

# VLAN Trunk协议(VTP)故障排除

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[了解 VTP](#)

[配置 VTP](#)

[VTP 故障排除和警告](#)

[在 show run 命令输出中无法看到 VLAN 的详细情况](#)

[Catalyst 交换机不交换 VTP 信息](#)

[Catalyst 交换机自动将 VTP 模式从客户端模式切换到透明模式](#)

[VTP 域间的数据流量被阻塞](#)

[CatOS 交换机切换到 VTP 透明模式，VTP-4-UNSUPPORTEDCFGRCVD:](#)

[最近加入的交换机怎样会导致网络问题](#)

[最近添加的交换机无法从 VTP 服务器获取 VLAN](#)

[重置配置修订版号](#)

[重新通电后所有端口均变为非活动状态](#)

[中继关闭导致 VTP 问题](#)

[VTP 和 STP \(逻辑生成树端口\)](#)

[VLAN 1 案例](#)

[对 show vtp statistics 命令输出中显示的 VTP 配置修订版号错误进行故障排除](#)

[对 show vtp statistics 命令输出中显示的 VTP 配置摘要错误进行故障排除](#)

[无法从服务器/透明模式切换交换机的 VTP 模式](#)

[VTP 域中的 OSPF Hello 被阻塞](#)

[SW VLAN-4-VTP USER NOTIFICATION](#)

[在 show running-config 命令输出中，单个 Switchport Trunk Allowed vlan 命令显示为多个命令  
内部 VLAN 使用](#)

[相关信息](#)

## 简介

本文档提供有关如何对 VLAN 中继协议 (VTP) 进行故障排除的信息。

## 先决条件

### 要求

本文档没有任何特定的要求。

## [使用的组件](#)

本文档不限于特定的软件和硬件版本。

## [规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## [了解 VTP](#)

有关 VTP 的详细信息，请参阅[了解 VLAN 中继协议 \(VTP\)](#)。

## [配置 VTP](#)

有关如何配置 VTP 的信息，请参阅[配置 VLAN 中继协议 \(VTP\)](#)。

## [VTP 故障排除和警告](#)

本部分讨论 VTP 的一些常见故障排除情况。

### [在 show run 命令输出中无法看到 VLAN 的详细情况](#)

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 running-config startup-config** 命令，Cisco IOS 软件不保存对 NVRAM 的配置更改。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 更新模型需要替代的更新操作。

为了满足这一变更，Cisco IOS 软件中引入了 VLAN 数据库，将其作为一种立即保存 VTP 客户端和服务器的 VTP 更新的方法。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。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。

如果在处于 VTP 服务器/客户端模式的交换机上发出 **copy running-config startup-config** 命令，则这些系统不会将整个 VTP/VLAN 配置保存到 NVRAM 中的启动配置文件。系统会将配置保存到 vlan.dat 文件。这不适用于以 VTP 透明模式运行的系统。当您发出 **startup-config** 命令时的 **copyrunning** 设置 VTP 透明系统保存整个 VTP/VLAN 配置到在 NVRAM 的启动配置文件。例如，如果在服务器或客户端模式下配置 VTP 后删除了 vlan.dat 文件，然后重新加载交换机，则 VTP 配置会重置为默认设置。但是，如果在透明模式下配置 VTP，然后删除 vlan.dat 文件并重新加载交换机，VTP 配置将保持不变。

以下是默认 VTP 配置的一个示例：

```
Switch#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 5
```

```
VTP Operating Mode           : Client
VTP Domain Name             : CISCO
VTP Pruning Mode            : Disabled
VTP V2 Mode                  : Disabled
VTP Traps Generation        : Disabled
MD5 digest                   : 0xD3 0x78 0x41 0xC8 0x35 0x56 0x89 0x97
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

当交换机处于 VTP 服务器模式或 VTP 透明模式时，可配置正常范围内的 VLAN ( 2 到 1000 )。但是，只能在处于 VTP 透明模式的交换机中配置扩展范围内的 VLAN ( 1025 到 4094 )。

- 必须发出 **show vlan** 命令，才能显示二进制文件中存储的所有 VLAN 配置、VLAN ID、名称等。

• 您可以使用 **show vtp status** 命令来显示 VTP 信息、模式、域等。

- 当交换机处于 VTP 服务器/客户端模式时，**show running-config** 命令输出中不会显示 VLAN 信息和 VTP 信息。这是正常的交换机行为。Router#show run | include vlan

```
vlan internal allocation policy ascendingRouter#show run | include vtp
```

- 处于 VTP 透明模式的交换机可在 **show running-config** 命令输出中显示 VLAN 和 VTP 配置，因为此信息也存储在配置文本文件中。Router#show run | include vlan

```
vlan internal allocation policy ascending
```

```
vlan 1
```

```
tb-vlan1 1002
```

```
tb-vlan2 1003
```

```
vlan 20-21,50-51
```

```
vlan 1002
```

```
tb-vlan1 1
```

```
tb-vlan2 1003
```

```
vlan 1003
```

```
tb-vlan1 1
```

```
tb-vlan2 1002
```

```
vlan 1004
```

```
vlan 1005
```

```
Router#show run | include vtp
```

```
vtp domain cisco
```

```
vtp mode transparent
```

**注意：** 3500XL 不支持扩展范围内的 VLAN。2900XL 和 3500XL 只能使用 1-1001 范围内的 VLAN，它们不支持扩展范围内的 VLAN。如果升级交换机的软件，这不会使交换机增强为支持配置扩展范围内的 VLAN。

## [Catalyst 交换机不交换 VTP 信息](#)

VTP 允许交换机在相同 VTP 域中的其他成员之间通告 VLAN 信息。通过使用 VTP，所有交换机之间可具有一致的交换网络视图。有几个原因会导致无法交换 VLAN 信息。

如果运行 VTP 的交换机无法交换 VLAN 信息，请检查以下项目：

- VTP 信息只通过中继端口。确保实现交换机互连的所有端口均配置为中继，并且实际正在进行中继。确保当两台交换机之间创建了 EtherChannel 时，只有第 2 层 EtherChannel 传播 VLAN 信息。
- 确保 VLAN 在所有设备中都处于活动状态。
- 在 VTP 域中，必须有一台交换机是 VTP 服务器。所有的 VLAN 更改都必须在此交换机上进行，以便将更改传播到 VTP 客户端。
- VTP 域名必须匹配，并且要区分大小写。CISCO 和 cisco 是两个不同的域名。
- 确保服务器与客户端之间未设置口令。如果设置了口令，确保两端的口令相同。
- VTP 域中的每台交换机必须使用相同的 VTP 版本。相同 VTP 域中的交换机上的 VTP V1 和

VTP V2 不兼容。除非 VTP 域中的每台交换机都支持 VTP V2，否则不要启用 VTP V2。**注意**：默认情况下，支持 VTP V2 的交换机上的 VTP V2 处于禁用状态。在一台交换机上启用 VTP V2 后，VTP 域中支持 VTP V2 的每台交换机都会启用 VTP V2。您只能在处于 VTP 服务器模式或透明模式的交换机上配置版本。

- 如果在透明模式下运行的交换机不在相同的 VTP 域中，则这些交换机会丢弃 VTP 通告。
- 不能传播扩展范围内的 VLAN。因此，必须在每台网络设备上手动配置扩展范围内的 VLAN。**注意**：Catalyst 6500 Cisco IOS 软件交换机将来会支持 VTP 版本 3。该版本能够传输扩展范围内的 VLAN。目前，只有 CatOS 支持 VTP 版本 3。有关 VTP 版本 3 的详细信息，请参阅[配置 VTP 的了解 VTP 版本 3 的工作方式](#)部分。
- 安全关联标识符 (SAID) 值必须是唯一的。SAID 是可由用户配置的 4 字节 VLAN 标识符。SAID 标识属于特定 VLAN 的流量。SAID 还确定每个数据包被交换到的 VLAN。SAID 值是 100,000 与 VLAN 编号之和。以下是两个示例：VLAN 8 的 SAID 是 100008。VLAN 4050 的 SAID 是 104050。
- 如果客户端已经有较高的 VTP 修订版本号，则来自 VTP 服务器的更新内容不会在客户端进行更新。此外，如果客户端的修订版本号比 VTP 服务器发送的修订版本号高，则客户端不允许这些更新流入其下游 VTP 客户端。

## [Catalyst 交换机自动将 VTP 模式从客户端模式切换到透明模式](#)

某些 Catalyst 第 2 层和第 3 层固定配置交换机自动将 VTP 模式从客户端模式切换到透明模式，并生成以下错误消息：

```
%SW_VLAN-6-VTP_MODE_CHANGE: VLAN manager changing device mode from  
CLIENT to TRANSPARENT.
```

以下任一原因都可能导致这些交换机自动切换 VTP 模式：

- **基于生成树协议 (STP) 运行的 VLAN 的数量超过交换机可以支持的 VLAN 数量。**在使用每 VLAN 生成树+ (PVST+) 协议的情况下，Catalyst 第 2 层和第 3 层固定配置交换机支持的最大 STP 实例数会有所不同。例如，在 PVST+ 模式下，Catalyst 2940 支持 4 个 STP 实例，而 Catalyst 3750 支持 128 个 STP 实例。如果 VTP 中定义的 VLAN 数量超过最大值，则剩余的 VLAN 会在禁用 STP 的情况下运行。如果已在使用的 STP 实例的数量超过最大值，则可以禁用其中一个 VLAN 上的 STP，然后在您希望运行 STP 的 VLAN 上启用 STP。发出 **no spanning-tree vlan vlan-id** 全局配置命令可禁用特定 VLAN 上的 STP。然后，发出 **spanning-tree vlan vlan-id** 全局配置命令可启用所需 VLAN 上的 STP。**注意**：不运行 STP 的交换机仍会转发其收到的网桥协议数据单元 (BPDU)。这样，VLAN 中其他正在运行 STP 的交换机就可以断开环路。因此，要断开网络中的所有环路，必须在足够多的交换机上运行 STP。例如，VLAN 中的每个环路上至少一台交换机必须运行 STP。不需要在 VLAN 中的所有交换机上运行 STP。但是，如果只在极少数交换机上运行 STP，则网络变更可能会使网络中产生环路，从而可能导致广播风暴。**应急方案**：将配置的 VLAN 的数量减少到交换机可以支持的数量。在交换机上配置 IEEE 802.1s 多重 STP (MSTP)，以便将多个 VLAN 映射到单个 STP 实例。使用支持更大数量的 VLAN 的交换机和/或映像 (增强映像 [EI])。
- **交换机从相连的交换机接收到的 VLAN 数量超过其可支持的 VLAN 数量。**如果交换机收到的 VLAN 配置数据库消息中所包含的 VLAN 数量超过设置的 VLAN 数量，则也会自动进行 VTP 模式切换。当 Catalyst 第 2 层和第 3 层固定配置交换机所连接到的 VTP 域中包含的 VLAN 数量超过本地支持的 VLAN 数量时，这些交换机中通常会出现上述情况。**应急方案**：在连接的交换机的中继端口上配置允许的 VLAN 列表，以便限制传递给客户端交换机的 VLAN 数量。在 VTP 服务器交换机上启用修剪。使用支持更大数量的 VLAN 的交换机和/或映像 (EI)。

## VTP 域间的数据流量被阻塞

有时需要连接属于两个不同 VTP 域的交换机。例如，有两个名为 Switch1 和 Switch2 的交换机。Switch1 属于 VTP 域 cisco1，而 Switch2 属于 VTP 域 cisco2。使用动态中继协商 (DTP) 配置这两台交换机之间的中继时，中继协商失败，并且交换机之间的中继未形成，这是因为 DTP 在 DTP 数据包中发送 VTP 域名。因此，数据流量无法在交换机之间传输。

```
Switch1#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 9
VTP Operating Mode         : Server
VTP Domain Name            : cisco1
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
```

```
Switch2#show vtp status
VTP Version                : 2
Configuration Revision     : 2
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 42
VTP Operating Mode         : Server
VTP Domain Name            : cisco2
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
```

```
Switch1#show interface fastethernet 1/0/23 trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fal/0/23	auto	802.1q	<b>not-trunking</b>	1

Port	Vlans allowed on trunk
Fal/0/23	1

Port	Vlans allowed and active in management domain
Fal/0/23	1

Port	Vlans in spanning tree forwarding state and not pruned
Fal/0/23	1

您可能还会看到以下错误消息。

**注意：**某些交换机不显示以下错误消息。

```
Switch1#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 9
VTP Operating Mode         : Server
VTP Domain Name            : cisco1
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
```

```
Switch2#show vtp status
VTP Version                : 2
Configuration Revision     : 2
```

```
Maximum VLANs supported locally : 1005
Number of existing VLANs       : 42
VTP Operating Mode             : Server
VTP Domain Name                : cisco2
VTP Pruning Mode               : Disabled
VTP V2 Mode                    : Disabled
VTP Traps Generation           : Disabled
```

```
Switch1#show interface fastethernet 1/0/23 trunk
```

```
Port      Mode      Encapsulation  Status      Native vlan
Fa1/0/23  auto     802.1q         not-trunking  1
```

```
Port      Vlans allowed on trunk
Fa1/0/23  1
```

```
Port      Vlans allowed and active in management domain
Fa1/0/23  1
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Fa1/0/23  1
```

此问题的解决方案是手动强制形成中继，而不是依赖于 DTP。使用 **switchport mode trunk** 命令配置交换机之间的中继端口。

```
Switch1(config)#interface fastethernet 1/0/23
switch1(config-if)#switchport mode trunk
```

```
Switch2(config)#interface fastethernet 3/3
switch2(config-if)#switchport mode trunk
```

```
switch1#show interface fastethernet 1/0/23 trunk
```

```
Port      Mode      Encapsulation  Status      Native vlan
Fa1/0/23  on       802.1q         trunking    1
```

```
Port      Vlans allowed on trunk
Fa1/0/23  1-4094
```

```
Port      Vlans allowed and active in management domain
Fa1/0/23  1-5
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Fa1/0/23  1-5
```

## [CatOS 交换机切换到 VTP 透明模式，VTP-4-UNSUPPORTEDCFGRCVD:](#)

CatOS 的一个最新更改是加入了一种保护功能，该功能可使 CatOS 交换机进入 VTP 透明模式，从而防止由于监视器超时导致交换机重置的可能性。以下 Cisco bug ID 中记录了此更改：

- [CSCdu32627](#) (仅限注册用户)
- [CSCdv77448](#) (仅限注册用户)

### [如何确定交换机是否可能受影响？](#)

如果满足以下两个条件，则表明监视器超时：

- 令牌环 VLAN (1003) 转换为 VLAN 1。

- 您在 VLAN 1 中进行了更改。

在 Catalyst 上发出 **show vlan** 命令，以便观察令牌环 VLAN 转换。以下是 **show vlan** 命令输出的一个示例：

```
Switch1(config)#interface fastethernet 1/0/23
switch1(config-if)#switchport mode trunk
```

```
Switch2(config)#interface fastethernet 3/3
switch2(config-if)#switchport mode trunk
```

```
switch1#show interface fastethernet 1/0/23 trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa1/0/23	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa1/0/23	1-4094

Port	Vlans allowed and active in management domain
Fa1/0/23	1-5

Port	Vlans in spanning tree forwarding state and not pruned
Fa1/0/23	1-5

### [CatOS 版本 6.3\(3\) 如何防止交换机出现监视器超时？](#)

此 CatOS 版本中有一个保护功能，用于防止监视器超时。Catalyst 交换机可从 VTP 服务器或客户端模式切换到 VTP 透明模式。

### [如何确定交换机是否已切换到 VTP 透明模式来防止监视器超时？](#)

如果 VTP 的日志记录级别上升到 4，则说明交换机已切换到 VTP 透明模式。

```
Console> (enable) set logging level vtp 4 default
```

进行切换时，您可以看到以下消息：

```
Console> (enable) set logging level vtp 4 default
```

### [交换机切换到 VTP 透明模式后有什么负面影响？](#)

- 如果启用了修剪，则中继将关闭。
- 如果中继关闭且该 VLAN 中没有其他端口，则安装的 Multilayer Switch Feature Card (MSFC) 中的 VLAN 接口将关闭。

如果出现这些情况，并且此交换机位于网络的核心位置，则网络可能受到负面影响。

### [不受支持的 VTP 配置来自何处？](#)

任何基于 Cisco IOS 软件的交换机（例如以下列表中的交换机）都可能提供不受支持的 VTP 配置：

- Catalyst 2900/3500XL
- Cisco IOS 软件 Catalyst 6500
- 基于 Cisco IOS 软件的 Catalyst 4000

默认情况下，这些产品会将 1003 VLAN 转换为 VLAN 1。



## [解决方案是什么？](#)

基于 CatOS 的交换机的解决方案使交换机能够正确处理此转换的信息。基于 Cisco IOS 软件的交换机的解决方案是除去此默认转换，并与基于 CatOS 的交换机的行为匹配。以下是当前可用的集成已修复版本：

Catalyst 交换机	已修复版本
CatOS 交换机	5.5(14)及以上版本 6.3(6)及以上版本 7.2(2)及以上版本
Catalyst 4000 ( Supervisor 引擎 III )	不受影响
Catalyst 6500 ( Supervisor 引擎 Cisco IOS 软件 )	Cisco IOS 软件版本 12.1(8a)EX 及更高版本
Catalyst 2900 和 3500XL	Cisco IOS 软件版本 12.0(5)WC3 及更高版本

如果无法升级到集成了这些修复程序的映像，则可以修改基于 Cisco IOS 软件的交换机中的配置。如果交换机是 VTP 服务器，请使用以下过程：

```
goss#vlan data

goss(vlan)#no vlan 1 tb-vlan1 tb-vlan2

Resetting translation bridge VLAN 1 to default
Resetting translation bridge VLAN 2 to default

goss(vlan)#no vlan 1003 tb-vlan1 tb-vlan2

Resetting translation bridge VLAN 1 to default
Resetting translation bridge VLAN 2 to default

goss(vlan)#apply

APPLY completed.

goss(vlan)#exit

APPLY completed.
Exiting....
```

可以转换 1002 VLAN，但如果您的配置中包括以下内容，还可以除去 1002 VLAN：

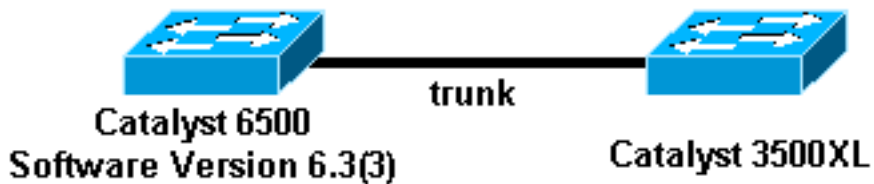
```
goss(vlan)#no vlan 1002 tb-vlan1 tb-vlan2

Resetting translation bridge VLAN 1 to default
Resetting translation bridge VLAN 2 to default
```

## [交换机切换到 VTP 透明模式的确切时间是在什么时候？](#)

关于切换到 VTP 透明模式的时间存在一些混淆。本部分中的方案提供可能发生切换的时间的示例。





- **示例 1** 以下是初始情况：Catalyst 6500 和 Catalyst 3500XL 是具有相同 VTP 配置修订版号的 VTP 服务器。这两台服务器具有相同的 VTP 域名和相同的 VTP 口令（如果配置了口令）。Catalyst 3500XL 具有已转换的令牌环 VLAN。您在这两台服务器断开连接的情况下启动了它们。如果连接这两台交换机，则 Catalyst 6500 将切换到 VTP 透明模式。当然，如果 Cisco 3500XL 的 VTP 配置修订版号高于 Catalyst 6500 的配置修订版号，则 Catalyst 6500 也会切换到 VTP 透明模式。此外，如果实际连接这两台交换机时切换到 VTP 透明模式，则您有理由认为在交换机已连接的情况下首次引导 Catalyst 6500 时也会进行切换。
- **示例 2** 以下是初始情况：Catalyst 6500 是 VTP 服务器。Catalyst 3500XL 是 VTP 客户端。Catalyst 3500XL 的 VTP 配置修订版号高于 Catalyst 6500 的配置修订版号。这两台交换机具有相同的 VTP 域和相同的 VTP 口令（如果配置了口令）。Catalyst 3500XL 具有已转换的令牌环 VLAN。您在这两台服务器断开连接的情况下启动了它们。如果连接这两台交换机，则 Catalyst 6500 将切换到 VTP 透明模式。在此方案中，如果 Catalyst 3500XL 的配置修订版号低于 Catalyst 6500 的配置修订版号，则 Catalyst 6500 不会切换到 VTP 透明模式。如果 Catalyst 3500XL 具有相同的配置修订版号，则 Catalyst 6500 不会切换到 VTP 透明模式。但是，Catalyst 3500XL 中仍会进行转换。

### [网络中发生转换后如何最快进行恢复？](#)

即使您在一台交换机（如出现故障的交换机）中更正令牌环 VLAN 信息，该信息也会在整个网络中传播。可以使用 **show vlan** 命令确定是否如此。因此，最快的恢复方法是执行以下步骤：

1. 采用基于 Cisco IOS 软件的交换机（例如，连接到网络的 Catalyst XL），并将该交换机更改为 VTP 服务器。
2. 除去已转换的 VLAN。
3. 在交换机中应用更改后，重新将交换机连接到网络。更改应传播到所有其他 VTP 服务器和客户端。可以使用 **show vlan** 命令验证网络中的转换是否已不存在。此时，您应该能够将受影响的 CatOS 6.3(3) 交换机重新更改为 VTP 服务器。**注意：** Catalyst XL 交换机支持的 VLAN 数量小于 Catalyst 6500 支持的 VLAN 数量。在重新连接交换机之前，请确保 Catalyst 6500 中的所有 VLAN 都存在于 Catalyst XL 交换机中。例如，您不想将具有 254 个 VLAN 和较高 VTP 配置修订版号的 Catalyst 3548XL 连接到配置了 500 个 VLAN 的 Catalyst 6500。

### [最近加入的交换机怎样会导致网络问题](#)

当一个较大的交换域全部位于相同 VTP 域中，并且您要在网络中增加一台交换机时，就会出现此问题。

此交换机之前在实验室中使用过，并且输入了一个较好的 VTP 域名。将此交换机配置为 VTP 客户端并连接到其余网络。然后，接通与其余网络连接的 ISL 链路。仅在几秒内，整个网络就瘫痪了。这是怎么发生的？

您加入的交换机的配置修订版号高于 VTP 域的配置修订版号。因此，您最近加入的交换机（几乎未

配置任何 VLAN ) 清除了 VTP 域中的所有 VLAN。

无论此交换机是 VTP 客户端还是 VTP 服务器，都会发生上述情况。VTP 客户端可清除 VTP 服务器上的 VLAN 信息。当网络中的许多端口进入不活动状态，但仍继续被分配给不存在的 VLAN 时，您就可以断定发生了上述情况。

## 解决方案

快速在其中一台 VTP 服务器上重新配置所有 VLAN。

## 要切记的内容

始终确保加入到 VTP 域中的所有交换机的配置修订版本号低于 VTP 域中已存在的交换机的配置修订版本号。

如果从您的 Cisco 设备中获得 `show tech-support` 命令的输出，则可以使用[命令输出解释程序](#) ([仅限注册用户](#)) 来显示潜在的问题和解决方法。

## 示例

完成以下步骤可查看此问题的一个示例：

1. 发出以下命令，可看到 clic 有 7 个 VLAN ( VLAN 1、VLAN 2、VLAN 3 和默认 VLAN )，clic 是名为 test 的域中的 VTP 服务器，以及端口 2/3 位于 VLAN 3 中：`clic (enable) show vlan`

```
1993 May 25 05:09:50 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1 lan
VLAN Name                Status    IfIndex Mod/Ports, Vlans
-----
1    default                active    65      2/2,2/4-50
2    VLAN0002               active    70
3    VLAN0003               active    71      2/3
1002 fddi-default           active    66
1003 token-ring-default     active    69
1004 fddinet-default       active    67
1005 trnet-default         active    68      68
```

```
clic (enable) show vtp domain
```

```
Domain Name                Domain Index VTP Version Local Mode Password
-----
test                        1            2            server      -
```

```
Vlan-count Max-vlan-storage Config Revision Notifications
-----
7          1023          0            disabled
```

```
Last Updater    V2 Mode Pruning PruneEligible on Vlans
-----
0.0.0.0         disabled disabled 2-1000
```

```
clic (enable) show port 2/3
```

```
Port Name                Status    Vlan    Level Duplex Speed Type
-----
2/3                    connected 3        normal 10    half 10/100BaseTX
```

2. 连接 bing，它是一台其上创建了 VLAN 4、VLAN 5 和 VLAN 6 的实验室交换机。**注意：**此交

交换机中的配置修订版本号是 3。bing (enable) **show vlan**

VLAN Name	Status	IfIndex	Mod/Ports, Vlans
1 default	active	4	2/1-48 3/1-6
4 VLAN0004	active	63	
5 VLAN0005	active	64	
6 VLAN0006	active	65	
1002 fddi-default	active	5	
1003 token-ring-default	active	8	
1004 fddinet-default	active	6	
1005 trnet-default	active	7	

3. 将 bing 放置在相同的 VTP 域 (test) 中。bing (enable) **show vtp domain**

Domain Name	Domain Index	VTP Version	Local Mode	Password
test	1	2	server	-

Vlan-count	Max-vlan-storage	Config Revision	Notifications
8	1023	3	disabled

Last Updater	V2 Mode	Pruning	PruneEligible on Vlans
10.200.8.38	disabled	disabled	2-1000

4. 配置两台交换机之间的中继，以便将 bing 集成在网络中。Bing 清除了 clic 的 VLAN，现在 clic 有 VLAN 4、VLAN 5 和 VLAN 6。但是，clic 不再有 VLAN 2 和 VLAN 3，并且端口 2/3 处于不活动状态。clic (enable) **show vtp domain**

Domain Name	Domain Index	VTP Version	Local Mode	Password
test	1	2	server	-

Vlan-count	Max-vlan-storage	Config Revision	Notifications
8	1023	3	disabled

Last Updater	V2 Mode	Pruning	PruneEligible on Vlans
10.200.8.38	disabled	disabled	2-1000

clic (enable)

clic (enable) **show vlan**

VLAN Name	Status	IfIndex	Mod/Ports, Vlans
1 default	active	65	2/2,2/4-50
4 VLAN0004	active	72	
5 VLAN0005	active	73	
6 VLAN0006	active	74	
1002 fddi-default	active	66	
1003 token-ring-default	active	69	
1004 fddinet-default	active	67	
1005 trnet-default	active	68	68

clic (enable) **show port 2/3**

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
2/3		inactive	3	normal	auto	auto	10/100BaseTX

## [最近添加的交换机无法从 VTP 服务器获取 VLAN](#)

确保最近添加的交换机的配置修订版本号低于域的当前修订版本号。有关详细信息，请参阅[最近加入的交换机怎样会导致网络问题](#)和[重置配置修订版本号](#)部分。

新的交换机可能不会立即收到来自 VTP 服务器的已配置 VLAN 列表。要解决此问题，请对 VLAN 数据库进行以下任一种修改：

- 创建任意 VLAN。
- 删除任意 VLAN。
- 修改任何当前 VLAN 的属性。

在相同域中的任何 VTP 服务器上修改 VLAN 数据库。

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 50
Switch(config-vlan)#name 50thVLAN
Switch(config-vlan)#end
Switch#
```

修改完成后，新添加的交换机就能收到来自 VTP 服务器的 VLAN 信息。

## [重置配置修订版本号](#)

按照本部分中提供的两个过程的任何一个进行操作，都可以很容易地重置配置修订版本号。

### [使用域名重置配置修订版本号](#)

要通过更改域名来重置配置修订版本号，请完成以下步骤：

1. 发出以下命令，以查看配置是否为空：`clac (enable) show vtp domain`

```
Domain Name                Domain Index VTP Version Local Mode Password
-----
                            1             2             server      -
```

```
Vlan-count Max-vlan-storage Config Revision Notifications
-----
5           1023              0             disabled
```

```
Last Updater V2 Mode Pruning PruneEligible on Vlans
-----
0.0.0.0      disabled disabled 2-1000
clac (enable)
```

2. 配置域名（在本示例中为 **test**），然后创建两个 VLAN。配置修订版本号上升为 2：`clac (enable) set vtp domain test`

```
VTP domain test modified
```

```
clac (enable) set vlan 2
```

```
Vlan 2 configuration successful
```

```
clac (enable) set vlan 3
```

```
Vlan 3 configuration successful
```

```
clic (enable) show vtp domain
```

```
Domain Name                Domain Index VTP Version Local Mode Password
-----
test                        1           2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
-----
7           1023           2           disabled

Last Updater V2 Mode Pruning PruneEligible on Vlans
-----
0.0.0.0      disabled disabled 2-1000
```

```
clic (enable)
```

3. 将域名从 test 更改为 cisco。配置修订版号将改回为 0，并且所有 VLAN 仍存在：clic

```
(enable) set vtp domain cisco
```

```
VTP domain cisco modified
```

```
clic (enable) show vtp domain
```

```
Domain Name                Domain Index VTP Version Local Mode Password
-----
cisco                      1           2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
-----
7           1023           0           disabled

Last Updater V2 Mode Pruning PruneEligible on Vlans
-----
0.0.0.0      disabled disabled 2-1000
```

4. 将 VTP 域名从 cisco 更改回为 test。配置修订为 0。此过程没有清除任何内容的风险，并且先前配置的所有 VLAN 都将保留：clic (enable) set vtp domain test

```
VTP domain test modified
```

```
clic (enable) show vtp domain
```

```
Domain Name                Domain Index VTP Version Local Mode Password
-----
test                        1           2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
-----
7           1023           0           disabled

Last Updater V2 Mode Pruning PruneEligible on Vlans
-----
0.0.0.0      disabled disabled 2-1000
```

```
clic (enable)
```

## [使用 VTP 模式重置配置修订版号](#)

要通过更改 VTP 模式来重置配置修订版号，请完成以下步骤：

1. 发出以下命令，以查看配置是否为空：clic (enable) show vtp domain

```
Domain Name                Domain Index VTP Version Local Mode Password
-----
1                           2           server      -
```

```
Vlan-count Max-vlan-storage Config Revision Notifications
-----
5          1023          0          disabled
```

```
Last Updater V2 Mode Pruning PruneEligible on Vlans
-----
0.0.0.0      disabled disabled 2-1000
clic (enable)
```

2. 配置域名 ( 在本示例中为 **test** ) , 然后创建两个 VLAN。配置修订版本号上升为 2 : clic (enable) **set vtp domain test**

```
VTP domain test modified
```

```
clic (enable) set vlan 2
```

```
Vlan 2 configuration successful
```

```
clic (enable) set vlan 3
```

```
Vlan 3 configuration successful
```

```
clic (enable) show vtp domain
```

```
Domain Name          Domain Index VTP Version Local Mode Password
-----
test                 1           2           server      -
```

```
Vlan-count Max-vlan-storage Config Revision Notifications
-----
7          1023          2          disabled
```

```
Last Updater V2 Mode Pruning PruneEligible on Vlans
-----
0.0.0.0      disabled disabled 2-1000
clic (enable)
```

3. 将 VTP 模式从服务器模式更改为透明模式。配置修订版本号将改回为 0 , 并且所有 VLAN 仍存在 : clic (enable) **set vtp mode transparent**

```
VTP domain test modified
```

```
clic (enable) show vtp domain
```

```
Domain Name          Domain Index VTP Version Local Mode Password
-----
test                 1           2           transparent -
```

```
Vlan-count Max-vlan-storage Config Revision Notifications
-----
7          1023          0          disabled
```

```
Last Updater V2 Mode Pruning PruneEligible on Vlans
-----
0.0.0.0      disabled disabled 2-1000
```

4. 将 VTP 模式从透明模式更改为服务器模式或客户端模式。配置修订为 0。此过程没有清除任何内容的风险 , 并且先前配置的所有 VLAN 都将保留 : clic (enable) **set vtp mode server**

```
VTP domain test modified
```

```
clic (enable) show vtp domain
```

```
Domain Name          Domain Index VTP Version Local Mode Password
```

```

-----
test                1                2                server        -

Vlan-count Max-vlan-storage Config Revision Notifications
-----
7             1023             0             disabled

Last Updater      V2 Mode  Pruning  PruneEligible on Vlans
-----
0.0.0.0          disabled disabled 2-1000
clic (enable)

```

## 重新通电后所有端口均变为非活动状态

当交换机端口是 VLAN 数据库中不存在的 VLAN 的成员时，这些端口会变为不活动状态。常见问题是重新通电后所有端口均变为不活动状态。通常，使用某个 VLAN (不是 VLAN 1) 中的上行链路中继端口将交换机配置为 VTP 客户端时，会出现此问题。由于交换机处于 VTP 客户端模式，因此当交换机重置时，会丢失其 VLAN 数据库，并导致上行链路端口和其他所有不是 VLAN 1 成员的端口进入不活动模式。

要解决此问题，请完成以下步骤：

1. 暂时将 VTP 模式更改为透明模式。switch (enable) set vtp mode transparent

```

VTP domain austinlab modified
switch (enable)

```

2. 将上行链路端口所属的 VLAN 添加到 VLAN 数据库中。**注意：**本示例假定 VLAN 3 是分配给上行链路端口的 VLAN。switch (enable) set vlan 3

```

VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 3 configuration successful
switch (enable)

```

3. 在上行链路端口开始转发之后，将 VTP 模式改回客户端模式。switch (enable) set vtp mode client

VTP domain austinlab modified 完成这些步骤后，VTP 应该从 VTP 服务器重新填充 VLAN 数据库。重新填充会使作为 VTP 服务器通告的 VLAN 成员的所有端口重新变为活动状态。

## 中继关闭导致 VTP 问题

请记住，VTP 数据包在 VLAN 1 中传输，但仅通过中继 (ISL、dot1q 或 LAN 仿真 [LANE]) 传输。

如果在网络两个部分之间的中继关闭或 LANE 连接断开时更改 VLAN，则可能会丢失 VLAN 配置。当中继连接恢复后，网络的两端会重新同步。因此，具有最高配置修订版号的交换机会清除具有最低配置修订版号的交换机的 VLAN 配置。

## VTP 和 STP (逻辑生成树端口)

当您有一个较大的 VTP 域时，也就有一个较大的 STP 域。VLAN 1 必须跨越整个 VTP 域。因此，将在整个域中对该 VLAN 运行一个唯一的 STP。

如果在使用 VTP 时创建了一个新的 VLAN，则该 VLAN 将在整个 VTP 域中传播。然后，VTP 域中的所有交换机上都会创建该 VLAN。所有 Cisco 交换机都使用 PVST，这表示交换机对每个 VLAN



运行一个单独的 STP。这就增大了交换机的 CPU 负载。要了解每台交换机上可以拥有的 STP 数量，您必须参考交换机支持的最大逻辑端口数（对于 STP）。逻辑端口数大致等于运行 STP 的端口数。

**注意：** 中继端口对中继上的每个活动 VLAN 运行一个 STP 实例。

您可以使用以下公式快速计算您的交换机的这个值：

```
switch (enable) set vtp mode client
```

```
VTP domain austinlab modified
```

每台交换机的这个值（即，STP 的最大逻辑端口数）都不同，该值记录在每个产品的发行版本注释中。例如，在配有 Supervisor 引擎 2 的 Catalyst 5000 上，最多可以有 1500 个 STP 实例。每次使用 VTP 创建一个新的 VLAN 时，默认情况下该 VLAN 会传播到所有交换机，并且随后在所有端口上被激活。您可能需要修剪中继上不必要的 VLAN，避免逻辑端口的数量过多。

**注意：** 可以使用以下方法之一修剪中继上不必要的 VLAN：

- **手动修剪中继上不必要的 VLAN** - 这是最佳方法，该方法可避免使用生成树。相反，该方法运行中继上已修剪的 VLAN。本文档的 [VTP 修剪](#) 部分对手动修剪进行了详细说明。
- **VTP 修剪** - 如果您的目标是减少 STP 实例的数量，请避免使用此方法。中继上使用 VTP 修剪的 VLAN 仍是生成树的一部分。因此，使用 VTP 修剪的 VLAN 不会减少生成树端口实例的数量。

## [VTP 修剪](#)

VTP 修剪可增大可用的带宽。VTP 修剪限制泛洪流量只能进入要访问相应的网络设备时这些流量必须使用的中继链路。默认情况下，VTP 修剪处于禁用状态。在 VTP 服务器上启用 VTP 修剪会对整个管理域启用修剪。`set vtp pruning enable` 命令自动修剪 VLAN，并在不需要帧的情况下停止帧的无效泛洪。默认情况下，VLAN 2 到 VLAN 1000 适合修剪。VTP 修剪不会修剪来自不适合修剪的 VLAN 的流量。VLAN 1 总是不适合修剪；不能修剪来自 VLAN 1 的流量。

**注意：** 不同于手动 VLAN 修剪，自动修剪不限制生成树直径。

管理域中的所有设备都必须支持 VTP 修剪，这样 VTP 修剪才会生效。在不支持 VTP 修剪的设备上，必须手动配置中继上允许的 VLAN。可以使用 `clear trunk mod/port` 命令和 `clear trunk vlan_list` 命令手动修剪中继上的 VLAN。例如，您可以选择每个中继上只允许一台核心交换机连接到实际需要的 VLAN。这有助于减少所有交换机（核心交换机和接入交换机）的 CPU 负载，并避免对贯穿整个网络的 VLAN 使用 STP。这种修剪限制了 VLAN 中的 STP 问题。

示例如下：

- **拓扑** - 拓扑为两台相互连接的核心交换机，每台交换机都有 80 个中继连接到 80 台不同的接入交换机。按照此设计，每台核心交换机有 81 个中继，而每台接入交换机有两个上行链路中继。假定接入交换机除了有两个上行链路外，还有两个或三个连接到 Catalyst 1900 的中继。这样，每台接入交换机总共有 4-5 个中继。
- **平台** - 核心交换机是运行软件版本 5.5(7) 的 Catalyst 6500，配有 Supervisor 引擎 1A 和 Policy Feature Card 1 (PFC1)。根据 [Catalyst 6000/6500 软件版本 5.x 发行版本注释](#)，此平台的 STP 逻辑端口数不能超过 4000 个。
- **接入交换机** - 接入交换机是以下交换机之一：配有 Supervisor 引擎 2 的 Catalyst 5000 交换机，该交换机最多支持 1500 个 STP 逻辑端口配有 Supervisor 引擎 1 和 20 MB 的 DRAM 的

Catalyst 5000 交换机，该交换机最多支持 400 个 STP 逻辑端口

- **VLAN 数量** - 请切记要使用 VTP。VTP 服务器上的 VLAN 将在网络中的所有交换机上创建。如果有 100 个 VLAN，则核心交换机必须处理大约 8100 个逻辑端口 ( 100 个 VLAN x 81 个中继 )，这超出了限制。接入交换机必须处理 500 个逻辑端口 ( 100 个 VLAN x 5 个中继 )。在这种情况下，核心 Catalyst 交换机超过了支持的逻辑端口数，并且配有 Supervisor 引擎 1 的接入交换机也超出了限制。
- **解决方案** - 如果假定每台接入交换机上实际只需要 4 个或 5 个 VLAN，则可以在核心层修剪中继上的所有其他 VLAN。如果连接到该接入交换机的中继 3/1 上只需要 VLAN 1、VLAN 10、VLAN 11 和 VLAN 13，则核心交换机上的配置如下：  
Praha> (enable) set trunk 1/1 des

```
Port(s) 1/1 trunk mode set to desirable.
```

```
Praha> (enable) clear trunk 1/1 2-9,12,14-1005
```

```
Removing Vlan(s) 2-9,12,14-1005 from allowed list.
```

```
Port 1/1 allowed vlans modified to 1,10,11,13.
```

```
Praha> (enable) clear trunk 1/1 2-9,12,14-1005
```

**注意：**即使未超过允许的逻辑端口数，也要修剪中继上的 VLAN。这是因为一个 VLAN 中的 STP 环路仅延伸到允许该 VLAN 的位置，它不会穿过整个园区。一个 VLAN 中的广播不会到达不需要该广播的交换机。在低于软件版本 5.4 的版本中，您不能从中继中清除 VLAN 1。在较高版本中，可以使用以下命令清除 VLAN 1：  
Praha> (enable) clear trunk 1/1 1

Default vlan 1 cannot be cleared from module 1. 本文档的 [VLAN 1 案例](#) 部分讨论有关防止 VLAN 1 跨越整个园区的技术。

## 未修剪 VLAN

如果交换机 A 与交换机 B 通过交换机 A 的一个端口连接，并且该端口已配置作为中继且连接到 IP 电话，则 VTP 会加入到从交换机 A 传递到交换机 B 的消息中。因此，交换机 B 无法修剪未使用的 VLAN。

如果将连接到 IP 电话的端口配置作为接入端口语音 VLAN，则可以解决此问题。

```
Switch#interface FastEthernet0/1
switchport access vlan <vlan number>
switchport voice vlan <vlan number>
```

## VLAN 1 案例

要能够传输 VTP、Cisco 发现协议 [CDP] 流量和其他控制流量，不能对每个地方都需要的 VLAN 和园区中的所有交换机上都允许的 VLAN 应用 VTP 修剪。但是，有一种限制 VLAN 1 的范围的功能。该功能称为禁用中继上的 VLAN 1。运行 CatOS 软件版本 5.4(x) 及更高版本的 Catalyst 4500/4000、5500/5000 和 6500/6000 系列交换机上提供该功能。通过使用该功能，您可以修剪中继上的 VLAN 1，就像修剪任何其他 VLAN 一样。此修剪不包括中继上仍允许的所有控制协议流量 ( DTP、PAGP、CDP、VTP 等 )。但是，修剪会阻塞该中继上的所有用户流量。使用此功能可防止 VLAN 跨越整个园区。STP 环路的范围受到限制，即使在 VLAN 1 中也是如此。像配置要从中继中清除的其他 VLAN 一样配置要禁用的 VLAN 1：

```
Console> (enable) set trunk 2/1 desirable
```

```
Port(s) 2/1 trunk mode set to desirable.
```

```
Console> (enable) clear trunk 2/1 1
```

```
Removing Vlan(s) 1 from allowed list.  
Port 2/1 allowed vlans modified to 2-1005.
```

UDLD 使用本地 VLAN 与邻居通信。因此，要使 UDLD 正常工作，在中继端口中不能修剪本地 VLAN。

## [对 show vtp statistics 命令输出中显示的 VTP 配置修订版本号错误进行故障排除](#)

VTP 是为以下管理环境而设计的：在任何时候一次只在一台交换机上更改域的 VLAN 数据库。它假定新修订在整个域中传播后，才进行另一个修订。如果在管理域中的两台不同设备上同时更改数据库，则可能会导致生成两个具有相同修订版本号的不同数据库。这些数据库传播并覆盖现有信息，直到在网络中的中间 Catalyst 交换机上交汇为止。由于数据包具有相同的修订版本号但有不同的 MD5 值，因此，此交换机不能接受任一通告。当交换机检测到这种情况时，它会使 No of config revision errors 计数器递增。

**注意：**本部分中的 `show vtp statistics` 命令输出是一个示例。

如果您发现某台交换机上的 VLAN 信息未更新，或者您遇到其他类似问题，请发出 `show vtp statistics` 命令。确定存在配置修订版本号错误的 VTP 数据包的计数是否在递增：

```
Console> (enable) show vtp statistics
```

```
VTP statistics:  
summary advts received          4690  
subset advts received           7  
request advts received          0  
summary advts transmitted       4397  
subset advts transmitted        8  
request advts transmitted       0  
No of config revision errors   5  
No of config digest errors      0  
VTP pruning statistics:  
Trunk      Join Transmitted  Join Received  Summary advts received from  
non-pruning-capable device  
-----  
1/1        0                0              0  
1/2        0                0              0
```

```
Console> (enable)
```

如果您发现配置修订版错误，请用某种方式更改 VLAN 数据库，以便创建一个其修订版本号比竞争的数据库的修订版本号要高的 VTP 数据库，这样就可以解决此问题。例如，在充当主 VTP 服务器的交换机上，在管理域中添加或删除一个错误的 VLAN。此更新的修订将在整个域中传播，并覆盖所有设备中的数据库。当域中的所有设备都通告同一个数据库时，错误就不再出现。

## [对 show vtp statistics 命令输出中显示的 VTP 配置摘要错误进行故障排除](#)

本部分说明如何对发出 `show vtp statistics` 命令时出现的 VTP 配置摘要错误进行故障排除。示例如下：

```
Console> (enable) show vtp statistics
```

```
VTP statistics:  
summary advts received          3240  
subset advts received           4  
request advts received          0  
summary advts transmitted       3190  
subset advts transmitted        5  
request advts transmitted       0
```

```

No of config revision errors    0
No of config digest errors     2
VTP pruning statistics:
Trunk      Join Transmitted  Join Received  Summary advts received from
              non-pruning-capable device
-----
1/1         0                0              0
1/2         0                0              0
Console> (enable)

```

MD5 值的一般用途是验证收到的数据包的完整性，并检测传输过程中数据包是否进行了任何更改或数据包是否已损坏。当交换机检测到新的修订版号与当前存储的值不同时，交换机会发送一条请求消息给 VTP 服务器，请求 VTP 子集。子集通告包含 VLAN 信息列表。交换机计算子集通告的 MD5 值，然后将该值与 VTP 汇总通告的 MD5 值进行比较。如果这两个值不同，交换机会使 No of config digest errors 计数器递增。

这些摘要错误的常见原因是 VTP 域中所有 VTP 服务器上配置的 VTP 口令不一致。请将这些错误作为配置错误或数据毁坏问题进行故障排除。

对此问题进行故障排除时，请确保错误计数器显示的不是历史数据。统计信息菜单计算自最近设备重置或 VTP 统计信息重置以来出现的错误数。

## [无法从服务器/透明模式切换交换机的 VTP 模式](#)

如果交换机是独立的（也就是说，未连接到网络），并且您要将 VTP 模式配置为客户端模式，则在重新启动后，交换机将处于 VTP 服务器模式或 VTP 透明模式，具体取决于在将交换机配置为 VTP 客户端模式之前它的 VTP 模式。当附近没有 VTP 服务器时，交换机不允许将自身配置为 VTP 客户端。

## [VTP 域中的 OSPF Hello 被阻塞](#)

如果 VTP 域中的交换机从服务器模式或客户端模式切换到透明模式，则开放最短路径优先 (OSPF) Hello 数据包可能被阻塞，并且邻接关系可能被丢弃。如果域中启用了 VTP 修剪，则可能会出现此问题。

使用以下任一方法可解决此问题：

- 对 OSPF 邻居进行硬编码。
- 禁用域中的 VTP 修剪。
- 将交换机的 VTP 模式恢复为服务器模式或客户端模式。

## [SW\\_VLAN-4-VTP\\_USER\\_NOTIFICATION](#)

本部分讨论此错误消息的常见变体：

```

Console> (enable) show vtp statistics

VTP statistics:
summary advts received          3240
subset advts received           4
request advts received          0
summary advts transmitted       3190
subset advts transmitted        5
request advts transmitted       0
No of config revision errors    0

```

```

No of config digest errors      2
VTP pruning statistics:
Trunk      Join Transmitted  Join Received  Summary advts received from
              non-pruning-capable device
-----
1/1         0                0              0
1/2         0                0              0
Console> (enable)

```

### [%SW\\_VLAN-4-VTP\\_USER\\_NOTIFICATION : VTP protocol user notification:Version 1 device detected on \[int\] after grace period has ended](#)

默认情况下，Cisco 交换机上的 VLAN 中继协议 (VTP) 版本为版本 2 且与版本 1 兼容。此消息只是一个通知，指示与端口 Gig0/10 连接的交换机运行 VTP 版本 1。除非您运行 IPX，否则一切正常，并且对交换机没有任何损害。

要解决此问题，请使用以下命令更改 VTP 版本。

对于 Cisco IOS 交换机，请使用以下命令：

```

Switch#vlan database
Switch(vlan)#vtp v2-mode

```

对于 CatOS 交换机，请使用以下命令：

```

Console> (enable) set vtp version 2 enable

```

### [%SW\\_VLAN-SP-4-VTP\\_USER\\_NOTIFICATION : VTP protocol user notification:MD5 digest checksum mismatch on receipt of equal revision summary on trunk:\[int\]](#)

要了解有关该问题的原因的详细信息并解决问题，请参阅[对 show vtp statistics 命令输出中显示的 VTP 配置摘要错误进行故障排除](#)部分。

### [%SW\\_VLAN-4-VTP\\_USER\\_NOTIFICATION : VTP protocol user notification:Error detected in VTP Revision Number for VTP Domain Index \[dec\]](#)

要了解有关该问题的原因的详细信息并解决问题，请参阅[对 show vtp statistics 命令输出中显示的 VTP 配置修订版本号错误进行故障排除](#)部分。

### [在 show running-config 命令输出中，单个 Switchport Trunk Allowed vlan 命令显示为多个命令](#)

当允许的 VLAN 数量超过某个特定的字符数（即，默认终端宽度）时，**show running-config** 命令会分行显示，将 **switchport trunk allowed vlan add** 命令添加到另一行。这是 Cisco IOS 处理 **switchport trunk allowed vlan** 命令中的长列表的方式。

```

Switch#configure terminal
Switch(config)#int fa3/30
Switch(config-if)#switchport trunk allowed vlan 14, 105, 110, 115, 120, 125, 130-132,
140, 150, 155, 200, 210, 220, 222, 230, 232, 240, 301-309, 840, 860-862, 870, 880,
881, 884-886, 889, 896, 898, 411, 412, 413, 421
!--- The previous command should be in a single line. It has been wrapped into three lines for
proper formatting.

```

**show running-config** 的输出类似以下内容：

```

Switch#show running-config | begin 3/30
interface FastEthernet3/30

```

```
switchport
switchport trunk allowed vlan 14,105,110,115,120,125,130-132,140,150,155,200
switchport trunk allowed vlan add 210,220,222,230,232,240,301-309,411-413,421
switchport trunk allowed vlan add 840,860-862,870,880,881,884-886,889,896,898
!
```

*!--- rest of output elided*

您还可以注意到命令输出中 VLAN 列表按升序显示。

从允许的列表中删除 VLAN 1，以便您可以禁用任何单独的 VLAN 中继端口上的 VLAN 1，从而降低形成生成树环路或风暴的危险。从中继端口中删除 VLAN 1 时，接口继续发送和接收 VLAN 1 中的管理流量，例如 Cisco 发现协议 (CDP)、端口聚合协议 (PAgP)、链路聚合控制协议 (LACP)、动态中继协议 (DTP) 和 VLAN 中继协议 (VTP)。

allowed vlan 命令的 no 形式将列表重置为默认列表，默认列表允许所有的 VLAN。

## [内部 VLAN 使用](#)

所有发送到 EARL 的数据包都必须以 VLAN ID 作为前缀，因为这是 EARL 期望的数据包格式。路由端口没有可视的 VLAN ID，因为未显式配置 VLAN ID。因此，交换机从其 VLAN 池（共 4096 个 VLAN）中借用一个 VLAN。通过使用全局配置模式 **vlan allocation policy** 命令，您可以指示 Catalyst 6500 系列交换机开始借用小于 VLAN 4096 或者大于 VLAN 1006 的 VLAN。

```
Switch(config)#vlan internal allocation policy {ascending | descending}
```

因此，路由接口或 WAN 接口利用内部 VLAN 就是正常的行为。

## [相关信息](#)

- [LAN 产品支持](#)
- [LAN 交换技术支持](#)
- [技术支持和文档 - Cisco Systems](#)