其缓冲区拥塞现象。

此功能最适用于接入端口和终端主机之间的链路，在这些链路中，主机输出缓冲区与其虚拟内存的大小可能相同。在交换机到交换机的链路中使用此功能受益有限。

发出以下接口命令可在交换机端口上实现此控制：

```
flowcontrol {receive | send} {off | on | desired}
```

```
>show port flowcontrol

 Port  Send FlowControl    Receive FlowControl   RxPause TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ------- -------
 6/1   off      off        on       on           0       0
 6/2   off      off        on       on           0       0
 6/3   off      off        on       on           0       0
```

注意：所有Catalyst模块都会响应PAUSE帧（如果协商）。由于某些模块（例如 WS-X5410 和 WS-X4306）是无阻塞模块，因此它们永远不会发送 PAUSE 帧，即使它们协商要执行此操作。

动态中继协议 (DTP)

目的

为了在设备之间扩展 VLAN，中继可临时识别和标记（本地链路）原始以太网帧。此操作使帧能够在单个链路中实现多路复用。此操作也确保了能在交换机之间维护单独的 VLAN 广播域和安全域。CAM 表用于维护交换机范围内的帧到 VLAN 映射。

操作概述

DTP 是第二代动态 ISL (DISL)。DISL 只支持 ISL。DTP 支持 ISL 和 802.1Q。此支持可确保中继两端的交换机对中继帧的不同参数达成协议。此类参数包括：

- 配置的封装类型
- Native VLAN
- 硬件功能

DTP 支持还有助于防止由无中继端口导致的已标记帧的泛洪，从而避免潜在的严重安全风险。因为 DTP 可确保端口及其邻居状态一致，因此可防止发生此类泛洪。

中继模式

DTP 是用于在交换机端口及其邻居之间协商配置参数的第 2 层协议。DTP使用另一个众所周知的组播MAC地址01-00-0c-cc-cc-cc和SNAP协议类型0x2004。下表介绍了每种可能的DTP协商模式的功能：

模式	功能	是否传输 DTP 帧？	最终状态（本地端口）
Dynamic Auto CatOS Auto	使端口愿意将链路转换为中继。如果邻接端口设置为 on desirable	是，定期	
Trunk CatOS ON	将端口置于永久 trunking 模式，并通过协商把链路转换成中继。该端口成为中继端口，即使其邻接端口不同意此更改。	是，定期	Trunking，无条件
Nonegotiate	将端口置于永久 trunking 模式，但是不允许端口生成 DTP 帧。必须将邻接端口手动配置为中继端口，才能建立中继链路。这对不支持 DTP 的设备非常有用。	无	Trunking，无条件
Dynamic desirable CatOS desirable	使端口主动尝试将链路转换成中继链路。如果邻接端口设置为 on、desirable 或 auto 模式，那么该端口将变成中继端口。	是，定期	仅当远程模式为 on、auto 或 desirable 时，才会最终处于 trunking
	将端口置于永久 non-trunking 模式，然后通过协商将链路转换成非中继链路。该端口成为非中继端口，即使其邻接端口不同意此更改。	在稳定状态下不会传输，但从 on 模式更改至其他模式后，会传输通知以加快远程终端检测。	

注意：可以设置或协商ISL和802.1Q封装类型。

在默认配置中，DTP 假定链路具有以下特性：

- 点对点连接和 Cisco 设备支持仅采用点对点连接的 802.1Q 中继端口。

- 在 DTP 协商中，端口不会参与 STP。仅在端口类型已成为以下三种类型之一后，才会将该端口添加到 STP：接入ISL802.1QPAgP 是端口加入 STP 之前将要运行的下一个进程。PAgP 用于 EtherChannel 自动协商。
- VLAN 1 总是存在于中继端口上。如果端口在ISL模式下中继，则DTP数据包在VLAN 1上发出。如果端口在ISL模式下不中继，则DTP数据包在本征VLAN上发送（对于802.1Q中继或非中继端口）。
- DTP 数据包传输 VTP 域名，以及中继配置和管理状态。VTP 域名必须匹配才能连通协商中继。协商期间将每秒发送一次这些数据包；协商之后将每 30 秒发送一次这些数据包。如果在

```
auto  desirable  5  5  DTP
```

注意：您必须了解模式TRUNK、nonegotiate和访问**明确指定端口的最终状态。**错误的配置可能导致一端是中继而另一端不是中继的危险/不一致状态。

有关 ISL 的更多详细信息，请参阅在 Catalyst 5500/5000 和 6500/6000 系列交换机上配置 ISL 中继。有关 802.1Q 的更多详细信息，请参阅使用 802.1Q 封装和 Cisco CatOS 系统软件在 Catalyst 4500/4000、5500/5000 和 6500/6000 系列交换机之间建立中继。

封装类型

ISL 操作概述

ISL 是 Cisco 的专有中继协议（VLAN 标记方案）。ISL 已被采用了许多年。相比之下，802.1Q 要新得多，但 802.1Q 是 IEEE 标准。

ISL 将原始帧完全封装在两层标记方案中。通过这种方式，ISL 实际上是一种隧道协议，并且还具有能够传送非以太网帧的优点。ISL 向标准以太网帧添加了 26 字节的报头和 4 字节的 FCS。配置为中继的端口预期的是更大的以太网帧，并可进行相应处理。ISL 支持 1024 个 VLAN。

帧格式 - ISL 标记被遮蔽

40 Bits	4 Bits	4 Bits	48 Bits	16 Bits	24 Bits	24 Bits	15 Bits	1 Bit	16 Bits	16 Bits
DA	Type	USER	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	INDEX	Reserve
01-00-0c-00-00					AAAA03	00000C				

Encapsulated Frame	FCS
Variable length	32 bits

有关详细信息，请参阅交换机间链路和 IEEE 802.1Q 帧格式。

802.1Q 操作概述

虽然 IEEE 802.1Q 标准只适合以太网，但该标准规定了更多远超过封装类型的应用。802.1Q 包括通用属性注册协议 (GARP) 的以下几种功能：生成树增强和 802.1p QoS 标记。有关详细信息，请参阅 IEEE 标准在线。

802.1Q 帧格式将保留原始的以太网 SA 和 DA。但是，交换机现在肯定会预期收到小巨型帧，即使在主机使用标记来表示 QoS 信令的 802.1p 用户优先级的接入端口上，也是如此。802.1Q 标记为 4 个字节。802.1Q 以太网 v2 帧包含 1522 个字节（IEEE 802.3ac 工作组取得的成果）。802.1Q 还支持对 4096 个 VLAN 的空间进行编号。

传输和接收的所有数据帧都带有 802.1Q 标记，但本地 VLAN 上的数据帧除外。在这种情况下，存在基于交换机输入端口配置的隐式标记。本地 VLAN 上的帧始终以无标记方式传输，并且通常以无标记方式接收。但是，也可以以带标记方式接收这些帧。

有关详细信息，请参阅以下文档：

- VLAN 互操作性
- 使用 802.1q 封装和 Cisco CatOS 系统软件，在 Catalyst 4500/4000、5500/5000 和 6500/6000 系列交换机之间建立中继

802.1Q/802.1p 帧格式

		Tag Header						
		TPID	TCI					
48 bits	48 bits	16 bits	3 bits	1 bit	12 bits	16 bits	Variable length	32 bits
DA	SA	TPID	Priority	CFI	VLAN ID	Length/ Type	Data with PAD	FCS
		0x8100	0 – 7	0-1	0-4095			

Cisco 配置建议

Cisco 设计的一条主要原则是在可能一致的网络中尽力保持一致性。所有较新的 Catalyst 产品均支持 802.1Q，而部分产品只支持 802.1Q（例如 Catalyst 4500/4000 和 Catalyst 6500 系列的早期模块）。所以，所有新的实施应遵从此 IEEE 802.1Q 标准并且应逐渐从 ISL 迁移较旧的网络。

发出此接口命令可启用特定端口上的 802.1Q 中继：

```
Switch(config)#interface type slot#/port#
Switch(config-if)#switchport
!--- Configure the interface as a Layer 2 port. Switch(config-if)#switchport trunk encapsulation
dot1q
```

IEEE 标准允许供应商执行互操作。随着支持 802.1p 的新型主机 NIC 和设备的问世，供应商互操作性将有利于所有 Cisco 环境。虽然 ISL 和 802.1Q 实施方案非常不错，但 IEEE 标准最终会得到更广泛的应用，并获得更多的第三方技术支持，包括网络分析程序的支持。并且，一个次要的考虑事项是 802.1Q 标准还具有比 ISL 更低的封装开销。

对于完整性而言，本地 VLAN 上的隐式标记会产生安全问题。可能在不经过路由器的情况下，将帧从一个 VLAN，即 VLAN X，传输到另一个 VLAN，即 VLAN Y。如果源端口 (VLAN X) 与同一台交换机上 802.1Q 中继的本地 VLAN 处于同一 VLAN 内，那么在没有路由器的情况下也能发生传输。解决方法是为中继的本地 VLAN 使用虚拟 VLAN。

发出下列接口命令，建立一个 VLAN 以作为特定端口上 802.1Q 中继的本地（默认）VLAN：

```
Switch(config)#interface type slot#/port#
Switch(config-If)#switchport trunk native vlan 999
```

由于所有更新的硬件均支持 802.1Q，因此所有新的实施方案遵守 IEEE 802.1Q 标准，并且逐步从 ISL 迁移旧的网络。目前，许多 Catalyst 4500/4000 模块已不支持 ISL。因此，802.1Q 是以太网中继的唯一选择。请参阅 CatOS 的 **show interface capabilities** 命令或 show port capabilities 命令的输出。由于中继支持需要相应的硬件，因而不支持 802.1Q 的模块永远无法支持 802.1Q。不能通过软件升级提供 802.1Q 支持。Catalyst 6500/6000 和 Catalyst 4500/4000 交换机的大多数新硬件均支持 ISL 和 802.1Q。

如果VLAN 1从中继中清除，如交换机管理接口和本征VLAN部分所讨论，虽然未传输或接收用户数据，但NMP仍在VLAN 1上传递控制协议。控制协议的示例包括CDP和VTP。

并且，如 VLAN 1 部分所讨论的，在建立中继时，CDP、VTP 和 PAgP 数据包始终通过 VLAN 1 发送。采用 dot1q (802.1Q) 封装时，如果交换机的本地 VLAN 发生更改，这些控制帧将带有 VLAN 1 标记。如果交换机上到路由器和本地 VLAN 的 dot1q 中继已经发生改变，则需要使用 VLAN 1 中的子接口，以便接收带标记的 CDP 帧，并在路由器上提供 CDP 邻居可见性。

注意：dot1q可能会考虑本征VLAN的隐式标记引起的安全问题。可能将帧从一个 VLAN 传输到另外一个 VLAN，而不经过路由器。有关更多详细信息，请参阅入侵检测 FAQ。 解决方法是对不用于最终用户访问的中继本地 VLAN 使用 VLAN ID。大多数 Cisco 客户只需将 VLAN 1 保留为中继上的本地 VLAN，并将接入端口指定到除 VLAN 1 以外的 VLAN 即可实现此目标。

Cisco 建议在两端采用显式中继模式配置 `dynamic desirable`此模式是默认模式。在此模式中，网络操作员可以信任端口为 `up trunking syslog` 此模式与 `on` 另外，在链路的一端无法成为中继或丢弃中继状态的情况下，`desirable`

如果多台交换机之间使用 DTP 就封装类型进行协商，并且如果因为两端都支持 ISL 而默认优先选择了 ISL，那么必须发出此接口命令以指定 dot1q1：

```
switchport trunk encapsulation dot1q
```

[1]包括WS-X6548-GE-TX和WS-X6148-GE-TX的某些模块不支持ISL中继。这些模块不接受命令 **switchport trunk encapsulation *dot1q***。

注意：发出**switchport mode access**命令以禁用端口上的中继。此禁用有助于在启动主机端口时避免浪费协商时间。

```
Switch(config-if)#switchport host
```

其他选项

另一个常见的用户配置是在分配层使用 `dynamic desirable` `dynamic auto` 某些交换机（如 Catalyst 2900XL、Cisco IOS 路由器或其他供应商设备）目前不支持通过 DTP 进行中继协商。对于这些设备，您可以使用 `nonegotiate` 此模式有助于标准化整个园区的通用设置。

当您连接到 Cisco IOS 路由器时，Cisco 建议使用 `nonegotiate`在整个桥接过程中，从配置为 **switchport mode trunk 的端口接收的一些 DTP 帧可能返回到中继端口。**交换机端口接收到 DTP 帧后，它将尝试重新协商，而这种重新协商并非并要。为了重新协商，交换机端口将中继置于 `down up` 如果已启用 `nonegotiate DTP`

```
switch(config)#interface type slot#/port#
switch(config-if)#switchport mode dynamic desirable
!--- Configure the interface as trunking in desirable !--- mode for switch-to-switch links with
multiple VLANs. !--- And... switch(config-if)#switchport mode trunk
!--- Force the interface into trunk mode without negotiation of the trunk connection. !--- Or...
switch(config-if)#switchport nonegotiate
!--- Set trunking mode to not send DTP negotiation packets !--- for trunks to routers.
switch(config-if)#switchport access vlan vlan_number
!--- Configure a fallback VLAN for the interface. switch(config-if)#switchport trunk native vlan
999
!--- Set the native VLAN. switch(config-if)#switchport trunk allowed vlan vlan_number_or_range
!--- Configure the VLANs that are allowed on the trunk.
```

生成树协议

目的

生成树在冗余交换网络和网桥网络中维护一个无环路的第 2 层环境。没有 STP，帧会无限循环并/或倍增。这将导致网络崩溃，因为高流量将中断广播域中的所有设备。

从某些方面来看，STP 是较早的协议，最初是针对基于软件的慢速网桥规范 (IEEE 802.1D) 开发的。 但是要在具有以下功能的大型交换网络中成功实施，STP 可能变得非常复杂：

- 多个 VLAN
- 一个域中具有多台交换机
- 支持多家供应商
- 较新的 IEEE 增强功能

Cisco IOS 系统软件已经针对 STP 的新改进做出了调整。新 IEEE 标准（包括 802.1w 快速 STP 和 802.1s 多生成树 (MST) 协议）可提供快速收敛、负载共享和控制层面缩放。另外，STP 增强功能（如根保护、BPDU 过滤、Portfast BPDU 防护和环路防护）提供了额外的保护，可防止出现第 2 层转发环路。

PVST+ 操作概述

在每个 VLAN 中，选择具有最小根网桥标识符 (BID) 的交换机作为根网桥。 BID 由网桥优先级和交

换机 MAC 地址组合而成。

首先，从所有交换机发送 BPDU，这些 BPDU 包含每台交换机的 BID 和到达该交换机的路径成本。这可以确定根网桥和到根的成本最低的路径。从根发送的 BPDU 中传送的其他配置参数将覆盖本地配置的参数，以使整个网络采用一致的计时器。对于交换机从根接收的每个 BPDU，Catalyst 中央 NMP 都会处理和外发一个包含根信息的新 BPDU。

然后，通过以下步骤来收敛拓扑：

1. 为整个生成树域选择一个根网桥。
2. 在每个非根网桥上选择一个根端口（面对根网桥）。
3. 选择一个指定端口，以便在每个网段中转发 BPDU。
4. 非指定端口将被阻塞。

有关详细信息，请参阅以下文档：

- 配置 STP 和 IEEE 802.1s MST
- 了解快速生成树协议 (802.1w)

基本计时器默认值	名称	功能
2 秒	hello	控制 BPDU 的发出。
15 秒	转发延迟 (Fwd delay)	控制端口在 `listening  learning`
20 秒	maxage	控制交换机在寻找备用路径之前保持当前拓扑的时间。最大老化 (maxage) 时间过后，交换机会认为 BPDU 已过期，并从阻塞端口池中寻找新的根端口。如果没有任何阻塞端口可用，则交换机将在指定端口上将其自身声明为根。

Cisco 建议不要更改计时器，因为此操作可能对稳定性产生负面影响。不要调整已部署的大多数网络。可通过命令行（如 hello-interval、maxage 等）访问的一些简单 STP 计时器，包括繁多的其他所采用的计时器和固有计时器。因此，很难调整计时器和考虑所有分歧。此外，您可能会破坏 UDLD 保护。有关详细信息，请参阅单向链路检测 (UDLD)部分。

STP 计时器注释：

默认 STP 计时器值是基于这样的条件计算得出的，假定网络直径为 7 台交换机（从根到网络边缘 7 次交换机跳跃），时间为 BPDU 从根网桥传送到网络中边缘交换机（7 次跳跃）所需的时间。对于大多数网络而言，此假定计算均为可接受的计时器值。但是，您可以将这些计时器更改为更为合适的值，以缩短整个网络拓扑更改的收敛时间。

您可以使用特定 VLAN 的网络直径配置根网桥，并且相应地计算计时器值。如果必须进行更改

，Cisco 建议仅在 VLAN 的根网桥上配置直径和可选的 hello 时间参数。

```
spanning-tree vlan vlan-id [root {primary | secondary}] [diameter diameter-value [hello hello-time]]
!--- This command needs to be on one line.
```

此宏使指定 VLAN 的交换机根基于指定的直径和 hello 时间计算新的计时器值，并且将配置 BPDU 中的此信息传播到拓扑结构中的所有其他交换机。

新的端口状态和端口角色部分介绍了 802.1D STP，并且将 802.1D STP 与快速 STP (RSTP) 进行了比较和对比。 有关 RSTP 的详细信息，请参阅了解快速生成树协议 (802.1w)。

新的端口状态和端口角色

802.1D 采用以下四种不同的端口状态进行定义：

- 倾听
- 学习
- 阻塞
- 转发

有关详细信息，请参阅端口状态部分的表。端口的状态为混合状态（无论是阻塞还是转发流量），端口在活动拓扑中的作用（根端口、指定端口等等）也同样是多重的。 例如，从可运行角度看，blocking 状态的端口和 listening 状态的端口之间没有任何差异。这两种状态均丢弃帧，并且不能获知 MAC 地址。实际区别在于生成树分配给端口的角色。您可以放心地这样假设：监听端口为指定端口或根端口，并且正在进入 forwarding 状态。遗憾地是，一旦端口进入 forwarding 状态，就无法从端口状态推断端口是根端口还是指定端口。这一点凸显了此基于状态的术语的不足之处。RSTP 将端口的角色和状态拆分开来，从而解决了这一不足。

端口状态

STP 802.1D 中的端口状态

端口状态	方法	到下一状态的默认计时
	以管理方式关闭。	
	接收 BPDU 并且终止用户数据。	监控 BPDU 接收。等待 20 秒（以使 maxage 过期）或立即更改（如果检测到直接/本地链路故障）。
	发送或接收 BPDU 以检查是否需要返回到 blocking 状态。	等待 15 秒的 Fwddelay。
	生成拓扑/CAM 表。	等待 15 秒的 Fwddelay。
	发送/接收数据。	

基本拓扑更改时间总计：

- 如果等待 maxage 过期，则时间为 20 + 2 (15) = 50 秒

- 直接链路发生故障，则为 30 秒

RSTP 中仅保留了三种端口状态，分别对应于三种可能的运行状态。802.1D状态已禁用、阻塞和侦听已合并到唯一的802.1w丢弃状态。

STP (802.1D) 端口状态	RSTP (802.1w) 端口状态	端口是否包括在活动拓扑中？	端口是否可获知 MAC 地址？
禁用	丢弃	无	无
阻塞	丢弃	无	无
倾听	丢弃	Yes	无
学习	学习	Yes	Yes
转发	转发	Yes	Yes

端口角色

现在，角色是分配到给定端口的一个变量。根端口和指定端口的角色仍然保留，而阻塞端口的角色现已拆分为备用端口和替代端口角色。生成树算法 (STA) 根据 BPDU 确定端口的角色。对于 BPDU，请记住这一点以使工作简化：总有方法比较任意两个 BPDU 并决定哪一个更有用。判断依据为 BPDU 中存储的值，有时则根据接收 BPDU 的端口。本部分的余下内容阐述了确定端口角色的非常实用的方法。

根端口角色

网桥上接收最佳 BPDU 的端口即是根端口。就路径成本而言，根端口是最接近根网桥的端口。STA 在整个桥接网络（每个 VLAN）中选择一个根网桥。 根网桥发送的 BPDU 比任何其他网桥能够发送的 BPDU 都更有用。根网桥是该网络中唯一没有根端口的网桥。所有其他网桥在至少一个端口上接收 BPDU。

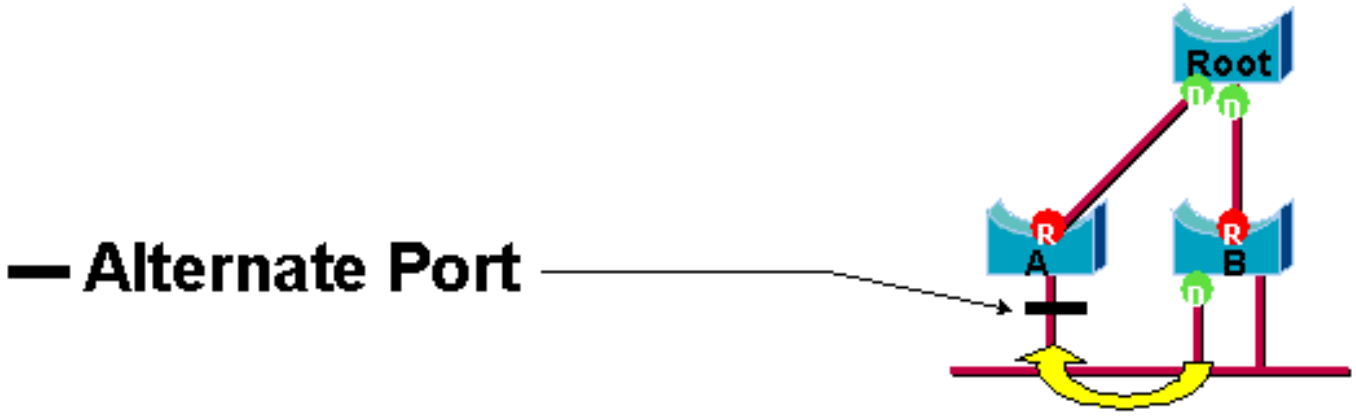
指定端口角色

如果端口可以在它所连接到的网段上发送最佳 BPDU，则它是指定端口。802.1D 网桥将不同网段（例如以太网段）链接在一起，以创建桥接域。在给定的网段上，只能有一条路径通往根网桥。如果有两条路径，则网络中会有桥接环路。连接到给定网段的所有网桥将监听其他网桥的 BPDU，并且同意将发送最佳 BPDU 的网桥作为网段的指定网桥。该网桥上对应的端口为指定端口。

替代端口和备份端口角色

这两个端口角色对应于 802.1D 的阻塞状态。阻塞端口定义为不是指定端口或根端口的端口。阻塞端口收到的 BPDU 比其在网段上发送的 BPDU 更有用。请记住，端口必须接收 BPDU 才能保持阻塞状态。为此，RSTP 引入了这两个角色。

备用端口是因从另一个网桥接收更有用的 BPDU 而被阻塞的端口。下图对此作了说明：



备份端口是因从它所在网桥接收更有用的 BPDU 而被阻塞的端口。下图对此作了说明：

在 802.1D 内部已实现了这种区分。这实质上是 Cisco UplinkFast 的工作原理。其基本原理是备用端口提供指向根网桥的备用路径。因此，如果根端口发生故障，此端口可取代根端口。当然，备份端口可提供到同一网段的冗余连接，但不能保证到根网桥的替代连接。因此，已从上行链路组中排除了备份端口。

因此，RSTP 针对与 802.1D 使用相同标准的生成树计算最终拓扑。在使用不同网桥和端口优先级的方式上没有任何变化。“阻塞”这一名称用于描述 Cisco 实施中的丢弃状态。CatOS 7.1 版及更高

版本仍然显示监听和学习状态，这会提供有关某个端口的更多信息，这些信息量超过了 IEEE 标准的要求。然而，新特点是协议已为端口确定的角色现在与端口的当前状态之间存在差异。例如，现在端口可以同时是指定端口和阻塞端口。然而这种情况持续的时间一般非常短，它仅意味着此端口正处于转换到指定转发状态的过渡状态。

STP 与 VLAN 相互作用

可以采用三种不同的方法将 VLAN 与生成树相关联：

- 所有 VLAN 一个生成树，或通用生成树协议 (CST)，如 IEEE 802.1D
- 基于每个 VLAN 的生成树，或共享生成树，例如 Cisco PVST
- 每组 VLAN 一个生成树，或多生成树 (MST)，如 IEEE 802.1s

从配置的角度而言，由于这三种生成树模式涉及与 VLAN 交互，因此可以将它们配置为以下三种模式之一：

- **pvst - 每个 VLAN 一个生成树。**这实际上是实施 PVST+，但在 Cisco IOS 软件中却简单地记为 PVST。
- **rapid-pvst** - 802.1D标准的发展可缩短收敛时间，并融合了UplinkFast和BackboneFast基于标准的(802.1w)属性。
- **mst** — 这是每组VLAN或MST生成树的802.1s标准。还在该标准内引入了 802.1w 快速组件。

针对所有 VLAN 的单一生成树仅允许一个活动拓扑，因此无法实现负载均衡。STP 阻塞端口会阻塞所有 VLAN 并且不会传送数据。

每个 VLAN 或 PVST+ 一个生成树，允许负载均衡，但随着 VLAN 数量的增加，需要更多的 BPDU CPU 处理工作。

新的 802.1s 标准 (MST) 支持定义多达 16 个活动的 STP 实例/拓扑，并支持将所有 VLAN 映射到这些实例。在典型的园区环境中，仅需定义两个实例。此技术允许 STP 扩展到数千个 VLAN，同时支持负载均衡。

在适用于 Catalyst 6500 的 Cisco IOS 软件版本 12.1(11b)EX 和 12.1(13)E 中引入了对 Rapid-PVST 和预标准 MST 的技术支持。配备 Cisco IOS 软件版本 12.1(12c)EW 及更高版本的 Catalyst 4500 支持预标准 MST。适用于 Catalyst 4500 平台的 Cisco IOS 软件版本 12.1(19)EW 中增加了快速 PVST 支持。适用于 Catalyst 6500 的 Cisco IOS 软件版本 12.2(18)SXF 和适用于 Catalyst 4500 系列交换机的 Cisco IOS 软件版本 12.2(25)SG 支持符合标准的 MST。

有关详细信息，请参阅了解快速生成树协议 (802.1w) 和了解多个生成树协议 (802.1s)。

生成树逻辑端口

Catalyst 4500 和 6500 发行版本注释在每个交换机的生成树中提供了逻辑端口数指导。所有逻辑端口的总数等于交换机上的中继数乘以中继上活动 VLAN 的数量，再加上交换机上非中继接口的数量。如果逻辑接口的最大数超出限制，则 Cisco IOS 软件将生成系统日志消息。建议逻辑接口的数量不要超过建议的指导数。

下表将各种 STP 模式和 Supervisor 类型支持的逻辑端口数进行了比较：

监控程序	PVST+	RPVST+	MST
Catal	每个交换模块	每个交换模块总计	每个交换模块共

yst 6500 Supervisor 1	总计6,000 1个1,200个	6,000个1,200个	25,000个3,000个2,000个
Catalyst 6500 Supervisor 2	每个交换模块总计18002个，共13000个	每个交换模块共1,800 2个，共10,000个	每个交换模块共50,000个6,000个2个
Catalyst 6500 Supervisor 720	每个交换模块总计1,800 2个13,000个	每个交换模块共1,800 2个，共10,000个	每个交换模块共50,003个6,000 2个，
Catalyst 4500 Supervisor II plus	共 1,500 个	共 1,500 个	共 25,000 个
Catalyst 4500 Supervisor II plus-10GE	共 1,500 个	共 1,500 个	共 25,000 个
Catalyst 4500 Supervisor IV	共 3,000 个	共 3,000 个	共 50,000 个
Catalyst 4500 Supervisor V	共 3,000 个	共 3,000 个	共 50,000 个
Catalyst 4500 Supervisor V	共 3,000 个	共 3,000 个	共 80,000 个

10GE			

[1]早于Cisco IOS软件版本12.1(13)E的PVST+支持的逻辑端口总数最大为4,500。

[2] 10 Mbps、10/100 Mbps和100 Mbps交换模块最多支持每个模块1,200个逻辑接口。

[3]在Cisco IOS软件版本12.2(17b)SXA之前，MST支持的最大逻辑端口总数为30,000。

建议

在未获得诸如硬件、软件、设备数和 VLAN 数之类的详细信息的情况下提供生成树模式建议是很困难的。通常，如果逻辑端口数没有超出建议的指导数，建议采用 Rapid PVST 模式部署新网络。Rapid PVST 模式提供快速网络收敛，无需进行其他配置，如 Backbone Fast 和 Uplink Fast。发出以下命令可在快速 PVST 模式下设置生成树：

```
spanning-tree mode rapid-pvst
```

其他选项

在同时具有过时硬件和较旧版本的软件的网络中，建议采用 PVST+ 模式。发出以下命令可在 PVST+ 模式下设置生成树：

```
spanning-tree mode pvst
----This is default and it shows in the configuration.
```

对于设计时包含大量 VLAN 的网络，建议为 VLAN 启用 MST 模式。对于此网络，逻辑端口的总数可以超出 PVST 和 Rapid-PVST 的指导数。发出以下命令可在 MST 模式下设置生成树：

```
spanning-tree mode mst
```

BPDU 格式

为支持 IEEE 802.1Q 标准，Cisco 扩展了现存的 PVST 协议，以提供 PVST+ 协议。PVST+ 增加了对 IEEE 802.1Q 单一生成树区域间链路的支持。PVST+ 与 IEEE 802.1Q 单一生成树和现存的 Cisco PVST 协议均兼容。另外，PVST+ 增加了检查机制，以确保交换机间的端口中继和 VLAN ID 不存在配置不一致情况。PVST+ 是与 PVST 兼容的即插即用式协议，不需要新的命令行接口 (CLI) 命令或配置。

下面是 PVST+ 协议运行理论的一些要点：

- PVST+ 与 802.1Q 单一生成树交互操作。PVST+ 通过 802.1Q 中继与公共 STP 上符合 802.1Q 的交换机交互操作。默认情况下，公共生成树位于 VLAN 1（本地 VLAN）。一个公共生成树 BPDU 是通过 IEEE 标准网桥组 MAC 地址（01-80-c2-00-00-00，协议类型为 0x010c）在 802.1Q 链路间进行发送或接收的。公共生成树可以在 PVST 或单一生成树区域中找到。
- PVST+ 通过隧道在 802.1Q VLAN 区域中以多播数据的形式传输 PVST BPDU。对于中继上的每个 VLAN，通过 Cisco 共享生成树协议 (SSTP) MAC 地址 (01-00-0c-cc-cd) 发送或接收

BPDU。对于与 Port VLAN 标识符 (PVID) 相同的 VLAN，BPDU 不带标记。对于所有其他 VLAN，BPDU 带标记。
- PVST+ 通过 ISL 中继与 PVST 上的现有 Cisco 交换机向后兼容。ISL 封装 BPDU 是通过 ISL 中继发送或接收的，这与以前的 Cisco PVST 相同。
- PVST+ 检查端口和 VLAN 的不一致性。PVST+ 会阻塞接收不一致 BPDU 的端口，以防止发生转发环路情况。PVST+ 还就任何不一致情况通过 syslog 消息通知用户。

注意：在ISL网络中，所有BPDU都使用IEEE MAC地址发送。

Cisco 配置建议

默认情况下，所有 Catalyst 交换机均启用 STP。即使您选择不包含第 2 层环路的设计并且不启用 STP，以便积极地维护阻塞端口，也得出于以下原因启用该功能：

- 如果存在环路，STP 可防止问题因多播数据和广播数据而变得更糟。通常，未进行修补、电缆故障或其他原因可导致形成环路。
- STP 可防止 EtherChannel 损坏。
- 大多数网络配置有 STP，因此可以获得最大的覆盖面。更多的暴露一般等同于更多的稳定代码。
- STP 可防止双连接 NIC 行为不当（或者在服务器上启用桥接）。
- 许多协议与代码中的 STP 紧密相关。示例包括：PAgPInternet 组消息协议 (IGMP) 监听中继如果在没有 STP 的情况下运行，可能会得到意外结果。
- 在报告的网络中断期间，Cisco 工程师通常建议不要在故障的核心位置使用 STP（如果一切都可以想到）。

为了在所有的 VLAN 上启用生成树，请发出以下全局命令：

```
Switch(config)#spanning-tree vlan vlan_id
!--- Specify the VLAN that you want to modify. Switch(config)#default spanning-tree vlan vlan_id
!--- Set spanning-tree parameters to default values.
```

不要更改计时器，这可能会对稳定性产生负面影响。不要调整已部署的大多数网络。可通过命令行访问的简单的 STP 计时器（如 hello 间隔和 maxage）有一组复杂的其他假定和固有计时器。因此，在您尝试调整计时器和考虑所有可能的后果时，可能会遇到很大困难。此外，您可能会破坏 UDLD 保护。

理想情况下，禁止在管理 VLAN 上传输用户流量。这不适用于 Catalyst 6500/6000 Cisco IOS 交换机。尽管如此，您仍需要在可能具有单独的管理接口的小型终端 Cisco IOS 交换机和 CatOS 交换机上考虑采纳此建议，并需要与 Cisco IOS 交换机集成。尤其是对于较旧的 Catalyst 交换机处理器，确保管理 VLAN 中不存在用户数据，以避免 STP 出现问题。行为不当的终端站可能会使 Supervisor 引擎处理器忙于处理广播数据包，以致可能漏掉一个或多个 BPDU。然而，较新的交换机拥有更强大 CPU 和扼杀控件，可以解除您的这一顾虑。有关详细信息，请参阅本文档的交换机管理接口和本地 VLAN 部分。

请勿过度设计冗余。这可能导致产生过多的阻塞端口，并且会给长期稳定性造成负面影响。保持总 SPT 直径不超过 7 跳。只要 Cisco 多层模型设计可行，请尽可能使用 Cisco 多层模型设计。模型功能：

- 较小的交换域
- STP 三角
- 确定性阻塞端口

影响并且知道根功能和阻塞端口所在的位置。记录有关拓扑图的此信息。了解您的生成树拓扑，这

对于故障排除工作至关重要。进行 STP 故障排除时首先应从阻塞端口开始。通常，根本原因分析关键在于对从阻塞状态变为转发状态的原因的分析。由于这些层被视为网络的最稳定部分，因此选择分布层和核心层作为根/辅助根所在的位置。检查最佳的第 3 层和热备用路由器协议 (HSRP) 是否由第 2 层数据转发路径覆盖。

此命令是用于配置网桥优先级的宏。根将优先级设置为远远低于默认值 (32,768)，辅助根将优先级设置为适当低于默认值：

```
Switch(config)#interface type slot/port
Switch(config)#spanning-tree vlan vlan_id root primary
!--- Configure a switch as root for a particular VLAN.
```

注意：此宏将根优先级设置为：

- 8192（默认值）
- 当前根优先级减 1（如果已知另一个根网桥）
- 当前根优先级（如果其 MAC 地址在当前根之下）

从中继端口修剪不必要的 VLAN，这是双向实施。此操作会限制不需要特定 VLAN 的网络部分的 STP 直径和 NMP 处理开销。VTP 自动修剪功能不会从中继中删除 STP。您还可以从中继中删除默认 VLAN 1。

有关其他信息，请参阅生成树协议问题及相关设计注意事项。

其他选项

Cisco 有另一个名为 **VLAN 网桥**的 STP 协议，它是通过使用已知目标 MAC 地址 01-00-0c-cd-cd-ce 和协议类型 0x010c 而运行的。

如果需要 VLAN 之间不可路由的网桥或传统协议不影响在这些 VLAN 上运行的 IEEE 生成树实例，则此协议特别有用。如果非桥接数据流的 VLAN 接口阻塞第 2 层数据流，覆盖的第 3 层数据流也会无意中被删除，这是一个我们不希望看到的负面影响。如果非桥接数据流的 VLAN 接口与 IP VLAN 参与相同的 STP，则此第 2 层阻塞会很容易发生。VLAN 网桥是桥接协议的 STP 的一个单独的实例。协议提供可以操作而不会影响 IP 数据流的单独的拓扑。

如果 Cisco 路由器（如 MSFC）上的 VLAN 之间需要桥接，请运行 VLAN 网桥协议。

STP PortFast 功能

您可以使用 PortFast 绕过在接入端口上正常的生成树操作。PortFast 可加快终端站与它们在链路初始化后需要连接的服务之间的连接。Microsoft DHCP 实施需要在链路状态升级后立即看到处于 `forwarding` `IP` 某些协议（如，互联网分组交换 (IPX)/序列分组交换 (SPX)）需要在链路状态升级后立即看到处于 `forwarding` `(GNS)`

有关详细信息，请参阅使用 PortFast 和其他命令解决工作站启动连接延迟问题。

PortFast 操作概述

PortFast 跳过正常 STP `listening`、learning 和 forwarding 状态。在发现链路连通后，该功能将端口直接从 `blocking` `forwarding` 如果未启用此功能，STP 将丢弃所有用户数据，直到确定端口已准备好转入 `forwarding` 该过程可能会长达 (2 x ForwardDelay) 的时间，默认情况下是 30 秒。

Portfast learning forwarding STP (TCN)TCN 是正常的。但是，大量 TCN 发送到根网桥时，可能会不必要地延长收敛时间。大量 TCN 通常发生在早晨，这时许多人打开 PC。

Cisco 接入端口配置建议

将所有已启用主机端口的 STP PortFast 设置为 on同时，将未使用的交换机-交换机链路和端口的 STP PortFast 显式设置为 off

在接口配置模式下输入 **switchport host 宏命令以实现接入端口的建议配置。**该配置还可以大幅提高自动协商和连接性能：

```
switch(config)#interface type slot#/port#

switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
!--- This macro command modifies these functions.
```

注意：PortFast并不表示在端口上完全不运行生成树。仍然发送、接收和处理 BPDU。LAN 要完全发挥作用，生成树是非常重要的。在没有循环检测和阻塞的情况下，环路可以无意中迅速造成整个 LAN 故障。

并且，禁用所有主机端口的中继和信道。默认情况下，会为建立中继和开辟信道而启用各个接入端口，但不会有意将相邻交换机放在主机端口上。如果任由这些协议协商，则随后端口激活中的延迟将导致不希望出现的情况。不会转发来自工作站的初始数据包，例如 DHCP 和 IPX 请求。

使用此命令在全局配置模式中默认配置 PortFast 是一个更好的选项：

```
Switch(config)#spanning-tree portfast enable
```

然后，在所有仅在一个 VLAN 中具有集线器或交换机的接入端口上，使用 **interface 命令禁用每个接口上的 PortFast 功能：**

```
Switch(config)#interface type slot_num/port_num
Switch(config-if)#spanning-tree portfast disable
```

其他选项

PortFast BPDU 防护提供一种防止环路的方法。在非中继端口上接收到 BPDU 时，BPDU 防护将该端口转换为 errDisable

在正常情况下，在为 PortFast 配置的接入端口上不会收到任何 BPDU 数据包。流入 BPDU 表明配置无效。最佳操作是关闭该接入端口。

Cisco IOS 系统软件提供一个有用的全局命令，该命令能够在任何已启用 UplinkFast 的端口上自动启用 BPDU-ROOT-GUARD*请始终 使用此命令*。该命令基于每台交换机运行，而不是基于每个端口。

发出此全局命令以启用 BPDU-ROOT-GUARD：

```
Switch(config)#spanning-tree portfast bpduguard default
```

如果端口关闭，简单网络管理协议 (SNMP) 陷阱或系统日志消息会通知网络管理员。您也可以为 `errDisabled` 有关更多详细信息，请参阅本文档的单向链路检测 (UDLD) 部分。

有关更多详细信息，请参阅生成树 PortFast BPDU 防护增强功能。

注意：Cisco IOS软件版本12.1(11b)E中引入了中继端口的PortFast。中继端口的 PortFast 旨在增加第 3 层网络的收敛时间。当您使用此功能时，请务必禁用每个接口上的 BPDU 防护和 BPDU 过滤器。

UplinkFast

目的

UplinkFast 提供在网络接入层中发生直接链路故障以后进行快速 STP 收敛的功能。UplinkFast 在不修改 STP 的情况下运行。其目的是加快特定情况下的收敛时间，使之减少到三秒以下，而不是通常的 30 秒延迟。请参阅了解和配置 Cisco UplinkFast 功能。

操作概述

通过在接入层使用 Cisco 多层设计模型，如果转发上行链路丢失，阻塞的上行链路将立即转换到 `forwarding` 该功能不用等待 `listening  learning`

上行链路组是每个 VLAN 上的一组端口，可以将其视为根端口和备用根端口。通常情况下，根端口确保从接入层到根的连通性。如果由于任何原因此主根连接失败，可以立即使用备用根链路，而无需经过通常为 30 秒的收敛延迟。

由于 UplinkFast 有效绕过正常 STP 拓扑改变处理过程（`listening  learning`该机制需要使用本地终端站能够通过备用路径到达的信息来更新域中的交换机。因此，运行 UplinkFast 的接入层交换机也可为其 CAM 表中的每个 MAC 地址生成帧，并发送到众所周知的多播 MAC 地址（01-00-0c-cd-cd-cd HDLC 协议 0x200a）。 此过程使用新拓扑更新域中所有交换机中的 CAM 表。

Cisco 建议

如果运行 802.1D 生成树，Cisco 建议您对带有阻塞端口的接入交换机启用 UplinkFast。如果没有获得备用根链路（通常是 Cisco 多层设计中的分布和核心交换机）的隐含拓扑信息，请勿在交换机上使用 UplinkFast。一般来说，请勿在使用超过两种方式传出网络的交换机上启用 UplinkFast。如果交换机在一个复杂接入环境中，并且有多个链路阻塞和一个链路转发，请避免在交换机上使用此功能，或咨询您的高级服务工程师。

发出以下全局命令以启用 UplinkFast：

```
Switch(config)#spanning-tree uplinkfast
```

Cisco IOS 软件中的此命令不会自动将所有网桥优先级值调整为高值。相反，该命令只更改那些使用尚未手动更改为某个其他值的网桥优先级的 VLAN。另外，不同于 CatOS，当您恢复已启用 UplinkFast 的交换机时，请使用该命令的 no 形式 (**no spanning-tree uplinkfast**) 将所有更改的值恢复到其默认值。所以，当您使用此命令时，*必须 在前后检查网桥优先级的当前状态，以确保达到预期结果。*

注意：启用协**议过**滤功能时，需要UplinkFast命令的all protocols关键字。当启用协议过滤时，由于 CAM 记录协议类型以及 MAC 和 VLAN 信息，所以必须为每个 MAC 地址上的每个协议生成 UplinkFast 帧。**rate 关键字指示 UplinkFast 拓扑更新帧的每秒数据包数。**建议使用默认值。对于 RSTP，不需要配置 UplinkFast，因为在 RSTP 中自带并会自动启用该机制。

BackboneFast

目的

BackboneFast 提供从间接链路故障中进行快速收敛的功能。BackboneFast 将收敛时间从默认值 50 秒降低到通常为 30 秒，并且以此方式将功能添加到 STP。同样，此功能只适用于运行 802.1D 时。当您运行快速 PVST 或 MST（其包括快速组件）时，请勿配置该功能。

操作概述

当交换机上的根端口或阻塞端口收到指定网桥发来的下级 BPDU 时，将启动 BackboneFast。当一台下游交换机丢失与根的连接，并且开始发送 BPDU 来选择一个新的根时，端口通常会接收下级 BPDU。下级 BPDU 将交换机同时标识为根网桥和指定网桥。

根据正常生成树规则，接收交换机会在配置的 maxage 时间内忽略下级 BPDU。默认情况下，maxage 为 20 秒。但是，有了 BackboneFast，交换机将下级 BPDU 当作拓朴可能更改的信号。该交换机使用根链路查询 (RLQ) BPDU，以确定是否有到根网桥的备用路径。添加此 RLQ 协议后，交换机可以检查根是否仍然可用。RLQ 可以更早地将阻塞端口转换为 `forwarding BPDU`

以下是该协议操作的一些要点：

- 交换机仅将 RLQ 数据包传出根端口（这意味着数据包向根传输）。
- 接收 RLQ 的交换机可以作出回复：自己是否是根交换机，或者发送 RLQ 的交换机是否知道自己已经断开与根的连接。如果该交换机不知道这些事实，它必须将查询从其根端口转发出去。
- 如果交换机失去了与根的连接，则该交换机必须以否定形式回复此查询。
- 回复必须从查询进来的端口发送出去。
- 根交换机必须始终使用肯定回复回应此查询。
- 如果回复是在非根端口上收到的，则丢弃回复。

由于 maxage 不必过期，因此该操作最多可以减少 20 秒钟的 STP 收敛时间。有关详细信息，请参阅[了解和配置 Catalyst 交换机上的 Backbone Fast。]

Cisco 建议

仅当整个生成树域都可以支持此功能时，才能在运行 STP 的所有交换机上启用 BackboneFast。您可以添加该功能而无需中断生产网络。

发出以下全局命令以启用 BackboneFast：

```
Switch(config)#spanning-tree backbonefast
```

注意：您必须在域中的所有交换机上配置此全局级别命令。该命令可为 STP 添加所有交换机需要了解的功能。

其他选项

Catalyst 2900XL 和 3500XL 交换机不支持 BackboneFast。一般来说，如果交换机域中除了 Catalyst 4500/4000、5500/5000 和 6500/6000 交换机以外还包含这些交换机，则您需要启用 BackboneFast。当您在带有 XL 交换机的环境中实现 BackboneFast 时，根据严格拓扑结构，如果 XL 交换机是线路中的最后一个交换机，并且仅在两个位置连接到核心，则可以启用此功能。如果 XL 交换机的体系结构为菊花链形式，请勿实现此功能。

您无需在 RSTP 或 802.1w 中配置 BackboneFast，因为 RSTP 中已经自带并自动启用了该机制。

生成树环路防护

环路防护是 Cisco 针对 STP 的专有优化。环路防护可防止第 2 层网络由于网络接口故障、CPU 繁忙或任何妨碍 BPDU 正常转发的问题而产生环路。在冗余拓扑中，当阻塞端口错误地转换为 forwarding 状态时，就会产生 STP 环路。发生这种情况通常是由于物理冗余拓扑中的一个端口（不一定是阻塞端口）停止接收 BPDU。

环路防护只是在交换机由点对点链路连接的交换机网络中才有用，如大多数现代园区和数据中心网络。其思路是在点对点链路上，指定网桥不可能在不发送下级 BPDU 或关闭链路的情况下消失。STP 环路防护功能是在用于 Catalyst 6500 交换机的 Catalyst Cisco IOS 软件的 Cisco IOS 软件版本 12.1(13)E 和用于 Catalyst 4500 交换机的 Cisco IOS 软件版本 12.1(9)EA1 中引入的。

有关环路防护的详细信息，请参阅使用环路防护和 BPDU 迟滞检测功能的生成树协议增强功能。

操作概述

环路防护检查根端口或替代/备用根端口是否接收 BPDU。如果该端口不接收 BPDU，环路防护将端口置于不一致状态 (blocking)，直到其再次开始接收 BPDU。处于不一致状态的端口不会传输 BPDU。如果此端口重新接收 BPDU，则该端口（和链路）将再次被视为可用。将从该端口删除环路不一致，并且 STP 会确定端口状态。采用这种方法，恢复将自动完成。

环路防护可隔离故障，并让生成树汇聚成稳定的拓扑，而不发生链路或网桥故障。环路防护以所使用的 STP 版本的速度防止出现 STP 环路。这不依赖于 STP 本身（802.1D 或 802.1w），也不受 STP 计时器调整的影响。由于以上原因，Cisco 建议在依赖 STP 并且软件支持相应功能的拓扑结构中，与 UDLD 一起实现环路防护。

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：

```
%SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010
```

在处于 loop-inconsistent STP 状态的端口收到 BPDU 后，该端口就会转换到其他 STP 状态。根据收到的 BPDU，这意味着恢复是自动进行的，无需进行干预。在恢复之后，会将以下消息记录到日志中：

```
%SPANTREE-SP-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet2/1 on
VLAN0010
```

与其他 STP 功能的交互作用

根防护

根防护始终强制指定某一端口。只有当端口是根端口或备用端口时，环路防护才有效，这意味着它们的功能互相排斥。因此，在一个端口上不能同时启用环路防护和根防护。

UplinkFast

环路防护与 UplinkFast 兼容。如果环路防护将根端口置于 blocking 状态，则 UplinkFast 会将一个新的根端口置于 forwarding 状态。并且，UplinkFast 不会选择 *loop-inconsistent 端口作为根端口。*

BackboneFast

环路防护与 BackboneFast 兼容。接收到来自指定网桥的下级 BPDU 时，会触发 BackboneFast。由于是从此链路接收的 BPDU，因此不启动环路防护。因此，BackboneFast 和环路防护兼容。

PortFast

一旦链接连通，PortFast 会立即将端口转换为转发指定状态。由于启用 PortFast 的端口不是根端口/备用端口，因此环路防护和 PortFast 是互相排斥的。

PAgP

环路防护使用 STP 已知的端口。因此，环路防护可利用 PAgP 提供的逻辑端口抽象概念。但是，为了形成信道，在信道中组合的所有物理端口必须有兼容的配置。PAgP 会在所有物理端口上强制实施统一的环路防护配置以形成信道。请注意，以下是在 EtherChannel 上配置环路防护时的一些警告：

- STP 始终选取信道中第一个正常运行的端口来发送 BPDU。如果此链路变为单向，那么即使信道中的其他链路正常工作，环路防护也会阻塞信道。
- 如果将已被环路防护阻塞的端口组合在一起以形成信道，则 STP 会丢失这些端口的所有状态信息，并且新的信道端口可能会获取具有指定角色的转发状态。
- 如果信道被环路防护阻塞且信道中断，则 STP 会丢失所有状态信息。即使形成信道的一个或多个链路为单向，各个物理端口也可能会获取具有指定角色的转发状态。

在最后两种情况中，都有产生环路的可能性，直到 UDLD 发现故障。但是环路防护无法检测到。

环路防护和 UDLD 功能比较

就防止由单向链路引起的 STP 故障而言，环路防护和 UDLD 功能有一部分重叠。这两个功能在问题解决方法以及功能方面有所不同。具体来说，存在特定的 UDLD 无法检测到的单向故障，例如由不能发送 BPDU 的 CPU 导致的故障。另外，使用主动 STP 计时器和 RSTP 模式可能会导致形成环路，直到 UDLD 可检测到该故障。

在共享链路上，或者在链路自链接以来已是单向链路的情况下，环路防护不起作用。在链路自链接以来已是单向链路的情况下，端口从不接收 BPDU 且不会成为指定端口。此行为可能是正常的，因此环路防护不包括此特定情况。UDLD 可以防止出现这样的情况。

同时启用 UDLD 和环路防护以提供最高级别的防护。有关环路防护和 UDLD 之间功能比较的详细信息，请参阅：

- *使用环路防护和 BPDU 迟滞检测功能的生成树协议增强功能的环路防护与单向链路检测 (UDLD) 部分。*
- 本文档的 UDLD 部分

Cisco 建议

Cisco 建议您在具有物理环路的交换机网络上全局启用环路防护。您可以在所有端口上全局启用环路防护。实际上，是在所有点对点链路上启用此功能。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。

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

其他选项

对于不支持全局环路防护配置的交换机，建议在各个端口（包括端口信道端口）上启用此功能。尽管在指定端口上启用环路防护没有任何优点，但不要认为该启用会发生任何问题。另外，有效的生成树重新收敛实际上可将指定端口变为根端口，这可使此功能在该端口上变得有用。

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard loop
```

如果意外形成环路，具有无环路拓扑的网络仍可从环路防护功能中受益。但是，在此类型的拓扑中启用环路防护可能会导致网络隔离问题。如果构建无环路拓扑并且希望避免网络隔离问题，您可以全局或单个禁用环路防护。请不要在共享链路上启用环路防护。

```
Switch(config)#no spanning-tree loopguard default
!--- This is the global configuration.
```

或

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no spanning-tree guard loop
!--- This is the interface configuration.
```

生成树根防护

根防护功能提供了在网络中强制执行根网桥安置的方法。根防护可确保启用根防护的端口为指定端口。通常，除非根网桥的两个或多个端口连接在一起，否则根网桥端口全部为指定端口。如果网桥在启用了根防护的端口上收到高级 STP BPDU，则网桥会将此端口转换为根不一致 STP 状态。此根不一致状态实际上等效于监听状态。此时不会通过此端口转发任何流量。根防护以这种方式强制确定根网桥的位置。根防护在早期的 Cisco IOS 软件版本 12.1E 及更高版本中可用。

操作概述

根防护是 STP 内置机制。根防护自身没有计时器，它仅依赖于接收 BPDU。当根防护被应用于某个端口时，它会拒绝此端口成为根端口的可能性。如果接收到 BPDU 会触发使指定端口成为根端口的生成树收敛，则会将该端口置于根不一致状态。此系统日志消息进行了说明：

```
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/1 on VLAN0010
```

端口停止发送高级 BPDU 后，该端口会再次解除阻塞。通过 STP，该端口从监听状态进入识别状态，并最终转换为转发状态。此 syslog 消息显示了过渡情况：

```
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/1
on VLAN0010
```

恢复是自动进行的。不需要人为干预。

由于根防护强制指定端口，并且仅当该端口是根端口或替代端口时环路防护才有效，因此这两种功能互相排斥。所以，您无法在端口上同时启用环路防护和根防护。

有关详细信息，请参阅生成树协议根防护增强功能。

Cisco 建议

Cisco 建议您在与不受直接管理控制的网络设备连接的端口上启用根防护功能。当您处于接口配置模式时，为了配置根防护，请使用以下这些命令：

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard root
```

EtherChannel

目的

EtherChannel 包括一种帧分配算法，该算法可以跨组件 10/100-Mbps 或千兆链路有效地多路复用帧。帧分配算法允许多信道逆向多路复用到单个逻辑链路。虽然在实施中每个平台与下一个平台有所不同，但您必须了解以下这些共同属性：

- 必须有一种通过多信道统计复用帧的算法。在 Catalyst 交换机中，这与硬件相关。如下面的示例所示：Catalyst 5500/5000s — 模块上是否存在以太网捆绑芯片(EBC)Catalyst 6500/6000s — 一种可进一步读取帧并通过IP地址多路复用的算法
- 存在逻辑信道的创建，以便可以运行 STP 的单个实例或使用单个路由对等，具体取决于它是第二层 EtherChannel 还是第三层 EtherChannel。
- 有一种管理协议可检查链路任一端的参数一致性，并帮助管理从链路故障或链路增加中恢复绑定。此协议可以是 PAgP 或链路聚合控制协议 (LACP)。

操作概述

EtherChannel 包括一种帧分配算法，该算法可以跨组件 10/100-Mbps、千兆链路或 10 千兆链路有效地多路复用帧。每个平台算法上的区别在于做出分配决策时，每种硬件类型提取帧头信息的能力不同。

负载分配算法是可用于两种信道控制协议的全局选项。PAgP 和 LACP 使用帧分配算法，这是因为 IEEE 标准不要求使用任何特定的分配算法。但是，任何分配算法均可确保在接收帧时，算法不会导致属于任何给定对话的帧顺序混乱或帧重复。

下表为每个列出的平台详细说明了帧分配算法：

Platform	信道负载均衡算法
Catalyst 3750 系列	Catalyst 3750 运行的 Cisco IOS 软件负载均衡算法使用 MAC 地址或 IP 地址，以及消息源或消息目标（或使用两者）。
Catalyst 4500 系列	Catalyst 4500 运行的 Cisco IOS 软件负载均衡算法使用 MAC 地址、IP 地址或第 4 层 (L4) 端口号，以及消息源或消息目标（或使用两者）。
Catalyst 6500	可以使用两种散列算法，具体取决于 Supervisor 引擎硬件。散列是在硬件中实施的十七次多项式。在任何情况下，散列均可使用 MAC 地址、IP 地址或

/6000 系列	IP TCP/UDP 端口号，利用该算法生成一个 3 位值。将针对 SA 和 DA 分别执行此过程。然后对结果执行 XOR 运算，以生成另一个 3 位值。该值确定信道中的哪个端口用于转发数据包。在 Catalyst 6500/6000 上可以在任意模块上的端口之间形成信道，端口最多可达八个。

下表说明各类 Catalyst 6500/6000 Supervisor 引擎模式支持的分配方法。该表也显示了默认行为：

Hardware	描述	分配方法
WS-F6020A（第2层引擎）WS-F6K-PFC（第3层引擎）	更高版本的Supervisor引擎I和Supervisor引擎IA Supervisor引擎IA/策略功能卡1(PFC1)	第 2 层 MAC：SA;DA;SA和DA第3层IP:SA;DA;SA和 DA（默认）
WS-F6K-PFC 2	Supervisor 引擎 II/PFC2	第 2 层 MAC：SA;DA;SA和DA第3层 IP:SA;DA;SA和 DA（默认）第4层会话：S 端口；D 端口；S 和 D 端口
WS-F6K-PFC3A WS-F6K-PFC3B WS-F6K-PFC3BXL	Supervisor引擎720/PFC3A Supervisor引擎 720/Supervisor引擎 32/PFC3B Supervisor引擎 720/PFC3BXL	第 2 层 MAC：SA;DA;SA和DA第3层 IP:SA;DA;SA和 DA（默认）第4层会话：S 端口；D 端口；S 和 D 端口

注意：在第4层分布中，第一个分片数据包使用第4层分布。所有后续数据包均使用第 3 层分配。

注意：要了解有关其他平台上EtherChannel支持以及如何配置EtherChannel并对其进行故障排除的更多详细信息，请参阅以下文档：

- 了解 Catalyst 交换机上的 EtherChannel 负载均衡和冗余
- 配置第 3 层和第 2 层 EtherChannel（Catalyst 6500 系列 Cisco IOS 软件配置指南，12.2SX）
- 配置第 3 层和第 2 层 EtherChannel（Catalyst 6500 系列 Cisco IOS 软件配置指南，12.1E）
- 配置 EtherChannel（Catalyst 4500 系列交换机 Cisco IOS 软件配置指南，12.2(31)SG）
- 配置 EtherChannel（Catalyst 3750 交换机软件配置指南，12.2(25)SEE）
- 在运行 CatOS 系统软件的 Catalyst 4500/4000、5500/5000 和 6500/6000 交换机之间配置 EtherChannel

Cisco 建议

默认情况下，Catalyst 3750、Catalyst 4500 和 Catalyst 6500/6000 系列交换机通过散列源和目标

IP 地址来执行负载均衡。如果假定 IP 为主要协议，那么建议采用此方式。若要设置负载均衡，请发出以下命令：

```
port-channel load-balance src-dst-ip
!--- This is the default.
```

其他选项

如果大部分数据流是在相同源和目标 IP 地址之间传输的，则您可以根据数据流的不同，使用第 4 层分配以改进负载均衡。您必须了解，当配置第 4 层分配时，散列运算对象只包括第 4 层源及目标端口。它不会将第 3 层 IP 地址加入到散列算法中。若要设置负载均衡，请发出以下命令：

```
port-channel load-balance src-dst-port
```

注意：Catalyst 3750系列交换机上无法配置第4层分布。

若要检查帧分配策略，请发出 **show etherchannel load-balance 命令。**

根据硬件平台的不同，您可以使用 CLI 命令来确定将使用 EtherChannel 中的哪个接口来转发特定的数据流（以帧分配策略为基础）。

对于 Catalyst 6500 交换机，请发出 **remote login switch 命令，以远程登录到交换机处理器 (SP) 控制台。**然后，发出以下命令：**test etherchannel load-balance interface port-channel number {ip | l4port | mac} [*source_ip_add* | *source_mac_add* | *source_l4_port*] [*dest_ip_add* | *dest_mac_add* | *dest_l4_port*]**命令。

对于 Catalyst 3750 交换机，发出以下命令：**test etherchannel load-balance interface port-channel number {ip | mac} [*source_ip_add* | *source_mac_add*] [*dest_ip_add* | *dest_mac_add*]**命令。

对于 Catalyst 4500，尚无等效命令可用。

EtherChannel 配置指南和限制

在将兼容端口聚合到单个逻辑端口之前，EtherChannel 会验证所有物理端口上的端口属性。配置指南和限制对不同交换机平台会有所不同。请遵循这些指南和限制，以避免出现绑定问题。例如，如果已启用 QoS，则在绑定具有不同 QoS 功能的 Catalyst 6500/6000 系列交换模块时，不会形成 EtherChannel。对于运行 Cisco IOS 软件的 Catalyst 6500 交换机，您可以使用 **no mls qos channel-consistency 端口信道接口命令，禁止对 EtherChannel 绑定执行 QoS 端口属性检查。**发出命令 **show interface capability *mod/port*** 可显示 QoS 端口功能并确定端口是否兼容。

请参阅以下针对不同平台的指南，以避免出现配置问题：

- 配置第 3 层和第 2 层 EtherChannel（Catalyst 6500 系列 Cisco IOS 软件配置指南，12.2SX）
- 配置第 3 层和第 2 层 EtherChannel（Catalyst 6500 系列 Cisco IOS 软件配置指南，12.1E）
- 配置 EtherChannel（Catalyst 4500 系列交换机 Cisco IOS 软件配置指南，12.2(31)SG）
- 配置 EtherChannel（Catalyst 3750 交换机软件配置指南，12.2(25)SEE）

所支持的 EtherChannel 最大数量也取决于硬件平台和软件版本。运行 Cisco IOS 软件版本 12.2(18)SXE 及更高版本的 Catalyst 6500 交换机最多支持 128 个端口信道接口。早于 Cisco IOS 软件版本 12.2(18)SXE 的软件版本最多支持 64 个端口信道接口。无论软件版本如何，可配置的组数均为 1 至 256。Catalyst 4500 系列交换机最多支持 64 个 EtherChannel。对于 Catalyst 3750 交

换机，我们建议在交换机堆栈上配置的 EtherChannel 不超过 48 个。

生成树端口成本计算

您必须了解 EtherChannel 的生成树端口成本计算。您可以通过短方法或长方法来计算 EtherChannel 的生成树端口成本。默认情况下，端口成本是采用短模式计算的。

下表根据带宽说明第2层EtherChannel的生成树端口开销：

带宽	旧STP值	新的长STP值
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
N x 1 Gbps	3	6660
10 Gbps	2	2,000
100 Gbps	不适用	200
1 Tbps	不适用	20
10 Tbps	不适用	2

注意：在CatOS中，端口通道成员链路故障后，EtherChannel的生成树端口开销保持不变。在 Cisco IOS 软件中，EtherChannel 的端口成本会立即更新，以反映新的可用带宽。如果需要避免多余的生成树拓扑更改，可以使用 **spanning-tree cost** ***cost*** 命令静态配置生成树端口成本。

端口聚合协议 (PAgP)

目的

PAgP 是用于检查链路任一端的参数一致性的管理协议。PAgP 还有助于信道在出现链路故障或链路增加的情况下做出相应调整。下面是 PAgP 的特性：

- PAgP 要求信道中的所有端口均属于同一 VLAN 或均配置为中继端口。由于动态 VLAN 可以强制将端口更改到不同的 VLAN，因此动态 VLAN 不能参与到 EtherChannel 中。
- 如果已存在一个链路捆绑，并已修改其中某一端口的配置，则将修改该链路捆绑中的所有端口以匹配该配置。例如，更改 VLAN 或更改 `trunking`
- PAgP 不会对以不同速度或端口双工运行的端口进行分组。如果在存在链路捆绑的情况下更改速度和双工，PAgP 会更改链路捆绑中所有端口的速度和双工。

操作概述

PAgP 端口控制要分组的每一个物理（或逻辑）端口。为了发送 PAgP 数据包，将使用用于 CDP 数据包的同一个多播组 MAC 地址。MAC 地址为 01-00-0c-cc-cc-cc。但是，协议值为0x0104。以下是协议操作的摘要：

- 只要物理端口开启，就会在检测期间每秒传输一次 PAgP 数据包，在稳定状态下每 30 秒传输一次该数据包。
- 如果收到数据包但没有收到 PAgP 数据包，则假设端口连接到不支持 PAgP 的设备。
- 对证明物理端口与另一支持 PAGP 的设备具有双向连接的 PAgP 数据包进行监听。
- 一旦在一组物理端口上收到两个这样的数据包，便尝试形成一个聚合端口。
- 如果 PAgP 数据包停止一段时间，则 `PAgP  down`

正常处理

以下概念有助于说明此协议的行为：

- Agport - 由同一聚合中的所有物理端口组成的逻辑端口，可由其自己的 SNMP ifIndex 标识。agport 不包含非操作端口。
- 信道 - 能满足形成条件的聚合。信道可以包含非操作端口并且是 agport 的超集。协议（包括 STP 和 VTP，但不包括 CDP 和 DTP）通过 agport 在 PAgP 上运行。直到 PAgP 将 agport 连接到一个或多个物理端口，这些协议才能发送或接收数据包。
- 组功能 - 每个物理端口和 agport 都拥有一个称为 group-capability 的配置参数。物理端口可以与具有相同 `group-capability` 的任何其他物理端口聚合，并且只能与这样的物理端口聚合。
- 聚合过程 - 当物理端口变成 UpData 或 UpPAgP 状态时，该端口会连接到适当的 agport 上。当该端口离开上述状态之一以进入另一个状态时，该端口与 agport 分离。

下表提供了有关状态的更多详细信息：

状态	含义
`UpData`	未接收到任何 PAgP 数据包。PAgP 数据包已发送。物理端口是连接到 agport 的唯一端口。非 PAgP 数据包在物理端口和 agport 之间传入和传出。
	恰好已接收到一个 PAgP 数据包，证明仅与一个相邻端口存在双向连接。物理端口未连接到任何 agport。PAgP 数据包已发送并且可以被接收到。
`UpPAgP`	此物理端口（可能与其他物理端口关联）已连接到 agport。PAgP 数据包在该物理端口上发送和接收。非 PAgP 数据包在物理端口和 agport 之间传入和传出。

连接的两端必须都同意分组。分组定义为连接的两端都允许的 agport 中的最大端口组。

当物理端口变成 `UpPAgP agport group-capability BiDir UpPAgP` 任何此类 `Bidir UpPAgP` 如果不存在其成员物理端口参数与新就绪的物理端口兼容的 agport，则该端口被分配给具有适当参数（这些参数没有关联的物理端口）的 agport。

在该物理端口已知的上一个相邻端口上可能会出现 PAgP 超时。超时的端口将从 agport 中予以删除。同时，也将删除同一 agport 上其计时器也已超时的所有物理端口。这将导致另一端已停止的 agport 突然关闭，而不是一次关闭一个物理端口。

出现故障的行为

如果信道中某一现有链路出现故障，agport 将进行更新，数据流通过其余的链路进行哈希处理，不会有任何损失。例如，此类故障包括：

- 端口被拔掉
- 千兆接口转换器 (GBIC) 被卸掉
- 光纤中断

注意：当关闭或移除模块时，当通道中的链路出现故障时，行为可能会有所不同。根据定义，信道需要两个物理端口。如果双端口信道的系统中丢失一个端口，则逻辑 agport 将关闭且将重新初始化与生成树有关的原始物理端口。在 STP 允许数据再次可以使用端口之前，可能会丢弃数据流。

当您规划网络的维护时，这两种故障模式的区别非常重要。当您执行模块的联机删除或插入时，可能需要考虑 STP 拓扑的更改。因为 agport 可以不受故障干扰，您必须使用网络管理系统 (NMS) 管理信道中的每条物理链路。

若要减少 Catalyst 6500/6000 上不需要的拓扑更改，请完成下列建议之一：

- 如果每个模块使用一个端口来形成信道，请使用三个或更多模块（总共为三个）。
- 如果信道跨越两个模块，请在每个模块上使用两个端口（总共为四个）。
- 如果在两个卡之间需要双端口信道，则只使用 Supervisor 引擎端口。

配置选项

可以将 EtherChannel 配置为不同模式，如下表所总结：

模式	可配置选项
	PAgP 未运行。不论相邻端口的配置方式如何，都对端口建立信道。如果相邻端口模式为 `on`，则形成信道。
	聚合处于 PAgP 的控制之下。端口置于被动协商状态。只有至少收到一个指示发送方运行在 `desirable PAgP PAgP`
	聚合处于 PAgP 的控制之下。端口置于活动协商状态，在该状态下，端口通过传输 PAgP 数据包启动与其他端口的协商。将与另一个处于 desirable 或 auto 模式的端口组形成信道。
这是Catalyst 5500/5000光纤FE和GE端口的默认值。	`auto desirable` 如果接口没有收到数据包，该接口没有连接到agport上，并且不能用于数据。由于某些链路故障会导致信道分离，因此为特定 Catalyst 5500/5000 硬件提供了此双向检查。启用 `non-silent` 默认情况下，在 Catalyst 4500/4000 和 6500/6000 系列硬件中提供了更灵活的捆绑和改进的双向检查。
这是所有Catalyst 6500/6000和4500/4000端口以及5500/5000铜缆端口的默认值。	`auto desirable` 如果接口上没有收到数据包，则在经过 15 秒超时时长之后，该接口单独连接到 agport。因此，该接口可以用于数据传输。 `PAgP Silent`

`silent/non-silent` 当端口由于物理接口有故障或者光纤或电缆中断而无法传输时，相邻端口可能仍处于操作状态。伙伴将继续传输数据。但是，由于无法收到返回数据流，数据会丢失。由于链路具有单向性，因此也可形成生成树环路。

一些光纤端口具有我们所期望的功能，即当端口丢失其接收信号时 (FEFI) 时，可将端口置于非操作状态。 此操作会导致伙伴端口变成非操作状态，并实际导致链路两端的端口断开。

当您使用传输数据 (BPDU) 的设备且无法检测到单向情况时，请使用 `non-silent` PAgP 检测到单向链路所花费的时间大约为 3.5*30 秒 = 105 秒。三十秒是两个连续的 PAgP 消息之间的时间。使用 UDLD，这是一个更快速的单向链路探测器。

当您使用不传输任何数据的设备时，请使用 `silent` 使用 `silent` 另外，对于可以检测到存在单向情况的那些端口，默认情况下使用 `silent` 例如，此类端口包括使用第 1 层 FEFI 和 UDLD 的更新平台。

若要在接口上关闭信道，请发出命令 **no channel-group number**：

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no channel-group 1
```

确认

本部分中的表概要描述了两台直接连接的交换机（交换机 A 和交换机 B）之间所有可能的 PAgP 信道模式方案。其中某些组合可能会导致 STP 将信道端的端口置于 `errdisable` 默认情况下，会启用 EtherChannel 配置错误防护功能。

交换机 A 信道模式	交换机 B 信道模式	交换机 A 信道状态	交换机 B 信道状态
开启	开启	信道（非 PAgP）	信道（非 PAgP）
开启	未配置	Not Channel (errdisable)	Not Channel
开启	自动	Not Channel (errdisable)	Not Channel
开启	期望	Not Channel (errdisable)	Not Channel
未配置	开启	Not Channel	Not Channel (errdisable)
未配置	未配置	Not Channel	Not Channel
未配置	自动	Not Channel	Not Channel
未配置	期望	Not Channel	Not Channel
自动	开启	Not Channel	Not Channel (errdisable)
自动	未配置	Not Channel	Not Channel
自动	自动	Not Channel	Not Channel
自动	期望	PAgP Channel	PAgP Channel
期望	开启	Not Channel	Not Channel
期望	未配置	Not Channel	Not Channel
期望	自动	PAgP Channel	PAgP Channel
期望	期望	PAgP Channel	PAgP Channel

Cisco 针对 L2 信道的配置建议

在所有 EtherChannel 链路上启用 PAgP 并且使用 `desirable-desirable` 有关详细信息，请参阅以下输出：

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no ip address
!--- This ensures that there is no IP !--- address that is assigned to the LAN port.
```

```
Switch(config-if)#channel-group number mode desirable
!--- Specify the channel number and the PAgP mode.
```

通过以下方法验证配置：

```
Switch#show run interface port-channel number
Switch#show running-config interface type slot#/port#
Switch#show interfaces type slot#/port# etherchannel
Switch#show etherchannel number port-channel
```

避免 EtherChannel 配置错误

您可能错误地配置 EtherChannel 并创建生成树环路。此错误配置可能会使交换机进程过载。Cisco IOS 系统软件包含 **spanning-tree etherchannel guard misconfig 功能以防止出现此问题。**

在将 Cisco IOS 软件作为系统软件运行的所有 Catalyst 交换机上发出以下配置命令：

```
Switch(config)#spanning-tree etherchannel guard misconfig
```

其他选项

当对不支持 PAgP 但是支持 LACP 的两个设备建立信道时，建议在设备两端将 LACP 配置为 active 模式以启用 LACP。有关详细信息，请参阅本文档的链路聚合控制协议 (LACP) 部分。

在对不支持 PAgP 或 LACP 的设备建立信道时，您必须将信道硬编码为 on。例如，此要求适用于以下设备：

- 服务器
- 本地控制器
- 内容交换机
- 路由器
- 装有较早软件的交换机
- Catalyst 2900XL/3500XL 交换机
- Catalyst 8540

发出以下命令：

```
Switch(config)#interface type slot#/port#
Switch(config-if)#channel-group number mode on
```

链路聚合控制协议 (LACP)

LACP 协议允许具有类似特性的端口通过与相邻的交换机进行动态协商来形成信道。PAgP 是 Cisco 专有的协议，只能在 Cisco 交换机和许可供应商发布的交换机上运行。但是 IEEE 802.3ad 中定义的 LACP 允许 Cisco 交换机用符合 802.3ad 规范的设备管理以太网信道。

以下平台和版本支持 LACP：

- 运行 Cisco IOS 软件版本 12.1(11b)EX 及更高版本的 Catalyst 6500/6000 系列
- 运行 Cisco IOS 软件版本 12.1(13)EW 及更高版本的 Catalyst 4500 系列
- 运行 Cisco IOS 软件版本 12.1(14)EA1 及更高版本的 Catalyst 3750 系列

LACP 和 PAgP 在功能方面几乎没有区别。两个协议都支持每个信道最多八个端口，并且在形成链路捆绑之前都会对相同的端口属性进行检查。这些端口属性包括：

- 速度
- 双工
- 本地 VLAN 和中继类型

LACP 和 PAgP 之间的显著差异包括：

- LACP 协议只能在全双工端口上运行，不支持半双工端口。
- LACP 协议支持热备用端口。LACP 始终尝试在一个信道中配置最大数量的兼容端口，即硬件允许的最大数量（八个端口）。 如果 LACP 无法聚合所有兼容端口（例如，如果远程系统有更严格的硬件限制），则无法有效包括在信道中的所有端口都会置于热备用状态，并仅在其中一个使用的端口出现故障时使用。

注意：对于Catalyst 4500系列交换机，您可以为其分配相同管理密钥的最大端口数为8。对于运行 Cisco IOS 软件的 Catalyst 6500 和 3750 交换机，LACP 会尝试在 EtherChannel 中配置最大数量的兼容端口，即硬件允许的最大数量（八个端口）。 另外八个端口可以配置为热备用端口。

操作概述

LACP 控制要捆绑的每一个物理（或逻辑）端口。LACP数据包是使用组播组MAC地址**01-80-c2-00-00-02发送的。类型/字段值为0x8809，子类型为0x01。以下是协议操作的摘要：**

- 协议依靠设备来通告它们的聚合功能和状态信息。将在每个可聚合链路上定期发送传输内容。
- 只要物理端口打开，检测时 LACP 数据包每秒传输一次，并在处于稳定状态时每 30 秒传输一次。
- 可聚合链路上的伙伴监听协议中发送的信息，并且决定要采取的操作。
- 兼容端口是在信道中进行配置的，兼容端口数最多为硬件允许的最大数量（八个端口）。
- 通过在链路伙伴之间定期、及时交换最新状态信息来维护聚合。如果配置更改（例如由于链路故障），则协议伙伴超时，并且根据系统的新状态采取适当操作。
- 除了定期 LACP 数据单元 (LACPDU) 传输外，如果状态信息有更改，则协议将把事件驱动的 LACPDU 传输给伙伴。协议伙伴根据系统的新状态采取适当的操作。

LACP 参数

为了允许 LACP 确定一组链路是否连接到同一个系统，以及从聚合角度看这些链路是否兼容，有必要建立以下对象：

- 加入链路聚合的每个系统的全局唯一标识符。必须为运行 LACP 的每个系统指定可自动选择的（默认优先级为 32768）或由管理员选择的优先级。系统优先级主要用于与系统的 MAC 地址一起形成系统标识符。
- 用于标识与给定系统所了解的每个端口及每个汇聚路由器相关联的功能集的方法。必须为系统中的每个端口自动指定优先级（默认优先级为 128）或由管理员指定优先级。优先级与端口号一起形成端口标识符。
- 用于标识链路聚合组及其相关汇聚路由器的方法。一个端口与另一个端口聚合的能力由一个称为“键”的严格大于零的简单 16 位整数参数来综合表示。每个键根据不同因素来确定，例如：端口物理特性，其中包括数据速率、双工性和点对点或者共享介质由网络管理员建立的配置约束以下两个键与每个端口相关联：管理键操作键管理键允许通过管理来处理键值，因此用户可以选择此键。系统使用操作键来形成聚合。用户不能直接选择或更改此键。共享同一操作键值的给定系统中的端口集被视为同一个键组的成员。

因此，在给定两个系统和一组具有相同管理键的端口的情况下，每个系统尝试从最高优先级系统中

具有最高优先级的端口开始聚集端口。此行为是可能的，因为每个系统都知道以下优先级：

- 自己的优先级，由用户或软件指定
- 伙伴的优先级，通过 LACP 数据包发现

出现故障的行为

LACP 的故障行为与 PAgP 的故障行为相同。如果现有信道中的链路出现故障（例如，如果端口被拔掉、GBIC 被卸掉或者光纤中断），则 agport 会进行更新，数据流会在 1 秒钟内通过其余的链路进行哈希处理。不需要在发生故障后重新进行哈希处理的任何数据流（继续在同一链路上发送的数据流）不会遭受任何损失。恢复故障链路将触发再次对 agport 进行更新，并且会再次对数据流进行哈希处理。

配置选项

可以将 LACP EtherChannel 配置为不同模式，如下表所总结：

模式	可配置选项
开启	不进行任何 LACP 协商，强制形成链路聚合。交换机既不发送 LACP 数据包，也不处理任何传入 LACP 数据包。如果相邻端口模式为 on，则形成信道。
Off（或）未配置	不论相邻端口的配置方式如何，都不会对端口建立信道。
Passive（默认值）	这类似于 PAgP 中的 **auto 模式。**交换机不启动信道，但可以识别传入的 LACP 数据包。对等交换机（处于活动状态）通过发出 LACP 数据包启动协商，交换机接收该数据包并进行回复，最终与对等交换机形成聚合信道。
主用	这类似于 PAgP 中的 **desirable 模式。**交换机启动协商以形成聚合链路。如果另一端以 LACP active 或 passive 模式运行，则形成链路聚合。

在 LACP EtherChannel 建立后 LACP 将使用一个 30 秒间隔计时器 (Slow_Periodic_Time)。使用长超时（Slow_Periodic_Time的3倍）时，收到的LACPDU信息失效前的秒数为90。建议将UDLD作为单向链路的更快速检测器。为了在形成信道后保持该信道，此时您不能调整 LACP 计时器，并且不能将交换机配置为使用快速协议数据单元 (PDU) 传输（每秒）。

确认

本部分中的表概要描述了两台直接连接的交换机（交换机 A 和交换机 B）之间所有可能的 LACP 信道模式方案。 其中一些组合可能导致 EtherChannel 防护功能将信道端的端口置于 errDisable 状态。默认情况下，会启用 EtherChannel 配置错误防护功能。

交换机 A 信道模式	交换机 B 信道模式	交换机 A 信道状态	交换机 B 信道状态
开启	开启	Channel（非 LACP）	Channel（非 LACP）
开启	关闭	Not Channel (errdisable)	Not Channel

开启	被动	Not Channel (errdisable)	Not Channel
开启	主用	Not Channel (errdisable)	Not Channel
关闭	关闭	Not Channel	Not Channel
关闭	被动	Not Channel	Not Channel
关闭	主用	Not Channel	Not Channel
被动	被动	Not Channel	Not Channel
被动	主用	LACP Channel	LACP Channel
主用	主用	LACP Channel	LACP Channel

Cisco 建议

Cisco 建议您对 Cisco 交换机之间的信道连接启用 PAgP。当对不支持 PAgP 但是支持 LACP 的两个设备建立信道时，建议在设备两端将 LACP 配置为 active 模式以启用 LACP。

在运行 CatOS 的交换机上，默认情况下 Catalyst 4500/4000 和 Catalyst 6500/6000 上的所有端口使用 PAgP 信道协议。为了配置端口以使用 LACP，您需要将模块上的信道协议设置为 LACP。LACP 和 PAgP 不能在运行 CatOS 的交换机的同一个模块上运行。此限制不适用于运行 Cisco IOS 软件的交换机。运行 Cisco IOS 软件的交换机可以支持同一个模块上的 PAgP 和 LACP。若要将 LACP 信道模式设置为 active 并指定一个管理键编号，请发出以下命令：

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode active
```

show etherchannel summary 命令为每个信道组显示一行概要，其中包括以下信息：

- 组数
- 端口信道数
- 端口状态
- 作为信道一部分的端口

show etherchannel port-channel 命令显示所有信道组的详细端口信道信息。输出包括以下信息：

- 信道状态
- 使用的协议
- 自从端口捆绑后经过的时间

为了显示特定信道组的详细信息（单独显示每个端口的详细信息），请使用 **show etherchannel *channel_number detail* 命令。**命令输出包括伙伴详细信息和端口信道详细信息。有关详细信息，请参阅配置 Catalyst 6500/6000 和 Catalyst 4500/4000 之间的 LACP (802.3ad)。

其他选项

当信道所连接的设备不支持 PAgP 或 LACP 时，您必须将信道硬编码为 on。此要求适用于以下设备：

- 服务器
- 本地控制器
- 内容交换机

- 路由器
- 使用早期版本软件的交换机
- Catalyst 2900XL/3500XL 交换机
- Catalyst 8540

发出以下命令：

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode on
```

单向链路检测 (UDLD)

目的

UDLD 是 Cisco 专有的轻量级协议，为检测设备之间的单向通信实例而开发。有其他方法（如 FEFI）可检测传输介质的双向状态。但仍有某些实例是第 1 层检测机制不足以检测的。这些情况可能导致：

- 不可预测的 STP 操作
- 不正确的或过度数据包泛洪
- 流量黑洞

UDLD 功能用于解决光纤和铜缆以太网接口上的这些故障情况：

- 监控实际布线配置 - 将任何布线错误的端口以 errDisabled 关闭。
- 防止单向链路引起的故障 - 在检测到由于介质或端口/接口故障导致的单向链路时，将受影响的端口以 errDisabled 关闭。生成相应的 syslog 消息。
- 此外，UDLD 主动模式检查以前视为双向的链路在由于拥塞而变得不可用时不会失去连接。UDLD 主动模式在整个链路上执行持续的连接测试。UDLD 主动模式的主要目的在于避免在某些正常模式 UDLD 未能解决的故障情况下出现流量黑洞。

有关详细信息，请参阅了解和配置单向链路检测协议 (UDLD) 功能。

生成树有稳定的单向 BPDU 流，并且可能出现本部分列出的故障。端口突然无法传输 BPDU，从而导致邻居上的 STP 状态从 `blocking  forwarding`但是，由于端口仍能接收，因而仍存在环路。

操作概述

UDLD 是在 LLC 层以上运行的第 2 层协议（目标 MAC 01-00-0c-cc-cc-cc，SNAP HDLC 协议类型 0x0111）。 当与 FEFI 和自动协商第 1 层机制一同运行 UDLD 时，可以验证链路的物理（第 1 层）和逻辑（第 2 层）完整性。

UDLD 提供了 FEFI 和自动协商无法执行的功能和保护。这些功能包括：

- 邻居信息的检测和缓存
- 关闭所有错误连接的端口
- 对非点对点链路上逻辑接口/端口故障或错误的检测**注意：**当链路不是点对点时，它们会通过介质转换器或集线器。

UDLD 使用了这两个基本机制。

1. UDLD 获得有关邻居的信息并将最新信息保存在本地缓存中。

2. 在 UDLD 检测到新的邻居时，或者只要邻居请求重新同步缓存，它就会发送一系列 UDLD probe/echo (hello) 消息。

UDLD 不断在所有端口发送 probe/echo 消息。端口上收到对应的 UDLD 消息时，将触发检测阶段和验证过程。如果符合所有有效条件，则启用端口。如果端口是双向的，并且布线正确，则符合条件。如果不符合条件，则端口为 `errDisabled`，这将触发此 syslog 消息：

```
UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link.
   Port disabled
UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link.
   Failed to disable port
UDLD-3-DISABLE: Unidirectional link detected on port disabled.
UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port.
UDLD-3-SENDFAIL: Transmit failure on port.
UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars]
   was detected.
```

有关按设备列出的系统消息的完整列表（包括 UDLD 事件），请参阅 UDLD 消息（Cisco IOS 系统信息，第 2 卷（共 2 卷））。

建立链路并归类为双向后，UDLD 继续以默认的 15 秒间隔通告 probe/echo 消息。

此表提供有关端口状态的信息：

端口状态	注释
未确定	正在进行检测，或者相邻的 UDLD 已禁用。
不适用	UDLD 已禁用。
shutdown	已检测到单向链路，并且端口已禁用。
双向	已检测到双向链路。

邻居缓存维护

UDLD 在每个活动接口上定期发送 hello probe/echo 数据包，以维护 UDLD 邻居缓存的完整性。收到 hello 消息时，将缓存该消息并将其在内存中保存一段最长期限（定义为“保持时间”）。当保持时间过期时，各缓存条目便会老化。如果在保持时间期限内收到新的 hello 消息，此新消息便会取代旧条目并重置对应的生存时间计时器。

每当禁用已启用 UDLD 的接口或者重置设备时，就将清除配置更改所影响接口的所有现有缓存条目。此清除将维护 UDLD 缓存的完整性。UDLD 传输至少一条消息，通知各个邻居需要刷新对应的缓存条目。

回声检测机制

回声机制构成了检测算法的基础。每当 UDLD 设备获得新邻居的信息或者从不同步邻居收到再次同步请求时，该设备会在连接端启动或重新启动检测窗口，并在应答中发送一条突发的回声消息。因为此行为在所有邻居中肯定都是相同的，所以回声发送人希望在应答中收到回声。如果检测窗口结束时仍然没有接收到任何有效的应答消息，则将链路视为单向链路。从此时开始，可以触发链路重建或端口关闭进程。设备检查的其他少见异常状况包括：

- 传输 (Tx) 光纤与相同端口的 Rx 连接器构成环回
- 共享介质互连（如集线器或类似设备）的情况下出现布线错误

收敛时间

为了防止出现 STP 环路，Cisco IOS 软件版本 12.1 及更高版本已将 UDLD 默认消息间隔从 60 秒降低到 15 秒。更改此间隔是为了在关闭单向链路之后 802.1D 生成树中以前阻塞的端口才可以转换为转发状态。消息间隔值确定了邻居在联结或检测阶段之后发送 UDLD 探测的速率。消息间隔在链路的两端不需要匹配，虽然在可能的情况下最好配置一致。当 UDLD 邻居建立时，已配置的消息间隔将发送到邻居，并且将该对等体的超时间隔计算为：

```
3 * (message interval)
```

因此，在丢失三次连续的 hello（或 probe）之后，对等关系便会超时。因为消息间隔在每一端上是不同的，所以此超时值在每一端上也是不同的，并且有一端可更快速地识别故障。

UDLD 检测到以前稳定的链路出现单向故障所需的大致时间为：

```
2.5 * (message interval) + 4 seconds
```

在默认消息间隔为 15 秒的情况下，此时间约为 41 秒。此时间远低于 STP 重新收敛通常需要的 50 秒。如果 NMP CPU 有一些空闲周期并且用户仔细监控其使用级别（一种好的做法），则可接受将消息间隔降低（甚至）至 7 秒的最小限度。另外，降低此消息间隔有助于大幅加快检测速度。

注意：在Cisco IOS软件版本12.2(25)SEC中，最低为1秒。

因此，UDLD 在默认生成树计时器上具有假定相关性。如果调整 STP 以便该 UDLD 更快地收敛，请考虑采用替代机制，例如 STP 环路防护功能。在您实现 RSTP (802.1w) 时，也请考虑采用替代机制，因为 RSTP 具有毫秒级的收敛特性，具体取决于拓扑结构。对于这些实例，请将环路防护与 UDLD 结合使用，以便提供最大的防护。环路防护以所使用的 STP 版本的速度防止出现 STP 环路。并且，UDLD 负责检测各个 EtherChannel 链路上或 BPDU 不沿断开方向流动的情况下出现的单向连接。

注意：UDLD与STP无关。UDLD 并不捕获每种 STP 故障情况，例如超过 (2 * Fwddelay + maxage) 时间不发送 BPDU 的 CPU 造成的故障。 由于以上原因，Cisco 建议您在依赖 STP 的拓扑中与环路防护一起实现 UDLD。

注意：请注意2900XL/3500XL交换机中使用不可配置的60秒默认消息间隔的UDLD早期版本。这些版本易受生成树环路的影响。

UDLD 主动模式

主动 UDLD 是专为解决那些需要对双向连接执行持续测试的少数情况而创建的。这样，主动模式功能在下列情况下便可针对危险的单向链路提供增强的防护：

- 当 UDLD PDU 对称丢失并且两端都超时时。在这种情况下，两个端口的状态都不为 errdisable。
- 链路的一端出现端口阻塞（Tx 和 Rx）。
- 链路的一端保持接通状态，而另一端却已经关闭。
- 自动协商或其他第 1 层故障检测机制已禁用。
- 减少对第 1 层 FEFI 机制的依赖是较为理想的方式。
- 需要针对点对点 FE/GE 链路上的单向链路故障提供最大的防护。特别是在两个邻居之间不允许存在故障的情况下，可将 UDLD 主动探测视为检测信号，该信号的存在可确保链路正常运行。

实施主动 UDLD 的最常见的情况是为了在自动协商或其他第 1 层故障检测机制禁用或不可用时，对链路捆绑的某个成员执行连接检查。这对 EtherChannel 连接特别有用，因为即使启用了 PAgP 和 LACP，在稳定状态下它们也不使用非常低的 hello 计时器。在这种情况下，主动 UDLD 具有防止可

能出现生成树环路的额外益处。

请注意 UDLD 正常模式会检查单向链路，即使在链路到达双向状态后也会如此。UDLD 的用途在于检测引起 STP 环路的第 2 层问题，并且那些问题通常是单向的（因为在稳定状态下 BPDU 仅沿一个方向流动）。 因此，将 UDLD 正常模式与自动协商和环路防护（用于依赖 STP 的网络）一起使用通常便足够了。启用 UDLD 主动模式时，在端口的所有邻居都老化之后（处于通告或检测阶段），UDLD 主动模式会重新启动联结序列，以尝试与任何可能不同步的邻居重新同步。如果一系列快速消息发出后（8 次失败的重新尝试），链路仍被视为未确定，则将端口置于 errdisable 状态。

注意：某些交换机不支持主动UDLD。目前，Catalyst 2900XL 和 Catalyst 3500XL 具有 60 秒的硬编码消息间隔。一般认为此间隔过长，不足以防止可能出现的 STP 环路（假设采用默认 STP 参数）。

UDLD 链路的自动恢复

默认情况下，全局禁用 Errdisable 恢复。在全局启用之后，如果端口进入 errdisable 状态，则在选定时间间隔后该端口将自动重新启用。默认时间为 300 秒，这是一个全局计时器且为交换机中的所有端口保持。根据软件版本的不同，如果使用 UDLD 的 errdisable 超时恢复机制将端口的 errdisable 超时设置为 disable，则可以手动阻止该端口重新启用：

```
Switch(config)#errdisable recovery cause udld
```

当您在不具备带外网络管理功能的情况下实现 UDLD 主动模式时，特别是在接入层或在发生 errdisable 情况时会从网络隔离的任何设备上，请考虑使用 errdisable 超时功能。

有关如何为处于 errdisable 状态的端口配置超时时间段的详细信息，请参阅 errdisable 恢复（Catalyst 6500 系列 Cisco IOS 命令参考，12.1 E）。

当接入交换机分布在园区环境中，手动访问每台交换机以重新启用两个上行链路要花费许多时间时，errdisable 恢复对于接入层中的 UDLD 特别重要。

Cisco 建议不要在网络核心处进行 errdisable 恢复，因为通常有多个入口点进入核心，并且核心内的自动恢复可能导致重复出现问题。所以，如果 UDLD 禁用某一端口，您必须在核心处手动重新启用该端口。

路由链路上的 UDLD

为便于此讨论，路由链路为以下两种连接类型之一：

- 两个路由器节点之间的点对点连接（配置有 30 位子网掩码）
- 具有多个端口但仅支持路由连接的 VLAN，如在分割第 2 层核心拓扑中

每个内部网关路由协议 (IGRP) 都具有与其如何处理邻居关系和路由收敛相关的特性。本部分通过将目前用到的两个较常见的路由协议（开放最短路径优先 (OSPF) 协议和增强 IGRP (EIGRP)）进行对比，介绍与此讨论相关的特性。

注意：任何点对点路由网络上的第1层或第2层故障几乎立即导致第3层连接断开。由于在发生第 1 层/第 2 层故障时该 VLAN 中的唯一交换机端口转换为非连接状态，因此接口自动状态功能会在大约两秒的时间内同步第 2 层和第 3 层端口状态，并将第 3 层 VLAN 接口置于打开/关闭状态（线路协议处于关闭状态）。

如果采用默认计时器值，则 OSPF 每 10 秒发送一次 hello 消息且间隔为 40 秒 (4 * hello)。 这些计

时器对 OSPF 点对点网络和广播网络是一致的。由于 OSPF 需要双向通信以便形成邻接关系，因此最坏情况下的故障切换时间是 40 秒。即使第 1 层/第 2 层故障不完全在点对点连接上发生，造成第 3 层协议必须处理未完成的方案，情况也是如此。由于 UDLD 的检测时间非常类似于要到期的 OSPF 停机计时器的检测时间（大约 40 秒），因此对 OSPF 第 3 层点对点链路配置 UDLD 正常模式的优势是有限的。

在许多情况下，EIGRP 的收敛速度比 OSPF 更快。但是请注意，不必采用双向通信也可使邻居交换路由信息。在非常特定的未完成故障情形下，EIGRP 易受持续不断的流量黑洞的攻击，直到某些其他事件通过激活邻居建立路由为止。UDLD 正常模式可以缓和这些情况，因为它会检测单向链路故障并且错误会使端口禁用。

对于使用任何路由协议的第 3 层路由连接，UDLD 正常模式仍可保护其不受初始链路激活时的问题（例如布线错误或硬件故障）的影响。另外，UDLD 主动模式对第 3 层路由连接也具有以下优势：

- 防止不必要的流量黑洞（在某些情况下需要最低的计时器）
- 将一个抖动链路置于 errdisable 状态
- 防止出现第 3 层 EtherChannel 配置导致的环路

UDLD 的默认行为

默认情况下，UDLD 全局禁用并准备在光纤端口上启用。由于 UDLD 是只在交换机之间才需要的基础结构协议，因此默认情况下在经常用于主机访问的铜线端口上禁用 UDLD。请注意，必须全局启用 UDLD 并将其置于接口级别，邻居才能达到双向状态。默认消息间隔是 15 秒。但是，在某些情况下，默认消息间隔会显示为 7 秒。有关详细信息，请参阅Cisco Bug ID CSCea70679 (仅注册客户)。默认消息间隔可在 7 到 90 秒之间进行配置，并且 UDLD 主动模式处于禁用状态。Cisco IOS 软件版本 12.2(25)SEC 进一步将此最低计时器值降低到 1 秒。

Cisco 配置建议

在绝大多数情况下，Cisco 建议在 Cisco 交换机之间的所有点对点 FE/GE 链路上启用 UDLD 正常模式，并在使用默认 802.1D 生成树计时器时，将 UDLD 消息间隔设置为 15 秒。另外，在依赖 STP 实现冗余和收敛的网络中（这表示拓扑中的一个或多个端口处于 STP 阻塞状态），请将 UDLD 与适当的功能和协议一起使用。这些功能包括 FEFI、自动协商、环路防护等等。一般情况下，如果启用了自动协商，则不必使用主动模式，因为自动协商可针对第 1 层的故障检测进行纠正。

发出以下两个命令选项之一以启用 UDLD：

注意：不同平台/版本的语法已发生更改。

-

```
udld enable
!--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default.
udld port
```

或

-

```
udld enable
!--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled
by individual port command.
```

您必须手动启用由于单向链路症状而关闭的端口。请使用以下方法之一：

```
udld reset
!--- Globally reset all interfaces that UDLD shut down. no udld port
udld port [aggressive]
!--- Per interface, reset and reenable interfaces that UDLD shut down.
```

errdisable recovery cause udld 和 **errdisable recovery interval** *interval* 全局配置命令可用于从 UDLD 错误禁用状态进行自动恢复。

如果对交换机的物理访问很困难，Cisco 建议您只在网络的接入层使用 errdisable 恢复机制，并使用 20 分钟或更长的恢复计时器。最佳的情况是在端口重新上线并导致网络不稳定性之前，让网络有时间稳定和排除故障。

Cisco 建议您*不要 在网络的核心处使用恢复机制，因为这可能导致每当有故障的链路重新接通时出现与收敛事件相关的不稳定性*。核心网络的冗余设计为发生故障的链路提供备用路径，并且留出时间来调查 UDLD 故障的原因。

在无 STP 环路防护的情况下使用 UDLD

对于第 3 层点对点链路或具有无环路 STP 拓扑（没有阻塞端口）的第 2 层链路，Cisco 建议您在 Cisco 交换机之间的点对点 FE/GE 链路上启用主动 UDLD。在这种情况下，消息间隔设置为 7 秒，并且 802.1D STP 使用默认计时器。

EtherChannel 上的 UDLD

无论是否已部署 STP 环路防护，对于任何 EtherChannel 配置，建议将 UDLD 主动模式与 desirable 信道模式一起使用。在 EtherChannel 配置中，如果信道链路捆绑解开，则在传送生成树 BPDU 和 PAgP 控制流量的信道的链路发生故障时，可能会导致信道伙伴之间立即出现环路。UDLD 主动模式会关闭有故障的端口。然后，PAgP（auto/desirable 信道模式）可以协商一条新的控制链路，并从信道中有效排除发生故障的链路。

UDLD 与 802.1w 生成树

为了防止出现环路，当您使用较新的生成树版本时，请将 UDLD 正常模式和 STP 环路防护与 RSTP（如 802.1w）一起使用。UDLD 可防止在联结阶段出现单向链路，而 STP 环路防护可防止在 UDLD 将链路建立为双向*之后 链路变为单向时出现 STP 环路*。由于不能将 UDLD 配置为比默认 802.1w 计时器更低，因此必须使用 STP 环路防护以完全防止在冗余拓扑中出现环路。

有关详细信息，请参阅[了解和配置单向链路检测协议 (UDLD) 功能。]

测试和监控 UDLD

如果在实验室中不存在确实有故障或者单向的组件（如发生故障的 GBIC），就不太容易测试 UDLD。此协议设计用来检测的故障情形要比实验室中经常出现的故障情形更为少见。例如，如果想执行一个简单测试（例如拔掉一个光纤束）以便观察所需的 `errdisable 1` 否则，物理端口会进入 `down` 状态，这会重置 UDLD 消息通信。在 UDLD 正常模式下，远程终端会进入 `undetermined UDLD errdisable`

有一种附加测试方法模拟 UDLD 的邻居 PDU 丢失。该方法使用 MAC 层过滤器阻止 UDLD/CDP 硬件地址，但您可以允许其他地址通过。当端口配置为交换端口分析程序 (SPAN) 目标时，某些交换机不发送 UDLD 帧，以模拟无响应的 UDLD 邻居。

为了监控 UDLD，请使用下面的命令：

```
show udld gigabitethernet1/1
Interface Gi1/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7
Time out interval: 5
```

另外，还可以从 Cisco IOS 软件版本 12.2(18)SXD 或更高版本的交换机中的启用模式发出 **show udld neighbor 隐藏命令来（以与 CDP 相同的方式）检查 UDLD 缓存内容。** 这通常对于将 UDLD 缓存与 CDP 缓存进行比较来验证是否存在特定于协议的异常非常有用。只要 CDP 也受影响，也就常常表示所有 BPDU/PDU 均受影响。因此，还需要检查 STP。例如，请检查是否存在最近进行的根身份更改或根/指定端口放置更改。

您可以使用 Cisco UDLD SNMP MIB 变量监控 UDLD 状态和配置的一致性。

多层交换

概述

在 Cisco IOS 系统软件中，Catalyst 6500/6000 系列支持多层交换 (MLS)，并且仅限于在内部支持。这表示必须在交换机中安装路由器。比较新的 Catalyst 6500/6000 Supervisor 引擎支持 MLS CEF，其中会将路由表下载到每个卡上。这需要安装额外的硬件，其中包括安装 Distributed Forwarding Card (DFC)。CatOS 软件不支持 DFC，即使您选择在路由器卡上使用 Cisco IOS 软件也是如此。仅 Cisco IOS 系统软件支持 DFC。

用来在 Catalyst 交换机上启用 NetFlow 统计信息的 MLS 缓存是 Supervisor 引擎 I 卡和传统 Catalyst 交换机用于启用第 3 层交换的、基于流的缓存。默认情况下，MLS在带有MSFC或MSFC2的Supervisor引擎1（或Supervisor引擎1A）上启用。默认MLS功能无需其他MLS配置。您可以在以下三种模式中的一种模式中配置 MLS 缓存：

- 目的地
- 源-目标
- 源-目标端口

流掩码用于确定交换机的 MLS 模式。这些数据随后用于启用配有 Supervisor 引擎 IA 的 Catalyst 交换机中的第 3 层流。Supervisor 引擎 II 刀片不使用 MLS 缓存交换数据包，因为此卡支持硬件 CEF（一项更易于扩展的技术）。MLS 缓存保存在 Supervisor 引擎 II 卡中，以便只启用 NetFlow 统计信息导出功能。因此，可以根据需要对 Supervisor 引擎 II 启用全流，而不会对路由器产生负面影响。

配置

MLS 老化时间适用于所有 MLS 缓存条目。老化时间值直接应用于目标模式老化。将 MLS 老化时间值除以二可得到“源-至-目标”模式老化时间。将 MLS 老化时间值除以八可得到全流老化时间。默认 MLS 老化时间值为 256 秒。

您可以按 8 秒的增量在 32 到 4092 秒的范围内配置正常老化时间。任何不是 8 秒倍数的老化时间值都会被调整到最接近 8 秒倍数的值。例如，值65调整为64，值127调整为128。

其他事件可能导致 MLS 条目被清除。此类事件包括：

- 路由更改
- 链路状态变化例如，PFC 链路断开。

为使 MLS 缓存大小保持在 32,000 个条目以下，请在发出 **mls aging 命令之后启用以下参数：**

```
Normal: configures the wait before aging out and deleting shortcut entries in
the L3 table.

Fast aging: configures an efficient process to age out entries created for flows that
only switch a few packets and then are never used again. The fast aging parameter uses
the time keyword value to check if at least the threshold keyword value of packets has
been switched for each flow. If a flow has not switched the threshold number of packets
during the time interval, then the entry in the L3 table is aged out.

Long: configures entries for deletion that have been up for the specified value even if
the L3 entry is in use. Long aging is used to prevent counter wraparound, which could
cause inaccurate statistics.
```

配置

移除的典型缓存条目是在创建之后可能就再也不被使用的、流入和流出域名服务器 (DNS) 或 TFTP 服务器的条目。检测出这些条目并使之老化可节省 MLS 缓存中的空间以供其他数据流量使用。

如果需要启用 MLS 快速老化时间，请将初始值设为 128 秒。如果MLS缓存的大小继续增长超过32,000个条目，请减小设置，直到缓存大小保持在32,000以下。如果缓存继续增长超过32,000个条目，请缩短正常MLS老化时间。

Cisco 推荐的 MLS 配置

除非需要使用 NetFlow 导出功能，否则将 MLS 保留为默认值 destination only。如果需要使用 NetFlow，请仅在 Supervisor 引擎 II 系统上启用 MLS 全流。

发出下面的命令可启用 MLS 流目标：

```
Switch(config)#mls flow ip destination
```

巨型帧

最大传输单位

最大传输单元 (MTU) 是接口可以发送或接收而无需对数据包进行分段的最大数据报或数据包大小（以字节为单位）。

根据 IEEE 802.3 标准，最大以太网帧大小为：

- **对于常规帧为 1518 字节（1500 个字节加上以太网报头和 CRC 报尾的 18 个附加字节）**
- **对于 802.1Q 封装帧为 1522 字节（1518 加上标记的 4 个字节）**

小巨型帧：小巨型帧功能使交换机可以传输/转发比 IEEE 以太网 MTU 略大的数据包，而不是宣布这些帧过大而丢弃它们。

巨型:帧大小的定义取决于供应商，因为帧大小不在 IEEE 标准的规定范围内。超巨型帧是大于标准以太网帧大小（为 1518 字节，其中包括第 2 层报头和帧校验序列 [FCS]）的帧。

在单个端口上启用超巨型帧支持后，默认的 MTU 大小为 9216 字节。

何时期望大于 1518 字节的数据包

为了跨交换网络传输数据流，必须确保被传输的数据流 MTU 不超过交换机平台支持的大小。以下多种原因均会造成某些帧的 MTU 大小被截断：

- **供应商特定的要求 - 应用程序和某些 NIC 可能会指定超出标准的 1500 字节的 MTU 大小。**之所以会出现此更改，是因为有研究证明增加以太网帧的大小可以增加平均吞吐量。
- **中继 — 为了在交换机或其他网络设备之间传递 VLAN ID 信息，使用中继来增大标准的以太网帧。**目前，最为常见的两种中继形式是：Cisco 专有的 ISL 封装802.1Q
- **多协议标签交换 (MPLS) - 在某个接口上启用 MPLS 之后，MPLS 有可能会增大数据包的帧大小，具体取决于 MPLS 标记数据包的标签堆栈中的标签数量。**一个标签的总大小为 4 字节。标签堆栈的总大小为：
  ```
  n * 4 bytes
  ```
  如果形成了标签堆栈，则帧数可能会超过 MTU。
- **802.1Q隧道** - 802.1Q隧道数据包包含两个802.1Q标记，其中每次只有一个标记通常对硬件可见。因此，内部标记会对 MTU 值（有效负载大小）添加 4 字节。
- **通用传输接口(UTI)/第2层隧道协议第3版（第2层TPv3）** - UTI/第2层TPv3封装要通过IP网络转发的第2层数据。UTI/Layer 2TPv3 可将原始帧大小增大多达 50 字节。新的帧包括一个新的 IP 报头（20 字节）、一个 Layer 2TPv3 报头（12 字节）和一个新的第 2 层报头。Layer 2TPv3 有效负载包括完整的第 2 层帧，而第 2 层帧包括第 2 层报头。

目的

基于硬件的高速（1 Gbps 和 10 Gbps）交换技术使超巨型帧成为针对非优化吞吐量问题的、一种非常具体的解决方案。即使超巨型帧大小没有正式标准，但此领域中经常采用的一个相当常见的值为 9216 字节 (9 KB)。

网络效率注意事项

您可通过将数据包转发的有效负载大小除以开销值和有效负载大小的总和来计算数据包转发的网络效率。

即使超巨型帧只能适度增加网络效率，从 94.9%（1500 字节）增加到 99.1%（9216 字节），但网络设备和终端主机的处理开销（CPU 使用率）也会与数据包大小成比例地降低。这就是高性能的 LAN 和 WAN 网络技术趋向于使用在一定程度上大一些的最大帧大小的原因。

仅当执行长数据传输时，才有可能提高性能。应用示例包括：

- 服务器背靠背通信（例如，网络文件系统 [NFS] 事务）
- 服务器集群
- 高速数据备份
- 高速超级计算机互连
- 图形应用程序数据传输

网络性能方面

现已对 WAN (Internet) 上的 TCP 性能进行了广泛的研究。下面的公式解释了以下因素如何决定 TCP 吞吐量的上限：

- 最大数据段大小 (MSS)，即 MTU 长度减去 TCP/IP 报头长度
- 往返时间 (RTT)
- 数据包丢失率

$$Throughput \leq\sim 0.7 \times MSS / \left(RTT \times \sqrt{packet\_loss}\right)$$

根据上面的公式，可达到的最大 TCP 吞吐量与 MSS 成正比。这表示在 RTT 和数据包丢失率恒定的情况下，如果数据包大小加倍，可使 TCP 吞吐量也加倍。同样，在使用超巨型帧而不使用 1518 字节帧的情况下，数据包大小增加六倍有可能使以太网连接上的 TCP 吞吐量也增加六倍。

操作概述

IEEE 802.3 标准规范定义了一个最大以太网帧大小 **1518**。后来，根据 IEEE 标准 802.3ac-1998 附录，在 802.3 规范中增加了 802.1Q 封装的帧（长度介于 1519 和 1522 字节之间）。有时在文件中称它们为**小巨型帧**。

通常，当数据包超过特定以太网连接的指定以太网最大长度时，就会将数据包归类为**巨型帧**。巨型数据包也称为**超巨型帧**。

超巨型帧最容易让人混淆的一点是配置：不同的接口支持不同的最大数据包大小，有时处理大数据包的方式也稍有不同。

Catalyst 6500 系列

下表尝试总结了 Catalyst 6500 平台上的不同卡目前所支持的 MTU 大小：

线路卡	MTU 大小
默认	9216 字节
WS-X6248-RJ-45、WS-X6248A-RJ-45、WS-X6248-TEL、WS-X6248A-TEL、WS-X6348-RJ-45、WS-X6348-RJ45V、WS-X6348-RJ-21 和 WX-X6348-RJ21V	8092 字节（受 PHY 芯片限制）
WS-X6148-RJ-45(V)、WS-X6148-RJ-21(V)、WS-X6148-45AF 和 WS-X6148-21AF	9100字节 (100 Mbps)9216 字节(10 Mbps)
WS-X6516-GE-TX	8092字节 (100 Mbps)9216 字节（10或1000 Mbps）
WS-X6148(V)-GE-TX、WS-X6148-GE-45AF、WS-X6548(V)-GE-TX 和 WS-X6548-GE-45AF	1500 字节
OSM ATM (OC12c)	9180 字节
OSM CHOC3、CHOC12、CHOC48 和 CT3	9216字节（OCx和DS3）7673

	字节(T1/E1)
FlexWAN	7673字节(CT3 T1/DS0)9216字节(OC3c POS)7673字节(T1)
WS-X6148-GE-TX 和 WS-X6548-GE-TX	不支持

有关详细信息，请参阅配置以太网、快速以太网、千兆以太网和 10 千兆以太网交换。

Catalyst 6500/6000 Cisco IOS 软件中的第 2 层和第 3 层超巨型帧支持

配置为第 2 层和第 3 层物理接口的所有 GE 端口上存在 PFC/MSFC1、PFC/MSFC2 和 PFC2/MSFC2 对第 2 层和第 3 层超巨型帧的支持。无论这些端口是中继还是信道，都存在这些支持。Cisco IOS 软件版本 12.1.1E 及更高版本中提供了此功能。

- 所有启用超巨型帧的物理端口的 MTU 大小均绑定在一起。只要其中一个改变，所有其他的也会随着改变。启用它们之后，它们总是保持相同的超巨型帧 MTU 大小。
- 配置时，要么对同一 VLAN 中的所有端口启用超巨型帧，要么不对任何端口启用超巨型帧。
- 分别设置交换虚拟接口 (SVI)（VLAN 接口）MTU 大小和物理端口 MTU。物理端口 MTU 的变化不会更改 SVI MTU 的大小。此外，SVI MTU 的变化不影响物理端口 MTU。
- FE接口上的第2层和第3层巨型帧支持始于Cisco IOS软件版本12.1(8a)EX01。**mtu 1500** 命令禁用FE上的巨型帧，**mtu 9216** 命令启用FE上的巨型帧。请参阅Cisco Bug ID CSCdv90450 (仅限注册客户)。
- 仅以下卡支持 VLAN 接口上的第 3 层超巨型帧：PFC/MSFC2（Cisco IOS 软件版本 12.1(7a)E 及更高版本）PFC2/MSFC2（Cisco IOS 软件版本 12.1(8a)E4 及更高版本）
- 建议不要对 PFC/MSFC1 的 VLAN 接口 (SVI) 使用超巨型帧，因为 MSFC1 可能无法按要求处理分段。
- 不支持对同一 VLAN（第 2 层超巨型帧）内的数据包进行分段。
- VLAN/子网（第 3 层超巨型帧）上需要分段的数据包会发送到软件以进行分段。

了解 Catalyst 6500/6000 Cisco IOS 软件中的超巨型帧支持

超巨型帧是大于默认以太网帧大小的帧。若要启用超巨型帧支持，应在端口或 VLAN 接口上配置大于默认值的 MTU 大小，而对于 Cisco IOS 软件版本 12.1(13)E 及更高版本，应配置全局 LAN 端口 MTU 大小。

Cisco IOS 软件中的桥接和路由流量大小检查

线路卡	入口	出口
10、10/100、100 Mbps 端口	MTU 大小检查完成。超巨型帧支持比较配置有非默认 MTU 大小的入口 10、10/100 和 100 Mbps 以太网以及 10 GE LAN 端口上的入口流量大小与全局 LAN 端口 MTU 大小。端口将丢弃过大的数据流。	MTU 大小检查未完成。配置有非默认 MTU 大小的端口传输包含大于 64 字节所有大小的数据包的帧。配置非默认 MTU 大小后，10、10/100 和 100 Mbps 以太网 LAN 端口不检查过大的出口帧。

GE 端口	MTU 大小检查未完成。配置有非默认 MTU 大小的端口接受包含大于 64 字节的所有大小的数据包的帧，并且不检查过大的入口帧。	MTU 大小检查完成。超巨型帧支持比较配置有非默认 MTU 大小的出口 GE 和 10 GE LAN 端口上的出口流量大小和全局出口 LAN 端口 MTU 大小。端口将丢弃过大的数据流。
10 GE 端口	MTU 大小检查完成。端口将丢弃过大的数据流。	MTU 大小检查完成。端口将丢弃过大的数据流。
SVI	MTU 大小检查未完成。SVI 不检查入口端的帧大小。	MTU 大小检查完成。在 SVI 的出口端检查了 MTU 大小。
	PFC	
所有路由的数据流	对于必须路由的数据流，PFC 上的超巨型帧支持可比较数据流大小与配置的 MTU 大小；如果接口所配置的 MTU 大小足以容纳超巨型帧数据流，此支持可为此类接口之间的超巨型帧数据流提供第 3 层交换。在没有配置有足够大的 MTU 大小的接口之间： • 如果没有设置“不分段”(DF) 位，则 PFC 将数据流发送到 MSFC 以便在软件中进行分段和路由。 • 如果设置 DF 位，PFC 会丢弃数据流。	

Cisco 建议

如果以适当的方法实施，超巨型帧可能使以太网连接的 TCP 吞吐量增长六倍，并降低分段开销（还可降低终端设备上的 CPU 开销）。

您必须确保连接之间不会出现无法处理指定 MTU 大小的设备。如果此设备分段并且转发数据包，将使整个过程无效。这将给此设备带来数据包分段和重组的额外开销。

在此类情况下，IP 路径 MTU 发现有助于发送方查找适合沿每条路径传输数据流的最低公共数据包长度。或者，您可以使用网络中所有支持的 MTU 大小中最小的一个来配置支持超巨型帧的主机设备。

您必须仔细检查每个设备以确保其可以支持相应的 MTU 大小。请参阅此部分中的 MTU 大小支持表。

可以在以下类型的接口上启用超巨型帧支持：

- 端口信道接口
- SVI
- 物理接口（第 2 层/第 3 层）

您可以在端口信道或加入端口信道的物理接口上启用超巨型帧。确保所有物理接口上的 MTU 相同非常重要。否则，可能导致接口暂停。因为这会更改所有成员端口的 MTU，因此需要更改端口信道接口的 MTU。

注意：如果成员端口的MTU不能更改为新值，因为成员端口是阻塞端口，则端口通道将挂起。

请始终确保在 SVI 上配置超巨型帧支持之前，将 VLAN 中的所有物理接口配置为支持超巨型帧。在 SVI 的输入端不检查数据包的 MTU。但是，在 SVI 的输出端会进行此检查。如果数据包 MTU 大于输出 SVI MTU，则数据包由软件分段（如果没有设置 DF 位），这将导致性能低下。软件分段仅在第 3 层交换时发生。当数据包转发到具有较小 MTU 的第 3 层端口或 SVI 时，将发生软件分段。

SVI 的 MTU 必须总是小于 VLAN 中所有交换机端口中最小的 MTU。

Catalyst 4500 系列

超巨型帧主要在 Catalyst 4500 板卡的无阻塞端口上受到支持。这些无阻塞 GE 端口具有到 Supervisor 引擎交换结构的直接连接并且支持超巨型帧：

- Supervisor 引擎WS-X4515、WS-X4516 - Supervisor引擎IV或V上的两个上行链路GBIC端口WS-X4516-10GE — 两个10 GE上行链路和四个1 GE小型封装热插拔(SFP)上行链路WS-X4013+ — 两个1 GE上行链路WS-X4013+10GE — 两个10 GE上行链路和四个1 GE SFP上行链路WS-X4013+TS - 20个1-GE端口
- 线卡WS-X4306-GB — 六端口1000BASE-X(GBIC)GE模块WS-X4506-GB-T — 六端口10/100/1000-Mbps和六端口SFPWS-X4302-GB — 双端口1000BASE-X(GBIC)GE模块18 端口服务器交换 GE 模块 (WS-X4418-GB) 的前两个 GBIC 端口和 WS-X4232-GB-RJ 模块的 GBIC 端口
- 固定配置交换机WS-C4948 — 所有48个1-GE端口WS-C4948-10GE — 所有48个1-GE端口和两个10-GE端口

您可以使用这些无阻塞 GE 端口以支持 9 KB 超巨型帧或硬件广播抑制（仅限 Supervisor 引擎 IV）。 所有其他板卡支持小巨型帧。对于 MPLS 桥接或最大有效负载为 1552 个字节的 Q in Q 通过能力，可以使用小巨型帧。

注意：帧大小随ISL/802.1Q标记而增加。

小巨型帧和超巨型帧对于带有 Supervisor 引擎 IV 和 V 的其他 Cisco IOS 功能是透明的。

Cisco IOS 软件安全功能

基本安全功能

曾有一段时间，安全在园区网络设计中经常被忽略了。但是，现在安全是每个企业网络的重要部分。通常情况下，客户端已建立了安全策略以帮助定义可以适用哪些 Cisco 工具和技术。

基本口令保护

大多数 Cisco IOS 软件设备配置有两个级别的口令。第一个级别用于通过 Telnet 访问设备（也称 vty 访问）。在准许 vty 访问后，您需要获得对 enable 模式或特权 exec 模式的访问权限。

确保交换机 Enable 模式的安全

通过启用口令用户可以获得设备的完全访问权限。请仅向可靠人员提供启用口令。

```
Switch(config)#enable secret password
```

务必使口令遵循以下规则：

- 口令必须包含 1 至 25 个大写和小写字母数字字符。
- 口令的第一个字符不能是数字。
- 您可以使用前置空格，但是会被忽略。中间和尾部空格可被识别。
- 口令检查区分大小写。例如，口令 Secret 与口令 secret 不同。

注意：使能加密命令使用单向加密消息摘要5(MD5)散列函数。如果发出 **show running-config 命令，您可以看到此加密口令。**使用 **enable password 命令是设置启用命令的另一种方式。**但是，与 **enable password 命令一起使用的加密算法很弱，容易通过反向工程获得口令。**所以，请勿使用 **enable password 命令。**请使用 **enable secret 命令以获得更高的安全性。**有关详细信息，请参阅 Cisco IOS 口令加密相关信息。

保障对交换机的 Telnet/VTY 访问的安全性

默认情况下，Cisco IOS 软件支持 5 个活动 Telnet 会话。这些会话称为vty 0到4。您可以启用这些线路进行访问。但是为了启用登录，您还需要设置这些线路的口令。

```
Switch(config)#line vty 0 4
Switch(config-line)#login
Switch(config-line)#password password
```

login 命令用于配置这些线路以进行 Telnet 访问。password 命令用于配置口令。务必使口令遵循以下规则：

- 第一个字符不能为数字。
- 字符串可以包含任何字母数字字符，最多 80 个字符。字符包含空格。
- 不能以“数字-空格-字符”格式指定口令。在数字后的空格容易引起问题。例如，hello 21 是一个合法的口令，但是 21 hello 不是一个合法的口令。
- 口令检查区分大小写。例如，口令 Secret 与口令 secret 不同。

注意：使用此vty线路配置，交换机以明文形式存储密码。如果某个用户发出 **show running-config 命令，则可以看到此口令。**为了避免此情况，请使用 **service password-encryption 命令。**该命令可以松散地加密口令。该命令只加密 vty 线路口令和通过 **enable password 命令配置的启用口令。**通过 **enable secret 命令配置的启用口令使用更强的加密。**建议采用通过 **enable secret 命令进行配置的方法。**

注意：为了在安全管理方面具有更大的灵活性，请确保所有Cisco IOS软件设备都实施身份验证、授权和记帐(AAA)安全模型。AAA 可以使用本地、RADIUS 和 TACACS+ 数据库。有关详细信息，请参阅 TACACS+ 身份验证配置部分。

AAA 安全服务

AAA 操作概述

访问控制用来控制哪些用户有权访问交换机，并且控制这些用户可以使用什么服务。AAA 网络安全服务提供用于在交换机上设置访问控制的主要框架。

以下部分详细描述 AAA 的各个方面：

- 身份验证 - 此过程验证最终用户或设备所声称的身份。首先，指定可以用来验证用户的多种方法。这些方法定义了要执行的身份验证类型（例如，TACACS+ 或 RADIUS）。 此外，还定义了尝试这些身份验证方法的顺序。然后将这些方法应用至适当的接口，从而激活身份验证。
- 授权 - 此过程向用户、用户组、系统或者某个进程授予访问权限。AAA 过程可执行一次性授权或者基于每个任务进行授权。该过程定义了用户具有执行权限的属性（在 AAA 服务器上）。每当用户试图启动一项服务时，交换机就会查询 AAA 服务器，并请求允许对该用户进行授权。如果 AAA 服务器批准，则对该用户授权。如果 AAA 服务器不批准，则用户没有获得执行该服务的权限。您可以使用此过程以指定某些用户只能执行特定的命令。
- 记账 - 使用此过程可以追踪用户访问的服务，以及用户使用的网络资源数量。当启用记账时，交换机将以计费记录的形式向 AAA 服务器报告用户活动情况。例如，报告的用户活动情况包括会话时间以及开始和截止时间。然后，可以分析此活动情况以实现管理或计费目的。

虽然 AAA 是访问控制的主要和推荐方法，不过除 AAA 之外，Cisco IOS 软件还提供了用于简单访问控制的附加功能。这些附加功能包括：

- 本地用户名验证
- 线路口令验证
- 启用口令身份验证

但是这些功能不可能提供与 AAA 同一程度的访问控制。

为了更好地了解 AAA，请参阅以下文档：

- 验证、授权和记帐 (AAA)
- 在接入服务器上配置基本 AAA
- TACACS+ 和 RADIUS 的比较

这些文档不一定提及交换机。但是这些文档描述的 AAA 概念适用于交换机。

TACACS+

目的

默认情况下，非特权和特权模式口令是全局口令。这些口令适用于每个访问交换机或路由器的用户，无论这些用户是从控制台端口访问，还是通过网络上的 Telnet 会话访问。这些口令在网络设备上的实施过程很耗时，并且不是集中处理。此外，使用易于引起配置错误的访问控制列表 (ACL) 来实施访问限制可能存在困难。为了解决这些问题，我们可以采取集中方式，在中央服务器上配置用户名、口令和访问策略。此服务器可以是 Cisco 安全访问控制服务器 (ACS) 或任何第三方服务器。对这些设备进行配置以使用这些集中式数据库执行 AAA 功能。这里所指的设备是 Cisco IOS 软件交换机。以下是可用于该设备和中央服务器之间的协议：

- TACACS+
- RADIUS
- Kerberos

TACACS+ 是 Cisco 网络中的常见部署，同时也是本部分的重点。TACACS+ 提供以下功能：

- 身份验证 - 识别和验证用户的过程。可以使用多种方法来验证用户。但是最常用的方法包括组合使用用户名和口令。
- 授权 - 当用户尝试执行命令时，交换机可与 TACACS+ 服务器核对，以确定用户是否获得使用该特定命令的授权。
- 记账 - 此过程记录用户在设备上执行或已执行的操作。

有关 TACACS+ 和 RADIUS 之间的比较，请参阅 TACACS+ 与 RADIUS 的比较。

操作概述

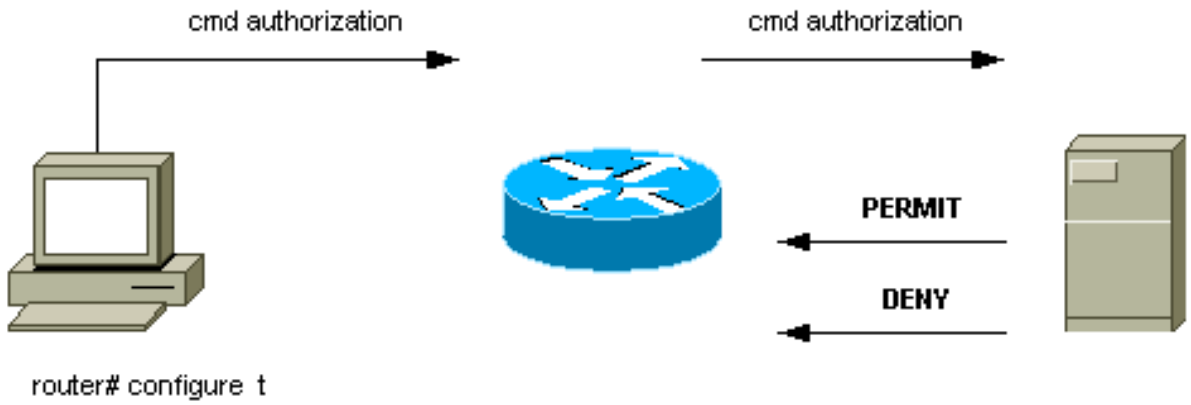
TACACS+ 协议将用户名和口令转发到集中式服务器。此信息在网络上使用 MD5 单向哈希算法进行加密。有关详细信息，请参阅 RFC 1321。 TACACS+ 使用 TCP 端口 49 作为传输协议，这与使用 UDP 相比有下列优点：

注意：RADIUS使用UDP。

- 面向连接的传输
- 表示已收到请求的单独确认（TCP 确认 [ACK]），与后台身份验证机制的加载方式无关
- 立即指示服务器崩溃情况（重置 [RST] 数据包）

在会话期间，如果需要进行额外的授权检查，那么交换机会与 TACACS+ 进行核对，以确定是否授予了用户使用特定命令的权限。此步骤能够更好地控制可在交换机上执行的命令，并实现与身份验证机制的分离。利用命令记账，可以审核特定用户在连接到特定网络设备期间该用户所发出的命令。

此图表显示的是所涉及的授权过程：



如果用户在尝试简单的 ASCII 登录时使用 TACACS+ 向网络设备进行身份验证，通常会发生以下过程：

- 建立连接后，交换机与 TACACS+ 后台程序联系以获得用户名提示。然后交换机向用户显示提示。用户输入用户名，交换机便与 TACACS+ 后台程序通信以获得口令提示。交换机向用户显示口令提示，用户输入口令，该口令也将发送到 TACACS+ 后台程序。
- 最后，网络设备从 TACACS+ 后台程序收到下列响应之一：ACCEPT - 如果网络设备配置为需要授权，则此时会开始授权。REJECT - 可能会拒绝用户进一步访问或者提示用户重试登录序列。具体结果取决于 TACACS+ 后台程序。ERROR - 此错误可能发生在后台程序中，也可能发生在后台程序和交换机之间的网络连接中。如果收到 ERROR CONTINUE -
- 用户必须首先成功完成 TACACS+ 身份验证才能进行 TACACS+ 授权。
- 如果需要 TACACS+ 授权，将再次联系 TACACS+ 后台程序。TACACS+ 后台程序返回 ACCEPT REJECT 如果返回 ACCEPT EXEC NETWORK 这将确定用户能访问哪些命令。

AAA 基本配置步骤

在您了解基本过程之后，配置 AAA 相当简单。要使用 AAA 在 Cisco 路由器或接入服务器上配置安全性，请执行下列这些步骤：

1. 要启用 AAA，请发出 **aaa new-model 全局配置命令。**
   ```
   Switch(config)#aaa new-model
   ```

   提示：在配置AAA命令之前保存配置。只有在您完成了所有 AAA 配置并对配置正确运行感到满意之后，才应当再次保存配置。然后，如果需要，您可以重新加载交换机，以便从未预见到的锁定恢复（在保存配置之前）。
2. 如果您决定使用独立的安全服务器，请配置安全协议参数，例如 RADIUS、TACACS+ 或 Kerberos。
3. 要定义身份验证的方法列表，请使用 **aaa authentication 命令。**
4. 要将方法列表应用于特定接口或线路，请使用 **login authentication 命令。**
5. 要配置授权，请发出可选的 **aaa authorization 命令。**
6. 要配置记账，请发出可选的 **aaa accounting 命令。**
7. 配置 AAA 外部服务器以处理来自交换机的身份验证和授权请求。**注意：** 有关详细信息，请参阅 AAA 服务器文档。

TACACS+ 身份验证配置

要配置 TACACS+ 身份验证，请执行下列步骤：

1. 要在交换机上启用 AAA，请在全局配置模式下发出 **aaa new-model 命令。**
2. 定义 TACACS+ 服务器和关联的密钥。此密钥用于对 TACACS+ 服务器和交换机之间的数据流进行加密。在 **tacacs-server host 1.1.1.1 key mysecretkey 命令中，TACACS+ 服务器位于 IP 地址 1.1.1.1，加密密钥为 mysecretkey。**为了验证交换机能够到达 TACACS+ 服务器，请从交换机启动 Internet 控制消息协议 (ICMP) ping。
3. 定义方法列表。方法列表定义了用于尝试各种服务的身份验证机制序列。各种服务可以是如下服务：enable登录（以进行 vty/Telnet 访问）**注：有**关vty/Telnet访问的信息，请参阅本文档的基本安全功能部分。控制台此示例仅考虑**登录。**您必须将方法列表应用于接口/线路：
   ```
   Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line
   Switch(config)#line vty 0 4
   Switch(config-line)#login authentication METHOD-LIST-LOGIN
   Switch(config-line)#password hard_to_guess
   ```

   在此配置中，**aaa authentication login 命令使用虚构的列表名称 METHOD-LIST-LOGIN 并在使用方法线路之前使用方法 tacacs+。**使用 TACACS+ 服务器作为第一种方法，对用户进行身份验证。如果 TACACS+ 服务器不响应或发送 ERROR 消息，则使用线路中配置的口令作为第二种方法。但是，如果 TACACS+ 服务器拒绝用户，并且使用 REJECT 消息来响应，则 AAA 将事务视为成功，不使用第二种方法。**注意：**在您将列表(METHOD-LIST-LOGIN)应用到vty线路之前，配置不完成。在线路配置模式下发出 **login authentication METHOD-LIST-LOGIN 命令，如示例所示。注意：**本示例为TACACS+服务器不可用时创建后门。安全管理员可能接受后门的实现，也可能不能接受后门的实现。请确保实现此类后门的决策符合站点的安全策略。

RADIUS 身份验证配置

RADIUS 配置几乎与 TACACS+ 配置完全相同。只需将配置中的 TACACS 一词替换为 RADIUS。下面是 COM 端口访问的示例 RADIUS 配置：

```
Switch(config)#aaa new-model
Switch(config)#radius-server host 1.1.1.1 key mysecretkey
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group radius line
Switch(config)#line con 0
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

登录 标识

创建适当的设备标语，这些标语专门陈述在遇到未经授权的访问时采取的操作。请勿将站点名称或网络信息发布给未经授权的用户。万一设备受到威胁，并且攻击者被捉住，那么这些标语将可提供追索权。要创建登录标语，请发出以下命令：

```
Switch(config)#banner motd ^C
*** Unauthorized Access Prohibited ***
^C
```

物理安全

确保需要正确的授权才能物理访问设备。将设备放置在一个受控的（加锁的）空间。为了确保网络一直运行正常，且不受恶意篡改或环境因素的影响，请确保所有设备具有：

- 适当的不间断电源 (UPS)，并尽可能有冗余电源
- 温度控制（空调）

请记住，如果恶意攻击者侵入物理访问，则他们更有可能通过口令恢复或其他手段进行干扰。

管理配置

网络图

目的

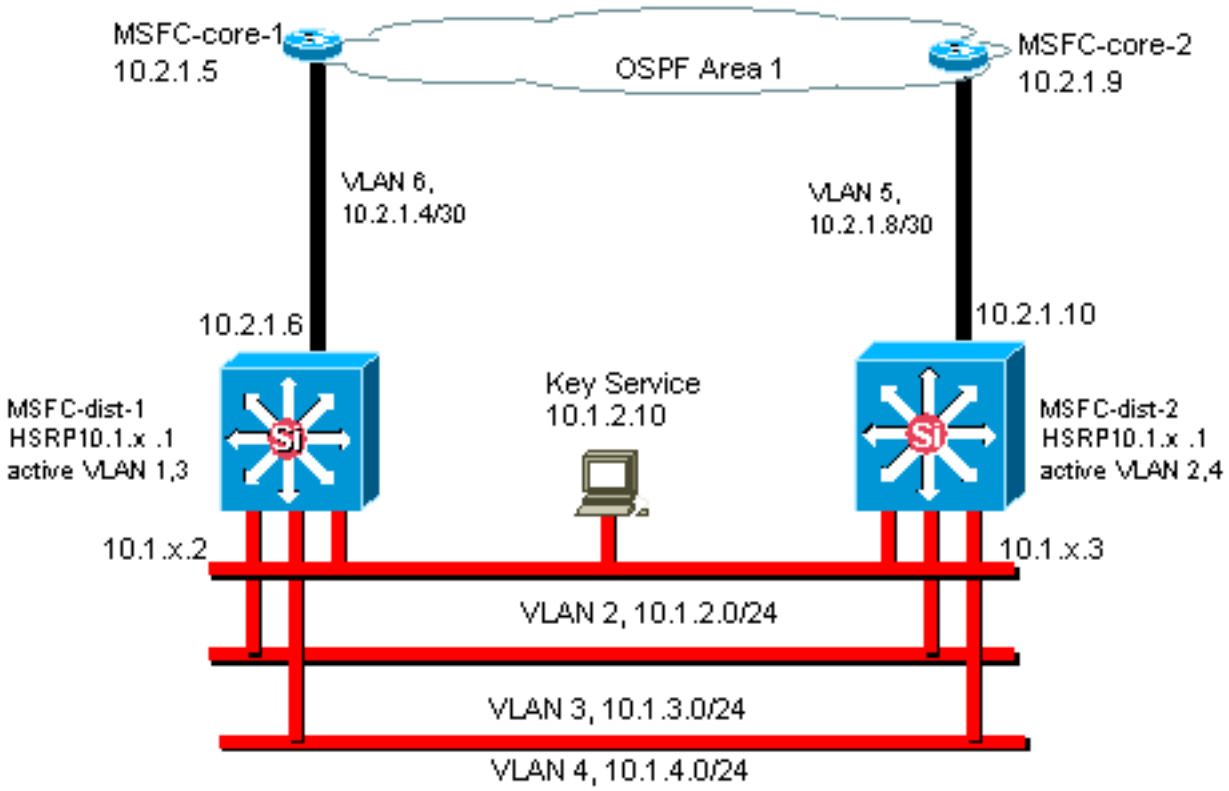
清晰的网络图是网络运行的一个基本部分。网络图在进行故障排除时非常重要，而且在由于发生中断而向供应商和合作伙伴上报时，网络图也是最为重要的信息交流工具。请勿低估网络图提供的准备、就绪和可访问性。

建议

下列三种图表是必需的：

- **整体图表 - 即使对于最大型的网络，显示端到端的物理或逻辑连接性的图表也是非常重要的。**通常，已实现层次化设计的企业会单独记录每一层。当您计划并解决问题时，了解域的链接方式是非常重要的。
- **物理图表 - 此图显示所有交换机和路由器硬件以及布线。**确保该图标记了下列方面中的每一个方面：中继链接速度信道组端口号插槽机箱类型软件VTP 域根网桥备份根网桥优先级Mac 地址每个 VLAN 的阻塞端口数为了清晰起见，将内部设备（例如 Catalyst 6500/6000 MSFC 路由器）表述为通过中继连接的单臂路由器。
- **逻辑图 - 此图仅显示第 3 层功能，这意味着它将路由器显示为对象，将 VLAN 显示为以太网**

段。确保该图标记了以下方面：IP 地址子网辅助编址活动和备用 HSRP接入核心分布层路由信息



交换机管理接口和本地 VLAN

目的

本节介绍使用默认VLAN 1的意义和潜在问题。本节还介绍在6500/6000系列交换机上与用户流量位于同一VLAN中的交换机上运行管理流量时可能出现的问题。

Catalyst 6500/6000 系列的 Supervisor 引擎和 MSFC 上的处理器将 VLAN 1 用于许多控制和管理协议。示例包括：

- 交换机控制协议：STP BPDUVTPDTPCDP
- 管理协议：SNMPTelnetSecure Shell 协议 (SSH)系统日志

当 VLAN 以此方式使用时，称为本地 VLAN。默认交换机配置将 VLAN 1 设置为 Catalyst 中继端口上的默认本地 VLAN。您可以保留 VLAN 1 作为本地 VLAN。但是请记住，默认情况下，在您的网络中运行 Cisco IOS 系统软件的所有交换机会将所有配置为第 2 层交换机端口的接口设置为 VLAN 1 中的接入端口。网络中某处的交换机很可能使用 VLAN 1 作为用户数据流的 VLAN。

在使用 VLAN 1 时主要关心的问题是：终端站点产生的大部分广播和多播数据流通常不需要中断 Supervisor 引擎 NMP。多播应用程序特别倾向于在服务器和客户端之间发送大量数据。Supervisor 引擎不需要查看此数据。如果当 Supervisor 引擎监听不必要的数据流时完全占用了 Supervisor 引擎的资源或缓冲区，则 Supervisor 引擎可能无法发现会导致生成树环路或 EtherChannel 故障的管理数据包（最坏的情况）。

show interfaces *interface_type slot/port* counters 命令和 show ip traffic 命令可以给予您下面一些指示：

- 广播数据流对单播数据流的比例
- IP 数据流对非 IP 数据流的比例（在管理 VLAN 中通常看不到）

VLAN 1 对大多数控制层面数据流进行标记和处理。默认情况下，在所有中继上启用 VLAN 1。对于较大的园区网络，您需要注意 VLAN 1 STP 域的直径。网络某部分的不稳定性会影响 VLAN 1，进而影响所有其他 VLAN 的控制层面稳定性和 STP 稳定性。您可以限制某接口上用户数据的 VLAN 1 传输以及 STP 的运行。请勿在中继接口上配置 VLAN。

如同网络分析器一样，此配置不会停止控制数据包在 VLAN 1 中交换机之间的传输。但是不会转发任何数据，并且 STP 不通过此链路运行。因此，这种技术可用于将 VLAN 1 分成更小的故障域。

注意：您无法清除VLAN 1从中继到Catalyst 2900XL/3500XL。

即使您小心地将用户 VLAN 限制到相当小的交换机域和相应很小的故障/第 3 层边界，一些客户仍试图以另外的方式对待管理 VLAN。这些客户尝试用一个管理子网覆盖整个网络。没有任何技术原因来要求中央 NMS 应用程序必须是应用程序所管理的设备的相邻第 2 层，而且这也不是合格的安全参数。将管理 VLAN 的直径限制为与用户 VLAN 一样的路由域结构。考虑将带外管理和/或 SSH 支持作为增强网络管理安全性的方法。

其他选项

在一些拓扑中，这些 Cisco 建议有一些设计注意事项。例如，理想的通用 Cisco 多层设计是避免使用活动生成树的设计。在此方法中，设计要求将每个 IP 子网/VLAN 限制到一台接入层交换机（或交换机集群）。 在这些设计中，不能将中继向下配置到接入层。

是否要创建单独的管理 VLAN 并启用中继，以便在第 2 层接入层和第 3 层分布层之间传输它？此问题没有一个简单的答案。在与 Cisco 工程师进行设计审核时，请考虑以下两个选项：

- **选项 1 - 将两个或三个唯一 VLAN 从分布层向下中继到每台接入层交换机。**此配置使得数据 VLAN、语音 VLAN 和管理 VLAN 仍然具有 STP 处于未激活状态时的优势。要从中继清除 VLAN 1，需要额外的配置步骤。在此解决方案中，为了在故障恢复期间暂时避免路由数据流产生黑洞，在设计中还需要注意几点。将 STP PortFast 用于中继（在将来），或者将 VLAN 自动状态同步用于 STP 转发。
- **选项 2 - 用于数据和管理的单个 VLAN 是可以接受的。**如果您想要将 sc0 接口与用户数据分开，更新的交换机硬件可以使此方案产生比以前少的问题。更新的硬件提供：更强大的 CPU 和控制层面速率限制控制多层设计所提倡的相当小的广播域设计为了做出最终决策，请检查 VLAN 的广播流量配置文件，并与 Cisco 工程师讨论交换机硬件的功能。如果管理 VLAN 包含该接入层交换机的所有用户，请根据 Cisco IOS 软件安全功能部分所述，使用 IP 输入过滤器来避免用户为交换机带来风险。

Cisco 管理接口和本地 VLAN 建议

管理接口

Cisco IOS 系统软件允许您选择将接口配置为 VLAN 中的第 3 层接口或第 2 层交换机端口。当您在 Cisco IOS 软件中使用 **switchport 命令时，默认情况下所有交换机端口都是 VLAN 1 中的接入端口**。因此，除非另外配置，否则默认情况下用户数据可能还存在于 VLAN 1 中。

使管理 VLAN 成为 VLAN 而不是 VLAN 1。将所有用户数据保留在管理 VLAN 外面。相反，将 loopback0 接口配置为在每台交换机上的管理接口。

注意：如果使用OSPF协议，这也将成为OSPF路由器ID。

请确保环回接口有 32 位子网掩码，并将环回接口配置为交换机上的纯第 3 层接口。示例如下：

```
Switch(config)#interface loopback 0
Switch(config-if)#ip address 10.x.x.x 255.255.255.255
Switch(config-if)#end
Switch#
```

Native VLAN

将本地 VLAN 配置为从未在路由器上启用的明显虚拟 VLAN。Cisco 在以前推荐了 VLAN 999，但是您可以随意选择。

要将某 VLAN 设立为特定端口上进行 802.1Q 中继的本地（默认）VLAN，请发出下列接口命令：

```
Switch(config)#interface type slot/port
Switch(config-if)#switchport trunk native vlan 999
```

有关其他中继配置建议，请参阅本文档的动态中继协议部分。

带外管理

目的

如果在生产网络周围构建单独的管理基础架构，则可以更有效地提供网络管理。无论驱动的数据流或发生的控制层面事件如何，此设置都可以确保能够远程访问设备。下面是两个典型方法：

- 使用独有的 LAN 进行带外管理
- 使用终端服务器进行带外管理

操作概述

在管理 VLAN 中，可以为网络中的每个路由器和交换机提供一个带外以太网管理接口。在管理 VLAN 中的每个设备上配置一个以太网端口，并将其连接到生产网络以外的独立交换管理网络。

注意：Catalyst 4500/4000交换机在Supervisor引擎上有一个特殊的me1接口，仅用于带外管理，不用作交换机端口。

此外，如果使用 RJ-45 串行电缆配置 Cisco 2600 或 3600 路由器以访问布局中每个路由器和交换机的控制台端口，则可以实现终端服务器连接。使用终端服务器还使您无需配置备份方案，例如每个设备的辅助端口上的调制解调器。您可以在终端服务器的辅助端口上配置单个调制解调器。此配置在网络连接故障期间为其他设备提供拨号服务。有关详细信息，请参阅将调制解调器连接到 Catalyst 交换机上的控制台端口。

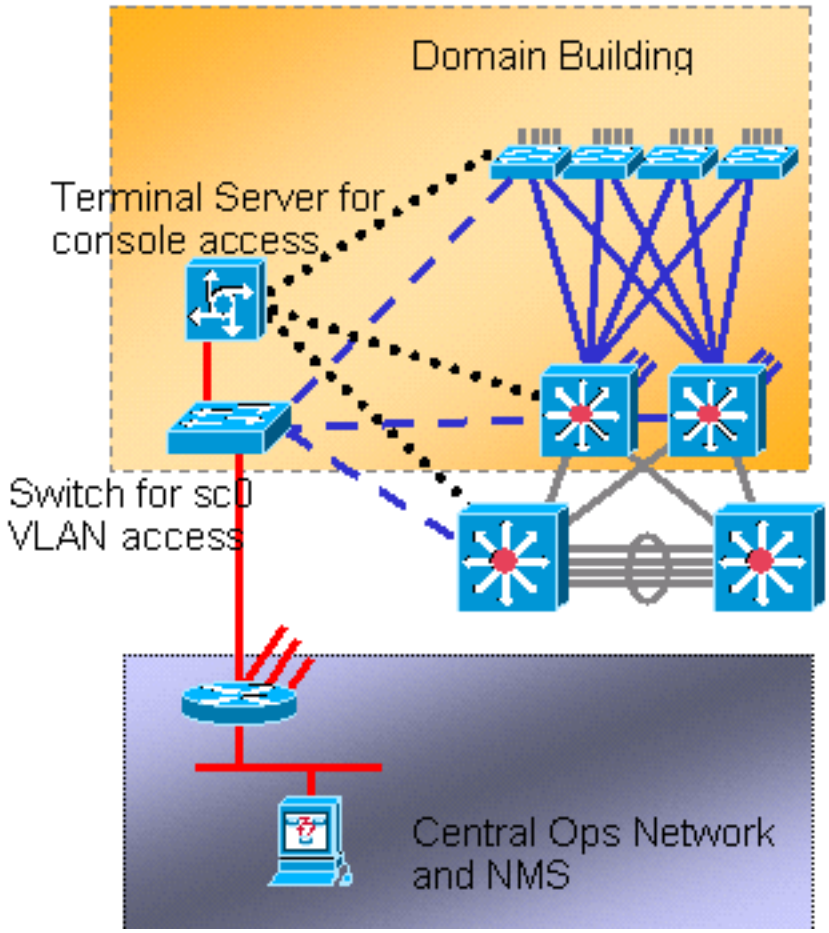
建议

使用此安排，除了提供很多带内路径外，还可以提供两个到每个交换机和路由器的带外路径。此安排启用高度可用的网络管理。其好处是：

- 此安排从用户数据分离管理数据流。
- 管理 IP 地址处于单独的子网、VLAN 和交换机中以确保安全。

- 更好地保证网络故障期间管理数据的发送。
- 在管理 VLAN 中没有活动的生成树。这里冗余并不重要。

下图显示了带外管理：



系统日志记录

目的

Syslog 消息特定于 Cisco，与标准 SNMP 比较，可以提供更具响应能力和更准确的信息。例如，管理平台（例如 Cisco Resource Manager Essentials (RME)）和网络分析工具包 (NATKit) 充分利用 syslog 信息来收集库存和配置更改。

Cisco Syslog 配置建议

系统日志记录是常见的、可被接受的操作做法。UNIX syslog 可以捕获和分析有关路由器的信息/事件，例如：

- 接口状态
- 安全警报
- 环境状况
- CPU 进程 hog
- 其他事件

Cisco IOS 软件可以执行到 UNIX syslog 服务器的 UNIX 日志记录。Cisco UNIX syslog 格式与 4.3 伯克利标准发布 (BSD) UNIX 兼容。请使用下列 Cisco IOS 软件日志设置：

- **no logging console - 默认情况下，所有系统消息都将发送到系统控制台。**控制台日志记录是 Cisco IOS 软件中的一项高优先级任务。此功能主要用于在系统发生故障前向系统操作员提供错误消息。在所有设备配置中禁用控制台日志记录，以避免路由器/交换机在设备等待来自终端的响应时可能挂起的情况。但是控制台消息在故障隔离时可能很有用。在这些实例中，启用控制台日志记录。要获取所需级别的消息日志记录，请发出 **logging console level 命令。**日志记录级别为从 0 到 7。
- **no logging monitor - 此命令禁用除系统控制台之外的终端线路的日志记录。**可能需要监控程序日志记录（使用 **logging monitor debugging 或另一命令选项）。** 在这种情况下，在活动所需的特定日志记录级别启用监控程序日志记录。有关日志记录级别的详细信息，请参阅此列表中的 **no logging console 项目。**
- **logging buffered 16384 - 日志记录缓冲的命令需要添加到内部日志缓冲区中的日志系统消息。**日志记录缓冲区是循环的。一旦日志记录缓冲区被充满，较旧的条目将被较新的条目覆盖。日志记录缓冲区的大小可由用户配置并以字节为单位指定。系统缓冲区的大小因平台而异。16384 是一个不错的默认值，它在大多数情况下提供足够的日志记录。
- **logging trap notifications - 此命令提供到指定 syslog 服务器的通知级别 (5) 消息传递。**所有设备（控制台、监控程序、缓冲区和陷阱）的默认日志记录级别为调试（第 7 级）。 如果将陷阱日志记录级别保留在 7，则生成许多额外的消息，它们通常与网络运行状况无关，或者关系很小。请将陷阱的默认日志记录级别设置为 5。
- **logging facility local7** — 此命令为UNIX syslogging设置默认日志记录设备/级别。配置针对同一个工具/级别接收这些消息的 syslog 服务器。
- **logging host - 此命令设置 UNIX 日志记录服务器的 IP 地址。**
- **logging source-interface loopback 0 - 此命令设置 syslog 消息的默认 IP SA。**对日志记录 SA 进行硬编码，以便更容易地识别发送消息的主机。
- **service timestamps debug datetime localtime show-timezone msec - 默认情况下，日志消息不加时间戳。**可以使用此命令启用日志消息的时间戳并配置系统调试消息的时间戳。时间戳提供被记录事件的相对计时，并增强了实时调试。此信息在用户向技术支持人员发送调试输出以获取帮助时特别有用。为了启用系统调试消息的时间戳，请在全局配置模式下使用该命令。只有当启用调试时，该命令才有效。

注意：此外，在所有基础设施千兆接口上启用链路状态和捆绑状态日志记录。

Cisco IOS 软件提供单一机制来为所有发往 syslog 服务器的系统消息设置工具和日志级别。请将日志记录陷阱级别设置为通知（第 5 级）。 如果将陷阱消息级别设置为通知，则可以最大程度地减少转发到 syslog 服务器的信息消息的数量。此设置可以大大减少网络上的 syslog 流量，并减轻对 syslog 服务器资源的影响。

要启用 syslog 消息传递，请向运行 Cisco IOS 软件的每个路由器和交换机添加以下命令：

- 全局 syslog 配置命令：

```
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging host-ip
logging source-interface loopback 0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
```

- 接口 syslog 配置命令：

```
logging event link-status
logging event bundle-status
```

SNMP

目的

可以使用 SNMP 检索在网络设备 MIB 中存储的统计数据、计数器和表。NMS（例如 HP OpenView）可以使用该信息进行以下操作：

- 生成实时警报
- 评估可用性
- 生成容量规划信息
- 帮助执行配置和故障排除检查

SNMP 管理接口操作

SNMP 是一种应用层协议，可以为 SNMP 管理器和代理之间的通信提供消息格式。SNMP 提供标准化框架和通用语言，用于监控和管理网络中的设备。

SNMP 框架包括以下三个部分：

- SNMP 管理器
- SNMP 代理
- MIB

SNMP 管理器是使用 SNMP 来控制和监控网络主机活动的系统。大多数普通管理系统称为 NMS。术语 NMS 可用于指代用于进行网络管理的专用设备或者在此类设备上使用的应用程序。有许多网络管理应用程序可配合 SNMP 一起使用。这些应用程序多种多样，从简单的 CLI 应用程序到功能丰富的 GUI（例如 CiscoWorks 系列产品）。

SNMP 代理是托管设备中的软件组件，该设备维护设备数据，并在需要时将这些数据报告给管理系统。代理和 MIB 驻留在路由设备（路由器、接入服务器或者交换机）上。 要在 Cisco 路由设备上启用 SNMP 代理，必须定义管理器和代理之间的关系。

MIB 是网络管理信息的虚拟信息存储区。MIB 包括托管对象的集合。在该 MIB 中，包含了在 MIB 模块中定义的相关对象的集合。MIB模块以SNMP MIB模块语言编写，如STD 58、RFC 2578 、RFC 2579 和RFC 2580定 义。

注意：单个MIB模块也称为MIB。例如，接口组 MIB (IF-MIB) 是您的系统上的 MIB 中的 MIB 模块。

SNMP 代理包含 MIB 变量，SNMP 管理器可以通过 get 或 set 操作来请求或更改 MIB 变量的值。管理器可以从代理获得值，或者将值存储到该代理中。代理从 MIB 收集数据，MIB 是设备参数和网络数据的信息库。代理还可以响应管理器请求以获取或设置数据。

管理器可以发送代理请求以获取和设置 MIB 值。代理可以响应这些请求。代理可以独立于此交互，向管理器发送未被请求的通知（陷阱或通知），以向管理器通告网络状况。借助一些安全机制，NMS 可以使用 `get and get next requests MIB` **set 命令来更改参数。**此外，可以将网络设备设置为生成发往 NMS 的陷阱消息，以提供实时警报。IP UDP 端口 161 和 162 用于陷阱。

SNMP 通知操作概述

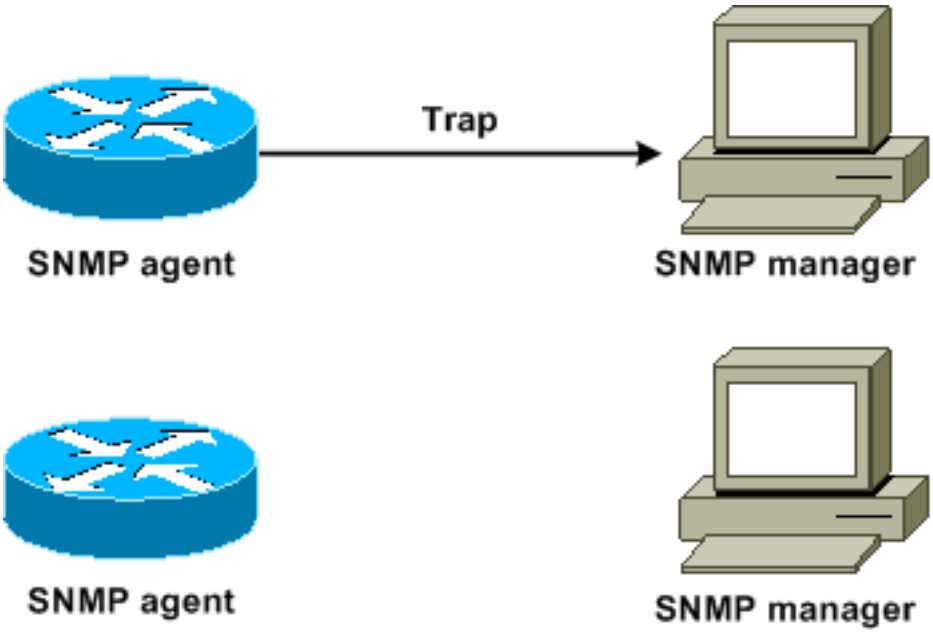
SNMP 的主要功能是能够从 SNMP 代理生成通知。这些通知不要求从 SNMP 管理器发送请求。未经请求的（异步）通知可以生成为陷阱或通知请求。陷阱是警告 SNMP 管理器注意网络上的情况的消息。通知请求（通知）是陷阱，包括对从 SNMP 管理器收到的信息的确认请求。通知可以指示重大事件，例如：

- 不适当的用户验证
- 重新启动
- 连接关闭
- 与相邻路由器的连接失败
- 其他事件

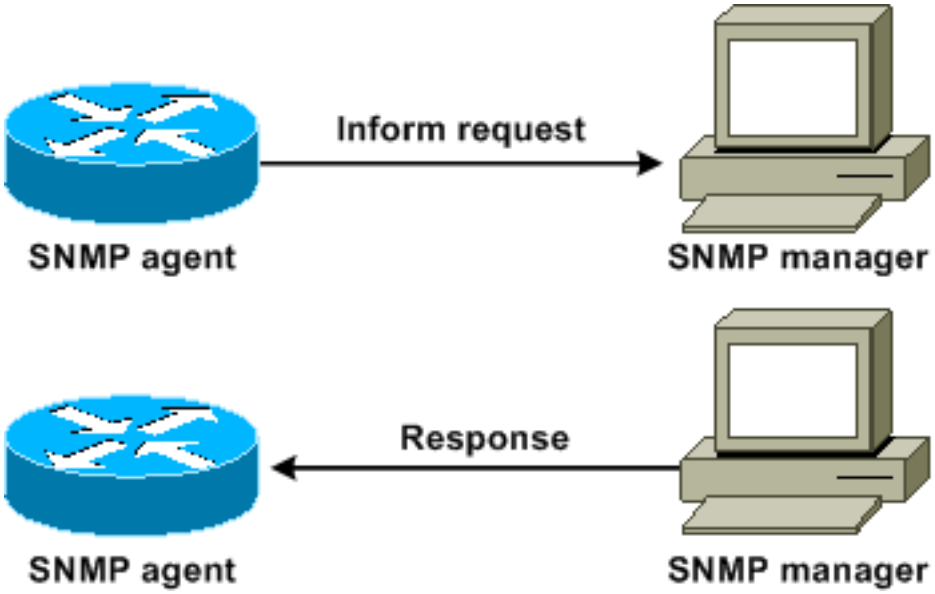
陷阱的可靠性低于通知，这是因为接收器在收到陷阱时不发送任何应答。发送者无法确定陷阱是否已被收到。收到通知请求的 SNMP 管理器使用 SNMP 响应协议数据单元 (PDU) 来应答消息。 如果管理器未收到通知请求，它就不发送响应。如果发送者从未收到响应，发送者可以再次发送通知请求。通知更可能到达预期目的地。

但是，常常首选陷阱，因为通知会消耗路由器和网络中的更多资源。只要一发送陷阱，就会丢弃陷阱。但是通知请求必须保留在内存中，直到收到响应或请求超时。另外，陷阱只能发送一次，而通知则可以重试多次。重试会增加流量，并且造成网络上的开销更高。因此，陷阱和通知请求提供了一个在可靠性和资源之间的折衷方案。如果需要 SNMP 管理器接收每个通知，请使用通知请求。但是，如果您关心的是网络上的流量或路由器中的内存，且不需要接收每个通知，则使用陷阱。

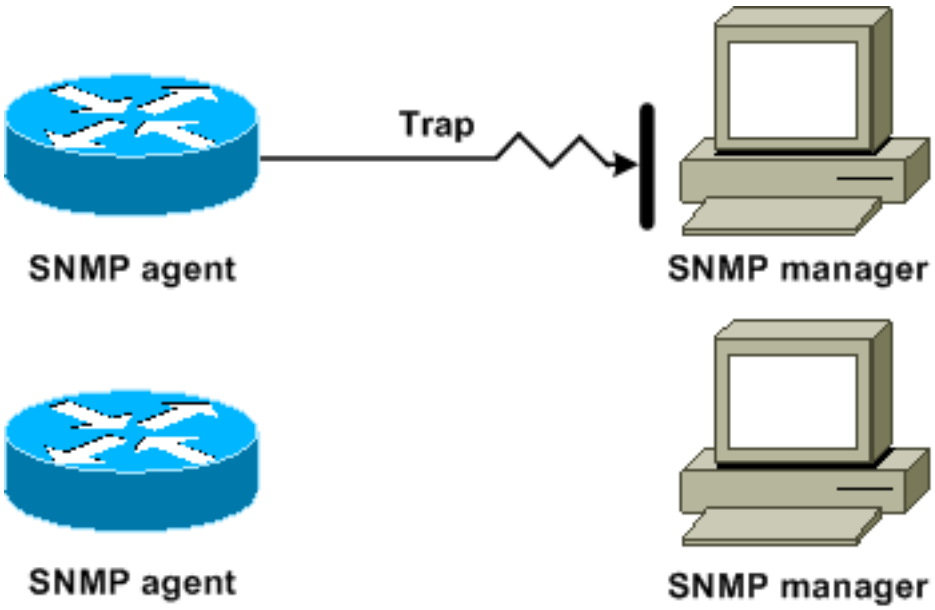
下面的图表说明了陷阱和通知请求之间的区别：



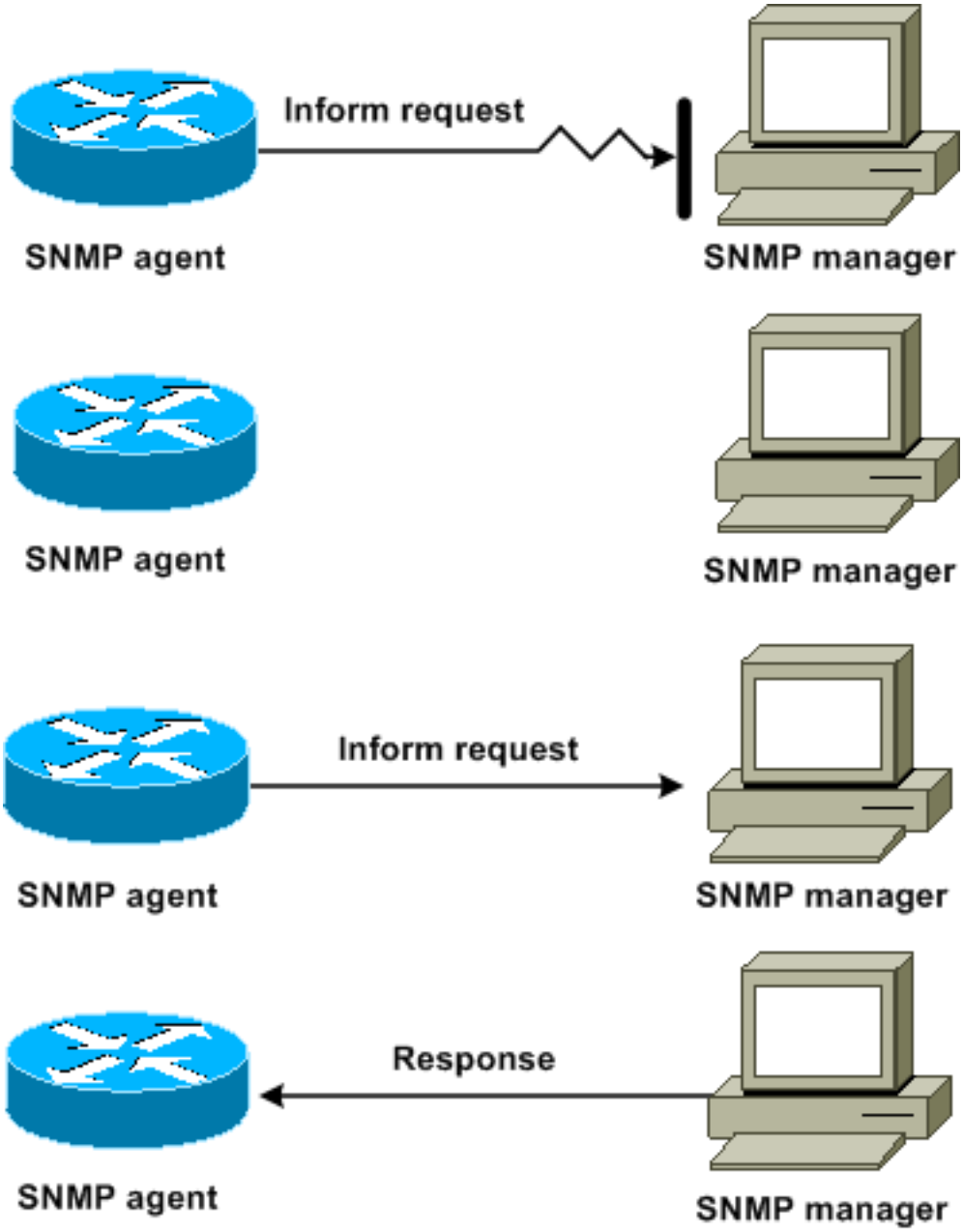
该图说明代理路由器如何向 SNMP 管理器成功发送一个陷阱。虽然管理器收到陷阱，但是它不向代理发送任何应答。代理无法知道陷阱已到达目标。



该图说明代理路由器如何向管理器成功发送通知请求。当管理器收到通知请求时，就会向代理器发送一条响应。这样，代理便知道通知请求已到达目的地。注意，在本示例中，有两倍的流量。但是代理知道管理器收到了通知。



在该图中，代理向管理器发送一个陷阱，但该陷阱未到达管理器。代理无法知道该陷阱未到达目的地，因此没有再次发送该陷阱。管理器从未收到陷阱。



在该图中，代理向管理器发送一个通知请求，但是该通知请求未到达管理器。由于管理器未收到通知请求，因此没有响应。一段时间以后，代理再次发送通知请求。第二次，管理器收到通知请求，并且通过响应进行回复。在本示例中，流量更大。但是通知到达 SNMP 管理器。

Cisco MIB 和 RFC 参考

RFC 文档通常定义 MIB 模块。RFC 文档被提交给国际标准化团体 Internet 工程任务组 (IETF)。个人或团体可以编写 RFC，以供 Internet 协会 (ISOC) 和 Internet 社区进行整体考虑。有关 IETF 的标准流程和活动的信息，请参阅 Internet 协会 主页。 有关 Cisco 文档引用的所有 RFC、Internet 草案 (I-D) 和 STD 的完整文本，请参阅 IETF 主页。

Cisco 对 SNMP 的实施使用以下定义：

- RFC 1213 说明的 MIB II 变量的定义
- RFC 1215 说明的 SNMP 陷阱的定义

Cisco 对每个系统提供其自己的专用 MIB 扩展。除非文档另行通知，否则 Cisco 企业 MIB 应符合相关 RFC 所述的准则。在 Cisco MIB 主页上，可以找到每个 Cisco 平台支持的 MIB 模块定义文件和 MIB 列表。

SNMP 版本

Cisco IOS 软件支持以下版本的 SNMP：

- SNMPv1 - RFC 1157定义的完整Internet标 准。RFC 1157 替换了作为 RFC 1067 和 RFC 1098 发布的早期版本。 安全性基于社区字符串。
- SNMPv2c - SNMPv2c是SNMPv2的基于社区字符串的管理框架。SNMPv2c（c代表社区）是一种实验性Internet协议，RFC 1901 、RFC 1905 和RFC 1906定 义。SNMPv2c 是 SNMPv2p (SNMPv2 Classic) 的协议操作和数据类型的更新。SNMPv2c 使用 SNMPv1 的基于社区的安全模型。
- SNMPv3 - SNMPv3是基于标准的可互操作协议，RFC 2273 、RFC 2274 和RFC 2275定 义。SNMPv3 使用身份验证和数据包加密的组合提供通过网络对设备的安全访问。SNMPv3 提供的安全功能有：消息完整性 - 确保数据包在传输中未被篡改。身份验证 - 确定消息来自有效的来源。加密 - 对数据包内容加扰，避免被未经授权的源发现。

SNMPv1 和 SNMPv2c 都使用基于社区形式的安全性。IP 地址 ACL 和口令定义了能够访问代理 MIB 的管理器社区。

SNMPv2c 支持包括批量检索机制和向管理站点报告的更详细的错误消息。批量检索机制支持对表和大量信息的检索，这最大程度地减少了所需的往返次数。SNMPv2c 改进的错误处理支持包括区分不同错误情况的扩展错误代码。这些情况通过SNMPv1中的单个错误代码报告。错误返回代码现在报告错误类型。

SNMPv3 同时提供了安全模型和安全等级。安全模式是为用户和用户驻留的组设置的身份验证策略。安全等级是安全模型中允许的安全级别。安全模型和安全等级的组合可确定在处理 SNMP 数据包时使用哪一种安全机制。

一般 SNMP 配置

要启用 SNMP 管理，请在所有客户交换机上发出以下命令：

- 针对 SNMP ACL 的命令：

```
Switch(config)#access-list 98 permit ip_address
!--- This is the SNMP device ACL.
```

- 全局 SNMP 命令：

```
!--- These are sample SNMP community strings. Switch(config)#snmp-server community RO-
community ro 98
snmp-server community RW-community rw 98
snmp-server contact Glen Rahn (Home Number)
snmp-server location text
```

SNMP 陷阱建议

SNMP 是网络管理的基础，在所有网络上均启用和使用。

一个 SNMP 代理可以与多个管理器进行通信。因此，您可以配置软件以支持与一个使用SNMPv1的管理站和另一个使用SNMPv2的管理站的通信。大多数客户和NMS仍然使用SNMPv1和SNMPv2c，因为NMS平台中的SNMPv3网络设备支持有些滞后。

请针对正在使用的所有功能启用 SNMP 陷阱。如果需要，可以禁用其他功能。在您启用陷阱之后

，可以发出 **test snmp 命令，并在 NMS 上设置针对错误的适当处理措施。**此类处理的示例包括寻呼机警报或弹出式警报。

默认情况下，禁用所有陷阱。在核心交换机上启用所有陷阱，如下例所示：

```
Switch(config)#snmp trap enable
Switch(config)#snmp-server trap-source loopback0
```

另外，对于关键端口（例如通往路由器和交换机的基础架构链路）和关键服务器端口，启用端口陷阱。对于其他端口（例如主机端口），不一定要启用端口陷阱。要配置端口并启用链路打开/关闭通知，请发出以下命令：

```
Switch(config-if)#snmp trap link-status
```

接下来，指定要接收陷阱并对陷阱进行相应操作的设备。现在，可以将每个陷阱目标分别配置为 SNMPv1、SNMPv2 或 SNMPv3 接收者。对于 SNMPv3 设备，可以发送可靠通知而不是 UDP 陷阱。下面是配置：

```
Switch(config)#snmp-server host ip_address [traps | informs] [version {1 | 2c | 3}] community-string
!--- This command needs to be on one line. !--- These are sample host destinations for SNMP traps and informs. snmp-server host 172.16.1.27 version 2c public
snmp-server host 172.16.1.111 version 1 public
snmp-server host 172.16.1.111 informs version 3 public
snmp-server host 172.16.1.33 public
```

SNMP 轮询建议

确保以下 MIB 是在园区网络中轮询或监控的关键 MIB：

注意：此建议来自思科网络管理咨询组。

Object Name	Object Description	OID	Period	Max
MIB-II				
SysUpTime	system uptime in 1/100ths of seconds	1.3.6.1.2.1.1.3	5 min	< 30000
CISCO-STACK-MIB				
ChassisPs1status	Status of power supply 1	1.3.6.1.4.1.9.5.1.2.4	10 min	≠ 2
ChassisPs2Status	Status of power supply 2	1.3.6.1.4.1.9.5.1.2.7	10 min	≠ 2
ChassisFanStatus	Status of Chassis Fan	1.3.6.1.4.1.9.5.1.2.9	10 min	≠ 2
ChassisMinorAlarm	Chassis Minor Alarm Status	1.3.6.1.4.1.9.5.1.2.11	10 min	≠ 1
chassis MajorAlarm	Chassis Major Alarm Status	1.3.6.1.4.1.9.5.1.2.12	10 min	≠ 1

Object Name	Object Description	OID	Period	Max
ChassisTempAlarm	Chassis Temperature Alarm status	1.3.6.1.4.1.9.5.1.2.13	10 min	≠ 1
ModuleStatus	Operational Status of the module	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min	≠ 2
CISCO-PROCESS-MIB				
CpmCPUTotal5min	The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5	5 min	
CISCO-STACK-MIB				
SysTraffic	% of bandwidth utilization for the previous polling interval	1.3.6.1.4.1.9.5.1.1.8	30 min	

Object Name	Object Description	OID	Period	Max
SysTrafficPeak	Peak traffic meter value since the last time the port counters were cleared or the system started	1.3.6.1.4.1.9.5.1.1.19	30 min	
BRIDGE-MIB				
CiscoEsStackSwitchBufferOverruns	Number of times the switch was out of buffers	1.3.6.1.4.1.9.5.14.2.1.1.17	30 min	

网络时间协议 (NTP)

目的

网络时间协议 (NTP) RFC 1305 用于在一组分布式时间服务器和客户端中同步计时。 NTP 允许在创建系统日志和发生其他特定于时间的事件时关联事件。

操作概述

最先对 NTP 进行说明的是 RFC 958。 但是 NTP 通过 RFC 1119 发展成 NTP 版本 2。 现在，RFC 1305 定义了 NTP，这是其第三个版本。

NTP 可将计算机客户端或服务器的时间与另一个服务器或参考时间源（例如无线电、卫星接收器或者调制解调器）同步。NTP 提供的相对于同步主服务器的客户端精度为，在 LAN 上通常为一毫秒内，在 WAN 上通常为数十毫秒内。例如，可以使用 NTP 通过全球定位服务 (GPS) 接收器对协调世界时 (UTC) 进行协调。

典型的 NTP 配置使用多台冗余服务器和不同的网络路径来实现高准确性和可靠性。一些配置包括加密身份验证，目的是防止偶然或恶意协议攻击。

NTP 通过 UDP 运行，而 UDP 又通过 IP 运行。所有 NTP 通信都使用 UTC，该时间与格林尼治标准时间相同。

目前，可以实施 NTP 版本 3 (NTPv3) 和 NTP 版本 4 (NTPv4)。正在使用的最新软件版本是 NTPv4，但官方的Internet标准仍是NTPv3。此外，一些操作系统供应商定制了协议的实施。

NTP 安全措施

NTP 实施还可尝试避免与时间可能不准确的计算机同步。NTP 通过两种方法实现这一点：

- NTP 不与自身未同步的计算机同步。
- NTP 始终比较由几台计算机报告的时间，不与时间显著不同于其他计算机的计算机同步（即使该计算机所处的层较低）。

关联

运行 NTP 的计算机之间的通信（称为关联）通常是静态配置的。为每台计算机提供了需要与其关联的所有计算机的 IP 地址。通过在具有关联的每对计算机之间交换 NTP 消息，可以实现准确的计时。但是在 LAN 环境中，可以将 NTP 配置为使用 IP 广播消息。使用此替代方法，可以将计算机配置为发送或接收广播消息，但是由于信息流只是单向的，因此计时精度会稍有降低。

如果网络与 Internet 隔离，Cisco NTP 实施允许您配置其中的一台计算机，这样的话，在该计算机实际上使用其他方法确定时间时，看起来和使用 NTP 同步一样。其他计算机使用 NTP 与该计算机同步。

NTP 关联可以是：

- 对等关联这意味着此系统可以与另一个系统同步，或允许另一个系统与其同步。
- 服务器关联这意味着仅此系统可与另一个系统同步。另一个系统不与此系统同步。

如果想要建立与另一个系统的 NTP 关联，请在全局配置模式下使用下列命令之一：

命令	目的
ntp peer *ip-address [normal-sync] [version number] [key key-id] [source interface] [prefer]*	建立与另一个系统的对等关联
ntp server *ip-address [version number] [key key-id] [source interface] [prefer]*	建立与另一个系统的服务器关联

注意：只需配置关联的一端。另一个系统会自动建立关联。

访问公共时间服务器

NTP 子网目前包括 50 多个公共主服务器，这些服务器通过无线电、卫星或者调制解调器直接与 UTC 同步。通常，客户端数量相对较少的客户端工作站和服务器无法与主服务器同步。大约有 100 个与主服务器同步的公共辅助服务器。这些服务器提供与 Internet 上总共 100,000 多个客户端和服务器的同步。公共 NTP 服务器 页维护最新列表，并经常更新。

此外，有许多通常不可公共使用的专用主服务器和辅助服务器。有关公共 NTP 服务器的列表和如何使用它们的信息，请参阅网络时间协议 (NTP) 项目。 不能保证这些公共 Internet NTP 服务器可用且可生成正确时间。所以，您必须考虑其他选项。例如，使用直接连接到许多路由器的各种独立 GPS 设备。

另外，还可使用设置为第 1 层主设备的各种路由器。但是，不建议使用这样的路由器。

层

NTP 使用层来描述计算机与可信时间源相距的 NTP 跳数。第 1 层时间服务器有直接连接的无线电或原子时钟。第 2 层时间服务器从第 1 层时间服务器接收时间，依此类推。自动运行 NTP 的计算机选择这样的计算机作为其时间源，配置为通过 NTP 通信时，具有最低层号的计算机。此策略有效生成了 NTP 发言方的自行组织树。

NTP 会避免与时间可能不准确的设备同步。有关详细信息，请参阅网络时间协议 (NTP) 的 *NTP 安全措施 部分。*

服务器对等关系

- 服务器会响应客户端请求，但不会尝试合并从客户端时间源获得的任何日期信息。
- 对等体会响应客户端请求，但会尝试将客户端请求用作更好时间源的潜在候选者，并协助保持时钟频率稳定性。
- 为了成为真正的对等体，连接的两端必须加入对等关系，而不是一个用户作为对等体而另一个用户作为服务器。让对等体交换密钥，以便只有可信的主机能够与其他作为对等体的主机交流。
- 在客户端对服务器的请求中，服务器会应答客户端，并会忘记客户端曾经询问过问题。
- 在对对等体的客户端请求中，服务器应答客户端。服务器保存有关客户端的状态信息，以便跟踪客户端在计时方面的情况及它在哪一层服务器上运行。

NTP 服务器可以处理数千个客户端而不会产生问题。但是，当 NTP 服务器处理若干个客户端（最多到几百）时，存储器会对服务器保存状态信息的能力带来影响。当 NTP 服务器处理的数量比建议数量多时，设备会使用更多的 CPU 资源和带宽。

与 NTP 服务器通信的模式

下面是两个与服务器进行通信的单独模式：

- 广播模式
- 客户端/服务器模式

在广播模式下，客户端进行监听。在客户端/服务器模式下，客户端轮询服务器。如果 WAN 链路由于其速度而未作使用，则可以使用 NTP 广播。要经由 WAN 链路，请使用客户端/服务器模式（通过轮询）。 广播模式专为 LAN 而设计，在 LAN 中许多客户端可能需要轮询服务器。没有广播模式，这样的轮询就可能会在网络上生成大量数据包。NTP 多播在 NTPv3 中还不可用，但是在 NTPv4 中已经可用。

默认情况下，Cisco IOS软件与NTPv3的使用进行通信。但该软件向后兼容早期版本的NTP。

轮询

NTP 协议允许客户端随时查询服务器。

当您第一次在 Cisco 设备中配置 NTP 时，NTP 以 `NTP_MINPOLL2^4=16 NTP_MAXPOLL 2^14 16,384 4 33 4` 此时间段是 NTP 在再次轮询以获取响应之前等待的最长时段。目前，Cisco 没有一种方法可让用户手动强制 `POLL`

NTP 轮询计数器的起点为 2^6 (64) 秒即 1 分 4 秒。此时间以2的幂递增，因为两台服务器彼此同步到2^10。根据服务器或对等体配置，您可以预期同步消息的发送间隔为64、128、256、512或1024秒之一。随着当前时钟由于锁相环而变得更加稳定，轮询之间的间隔时间会越来越长。锁相环将本地时钟晶体修整为最大 1024 秒（17 分钟）。

此时间在 64 秒和 1024 秒之间以 2 幂的间隔变化（即相当于每 64、128、256、512 或 1024 秒变化一次）。 该时间基于发送和接收数据包的锁相环。如果该时间段中有很多抖动，则轮询发生得更频繁。如果参考时钟准确，并且网络连接保持一致，您会发现两次轮询之间的轮询时间间隔会保持 1024 秒不变。

NTP 轮询间隔随着客户端和服务器之间的连接更改而更改。对于更好的连接，轮询间隔更长。在此

例中，更好的连接意味着 NTP 客户端收到了最后八个请求的八个响应。这样，轮询间隔便会加倍。缺少一个响应就会造成轮询间隔减半。轮询间隔最短为 64 秒，最长可达 1024 秒。在最佳情况下，轮询间隔从 64 秒到 1024 秒所需的时间为 2 小时略多一点。

广播

决不转发 NTP 广播。如果您发出 **ntp broadcast 命令，则路由器开始在配置它时所在的接口上启动 NTP 广播。**

通常，发出 **ntp broadcast 命令是为了将 NTP 广播发送到 LAN 上，以便为服务客户端站点和服务器提供服务。**

时间同步

客户端与服务器的同步包括若干个数据包交换。每个交换是一个请求/答复对。当客户端发送请求时，客户端将其本地时间存储到发送的数据包中。当服务器收到数据包时，它将其自己的估计当前时间存储到数据包，然后该数据包返回。当收到答复时，接收者再次记录自己的接收时间，以估计数据包的行程时间。

这些时间差可用于估计数据包从服务器传输到请求方所需的时间。在估计当前时间时，已将往返时间考虑在内。往返时间越短，对当前时间的估计越准确。

直到同意多次数据包交换后，才会接受此时间。为了估计示例质量，将一些必需的值放入了多级过滤器。通常，NTP 客户端与服务器同步大约需要 5 分钟。有趣的是，这也适用于根据定义没有任何延迟的本地参考时钟。

另外，网络连接的质量也影响最终精度。具有各种延迟的慢速网络和无法预测的网络会对时间同步产生负面影响。

NTP 同步要求时间差短于 128 毫秒。Internet 范围的典型精度为大约 5 毫秒到 100 毫秒，具体时间可能随网络延迟而变化。

NTP 流量级别

NTP 使用的带宽是最小的。对等体交换轮询消息的间隔时间通常可逐步增加到每 17 分钟（1024 秒）不超过一条消息。 通过认真规划，您可以在基于 WAN 链路的路由器网络中做到这一点。需将 NTP 客户端对等连接到本地 NTP 服务器，而不是一路经由 WAN 连接到作为第 2 层服务器的中心站点核心路由器。

收敛的 NTP 客户端平均每个服务器大约使用 0.6 位/秒 (bps)。

Cisco NTP 建议

- Cisco 建议您拥有多个时间服务器和不同的网络路径，以实现高精度和高可靠性。一些配置包括加密身份验证，目的是防止偶然或恶意协议攻击。
- 根据 RFC，NTP 实际上旨在允许您轮询几个不同的时间服务器并使用复杂统计分析以产生有效时间（即使您不确定您轮询的所有服务器都经过授权）。NTP 估计所有时钟的错误。所以，所有 NTP 服务器将时间与对当前错误的估计一起返回。当您使用多个时间服务器时，NTP 也希望这些服务器对某一时间达成协议。
- Cisco 对 NTP 的实施不支持第 1 层服务。您不能连接到无线电或原子时钟。Cisco 建议您的网络的时间服务从 IP Internet 上可用的公共 NTP 服务器派生。

- 使所有客户端交换机能够定期向 NTP 服务器发送时间请求。您可以为每个客户端配置多达 10 个服务器/对等体地址，以便实现快速同步。
- 为了减少协议开销，辅助服务器通过 NTP 将时间分布到其余的本地网络主机。为了实现可靠性，您可以为选定主机安装精度较低但比较便宜的时钟作为备用，以防主服务器和/或辅助服务器或者它们之间的通信路径出现故障。
- **ntp update-calendar - NTP 通常仅更改系统时钟。**此命令允许 NTP 更新日历上的日期/时间信息。只有当同步 NTP 时间时，才进行此更新。否则，日历保持其自己的时间，不受 NTP 时间或系统时钟的影响。请始终在高端路由器上使用此命令。
- **clock calendar-valid - 此命令声明日历信息是有效的且已同步。**请在 NTP 主设备上使用此选项。如果没有配置此设置，则具有日历的高端路由器仍认为其时间没有权威性（即使它有 NTP 主线路）。
- 任何超过 15 的层编号都被认为是不同步的。这就是您在路由器的 **show ntp status 命令输出中看到第 16 层的时钟不同步的原因。**如果主设备与公共 NTP 服务器同步，请确保 NTP 主线路上的层编号比您轮询的公共服务器上的最高层编号大一或二。
- 许多客户在 Cisco IOS 软件平台上的服务器模式下配置了 NTP，并与 Internet 的几种可靠时间源或无线时钟同步。就内部而言，运行大量交换机时替代服务器模式的一个更简单模式是在交换域中的管理 VLAN 上的广播模式下启用 NTP。此机制使 Catalyst 可以从单个广播消息接收时钟。但是，由于信息流是单向的，因此计时精度有些降低。
- 使用环回地址作为更新的源，也有助于提高一致性。您可以用两种方法解决安全性问题：使用 Cisco 建议的服务器更新控制使用身份验证

NTP 全局配置命令

```
!--- For the client: clock timezone EST  -5  ????
ntp source loopback 0 ?????
ntp server ip_address key 1
ntp peer ip_address
!--- This is for a peer association. ntp authenticate
ntp authentication-key 1 md5 xxxx
ntp trusted-key 1

!--- For the server: clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ntp source loopback0
ntp update-calendar

!--- This is optional: interface vlan_id ntp broadcast
!--- This sends NTP broadcast packets. ntp broadcast client
!--- This receives NTP broadcast packets. ntp authenticate
ntp authentication-key 1 md5 xxxxx
ntp trusted-key 1
ntp access-group access-list
!--- This provides further security, if needed.
```

NTP 状态命令

```
show ntp status

Clock is synchronized, stratum 8, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 249.9974 Hz, precision is 2**18
reference time is C6CF0C30.980CCA9D (01:34:00.593 IST Mon Sep 12 2005)
clock offset is 0.0000 msec, root delay is 0.00 msec
```

```
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```
当路由器作为 NTP 主设备时，这是 Cisco 路由器的参考时钟地址。如果路由器未与任何 NTP 服务器同步，路由器使用此地址作为参考 ID。有关配置和命令的详细信息，请参阅执行基本系统管理的配置 NTP 部分。

Cisco 发现协议

目的

CDP 在所有 Cisco 路由器、网桥、接入服务器和交换机的第 2 层（数据链路层）上运行。CDP 使网络管理应用程序可以发现作为已知设备邻居的 Cisco 设备。特别是，网络管理应用程序能够发现运行较低层透明协议的邻居。利用 CDP，网络管理应用程序可以了解邻接设备的设备类型和 SNMP 代理地址。此功能使应用程序可以向邻接设备发送 SNMP 查询。

与 CDP 功能关联的 **show 命令使网络工程师可以确定以下信息：**

- 其他启用 CDP 的邻接设备的模块/端口号
- 邻接设备的下列地址：Mac 地址IP 地址端口信道地址
- 邻接设备软件版本
- 有关邻接设备的下列信息：速度双工VTP 域本地 VLAN 设置

操作概述部分重点介绍了 CDP 版本 2 (CDPv2) 在 CDP 版本 1 (CDPv1) 基础上的一些改进。

操作概述

CDP 在支持 SNAP 的所有 LAN 和 WAN 介质上运行。

每个配置了 CDP 的设备都会将定期消息发送到多播地址。每个设备至少通告一个该设备能够收到 SNMP 消息的地址。该通告还包含生存时间（或称为保存时间）信息。此信息指示接收设备在丢弃 CDP 信息之前保存该信息的时间长度。

CDP 将 SNAP 封装与类型代码 2000 一起使用。在以太网、ATM 和 FDDI 上，使用了目标多播地址 01-00-0c-cc-cc-cc。在令牌环上，使用功能地址 c000.0800.0000。每分钟定期发送一次 CDP 帧。

CDP 消息包含一个或多个消息，允许目标设备收集并存储有关每个邻接设备的信息。

此表提供 CDPv1 支持的参数：

参数	类型	描述
1	Device ID	以 ASCII 表示的设备主机名或硬件序列号
2	地址	发送更新的接口的第 3 层地址
3	端口 ID	发送 CDP 更新时使用的端口
4	功能	按下列方式描述设备功能： • 路由器 :0x01 • SR[1网]桥：0x04 • 交换机：0x08（提供第 2 层和/或第 3 层交换）

		• 主机：0x10 • IGMP 有条件过滤：0x20 • 网桥或交换机不在非路由器端口上转发 IGMP 报告数据包。
5	version	一个包含软件版本的字符串 **注意：**show **version命**令输出显示相同信息。
6	Platform	硬件平台，例如WS-C5000、WS-C6009和Cisco RSP[2]

[1] SR =源路由。

[2] RSP =路由交换机处理器。

在 CDPv2 中，引入了其他类型、长度、值 (TLV)。CDPv2 支持任何 TLV。但是此表提供在交换环境中可能特别有用的、Catalyst 软件使用的参数。

当交换机运行 CDPv1 时，交换机丢弃 CDPv2 帧。当交换机运行 CDPv2 且在接口上接收 CDPv1 帧时，该交换机除了从该接口发出 CDPv2 帧以外，还将从中开始发送 CDPv1 帧。

参数	类型	描述
9	VTP 域	VTP 域（如果在设备上配置）
10	Native VLAN	在 dot1q 中，VLAN（如果端口未中继，则端口在该 VLAN 中）的帧没有加标签。这通常指本地 VLAN。
11	全双工/半双工	此 TLV 包含发送端口的双工设置。
14	设备 VLAN ID	允许 VoIP 数据流通过单独的 VLAN ID（辅助 VLAN）从其他数据流中区分开来。
16	功耗	连接的设备的预计消耗最大功率（以 mW 为单位）。
17	MTU	传输 CDP 帧所使用的接口的 MTU。
18	扩展信任	指示端口处于扩展信任模式下。
19	不可信端口的 COS	服务等级 (CoS) 值，用于标记在连接的交换设备的不可信端口收到的所有数据包。
20	系统名称	设备的完全限定域名（如果未知，则为 0）。
25	请求的功率	由可传输功率的设备传输，用于协商适当的功率电平。
26	可用的功率	由交换机传输。允许可传输功率的设备协商和选择适当的功率设置。

CDPv2/以太网供电

某些交换机，如 Catalyst 6500/6000 和 4500/4000，能够通过非屏蔽双绞线 (UTP) 电缆向可传输功率的设备提供功率。通过 CDP 收到的信息（参数 16、25、26）有助于优化交换机电源管理。

CDPv2/Cisco IP 电话交互

Cisco IP 电话为外部连接的 10/100 Mbps 以太网设备提供连接。此连接通过在 IP 电话中集成内部三端口第 2 层交换机来实现。内部交换机端口称为：

- P0（内部 IP 电话设备）
- P1（外部 10/100 Mbps 端口）
- P2（连接到交换机的外部 10/100 Mbps 端口）

如果配置 dot1q 访问中继端口，则可以在交换机端口上的独立 VLAN 中传输语音数据流。此附加 VLAN 称为辅助 (CatOS) 或语音（Cisco IOS 软件）VLAN。因此，来自 IP 电话的 dot1q 已标记数据流可以在辅助/语音 VLAN 上发送，未标记的数据流可以通过接入 VLAN 的电话的外部 10/100 Mbps 端口发送。

Catalyst 交换机可以通过 CDP 将语音 VLAN ID 通知给 IP 电话（参数 14：工具 VLAN-ID TLV）。因此，IP 电话使用适当的 VLAN ID 和 802.1p 优先级来标记所有与 VoIP 相关的数据包。此 CDP TLV 还用于标识是否通过工具 ID 参数连接 IP 电话。

当开发 QoS 策略时，可以利用此概念。可以用三种方法将 Catalyst 交换机配置为与 IP 电话交互：

- 信任设备 Cisco IP 电话仅在通过 CDP 检测到 IP 电话时，才有条件地信任 CoS。每当通过 CDP 参数 14 检测到 IP 电话时，端口信任状态即设置为“信任 COS”。如果未检测到 IP 电话，则端口为“不可信”。
- 扩展信任交换机可以通过 CDP（参数 18）通知 IP 电话信任在其外部 10/100 Mbps 设备端口上收到的所有帧。
- 重写不可信端口的 COS交换机可以通过 CDP（参数 19）通知 IP 电话重写在其外部 10/100 Mbps 设备端口上收到的 802.1p CoS 值。**注意：**默认情况下，IP电话外部10/100-Mbps端口上接收的所有流量都不可信。

注意： 这是如何将非思科IP电话连接到交换机的示例配置。

注意： 例如，

```
Switch(config)#interface gigabitEthernet 2/1
Switch(config-if)#switchport mode trunk

!--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-
if)#switchport trunk native vlan 10
Switch(config-if)#switchport trunk allow vlan 10,30
Switch(config-if)#switchport voice vlan 30
Switch(config-if)#spanning-tree portfast trunk

!--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

Cisco 配置建议

CDP 提供的信息在解决第 2 层连接问题时非常有用。在支持 CDP 操作的所有设备上启用 CDP。发出以下命令：

- 要在交换机上全局启用 CDP：

```
Switch(config)#cdp run
```

- 要在每个端口上启用 CDP：

```
Switch(config)#interface type slot#/port#
Switch(config-if)#cdp enable
```

配置清单

全局命令

登录、启用和进入全局配置模式以便开始交换机配置过程。

```
Switch>enable
Switch#
Switch#configure terminal
Switch(Config)#
```

通用全局命令（企业范围）

此全局命令部分列出应用于客户企业网络中的所有交换机的全局命令。

此配置包含要添加到初始配置中的建议的全局命令。必须先更改输出中的值，然后才能将文本复制并粘贴到 CLI。要应用全局配置，请发出以下命令：

```
vtp domain domain_name
vtp mode transparent
spanning-tree portfast bpduguard
spanning-tree etherchannel guard misconfig
cdp run
no service pad
service password-encryption
enable secret password
clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ip subnet-zero
ip host tftpserver your_tftp_server
ip domain-name domain_name
ip name-server name_server_ip_address
ip name-server name_server_ip_address
ip classless
no ip domain-lookup
no ip http server
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging syslog_server_ip_address
logging syslog_server_ip_address
logging source-interface loopback0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
access-list 98 permit host_ip_address_of_primary_snmp_server
```

```
access-list 98 permit host_ip_address_of_secondary_snmp_server
snmp-server community public ro 98
snmp-server community laneng rw 98
snmp-server enable traps entity
snmp-server host host_address traps public
snmp-server host host_address traps public
banner motd ^CCCCC

This is a proprietary system, NOT for public or personal use.  All work products,
communications, files, data or information directly or indirectly created, input
or accessed on this system are and shall become the sole property of the company.
This system is actively monitored and accessed by the company.  By logging onto
this system, the user consents to such monitoring and access.

USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT
THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES

^C
line console 0
exec-timeout 0 0
password cisco
login
transport input none
line vty 0 4
exec-timeout 0 0
password cisco
login
length 25
clock calendar-valid
ntp server ntp_server_ip_address
ntp server ntp_server_ip_address
ntp update-calendar
```

特定于每个交换机机箱的全局命令

本部分的全局命令特定于网络中安装的每个交换机机箱。

特定于机箱的配置变量

要设置日期和时间，请发出以下命令：

```
Switch#clock set hh:mm:ss day month year
```

要设置设备主机名，请发出以下命令：

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Cat6500
```

要配置用于管理的环回接口，请发出以下命令：

```
CbrCat6500(config)#interface loopback 0
Cat6500(config-if)#description Cat6000 - Loopback address and Router ID
Cat6500(config-if)#ip address ip_address subnet_mask
```

```
Cat6500(config-if)#exit
```

要显示 Supervisor 引擎 Cisco IOS 软件修订版，请发出以下命令：

```
Cbrcat6500#show version | include IOS
IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE
ASE SOFTWARE (fc1)
cat6500#
```

要显示 MSFC 启动文件修订版，请发出以下命令：

```
Cat6500#dir bootflash:
Directory of bootflash:/
 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a

15990784 bytes total (14111616 bytes free
```

要指定 SNMP 服务器联系信息和位置，请发出以下命令：

```
Cat6500(config)#snmp-server contact contact_information
Cat6500(config)#snmp-server location location_of_device
```

为了将启动配置从现有Supervisor引擎复制到新Supervisor引擎，可能会丢失一些配置，例如，现有Supervisor接口上的配置。思科建议将配置复制到文本文件，并将其粘贴到数据段中，以便查看是否存在任何配置问题。

接口命令

Cisco 功能端口类型

Cisco IOS 软件中的交换机端口称为接口。Cisco IOS 软件中有两种接口模式：

- 第 3 层路由接口
- 第 2 层交换机接口

接口功能是指您配置端口的方式。端口配置可以是：

- 路由接口
- 交换虚拟接口 (SVI)
- 接入端口
- 中继
- EtherChannel
- 这些的组合

接口类型是指端口类型。端口类型可以是：

- FE
- GE
- 端口信道

此列表简要描述了不同的 Cisco IOS 软件接口功能：

- 路由物理接口（默认值）- 在默认情况下，交换机上的每个接口都是路由第 3 层接口，类似于

所有 Cisco 路由器。路由接口必须安排到唯一的 IP 子网上。
- 接入交换机端口接口 - 此功能用于将接口放入同一 VLAN 中。端口必须从路由接口转换为交换接口。
- SVI - SVI 可以与包含 VLAN 间路由的接入交换机端口的 VLAN 产生关联。当您希望在不同 VLAN 的接入交换机端口之间进行路由或桥接时，应配置 SVI 与某个 VLAN 相关联。
- 中继交换机端口接口 - 此功能用于将多个 VLAN 传输到其他设备。端口必须从路由接口转换为中继交换机接口。
- EtherChannel - EtherChannel 用于将各个端口捆绑到单个逻辑端口，以实现冗余和负载均衡。

Cisco 功能端口类型建议

使用本部分中的信息以帮助确定应用于接口的参数。

注意：在可能的情况下，会合并一些特定于接口的命令。

自动协商

在以下任一情况下请勿使用自动协商：

- 对于支持网络基础架构设备（如交换机和路由器）的端口
- 对于其他非临时终端系统，例如服务器和打印机

将下列 10/100 Mbps 链路配置手动配置为高速和双工。这些配置通常是 100 Mbps 全双工：

- 交换机到交换机的 100 MB 链路
- 交换机到服务器的 100 MB 链路
- 交换机到路由器的 100 MB 链路

您可以按以下方式配置这些设置：

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed 100
Cat6500(config-if)#duplex full
```

Cisco 建议终端用户使用 10/100 Mbps 链路配置。移动工作者和临时主机需要自动协商，如以下示例所示：

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed auto
```

千兆接口上的默认值是 `auto-negotiation`。但是，仍请发出以下命令以确保启用自动协商。Cisco 建议启用千兆协商：

```
Cat6500(config-if)#interface gigabitethernet mod#/port#
Cat6500(config-if)#no speed
```

生成树根

考虑到网络的设计，请标识最适合作为每个 VLAN 的根的交换机。通常，选择网络中央功能强大的

交换机。将根网桥放在网络中央，并直接将根网桥连接到服务器和路由器。此设置通常可以缩短客户端到服务器和路由器的平均距离。有关详细信息，请参阅生成树协议问题及相关设计注意事项。

要强制使交换机成为指定 VLAN 的根，请发出以下命令：

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

生成树PortFast

PortFast 绕过接入端口上的正常生成树操作，以加速终端站连接到交换机时发生的初始连接延迟。有关 PortFast 的详细信息，请参阅使用 PortFast 和其他命令消除工作站启动连接延迟。

对于连接到单个主机的所有已启用的接入端口，将 STP PortFast 设置为 on。示例如下：

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet3/1 but will only have effect
when the interface is in a non-trunking mode.
```

UDLD

仅在光纤连接的基础设施端口或以太网铜缆上启用 UDLD，以监控电缆的物理配置。发出以下命令以启用 UDLD：

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#udld enable
```

VLAN 配置信息

用以下命令配置 VLAN：

```
Cat6500(config)#vlan vlan_number
Cat6500(config-vlan)#name vlan_name
Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id
Cat6500(config)#default spanning-tree vlan vlan_id
```

对每个 VLAN 重复这些命令，然后退出。发出以下命令：

```
Cat6500(config)#exit
```

发出此命令以验证所有 VLAN：

```
Cat6500#show vlan
```

路由 SVI

配置 VLAN 间路由的 SVI。发出以下命令：

```
Cat6500(config)#interface vlan vlan_id
Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description
Cat6500(config-if)#no shutdown
```

对包含路由 SVI 的每个接口功能重复这些命令，然后退出。发出以下命令：

```
Cat6500(config-if)#^Z
```

路由单个物理接口

发出以下命令以配置默认路由第 3 层接口：

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

对包含路由物理接口的每个接口功能重复这些命令，然后退出。发出以下命令：

```
Cat6500(config-if)#^Z
```

路由 EtherChannel (L3)

要在第 3 层接口上配置 EtherChannel，请发出此部分中的命令。

按以下方式配置一个逻辑端口信道接口：

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#description port_channel_description
Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

对形成该特定信道的端口执行此部分中的步骤。将剩余信息应用于端口信道，如本示例所示：

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#^Z
```

注意：在配置EtherChannel后，应用于端口通道接口的配置会影响EtherChannel。您应用到 LAN 端口的配置只会影响您应用此配置的 LAN 端口。

带中继的 EtherChannel (L2)

按以下方式为第 2 层 EtherChannel 配置中继：

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

仅对形成该特定信道的端口执行此部分中的步骤。

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

注意：在配置EtherChannel后，应用于端口通道接口的配置会影响EtherChannel。您应用到 LAN 端口的配置只会影响您应用此配置的 LAN 端口。

验证所有 EtherChannel 和中继的创建。示例如下：

```
Cat6500#show etherchannel summary
Cat6500#show interface trunk
```

接入端口

如果接口功能是配置为单个接口的接入端口，发出以下命令：

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id
Cat6500(config-if)#exit
```

对需要配置为第 2 层交换机端口的每个接口重复这些命令。

如果要将交换机端口连接到终端站，请发出以下命令：

```
Cat6500(config-if)#spanning-tree portfast
```

中继端口（单个物理接口）

如果接口功能是配置为单个接口的中继端口，请发出以下命令：

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport trunk encapsulation dot1q
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

对需要配置为中继端口的每个接口功能重复这些命令。

密码 信息

发出以下命令以获取口令信息：

```
Cat6500(config)#service password-encryption
Cat6500(config)#enable secret password

CbrCat6500(config)#line con 0
Cat6500(config-line)#password password

CbrCat6500(config-line)#line vty 0 4
Cat6500(config-line)#password password
Cat6500(config-line)#^Z
```

保存配置

发出此命令以保存配置：

```
Cat6500#copy running-config startup-config
```

Cisco IOS 软件版本 12.1(13)E 中新的软件功能

有关 IP 电话支持的详细信息，请参阅配置 Cisco IP 电话支持。

有关 LAN 端口的基于网络的应用程序识别 (NBAR) 的详细信息，请参阅基于网络的应用程序识别和基于分布式网络的应用程序识别。

注意：

- MSFC2 上的软件支持 LAN 端口的 NBAR。
- PFC2 为在配置 NBAR 的 LAN 端口上输入 ACL 提供硬件支持。
- 启用 PFC QoS 时，通过配置 NBAR 的 LAN 端口的数据流会通过输入和输出队列并丢弃阈值。
- 当启用 PFC QoS 时，MSFC2 将输出业务类别 (CoS) 设置为与输出 IP 优先级相等。
- 在数据流通过输入队列以后，所有数据流都在您配置 NBAR 的 LAN 端口的 MSFC2 上的软件中进行处理。
- 分布式 NBAR 在带 Cisco IOS 软件版本 12.1(6)E 及更高版本的 FlexWAN 接口上可用。

NetFlow 数据导出 (NDE) 增强包括：

- 目标-源接口和完全接口流掩码
- 来自 PFC2 的 NDE 版本 5
- 抽样 NetFlow
- 填充 NDE 记录中的以下附加字段的选项：下一跳路由器的 IP 地址输入接口 SNMP ifIndex输出接口 SNMP ifIndex源自治系统编号

有关以下增强功能的详细信息，请参阅配置 NDE。

其他功能增强包括：

- 配置 UDLD
- 配置 VTP
- 使用 WCCP 配置 Web 缓存服务

以下命令是新的命令：

- **standby delay minimum reload**
- **link debounce**
- **vlan internal allocation policy {ascending |降序}**
- **system jumbomtu**
- **clear catalyst6000 traffic-meter**

以下命令是增强命令：

- **show vlan internal usage - 此命令经过增强，以包括 WAN 接口使用的 VLAN。**
- **show vlan id - 此命令经过增强，以支持输入一组 VLAN。**
- **show l2protocol-tunnel** — 此命令已增强以支持VLAN ID的输入。

Cisco IOS 软件版本 12.1(13)E 支持以下软件功能，先前在 Cisco IOS 软件版本 12.1 EX 版本中已支持这些功能：

- 第 2 层 EtherChannel 配置，这些 EtherChannel 包括不同的配备 DFC 的交换模块上的接口请参阅Cisco Bug ID CSCdt27074（仅限注册客户）的12.1(13)E版中已解决的一般警告 (仅限注册客户)。
- 增强型路由器处理冗余 (RPR+) 冗余请参阅配置 RPR 或 RPR+ Supervisor 引擎冗余。**注意**：在Cisco IOS软件版本12.1(13)E及更高版本中，RPR和RPR+冗余功能取代了增强的高系统可用性(EHSA)冗余。
- 4,096 个第 2 层 VLAN请参阅配置 VLAN。**注意**：Cisco IOS软件版本12.1(13)E及更高版本支持配置4,096个第3层VLAN接口。在带 Supervisor 引擎 II 或 Supervisor 引擎 I 的 MSFC2 上配置的第 3 层 VLAN 接口和第 3 层端口组合总数不要超过 2,000 个。在 MSFC 上配置的第 3 层 VLAN 接口和第 3 层端口组合总数不要超过 1,000 个。
- IEEE 802.1Q 隧道请参阅配置 IEEE 802.1Q 隧道和第 2 层协议隧道。
- IEEE 802.1Q 协议隧道请参阅配置 IEEE 802.1Q 隧道和第 2 层协议隧道。
- IEEE 802.1s 多生成树 (MST)请参阅配置 STP 和 IEEE 802.1s MST。
- IEEE 802.1w 快速 STP (RSTP)请参阅配置 STP 和 IEEE 802.1s MST。
- IEEE 802.3ad LACP请参阅配置第 3 层和第 2 层 EtherChannel。
- PortFast BPDU 过滤请参阅配置 STP 功能。
- 自动创建第 3 层 VLAN 接口以支持 VLAN ACL (VACL)请参阅配置网络安全。
- VACL 捕获端口，可以是任何 VLAN 中任何第 2 层以太网端口请参阅配置网络安全。
- 各个第 3 层物理端口上的可配置 MTU 大小请参阅接口配置概述。
- 将 SPAN 目标端口配置为中继，以便标记所有 SPAN 数据流请参阅配置本地和远程 SPAN。

相关信息

- **工具和资源 - Cisco Systems**
- **交换机产品支持**
- **LAN 交换技术支持**
- **技术支持和文档 - Cisco Systems**