

第 4 章 Vlan 中继协议

【单元概述】

目前交换网络应用广泛,而交换机并不是都集中放置在机房中,如果没有集中管理 Vlan 的方法,那么需要在每个交换机上配置 Vlan,工作量较大。VTP 是一种消息协议,用于在 VTP 域内同步 Vlan 信息,而不必在每个交换上配置相同的 Vlan 信息,从而实现 Vlan 配置的一致性。

本章首先通过 VTP 项目引出本章的主要项目,通过项目知识点的分解,逐步了解 VTP 的基本工作原理、域、模式及配置,然后重点介绍应用 VTP 来配置 Vlan。

【知识要点及掌握程度】

- 4.1 VTP 项目设计:理解、运用。
- 4.2 VTP 概述:了解、运用。
- 4.3 配置 VTP:掌握、运用。
- 4.4 排查 VTP 配置故障:了解、运用。

【能力要点及掌握程度】

- (1)计算机基础知识:掌握 VTP 配置的基本语法,VTP 的概念、域及不同模式 VTP。(重要)
- (2)知识在设计中的应用:分析项目中涉及的知识点。(重要)
- (3)分析问题:掌握项目中需要的内容,通过分析找出解决问题的系统方法。(中等)

【教学重点与难点】

重点:

- (1)VTP 的域及 VTP 模式;
- (2)VTP 配置。

难点:

VTP 模式。

【教学设计与实施方法】

本单元主要采用讲授教学法和实验教学。讲授教学法通过教师课堂讲授实施,实验教学法通过学生课堂使用 Packet Tracer 软件设计实施章节项目。

4.1 VTP 项目设计

4.1.1 项目实训目标

- (1) 根据企业需求,完成应用 VTP 配置 Vlan 划分。
- (2) 通过实际操作,掌握 VTP 的配置命令。
- (3) 掌握 VTP 的配置方法。

4.1.2 项目实训环境

项目实训环境:

- (1) 安装 Packet Tracer 模拟器软件;
- (2) Cisco 2960 交换机 2 台、主机 4 台;
- (3) 链接线缆若干。

4.1.3 项目实训需求

市场部和技术部这两个部门部分员工分布在不同办公地点,为了部门网络安全,需要按部门划分 Vlan,使各部门之间不能互相访问。为了管理 Vlan 方便,应用 VTP 管理划分 Vlan。

4.1.4 项目实训设计

1. 项目拓扑设计

为完成项目需求所提出的要求,首先设计项目拓扑图如图 4.1 所示。市场部所属网段为 192.168.1.0/24,技术部所属网段为 192.168.2.0/24。另外,市场部的机器为 PC1 和 PC3,划分在 Vlan 10 中,而技术部的机器为 PC2 和 PC4,划分在 Vlan 20 中。

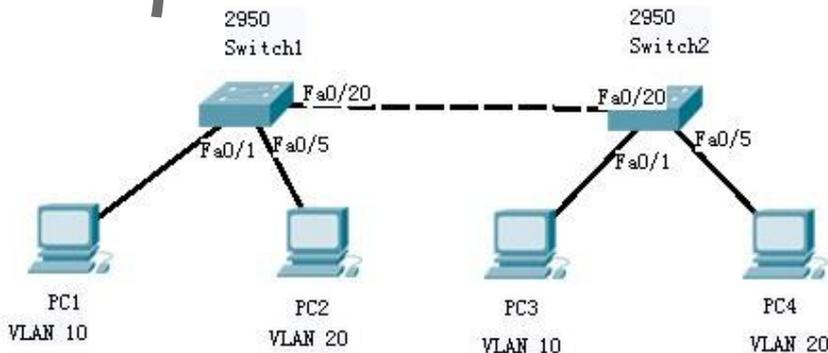


图 4.1 VTP 项目设计网络拓扑图

2. 项目 IP 及接口设计

项目涉及 IP 及接口设计如表 4.1 所示。

表 4.1 设备 IP 及接口列表

设备	接口	IP 地址	子网掩码	默认网关	Vlan
PC1	网卡	192.168.1.2	255.255.255.0	192.168.1.1	Vlan 10
PC2	网卡	192.168.2.2	255.255.255.0	192.168.2.1	Vlan 20
PC3	网卡	192.168.1.3	255.255.255.0	192.168.1.1	Vlan 10
PC4	网卡	192.168.2.3	255.255.255.0	192.168.2.1	Vlan 20

3. 项目实施过程设计

根据项目需求,分解相关技术知识点,分步骤完成总体项目,项目设计内容如下:

步骤 1. 恢复所有交换机的配置为出厂配置。

步骤 2. 进入交换机 1 的全局配置模式,配置 VTP 域和运行模式。

步骤 3. 进入交换机 1 的互联接口,配置 trunk。

步骤 4. 进入交换机 2 的全局配置模式,配置 VTP 域和运行模式。

步骤 5. 进入交换机 2 的互联接口,配置 trunk。

步骤 6. 进入交换机 1 的全局配置模式,创建 Vlan。

步骤 7. 进入交换机 1 的接口模式,分配端口到相应 Vlan 中。

步骤 8. 进入交换机 2 的接口模式,分配端口到相应 Vlan 中。

步骤 9. 查看各交换机的 VTP 信息和 Vlan、trunk 信息。

步骤 10. 验证各部门内部主机之间是否能访问,市场部主机是否能访问技术部主机。

4.2 VTP 概述

4.2.1 什么是 VTP

目前交换网络应用广泛,而交换机并不是都集中放置在机房中,如果没有集中管理 Vlan 的方法,那么需要在每个交换机上配置,工作量较大。是否可以让接入交换机从核心交换机自动学习 Vlan,修改、添加或者删除 Vlan 都在核心交换机上操作?

1. VTP 的概念

VTP(Vlan Trunking Protocol,Vlan 中继协议)是一种消息协议,用于在 VTP 域内同步 Vlan 信息,而不必在每个交换上配置相同的 Vlan 信息,从而实现 Vlan 配置的一致性。VTP 协议使得管理员可以在一个或者几个中央点(Server)上创建、修改和删除 Vlan,Vlan 信息通过 Trunk(中继)链路自动扩散到其他交换机,任何参与 VTP 的交换机都可以接受这些修改,所有交换机保持相同的 Vlan 信息。从而减少在多台设备上配置同一信息的工作量,而且方便管理。VTP 信息只能在 Trunk 端口上传播。

VTP 是 Cisco 公司开发的私有协议,目前华为等交换机也支持 VTP 协议。VTP 在称为 Vlan.dat 的 Vlan 数据库里存储对 Vlan 的配置。通过 VTP 可以管理网络中标准的 Vlan (即 Vlan ID 从 1~1005),扩展 Vlan(即 Vlan ID 大于 1005)不支持。

2. VTP 的优点

- (1) 保证网络中 Vlan 配置的一致性。
- (2) 便于跟踪和监视 Vlan。
- (3) 及时动态报告网络中添加的 Vlan。

4.2.2 VTP 域

为了方便管理 Vlan, VTP 允许将网络划分成更小的管理域(VTP Domain), 相同域中的交换机能共享 Vlan 信息。在具体应用中, VTP 支持的是服务器/客户端模式, 即在主交换机建立 VTP 域, 并将主交换机设置成 VTP Server, 分交换机设置为 VTP Client, VTP 服务器和 VTP 客户端建立中继之后, 在两台交换机之间即可交换 VTP 通告, 这样在设为 VTP 服务器的交换机上创建 Vlan, 同一域中的作为 VTP 客户端的交换机就会获得通知, 确保 Vlan 信息的准确, 便于集中管理。当然划分 VTP 域的另一个好处是: 如果发生配置更改错误时, 将限制该错误的传播范围。

一台交换机每次只能成为一个 VTP 域的成员。VTP 域中的 VTP 服务器创建、修改或删除 Vlan 时, Vlan 信息(通告)在整个 VTP 域中传播。当交换机处于不同的 VTP 域时, 它们将无法交换 VTP 通告。默认 VTP 配置都是 VTP 服务器, 且未配置 VTP 域名。

4.2.3 VTP 默认信息

在特权模式下, 通过命令 `show vtp status` 可以查看 VTP 默认状态信息。具体 VTP 默认状态信息如下:

```
Switch# show vtp status
VTP Version      :2
Configuration Revision :0
Maximum Vlans supported locally :255
Number of existing Vlans :5
VTP Operating Mode :Server
VTP Domain Name  :
VTP Pruning Mode :Disabled
VTP V2 Mode      :Disabled
VTP Traps Generation :Disabled
MD5 digest       :0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

其中 VTP Version: VTP 版本, 2 表示思科交换机支持两种 VTP 版本, 分别是 Version 1 和 Version 2, 默认运行的是 Version 1。

Configuration Revision: 交换机配置修正号, 当交换机的 Vlan 配置信息发生改变时, 该值会被加 1。0 表示初始状态, 配置修正号的值也表明交换机 Vlan 配置信息的新旧。

Maximum Vlans supported locally:交换机支持最大 Vlan 数,这个值与交换机的型号有关。

Number of existing Vlans:当前存在的 Vlan 数,默认存在 Vlan 有 1、1002、1003、1004 和 1005,所以默认为 5。Vlan 1 用于默认管理,1002~1005 保留给令牌环和 FDDI Vlan 使用。

VTP Operating Mode:表示当前 VTP 的操作模式,Server 表示服务器模式,还有 Client 客户模式和 Transparent 透明模式。

VTP Domain Name:VTP 域名,目前为空。

VTP Pruning Mode:VTP 修剪模式,Disabled 表示目前是未启用状态。

VTP V2 Mode:VTP 版本 2 模式,Disabled 表示没有使用版本 2,即默认使用的是版本 1。同一 VTP 域中所有交换机的 VTP 版本务必一致,否则 VTP 不能正常工作。

VTP Traps Generation:表示 VTP 每发生变化是否产生 Traps 信息,Traps 主要用来为 SNMP(Simple Network Management Protocol,简单网络管理协议)服务器发送消息,Disabled 表示不使用。

MD5 digest:VTP 验证时需要的散列值(从 VTP 信息计算得出的)。如果 Vlan 信息发生改变,则该散列值也随之改变。如果出现该值与 VTP 域中其他交换机的相应值不同时,将无法学习到新的 VTP 更新。

Configuration last modified:表示最后配置修改的时间。

Local updater ID:表示发送 VTP 消息的端口 IP 地址,可以指定发送 VTP 消息的端口,模拟器不支持该操作。

4.2.4 VTP 通告

VTP 域内的每台交换机都定期在每个 trunk 上发送通告到保留的 VTP 组播地址。VTP 告(或消息)会被邻接的交换机接收到,用于根据需要更新自己的 VTP 和 Vlan 配置。如图 4.2 所示,VTP 通告通过中继传播,共享 Vlan 信息。VTP 消息可以封装在 Cisco 特有的 ISL 数据帧或者 IEEE 802.1Q 帧内,添加了一个 4 字节的字段来标记每个帧。ISL 数据帧和 IEEE 802.1Q 帧中都带有 Vlan ID。

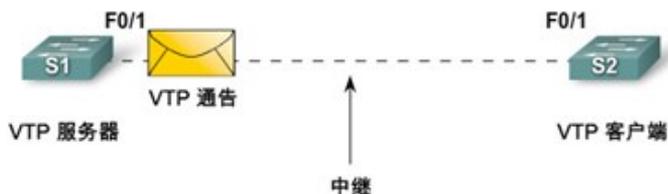


图 4.2 VTP 通告

1. VTP 帧详细信息

VTP 帧详细信息如图 4.3 所示。

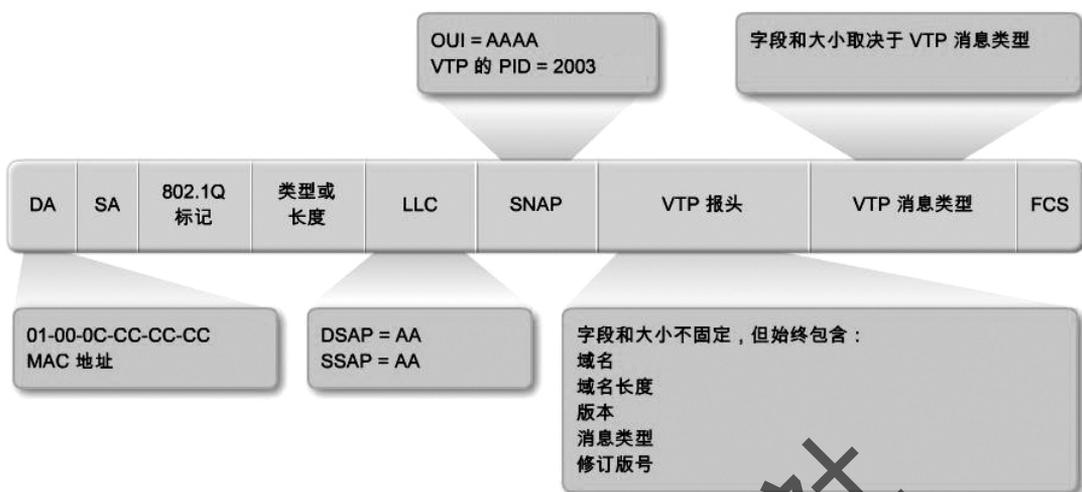


图 4.3 VTP 帧详细信息

目的 MAC 地址(DA):该地址设置为 01-00-0C-CC-CC-CC,这是为所有 VTP 消息保留的组播地址。

LLC 字段:逻辑链路控制 (LLC) 字段包含目的服务接入点 (DSAP) 和源服务接入点 (SSAP),两者的值都是 AA。

SNAP 字段:子网访问协议 (SNAP) 字段,该字段的 OUI 设置为 AAAA,类型设置为 2003。

VTP 消息字段:根据消息类型而变化。

VTP 帧头(报头)字段:此字段的内容取决于 VTP 消息类型(汇总、子集或请求),但其中始终包含以下 VTP 字段:

域名:标识交换机的管理域。

域名长度:域名的长度。

版本:设置为 VTP 1、VTP 2 或 VTP 3。Cisco 2960 交换机仅支持 VTP 1 和 VTP 2。

配置修订版号:交换机的当前配置修订版号。

2. VTP 通告过程

VTP 通告是以组播帧的方式发送的,VTP 通告中有一个字段称为修订号(Revision),初始值为 0。只要在 VTP Server 上创建、修改、删除 Vlan,通告的 Revision 就增加 1,通告中还包含了 Vlan 的变化信息。需要注意的是:高 Revision 的通告会覆盖低 Revision 的通告,而不管是 Server 还是 Client。交换机只接受比本地保存的 Revision 号更高的通告;如果交换机收到 Revision 号更低的通告,会用自己的 Vlan 信息反向覆盖。

当修改位于 VTP Server 上的 Vlan 配置时,该修改将传播至 VTP 域中所有的交换机。VTP 信息通告以多点传送到方式来进行,VTP 服务器和客户模式下会同步更新版本的通告信息,VTP 信息通告每隔 5 分钟或者有变化时发生,如图 4.4 所示。

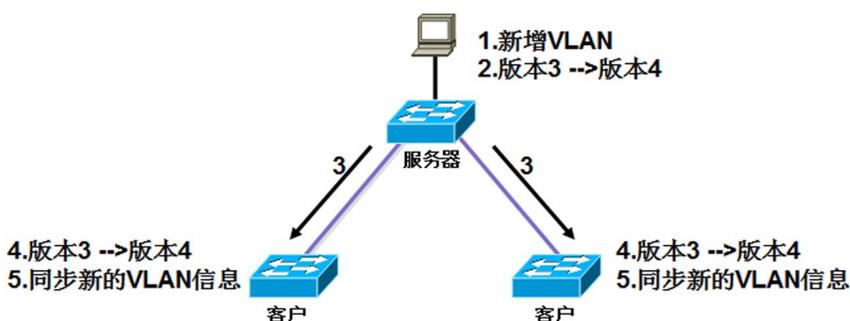


图 4.4 VTP 修改与传递

3. VTP 通告类型

VTP 通告类型包括:汇总通告、子集通告、通告请求和 VTP 加入消息,其中 VTP 加入消息是基于 VTP 修剪协议(VTP Pruning Protocol)的。下面简要介绍 VTP 使用的前 3 种 VTP 消息类型。

(1) 汇总通告

汇总通告用于通知邻接的 Catalyst 交换机目前的 VTP 域名和配置修改编号,默认情况下,Catalyst 交换机每 5 秒钟发送一次汇总通告。当交换机收到汇总通告数据包时,它对比 VTP 域名。如果域名不同,就忽略比较数据包;如果域名相同,则进一步对比配置修改编号。如果交换机自身的配置修改编号更高或与之相等,就忽略此数据包。如果更小,就发送通告请求。

汇总通告占 VTP 通告中的绝大部分。汇总通告包含 VTP 域名、当前修订版本号和其他 VTP 配置详细信息,详见如图 4.5 所示。

汇总通告			
版本	代码	跟随者	管理域名长度
管理域名 (用零补足 32 个字节)			
配置修订版号			
更新者身份			
更新时间戳 (12 字节)			
MD5 摘要 (16 字节)			

图 4.5 汇总通告的格式

(2) 子集通告

如果在 VTP 服务器上增加,删除和修改了 Vlan,“配置修改编号”就会增加,交换机首先会发送汇总通告,然后发送一个或多个子集通告,子集通告中包括 Vlan 列表和相应的 Vlan 信息,如果有多个 Vlan,为了通告所有的信息,可能需要发送多个子集通告。

子集通告包含 Vlan 信息,该信息被排序,使较低值的 Vlan 先出现。子集通告详见如图 4.6 所示,更具体的 Vlan 信息字段信息详见如图 4.7 所示。

子集通告			
版本	代码	序列号	管理域名长度
管理域名 (用零补足 32 个字节)			
配置修订版号			
VLAN 信息字段 1			
:			
VLAN 信息字段 N			

图 4.6 子集通告的格式

VLAN 信息			
信息长度	状态	VLAN 类型	VLAN 名称长度
ISL VLAN-id		MTU 大小	
802.10 索引			
VLAN 名称 (4 字节的倍数, 不足的位以 0 填充)			

图 4.7 子集通告的 Vlan 信息字段的格式

(3) 通告请求

在需要接收组播消息时用服务器发送。如果向相同 VTP 域中的 VTP 服务器发送请求通告时, VTP 服务器的响应方式是先发送总结通告, 接着发送所需数量的子集通告。当交换机重新启动后、VTP 域名变更后、交换机接到了配置修改编号比自己高的 VTP 汇总通告时会发出 VTP 请求通告。通告请求详见如图 4.8 所示。

通告请求			
版本	代码	Rsvd	管理域名长度
管理域名 (用零补足 32 个字节)			
起始值			

图 4.8 通告请求的格式

4.2.5 VTP 模式

根据交换机在 VTP 域中的作用不同, VTP 可以分为 3 种模式。这些模式的主要区别在于管理及通告 VTP 域和 Vlan 的方式的不同。

1. 服务器模式 (Server)

在 VTP 服务器上能创建、修改、删除 Vlan, 同时这些信息会通告给域中的其他交换机。也就是说, 服务器模式的交换机对 Vlan 的操作, 将影响整个 VTP 域。默认情况下, 交换机是服务器模式。每个 VTP 域必须至少有一台服务器, 域中的 VTP 服务器可以有多台。

服务器模式的交换机将对 Vlan 的操作保存到它的 NVRAM 中。它也监听网络中的 VTP 消息, 一旦有对于 Vlan 的新的改动发生 (即其他服务器模式的交换机所作的改动), 将同步该变化, 即更新自己所维护的 Vlan 信息, 同时转发表示该变化的 VTP 消息。

2. 客户端模式 (Client)

VTP 客户机上不允许创建、修改、删除 Vlan, 但它会监听来自其他交换机的 VTP 通告并更改自己的 Vlan 信息。接收到的 VTP 信息也会在 Trunk 链路上向其他交换机转发, 因此这种交换机还能充当 VTP 中继。当 VTP 客户端关机重启后, 其 Vlan 信息丢失, 将向 VTP 服务器发送请求通告, 来获得 Vlan 配置信息。

管理员可以将分散在网络中的无法集中管理的交换机改为客户端模式,以免有人恶意修改 Vlan 信息造成整个 VTP 域的 Vlan 信息混乱。

3. 透明模式 (Transparent)

这种模式的交换机不参与 VTP。管理员可以在这种模式的交换机上创建、修改、删除 Vlan,但是这些 Vlan 信息并不会通告给其他交换机,它也不接受其他交换机的 VTP 通告而更新自己的 Vlan 信息。然而需要注意的是,它会通过 Trunk 链路转发接收到的 VTP 通告从而充当了 VTP 中继的角色,因此完全可以把该交换机看成是透明的。

默认情况下,交换机处于 VTP 的服务器模式,且不传播 Vlan 信息,必须配置 VTP 域,用来跨 Trunk 链路传播 Vlan 信息。交换机间为了共享 Vlan 信息,VTP 的 Server 和 Client 必须处于同一个 VTP 域,且一个交换机只能属于一个 VTP 域中,另外 Catalyst 交换机必须是相邻的,所有的 Catalyst 交换机之间必须启用 Trunk 中继。

对这 3 种模式进行比较,如表 4.2 所示。

表 4.2 三种模式比较表

特性	服务器模式	客户端模式	透明模式
是否产生和监听 VTP 消息	是	是	否,本地 Vlan 配置不与 VTP 网络共享
是否建立 Vlan	是	否	是,但仅对本机有效
重新启动时是否保留全局 Vlan 配置	是,存储在 NVRAM	否,存储在 RAM	否,仅存储本地 Vlan 在 NVRAM

4.2.6 VTP 修剪

VTP 修剪是为了防止不必要的广播信息从一个 Vlan 泛洪(Flooded Traffic)到 VTP 域中所有的中继链路,如广播、多播、未知和泛洪的单播,从而提高网络带宽。VTP 修剪允许交换机协商将哪些 Vlan 分配到中继另一端的端口,修剪未分配到远程交换机端口的 Vlan。

默认 VTP 修剪功能被设置为禁用。只需要在域内一台设为 VTP 服务器的交换机上配置 VTP 修剪即可。在启用 VTP 修剪后,需要几秒才能生效。当一台远端交换机没有任何来自 Vlan 10 的可用设备,则 VTP 修剪可以阻止该交换机将 Vlan 10 的数据流发送到中继上,来防止带宽浪费。

VTP 修剪只修剪来自具有修剪资格的 Vlan 的数据通信。Vlan 10 没有修剪资格,因此 Vlan 1 的数据通信不能被修剪。

通过在全局配置模式,命令 vtp pruning 启用 VTP 修剪功能:

```
Switch(config)# vtp pruning
```

通过 show interfaces trunk 命令可以查看在中继上广播的 Vlan 信息,了解启用 VTP 修剪前后的不同,验证 VTP 修剪是否真正起作用。如图 4.9 所示,4 台交换机都启用 VTP,其中 S1 作为 VTP 服务器,启用 VTP 修剪。S2 和 S3 作为 VTP 客户端,在 S2 交换机上分配了 Vlan 10 和 Vlan 20,而在 S3 上未分配 Vlan 10,S3 不需要获得关于 Vlan 10 的任何消息。

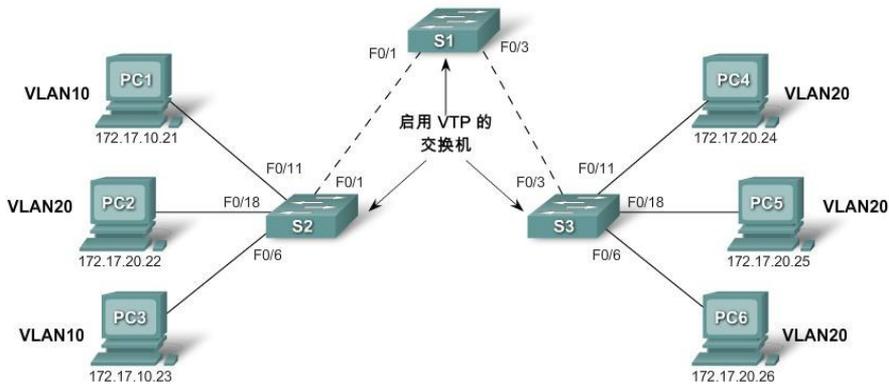


图 4.9 VTP 修剪

通过在特权模式,输入 show int trunk 命令,分别查看 S1、S2 和 S3 的信息如下。

1. 未启动 VTP 修剪

在 S1 上查看结果如下:

```
Switch# show int trunk
Port      Mode      Encapsulation  Status  Native vlan
Fa0/1    on        802.1q         trunking  1
Fa0/2    on        802.1q         trunking  1

Port      Vlans allowed on trunk
Fa0/1    1-1005
Fa0/2    1-1005

Port      Vlans allowed and active in management domain
Fa0/1    1,10,20
Fa0/2    1,10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,10,20
Fa0/2    1,10,20
```

在 S2 上查看结果如下:

```
Switch# show int trunk
Port      Mode      Encapsulation  Status  Native vlan
Fa0/1    on        802.1q         trunking  1

Port      Vlans allowed on trunk
Fa0/1    1-1005

Port      Vlans allowed and active in management domain
Fa0/1    1,10,20
```

```
Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         1,10,20
```

2. 启动 VTP 修剪

在 S2 上查看结果如下：

```
Switch# show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1

```
Port          Vlans allowed on trunk
```

```
Fa0/1         1-1005
```

```
Port          Vlans allowed and active in management domain
```

```
Fa0/1         1,10,20
```

```
Port          Vlans in spanning tree forwarding state and not pruned
```

```
Fa0/1         1, 20 //没有 10
```

因为 S3 没有 Vlan 10, Vlan 10 的流量不需要在这两个链路上传递。来自 PC1 的广播流量不应该进入 S1 和 S2 交换机的链路, 从上面输出信息可以看到 S2 已经从 f0/1 端口修剪掉了 Vlan 10 的信息, 所以在端口 f0/1 的中继链路上没有 Vlan 10 的流量。

注意: Packet Tracer 模拟器不能设置 VTP 修剪, 此部分不能在模拟器上进行练习。

4.3 配置 VTP

4.3.1 配置 VTP 域名

VTP 域名长度最多可达 32 个字符, 并且区分大小写。如果所配置的交换机是网络中的第一台交换机, 需要创建 VTP 域, 否则验证要加入到 VTP 域的名字。至少应该有一台交换机被设置为服务器模式。一台交换机不想与网络中的其他交换机共享 Vlan 信息, 则可以将它设置为透明模式。建议至少将两台核心交换机设置为 VTP 服务器模式, 而将其他交换机设置为 VTP 客户机模式。如果交换机掉电了, 它重启后可以从服务器处获得有效的 Vlan 信息。

在全局配置模式, 配置 VTP 域名的命令如下:

```
switch(config)# vtp domain test
```

其中 test 是设置的 VTP 域名。

4.3.2 配置 VTP 口令

如果不希望新交换机自动加入到 VTP 域中, 需要设置 VTP 口令。设置 VTP 口令后, 未正确设置 VTP 口令的新交换机就不能加入到已存在的 VTP 域中。为了使 VTP 域更安

全,VTP 域中每个交换机都需要配置域名和口令,并且同域中的域名和口令必须相同,只有这样 VTP 才能交互 Vlan 的配置信息。口令长度为 8~64 个字符。

在全局配置模式下,配置 VTP 口令的命令如下:

```
switch(config)# vtp password newpassword
```

其中 newpassword 是设置的 VTP 口令。

配置 VTP 口令之前,必须设置域名,否则执行上面命令配置 VTP 口令,将提示如下信息:

```
switch(config)# vtp passwordnewpassword
% The VTP password cannot be set for NULL domain
```

删除 VTP 域中的口令,恢复到缺省状态,命令如下:

```
switch(config)# no vtp password
```

4.3.3 配置 VTP 版本

在 VTP 域管理中,可以运行两种不同版本的 VTP,分别是 VTP 版本 1 和 VTP 版本 2。默认交换机 VTP 的版本是 VTP 版本 1。VTP 版本 1 和 VTP 版本 2 不能互操作。如果选择把 VTP 域中一台交换机配置成 VTP 版本 2,那么必须把该域中所有交换机都配置成 VTP 版本 2。

VTP 版本 2 增加了版本 1 所没有的以下主要功能:

(1)与版本相关的透明的模式:在 VTP 版本 1 中,一个 VTP 透明模式的交换机在用 VTP 转发信息给其他交换机时,先检查 VTP 版本号和域名是否与本机相匹配。匹配时,才转发该消息。VTP 版本 2 在转发信息时,不检查版本号和域名。

(2)令牌环支持:VTP 版本 2 支持令牌环交换和令牌环 Vlan,这是 VTP 版本 2 和版本 1 的最大区别。

在全局配置模式下,设置 VTP 版本 2 的命令如下:

```
switch(config)# vtp version 2
```

注意:一般不设置或修改 VTP 版本。

4.3.4 配置 VTP 模式

交换机 VTP 模式有 3 种,如果是 VTP 域中的第一台交换机,并且还需要添加其他交换机,那么设置该 VTP 运行模式为 Server 服务器。如果 VTP 域中还有其他交换机,设置交换机模式为 Client 客户端。如果某台交换机不会与网络中其他任何交换机共享 Vlan 信息,则将该交换机设置为 Transparent 透明模式。在透明模式,可以根据需要创建、删除和重命名 Vlan,而该交换机不会把这些改变传播给其他交换机。

在全局配置模式下配置 VTP 运行模式命令如下:

```
Switch(config)# vtp mode{client | server | transparent}
```

下面通过一个实例,演示说明配置 VTP 各种模式的过程和最终效果。实例拓扑图如图 4.10 所示,实例涉及设备 VTP 模式和创建 Vlan 信息如表 4.3 所示。最终通过合理的 VTP 模式配置,保证 Switch3 和 Switch4 能够获得来自 Switch1 的 Vlan 信息,而 Switch2 独立管理自己创建的 Vlan,Switch3 和 Switch4 获得不了 Vlan 50 信息。

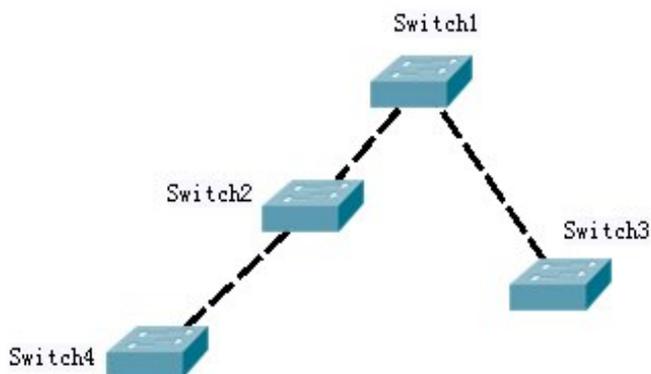


图 4.10 VTP 各种模式的应用的实例拓扑图

表 4.3

设备模式列表

设备	VTP 模式	创建 Vlan
Switch1	Server	Vlan 10 和 Vlan 20
Switch 2	Transparent	Vlan 50
Switch 3	Client	无
Switch 4	Client	无

这 4 台交换机已经是出厂配置,确保 VTP 修订号为 0。在配置 VTP 域之前,要确定使用版本 1 还是版本 2 的 VTP,本例使用的是版本 1。

1. 配置 VTP 服务器

在全局配置模式下配置 VTP 服务器如下:

```
Switch1(config)# vtp domain demo
```

```
Changing VTP domain name from NULL to demo
```

创建 VTP 域名为 demo,默认交换机已经是 VTP Server 模式,无需设置。

```
Switch1# show vtp status
```

```

VTP Version                :2
Configuration Revision      :0
Maximum Vlans supported locally :255
Number of existing Vlans   :5
VTP Operating Mode         :Server
VTP Domain Name            :demo
VTP Pruning Mode           :Disabled
VTP V2 Mode                :Disabled
VTP Traps Generation       :Disabled
MD5 digest                 :0x75 0x4A 0x67 0x29 0x54 0x7D 0x93 0xC4
Configuration last modified by0.0.0.0 at 0-0-00 00:00:00
Local updater ID is0.0.0.0 (no valid interface found)
  
```

进入互联端口模式,设置中继,然后在全局配置模式下,分别创建 Vlan 10 和 Vlan 20。

```
Switch1 (config) # vlan 10
```

```
Switch1 (config-vlan) # vlan 20
```

2. 配置 VTP 客户端

在全局配置模式下配置 VTP 客户端如下:

```
Switch3(config) # vtp mode client
```

```
Setting device to VTP CLIENT mode.
```

```
Switch3(config) # vtp domain demo
```

```
Changing VTP domain name from NULL to demo
```

```
Switch3 # show vtp status
```

```
VTP Version :                2
Configuration Revision       :0
Maximum Vlans supported locally :255
Number of existing Vlans     :5
VTP Operating Mode           :Client
VTP Domain Name              :demo
VTP Pruning Mode             :Disabled
VTP V2 Mode                  :Disabled
VTP Traps Generation         :Disabled
MD5 digest :0x75 0x4A 0x67 0x29 0x54 0x7D 0x83 0xC4
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Switch4 和 Switch3 配置 VTP 部分一样,不再重复。Switch4 进入互联端口模式,设置中继,以便传递 Vlan 消息。

注意:在这两台交换机上未创建 Vlan。

3. 配置 VTP 透明模式

在全局配置模式下配置 VTP 透明模式如下:

```
Switch2(config) # vtp mode transparent
```

```
Switch2(config) # vtp domain demo
```

```
Switch2 # show vtp status
```

```
VTP Version :                2
Configuration Revision       :0
Maximum Vlans supported locally :255
Number of existing Vlans     :7
VTP Operating Mode           :Transparent
VTP Domain Name              :test
VTP Pruning Mode             :Disabled
VTP V2 Mode                  :Disabled
VTP Traps Generation         :Disabled
MD5 digest                   :0x3A 0x12 0xDB 0x8C 0x44 0x8D 0x80 0xB9
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:49
```

在全局配置模式下,创建 Vlan 50。

```
Switch2(config)#vlan 50
```

4. 查看 VTP 信息

配置完毕后,验证各种 VTP 运行模式配置是否合理,能否达到预期效果。

```
Switch1#show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/2	on	802.1q	trunking	1

```
Port Vlans allowed on trunk
```

Fa0/1	1-1005
Fa0/2	1-1005

```
Port Vlans allowed and active in management domain
```

Fa0/1	1,10,20
Fa0/2	1,10,20

```
Port Vlans in spanning tree forwarding state and not pruned
```

Fa0/1	1,10,20
Fa0/2	1,10,20

```
Switch2#sh int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	auto	n-802.1q	trunking	1
Fa0/2	auto	n-802.1q	trunking	1

```
Port Vlans allowed on trunk
```

Fa0/1	1-1005
Fa0/2	1-1005

```
Port Vlans allowed and active in management domain
```

Fa0/1	1,10,20,50
Fa0/2	1,10,20,50

```
Port Vlans in spanning tree forwarding state and not pruned
```

Fa0/1	1,10,20,50
Fa0/2	1,10,20,50

说明:Switch2 设置透明模式,自己创建 Vlan 50,允许 Switch1 创建的 Vlan 10 和 20 通过中继,以便 Switch4 能获得来自 Switch1 的 Vlan 信息。

```
Switch4#show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1

```

Port          Vlans allowed on trunk
Fa0/1         1-1005

Port          Vlans allowed and active in management domain
Fa0/1         1,10,20

Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         1,10,20
Switch3# show int trunk
Port          Mode          Encapsulation  Status      Native vlan
Fa0/1         on            802.1q         trunking    1

Port          Vlans allowed on trunk
Fa0/1         1-1005

Port          Vlans allowed and active in management domain
Fa0/1         1,10,20

Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         1,10,20

```

说明: Switch3 和 Switch4 的中继都没有 Switch2 自己创建的 Vlan 50 信息,达到了预期效果。

4.4 排查 VTP 配置故障

4.4.1 VTP 配置的注意事项

配置 VTP 需要注意一些事项,这样可以减少 VTP 配置过程中的错误发生。

1. 配置 VTP 服务器

配置 VTP 之前,首先确认将要配置的所有交换机都已设置为默认设置。方法是通过 show vtp status 查看 VTP Operating Mode 为 Server,VTP Domain Name 为空。

在将配置过的交换机添加到 VTP 域之前,务必重置配置修订版本号。如果不重置配置修订版本号可能导致 VTP 域中其余交换机上的 Vlan 配置损坏。

如果已经有 VTP 域,请确保名称精确匹配。VTP 域名区分大小写。

如果要配置 VTP 口令,请确保对域内需要交换 VTP 信息的所有的交换机上设置相同的口令。没有口令或口令错误的交换机将拒绝 VTP 通告。

请确保所有的交换机都配置为使用相同的 VTP 协议版本。VTP 第 1 版与第 2 版并不兼容。默认情况下,Cisco Catalyst 交换机运行第 1 版,但它能够运行第 2 版。当 VTP 版本设置为第 2 版时,域中所有能够运行第 2 版的交换机都会通过 VTP 通告过程自动配置为使

用第2版。此后,所有仅支持第1版的交换机将不能加入 VTP 域。

在 VTP 服务器上启用 VTP 之后,再创建 Vlan。在启用 VTP 之前创建的 Vlan 会被删除。务必确保为域中互连的交换机配置了中继端口。VTP 信息仅可通过中继端口交换。

2. 配置 VTP 客户端

与 VTP 服务器交换机一样,请确认所有交换机都已恢复到默认设置。

配置 VTP 客户端模式:注意,交换机默认不是 VTP 客户端模式,必须配置该模式。

配置中继:VTP 通告通过中继链路工作。

连接到 VTP 服务器:连接到 VTP 服务器或另一台启用 VTP 的交换机时,与 VTP 服务器之间来回传输通告的过程需要消耗一段时间。

检验 VTP 状态:在开始配置接入端口之前,请先确认已更新了修订版模式和 Vlan 数量。

配置接入端口:当交换机处于 VTP 客户端模式时,不能添加新的 Vlan。仅可将接入端口指定到现有 Vlan。

4.4.2 VTP 配置排错

常见的 VTP 配置错误有以下几方面:

(1)VTP 版本不一致。VTP 版本 1 和版本 2 不兼容。通过 show vtp status 命令可以查看当前 VTP 版本是否保持一致。

(2)VTP 密码问题。如果配置了 VTP 密码,那么必须确保在同一个 VTP 域中,所有 VTP Server 和 VTP Client 的交换机配置 VTP 密码都相同。

(3)VTP 域名问题。确保在同一个 VTP 域中,所有 VTP Server 和 VTP Client 的交换机配置 VTP 域名都相同,域名是区分大小写的。通过 show vtp status 命令可以查看 VTP 域名情况。

(4)VTP 模式配置问题。确保在 VTP 域中至少有一台设置为 VTP Server 的交换机。

(5)VTP 修正号问题。确保新加入到 VTP 域中的交换机配置已经恢复到出厂配置,即修正号变成 0 以后,再加入到 VTP 域中。

4.5 项目实施

按照项目需求以及设计过程,具体项目实施如下:

步骤 1. 因为这两台交换机使用的都是默认出厂配置,这里可以省略该步骤。如果是工程中使用过的交换机,需要执行如下操作,然后重新启动交换机。

```
Switch>en
Switch# erase startup-config //删除启动配置文件
Switch# delete Vlan.dat //删除 Vlan 配置文件
```

步骤 2.

```
Switch1>en
Switch1 # conf t
Switch1(config)# vtp domain test //设置 VTP 域,域名为 test
Changing VTP domain name from NULL to test
```

步骤 3.

```
Switch1(config)# int f0/20
Switch1(config-if)# switchport mode trunk
```

步骤 4.

```
Switch2>en
Switch2 # conf t
Switch2(config)# vtp domain test
Changing VTP domain name from NULL to test
Switch2(config)# vtp mode client //从默认 server 模式改为 client 模式
Setting device to VTP CLIENT mode.
```

步骤 5.

```
Switch2(config)# int f0/20
Switch2(config-if)# switchport mode trunk
```

步骤 6.

```
Switch1 (config)# vlan 10
Switch1 (config-vlan)# vlan 20 //分别创建 Vlan 10 和 Vlan 20
```

步骤 7.

```
Switch1 (config)# int f0/1
Switch1 (config-if)# switchport access vlan 10
Switch1 (config-if)# int f0/5
Switch1 (config-if)# switchport access vlan 20
Switch1 (config-if)# end
```

步骤 8.

```
Switch2 (config)# int f0/1
Switch2 (config-if)# switchport access vlan 10
Switch2 (config-if)# int f0/5
Switch2 (config-if)# switchport access vlan 20
Switch2 (config-if)# end
```

步骤 9.

```
Switch1 # show vtp status
VTP Version                :2
Configuration Revision     :8
Maximum Vlans supported locally :255
Number of existing Vlans   :7
VTP Operating Mode        :Server
VTP Domain Name           :test
```

```
VTP Pruning Mode :Disabled
VTP V2 Mode :Disabled
VTP Traps Generation :Disabled
MD5 digest :0x93 0xEA 0xC7 0x4F 0xCD 0x5F 0xB5 0xEE
```

Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Local updater ID is 192.168.1.1 on interface V110 (lowest numbered Vlan interface found)

Switch1 上查看 VTP 状态信息,说明 Switch1 当前是 Server 运行模式,域名为 test。

```
Switch1 # show vlan
```

Vlan Name	Status	Ports
1 default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/24, Gig0/1, Gig0/2
10 10	active	Fa0/1
20 20	active	Fa0/5
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Switch1 上查看 Vlan 信息,说明 Switch1 当前分配 f0/1 端口到 Vlan 10,分配 f0/5 端口到 Vlan 20。

```
Switch1 # show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1

```
Port Vlans allowed on trunk
```

```
Fa0/20 1-1005
```

```
Port Vlans allowed and active in management domain
```

```
Fa0/20 1,10,20
```

```
Port Vlans in spanning tree forwarding state and not pruned
```

```
Fa0/20 1,10,20
```

Switch1 上查看中继信息,说明 Switch1 当前 f0/20 端口配置中继模式,允许管理域的 Vlan 有 1、10 和 20。

```
Switch2 # show vtp status
```

```
VTP Version :2
```

```
Configuration Revision :8
```

```

Maximum VLANs supported locally :255
Number of existing VLANs :7
VTP Operating Mode :Client
VTP Domain Name :test
VTP Pruning Mode :Disabled
VTP V2 Mode :Disabled
VTP Traps Generation :Disabled
MD5 digest :0x93 0xEA 0xC7 0x4F 0xCD 0x5F 0xB5 0xEE
Configuration last modified by0.0.0.0 at 3-1-93 00:00:00

```

Switch2 上查看 VTP 状态信息,说明 Switch2 当前是 Client 运行模式,域名为 test。

```
Switch2# show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/24, Gig0/1, Gig0/2
10 10	active	Fa0/1
20 20	active	Fa0/5
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Switch2 上查看 Vlan 信息,说明 Switch2 未创建 Vlan,是从 Switch1 获得 Vlan 信息。
当前分配 f0/1 端口到 Vlan 10,分配 f0/5 端口到 Vlan 20。

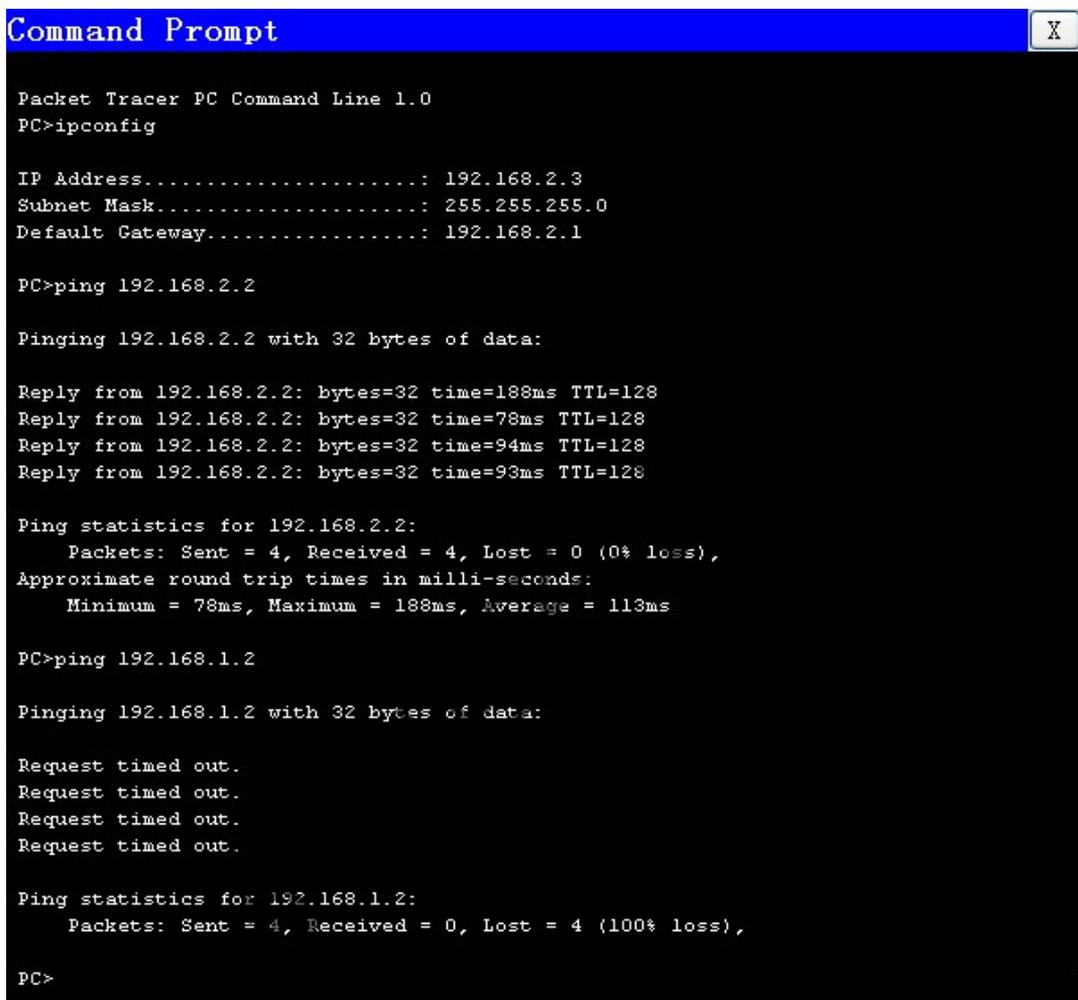
```
Switch2# show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa0/20	1-1005			
Port	Vlans allowed and active in management domain			
Fa0/20	1,10,20			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa0/20	1,10,20			

Switch2 上查看中继信息,说明 Switch2 当前 f0/20 端口配置中继模式,允许管理域的 Vlan 有 1、10 和 20。

步骤 10. 配置完成后,在技术部的 PC4 主机访问技术部的 PC2 主机,如图 4.11 所示,

PC4 主机可以 ping 通 PC2 主机,说明配置成功,Vlan 内部 PC 虽然不在一个交换机上,也能互相访问。再通过技术部的 PC4 主机访问市场部的 PC1 主机,如图 4.11 所示,无法访问,请求超时(Request Timeout)。说明配置成功,不同 Vlan 的 PC 拒绝访问,市场部主机不能访问技术部主机。



```
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig

IP Address.....: 192.168.2.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.1

PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=188ms TTL=128
Reply from 192.168.2.2: bytes=32 time=78ms TTL=128
Reply from 192.168.2.2: bytes=32 time=94ms TTL=128
Reply from 192.168.2.2: bytes=32 time=93ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 78ms, Maximum = 188ms, Average = 113ms

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

图 4.11 PC 间互访验证

4.6 本章小结

VTP 是一种消息协议,用于在 VTP 域内同步 Vlan 信息,而不必在每个交换上配置相同的 Vlan 信息,从而实现 Vlan 配置的一致性。本章首先通过 VTP 项目引出本章的主要项目,通过项目知识点的分解,逐步了解 VTP 的基本概念、工作原理,VTP 域、运行模式及配置方法,然后重点介绍应用 VTP 配置 Vlan。

4.7 实践环节设计

实验练习 1

在如图 4.12 所示的网络拓扑图中,三层交换机 Swtich1 设置为 VTP 服务器,二层交换机 Swtich2 设置为 VTP 客户端,通过 Swtich1 管理和创建 Vlan。根据如下要求,进行配置,列出详细配置过程,并验证最终效果。

(1)将 IP 地址设置为 192.168.1.0/24 网段的 PC 机划入 Vlan 10 中,将 IP 地址设置为 192.168.2.0/24 网段的 PC 机划入 Vlan 20 中,保证 Vlan 内部 PC 机可以互访,但两个 Vlan 之间 PC 机不能互访。

(2)因为业务有变动,需要保证不同 Vlan 间可以互访,在三层交换机 Swtich1 上设置路由,保证不同 Vlan 间可以互访。

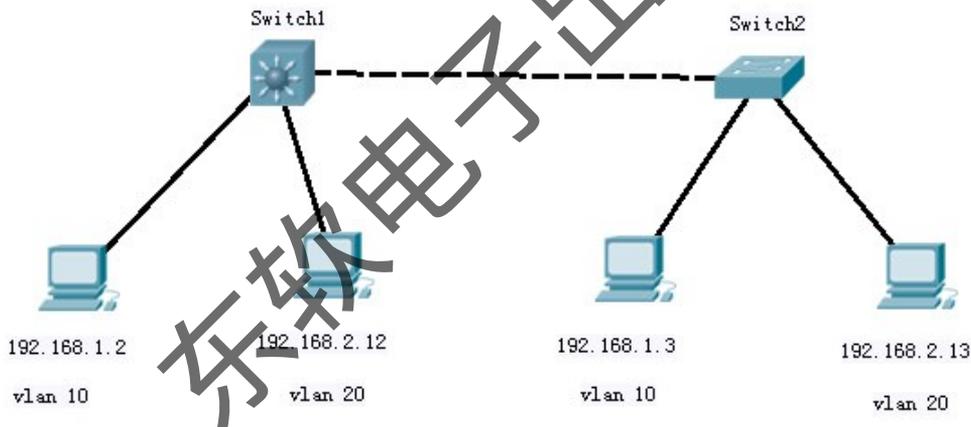


图 4.12 练习 1 网络拓扑图

实验练习 2

在如图 4.13 所示的网络拓扑图中,根据如下要求,配置适当 VTP 和划分 Vlan。请列出详细配置过程,并验证最终效果。

实验要求:Swtich1 设置为 VTP 服务器,Swtich2 设置为 VTP 透明模式,Swtich3 和 Swtich4 设置为客户端,根据图示将各 PC 机划分到对应 Vlan 中,各 PC 机 IP 地址根据情况设置,保证最终 Vlan 内部 PC 机可以互访,但各 Vlan 之间 PC 机不能互访。

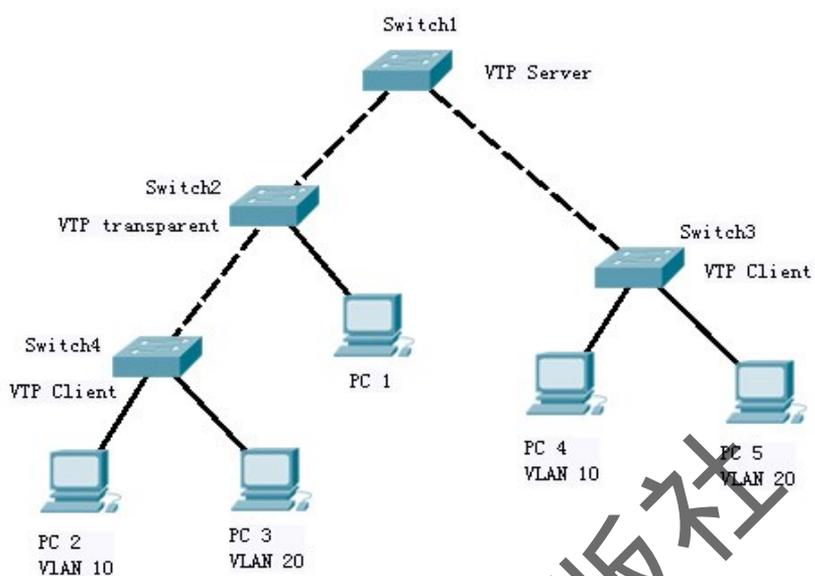


图 4.13 练习 2 网络拓扑图

东软电子出版社