交换机实验篇

第一章 交换机基本配置实验

1.1 实验背景知识

1.1.1 以太网交换机

以太网（Ethernet）由 Xerox 公司 PARC 研究中心于 1973 年首次提出，属于共享介质类型，这种网络对于介质的访问基于 CSMA/CD 算法，端口共享带宽。随着技术不断发展而产生的交换式以太网，与最早期的以太网有所区别，其中最大的不同是各个端口独享带宽。由于交换机内部转发数据帧的背板带宽远大于端口带宽，因此数据帧处于并行状态，效率较高，可以满足网络环境中大量数据并行处理的要求。交换式以太网的主要设备是以太网交换机。与其它计算机设备类似，以太网交换机是由软、硬件 2 部分构成的。它的硬件结构包括业务接口、主板、主处理器、内存、FLASH 和电源系统等，软件结构包括 BootRom 引导、初始化程序和 VRP 操作系统平台。衡量以太网交换机性能的指标包括它的系统特性，如可扩展接口模块种类、网线类型、输入电压、功耗、工作环境等；还有它的业务特性，如二层转发能力、交换模式、VLAN、组播技术、生成树协议、端口汇聚、MAC 地址表、服务质量（QoS）等。按照交换机的性能和工作性质可以把它划分为核心交换机、汇聚交换机、接入交换机等，但这种分类方式并不严格。

以太网交换机内部都有一张 MAC 地址表，当数据帧到来时，交换机过分析数据帧的头信息（其中包含了源 MAC 地址、目标 MAC 地址、信息长度等），取得目标 MAC 地址后，查找交换机中存储的地址对照表（MAC 地址对应的端口），确认具有此 MAC 地址的网卡连接在哪个端口上，然后仅将数据帧发送到对应端口。最初交换机的 MAC 地址表为空，MAC 地址表没有记录，数据帧到达后从其它所有端口转发出去，交换机通过识别数据帧的源 MAC 地址，学习 MAC 地址和端口对应关系，经过一段时间的学习，建立了完整的 MAC 地址和端口对应关系的 MAC 表之后，就可以通过 MAC 地址表实现数据帧的单点转发。

1.1.2 SNMP 简介

目前网络中用得最广泛的网络管理协议是 SNMP（Simple Network Management Protocol）。SNMP 是被广泛接受并投入使用的工业标准，用于保证管理信息在任意两点间传送，便于网络管理员在网络上的任何节点检索信息、修改信息、寻找故障、完成故障诊断、进行容量规划和生成报告。SNMP 的实现基于无连接的传输层协议 UDP。SNMP 分为 NMS 和 Agent 两部分，NMS（Network Management Station），是运行客户端程序的工作站，目前常用的网管平台有 Sun NetManager 和 IBM NetView；Agent 是运行在网络设备上的服务器端软件。NMS 可以向 Agent 发出 GetRequest、GetNextRequest 和 SetRequest 报文，Agent 接收到 NMS 的请求报文后，根据报文类型进行 Read 或 Write 操作，生成 Response 报文，并将报文返回给 NMS。Agent 在设备发生重新启动等异常情况时，也会主动向 NMS 发送 Trap 报文，向 NMS 汇报所发生的事件。

1.2 实验目的

本章节共 5 个实验内容，包括交换机的 Console 配置、Telnet 配置、SNMP 配置、Web 配置和常用命令练习。通过本章节实验，能够熟练掌握交换机的 Console 配置方法，对其它几种交换机配置方法有所了解，并能够掌握一些常用配置命令，为后面的实验打下基础。

1.3 实验内容

1.3.1 Console 配置

1、软硬件要求：交换机 1 台，计算机 1 台，Console 线 1 根，网线若干。
2、网络拓扑图：

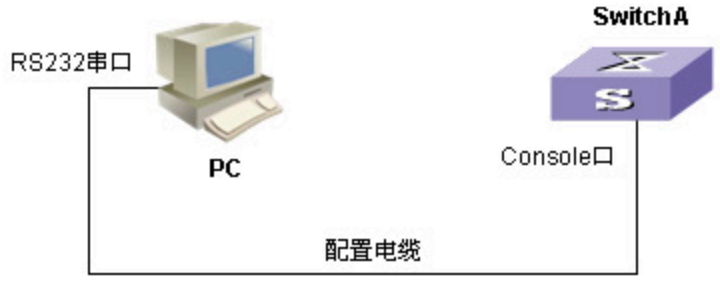

图 1-1 交换机 Console 配置连线

3、连线

第一次安装使用交换机时，只能通过配置口（Console）进行配置。

首先，关闭计算机和交换机的电源，将配置电缆的 DB-9（或 DB-25）孔式插头接到要对交换机进行配置的计算机的串口上。然后，将配置电缆的 RJ-45 一端连到交换机的配置口（Console）上。

4、设置超级终端参数

在计算机上运行 Windows 的终端仿真程序——超级终端。然后设置终端参数。

超级终端参数设置方法如下：在串口的属性对话框中设置波特率为 9600，数据位为 8，奇偶校验为无，停止位为 1，流量控制为无。单击[确定]按钮。这些参数与交换机的初始设定是一致的，如果在操作中改变了交换机的参数，那么超级终端的参数也要作相应的改变，以使电缆两端的参数保持一致才能通信。

图 1-2 COM 口参数设置

5、交换机上电

确认交换机与配置终端的连接正确，确认已经完成配置终端参数的设置后，即可对交换机上电。通电后交换机上出现自检内容。

```
          ********************************************************************
          *          Quidway S3928P EI BOOTROM, Version 223                  *
          *                                                                  *
          ********************************************************************

          Copyright(C) 2003 2005, Hangzhou Huawei 3Com Tech. Co., Ltd.

          All rights reserved.
          Creation date    : Sep 14 2005, 21:02:57
          Mac Address      : 000fe212dcbe

Press Ctrl B to enter Boot Menu... 0
Auto booting...
Decompress Image.....................................................................

.....................................................................................

.....................................................................................
.....................................................................................

.....................................................................................
..OK!
```

图 1-3 交换机自检

当交换机提示“Please Press ENTER”，敲完回车后请等待一下，设备需要一定的时间才能进入到命令行界面。

界面如下：

```
Press ENTER to get started.
<Quidway>
%Apr  1 23:57:31:849 2000 Quidway SHELL/5/LOGIN:- 1 - Console(aux0) in unit1 log
in
<Quidway>
```

图 1-4 进入命令行界面

6、交换机命令验证

命令验证内容参考本章 1.3.5 小节内容。

1.3.2 Telnet 配置

1、软硬件要求：交换机 1 台，计算机 1 台，Console 线 1 根，网线若干。

2、网络拓扑图：

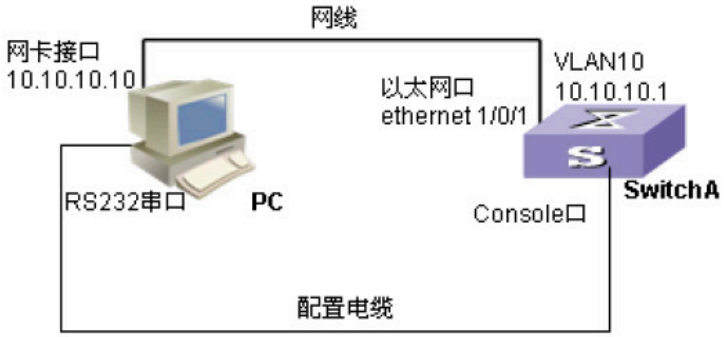

图 1-5 Telnet 配置实验

3、说明

通过 Telnet，用户可以远程管理和配置交换机。但在使用 Telnet 之前，必须通过 Console 口对交换机的 Telnet 功能进行初始配置。需要通过 Console 口在交换机上配置欲登录的 Telnet 用户名和认证口令，然后配置以太网交换机一个 VLAN 接口的 IP 地址，并指定与终端相连的以太网端口属于该 VLAN，这时就可以利用 Telnet 登录到以太网交换机，然后对以太网交换机进行配置。关于 VLAN 的知识和详细配置方法，会在后面章节讲到，这里只要了解 VLAN 在本次实验中所用到的配置命令即可。

4、连线和设置终端参数

关闭计算机和交换机的电源，按照图 1-5 连接网线和 Console 线。按照 Console 实验的内容设置超级终端参数。SwitchA 为三层交换机，设置 vlan10 地址 10.10.10.1/8，交换机 SwitchA 通过以太网口 ethernet 1/0/1 和 PC 机实现互连。

5、在 SwitchA 上配置 Telnet

命令如下：

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname SwitchA

[SwitchA] user-interface vty 0
//进入用户界面视图 (s2100 交换机无此虚接口)
[SwitchA -ui-vty0] set authentication password simple NWPU
//设置的 Telnet 用户登录口令为 NWPU。
[SwitchA -ui-vty0] user privilege level 3
```

//将用户的权限设置为 3，这样用户可以进入系统视图进行操作，否则只有 0 级的权限。

[SwitchA -ui-vty0] quit

6、在 SwitchA 上配置 VLAN

[SwitchA]vlan 10

//创建（进入）vlan10

[SwitchA-vlan10] port Ethernet 1/0/1

//将端口 Ethernet 1/0/1 加入到 vlan10 里

[SwitchA] interface Vlan-interface 10

//创建 vlan10 的虚接口

[SwitchA-Vlan-interface10] ip address 10.10.10.1 255.0.0.0

//给 vlan10 的虚接口配置 IP 地址

7、Telnet 登录

PC 机设定 IP 地址 10.10.10.10/8，在 PC 机上运行 Telnet 程序，输入与 PC 机相连的以太网口所属 VLAN 的虚接口 IP 地址 10.10.10.1，如图 1-6 所示。

图 1-6 运行 Telnet 程序

终端上显示如图 1-7，按照提示输入已设置的登录口令，口令区分大小写且不显示。口令输入正确后则出现命令行提示符（如<SwitchA>）。

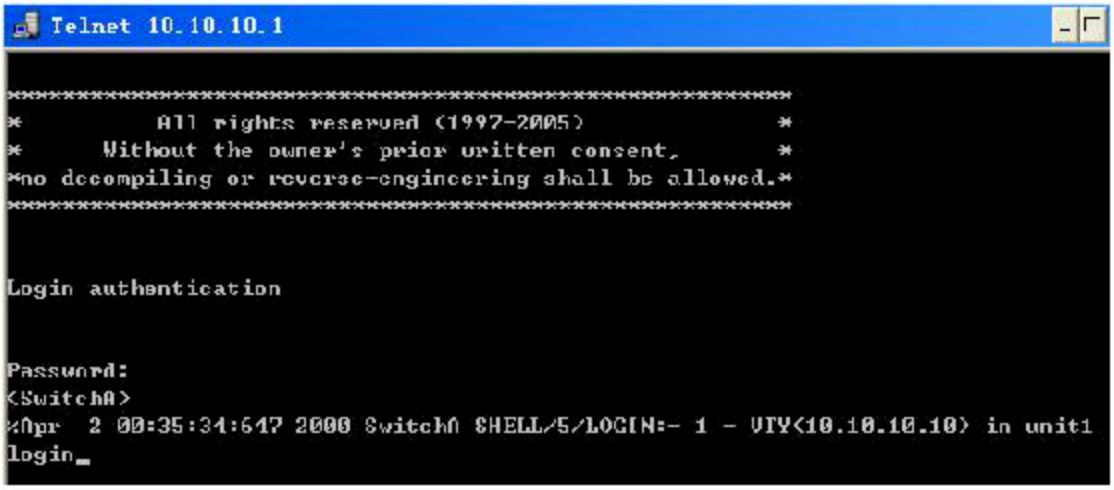

图 1-7 Telnet 登录

8、交换机命令验证

命令验证内容参考本章 1.3.5 小节内容。

1.3.3 SNMP 配置

1、软硬件要求：交换机 1 台，计算机 1 台，Console 线 1 根，网线若干。
2、网络拓扑图：

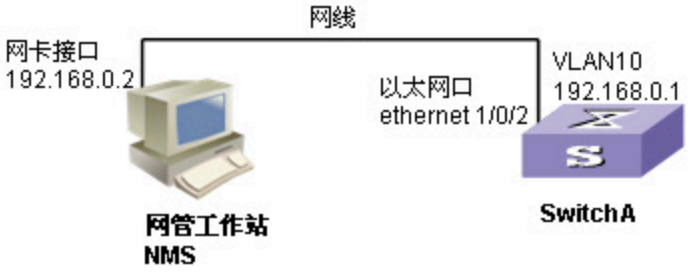

图 1-8 SNMP 配置实验

3、连线

按照图 1-8 连线。要在 PC 机上安装网管系统作为网管工作站（NMS），与以太网交换机通过以太网相连，网管工作站 IP 地址是 192.168.0.2，以太网交换机的 VLAN 虚接口的 IP 地址是 192.168.0.1。

4、配置步骤

<Quidway> system-view
// 进入系统视图
[Quidway] sysname SwitchA
//设置名称为 SwitchA

[SwitchA] vlan 10
//创建（进入）vlan10
[SwitchA-vlan10] port ethernet 1/0/2
//用于网管的端口 Ethernet1/0/2 加入到 vlan10
[SwitchA-vlan10] interface vlan 10
//创建（进入）vlan10 的虚接口
[SwitchA-Vlan-interface10] ip address 192.168.0.1 255.255.255.0
//给 vlan10 的虚接口配置 IP 地址
[SwitchA-Vlan-interface10]quit

[SwitchA] snmp-agent sys-info version all
[SwitchA] snmp-agent community write public
//设置团体名和访问权限
[SwitchA] snmp-agent mib include internet 1.3.6.1
[SwitchA] snmp-agent group v3 managev3group write internet
[SwitchA] snmp-agent usm v3 managev3user managev3group
[SwitchA] snmp-agent trap enable standard authentication
[SwitchA] snmp-agent trap enable standard coldstart
[SwitchA] snmp-agent trap enable standard linkup
[SwitchA] snmp-agent trap enable standard linkdown
//允许交换机发送 Trap 信息

[SwitchA] snmp-agent target-host trap address udp-domain 192.168.0.2 udp-port 5000 params securityname public

//允许向网管工作站（NMS）192.168.0.2 发送 Trap 报文，使用的团体名为 public

5、测试验证

网管所在的 PC 机需要进行登录设置。对于 Mib-Browser，登陆设置为：SNMPV1、V2 使用缺省的团体名 public 登录，SNMPV3 使用用户 managev3user 登陆。PC 能够 Ping 通交换机管理地址，以太网交换机支持 iManager Quidview 网管系统，常用的网管系统还有 Sun NetManager 和 IBM NetView 等，用户可利用网管系统完成对以太网交换机的查询和配置操作。

1.3.4 通过 Web 配置交换机

1、软硬件要求：交换机 1 台，计算机 1 台，Console 线 1 根，网线若干。

2、网络拓扑图：

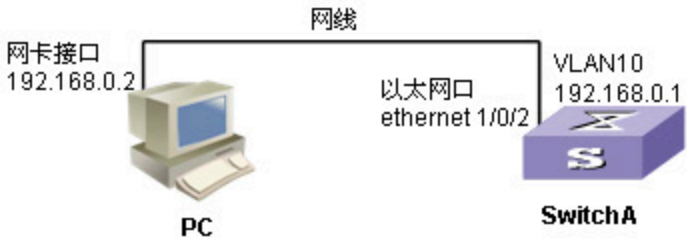

图 1-9 Web 配置实验

3、连线

按照图 1-9 连线。

4、配置命令

<Quidway> system-view

//进入系统视图

[Quidway] sysname SwitchA

//设置名称为 SwitchA

[SwitchA]vlan 10

//创建（进入）vlan10

[SwitchA-vlan10]port Ethernet 1/0/2

//将 E1/0/2 加入到 vlan10

[SwitchA-vlan10] interface Vlan-interface 10

//创建（进入）vlan10 的虚接口

[SwitchA-Vlan-interface10]ip address 192.168.0.1 255.255.255.0

//给 vlan10 的虚接口配置 IP 地址

[SwitchA-Vlan-interface10]quit

[SwitchA]snmp-agent sys-info version v3

//启动 Snmp Agent 的 V3 版本

[SwitchA]snmp-agent mib-view included wnmview internet

//创建一个范围为 internet 的 Snmp 视图

[SwitchA]snmp-agent group v3 wnmgroup authentication read-view wnmview write-view wnmview notify-view wnmview

//创建一个需要进行认证的 Snmp V3 的组 wnmgroup，读写和接受 Trap 的视图都使用 wnmview

[SwitchA]snmp-agent usm-user v3 wnm wnmgroup authentication-mode md5 123456

//创建一个 Snmp V3 的用户，用户名是 wnm，认证密码是 123456，采用 MD5 方式认证，不进行加密

[SwitchA]snmp-agent target-host trap address udp-domain 192.168.0.2 params securityname wnm v2c

//设置 Trap 主机地址是 192.168.0.2，接收 Trap 的用户名为 wnm，采用 TrapV2c 格式送 Trap

[SwitchA]snmp-agent trap enable standard

//激活标准 Trap

5、测试验证

交换机如果需要支持 Web 网管功能，在 FLASH 里需要加载 Web 网管的相关文件。PC 机和交换机的 IP 地址要设在同一个网段，PC 机上需要安装 JRE1.3 以上的版本。完成上述配置以后，在 PC 机打开浏览器，在地址栏输入交换机的 IP 地址，将在显示的页面中点击“图形管理界面”，就进入图形界面的 Web 网管。首先会弹出对话框，用户名输入 wnm，认证方式选择 MD5，加密方式选择空，认证密码输入 123456，点击确定。后面就可以根据菜单和对话框的提示通过 Web 网管对交换机进行查询和配置了。

1.3.5 命令行视图与常用命令

Quidway 系列以太网交换机向用户提供一系列配置命令以及命令行接口，方便用户配置和管理以太网交换机。交换机的命令行采用分级保护方式，防止未授权用户的非法侵入。命令行划分为参观级、监控级、系统级、管理级 4 个级别，同时对登录用户也划分为 4 个级别，分别与命令级别相对应，即不同级别的用户登录后，只能使用等于或低于自己级别的命令。各命令行视图是针对不同的配置要求实现的，它们之间有联系又有区别，比如，与以太网交换机建立连接即进入用户视图，它只完成查看运行状态和统计信息的简单功能，再键入 **system-view** 进入系统视图，在系统视图下，可以键入不同的命令进入相应的视图。在系统视图下，全部命令被分组，每组对应一个视图，可以用命令在不同的视图之间切换。一般情况下，在某个视图下只能执行限定的命令，但对一些常用命令（如 ping、display current-configuration、interface 等）在各种视图下均可执行。

命令行提供的视图很多，常用的命令视图的功能特性、进入各视图的命令等细则如下表所示：

视图	功能	提示符	进入命令	退出命令
用户视图	查看交换机的简单运行状态和统计信息	<Quidway>	与交换机建立连接即进入	quit 断开与交换机连接
系统视图	配置系统参数	[Quidway]	在用户视图下键入 system-view	quit 或 return 返回用户视图

视图	功能	提示符	进入命令	退出命令
以太网端口视图	配置以太网端口参数	[Quidway-Ethernet1/0/1]	百兆以太网端口视图 在系统视图下键入 interface ethernet 1/0/1	quit 返回系统视图 return 返回用户视图
		[Quidway-GigabitEthernet1/1/1]	千兆以太网端口视图 在系统视图下键入：interface gigabitethernet 1/1/1	
VLAN 视图	配置 VLAN 参数	[Quidway-Vlan10]	在系统视图下键入 vlan 10	quit 返回系统视图 return 返回用户视图
VLAN 接口视图	配置 VLAN 接口参数	[Quidway-Vlan-interface10]	在系统视图下键入 interface vlan-interface 10	quit 返回系统视图 return 返回用户视图
本地用户视图	配置本地用户参数	[Quidway-luser-user1]	在系统视图下键入 local-user user1	quit 返回系统视图 return 返回用户视图
用户界面视图	配置用户界面参数	[Quidway-ui0]	在系统视图下键入 user-interface 0	quit 返回系统视图 return 返回用户视图

表 1-1 常用的命令视图

在任一视图下，键入"?"获取该视图下所有命令及其简单描述。键入一命令，后接以空格分隔的"?"键，如果该位置为关键字，则列出全部关键字及其简单描述；如果该位置为参数，则列出有关的参数描述。键入一字符串，其后紧接"?"，列出以该字符串开头的所有命令。键入一命令，后接一字符串紧接"?"键，列出该命令以该字符串开头的所有关键字。

命令行接口可以将用户键入的历史命令自动保存，用户可以随时调用命令行接口保存的历史命令，并重复执行。命令行接口为每个用户缺省保存 10 条历史命令。操作如下表所示。

操作	按键或命令	结果
显示历史命令	display history-command	显示用户输入的历史命令
访问上一条历史命令	上光标键↑或<Ctrl+P>	如果还有更早的历史命令，则取出上一条历史命令
访问下一条历史命令	下光标键↓或<Ctrl+N>	如果还有更晚的历史命令，则取出下一条历史命令

表 1-2 访问历史命令

所有用户键入的命令，如果通过语法检查，则正确执行，否则向用户报告错误信息，常

见错误信息参见下表。

英文错误信息	错误原因
Unrecognized command	没有查找到命令
	没有查找到关键字
	参数类型错误
	参数值越界
Incomplete command	输入命令不完整
Too many parameters	输入参数太多
Ambiguous command	输入参数不明确

表 1-3 命令行常见错误信息表

下面列出一些常用命令供大家测试，执行时注意命令所在的视图，如果在当前视图下不能执行，输入“？”后回车，会显示更多的命令。

命令	功能
display	显示
undo	删除/取消
local-user	新建用户
quit	返回上级视图
sysname	设置交换机系统名称
undo sysname	恢复交换机系统名的缺省值
reboot	复位以太网交换机
reset saved-configuration	擦除以太网交换机配置文件
disp version	显示版本
disp current-configuration	显示当前配置
disp saved-configuration	显示已保存的配置

表 1-4 部分常用命令

1.4 思考题

（1）写出交换机前面板上端口的类型以及作用。

（2）写出配置的交换机以太网端口的速率、工作模式和其他参数设置。

（3）交换机命令视图有哪些类型？各有什么限制？

第二章 交换机端口实验

2.1 实验背景知识

2.1.1 端口分类

交换机的以太网端口有三种链路类型：Access、Hybrid 和 Trunk。Access 类型的端口只能属于 1 个 VLAN，一般用于连接计算机的端口；Trunk 类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，一般用于交换机之间连接的端口；Hybrid 类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。Hybrid 端口和 Trunk 端口的不同之处在于 Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签。

缺省情况下，端口为 Access 端口。Access 端口只属于 1 个 VLAN，所以它的缺省 VLAN 就是它所在的 VLAN，不用设置；Hybrid 端口和 Trunk 端口属于多个 VLAN，所以需要设置缺省 VLAN ID。如果设置了端口的缺省 VLAN ID，当端口接收到不带 VLAN Tag 的报文后，则将报文转发到属于缺省 VLAN 的端口；当端口发送带有 VLAN Tag 的报文时，如果该报文的 VLAN ID 与端口缺省的 VLAN ID 相同，则系统将去掉报文的 VLAN Tag，然后再发送该报文。本 Trunk 端口的缺省 VLAN ID 和相连的对端交换机的 Trunk 端口的缺省 VLAN ID 必须一致，否则报文将不能正确传输。缺省情况下，Trunk 端口的缺省 VLAN 为 VLAN 1，Access 端口的缺省 VLAN 是本身所属于的 VLAN。

2.1.2 MAC 地址表

MAC 地址表建于交换机内，它的表项包含了与以太网交换机相连的设备的 MAC 地址及与此设备相连的交换机的端口号。通过 MAC 地址表，交换机可以快速转发报文。

MAC 地址表中的动态表项（非手工配置）是由以太网交换机学习得来的。以太网交换机学习 MAC 地址的方法如下：如果从某端口（假设为端口 A）收到一个数据帧，以太网交换机就会分析该数据帧的源 MAC 地址（假设为 MAC-S），并认为目的 MAC 地址是 MAC-S 的报文可以由端口 A 转发；如果 MAC 地址表中已经包含 MAC-S，交换机将对应表项进行更新，如果 MAC 地址表中尚未包含 MAC-S，交换机则将这个新 MAC 地址（以及该 MAC 地址对应的转发端口）作为一个新的表项加入到 MAC 地址表中。用户可以根据网络实际情况人工配置（添加或修改）MAC 地址表项，添加或修改的表项可以是静态的表项或者动态的表项。

对于目的 MAC 地址能够在 MAC 地址表中找到的报文，系统会直接使用硬件转发；对于目的 MAC 地址不能在地址表中查到的报文，系统对报文采用广播方式进行转发。如果广播后，报文到达了目的 MAC 地址对应的网络设备，目的网络设备将应答此广播报文，应答报文中包含了此设备的 MAC 地址，以太网交换机通过地址学习将新的 MAC 地址加入到 MAC 地址转发表中。去往同一目的 MAC 地址的后续报文，就可以利用到该新增的 MAC 地址表项直接进行转发了。

以太网交换机提供 MAC 地址老化的功能。如果在一定时间内没有收到来自某网络设备的报文，交换机就会把与此设备相关的 MAC 地址表项删除。MAC 地址老化对静态 MAC 地址表项无效。

2.2 实验目的

本章节包括 4 个实验，分别是以太网端口绑定实验、端口汇聚、端口镜像和端口隔离实验。通过本章节的实验，可以了解以太网端口的分类方法，掌握以太网端口绑定方法，掌握交换机的工作原理——即 MAC 表是如何工作的。

2.3 实验内容

2.3.1 以太网端口绑定

1、软硬件要求：交换机 1 台，计算机 2 台，Console 线 1 根，网线若干。
2、网络拓扑图：

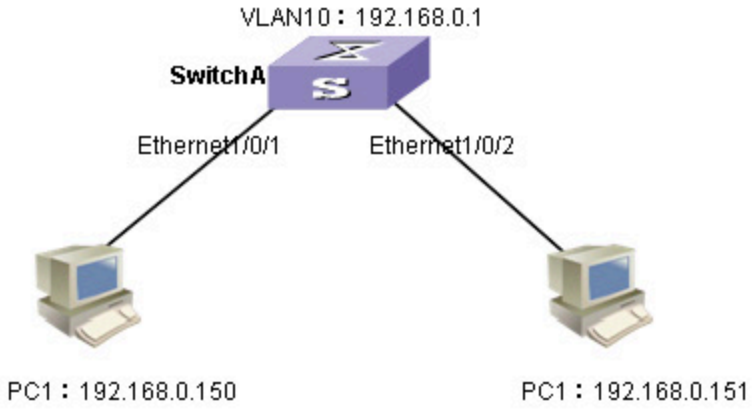

图 2-1 端口绑定实验

3、连接设备

关闭计算机和交换机电源→按照图 2-1 连接设备→打开计算机电源→打开交换机电源。其中 PC1 连接在交换机的端口 Ethernet1/0/1 上，PC2 连接在交换机的端口 Ethernet1/0/2 上。配置 PC1 的 IP 地址步骤：控制面板→网络和拨号连接→本地连接→属性→Internet 协议(TCP/IP)→将 IP 地址设置为 192.168.0.150，子网掩码为 255.255.255.0。

PC2 的配置过程与 PC1 相同，IP 地址是 192.168.0.151，子网掩码为：255.255.255.0。

4、查看 MAC 地址表

<Quidway> system-view
//进入系统视图
[Quidway] sysname SwitchA
//设置名称为 SwitchA
[SwitchA] display mac-address //显示 MAC 表
有如下相似结果：

```
MAC ADDR        VLAN ID    STATE          PORT INDEX              AGING TIME(s)

0013-4677-8894     1       Learned        Ethernet1/0/2           AGING
0013-4677-8ce9     1       Learned        Ethernet1/0/1           AGING

  ---  2 mac address(es) found  ---
```

图 2-2 MAC 地址表

上面列表中 MAC ADDR 项和 PORT INDEX 项的内容表明 E1/0/1 接口连接的主机 MAC 地址是 0013-4677-8ce9，E1/0/2 接口连接的主机 MAC 地址是 0013-4677-8894，VLAN ID 项的状态表示端口 E1/0/1 和 E1/0/2 同属 VLAN 1, STATE 项中的“Learned”状态表示地址是由交换机“学习”得到，AGING TIME（s）表示表项的老化时间。

将计算机与交换机的网线断开，再次显示 MAC 表，观察 MAC 地址表变化。有如下相似结果：

```
[SwitchA]display mac-address
No MAC addresses found.
[SwitchA]
```

图 2-3 MAC 地址表为空

再次连接网线，显示 MAC 表，观察 MAC 地址表变化。

5、添加静态 MAC 地址表项

[SwitchA] undo mac-address dynamic 0013-4677-8ce9 vlan 1

//删除 PC1 网卡的 MAC 地址表项

[SwitchA] mac-add static 0013-4677-8ce9 interface ethernet1/0/1 vlan 1

//添加 PC1 网卡的静态表项

[SwitchA] display mac-address

有如下相似结果：

```
[SwitchA]display mac-address
MAC ADDR        VLAN ID    STATE          PORT INDEX              AGING TIME(s)

0013-4677-8ce9     1       Config static  Ethernet1/0/1           NOAGED

  ---  1 mac address(es) found  ---
[SwitchA]
```

图 2-4 显示 MAC 地址表

6、对 PC1 进行地址端口绑定

端口绑定是指交换机的一个端口只能连接某个固定主机，而这个主机也只能连接这个端口。地址端口绑定的具体做法是将主机的 MAC 地址固定在交换机某个端口，然后禁止交换机所有的端口学习功能。PC1 网卡的 MAC 地址 0013-4677-8ce9，IP 地址 192.168.0.150，把 PC1 绑定在端口 E1/0/1，交换机地址设为 192.168.0.1。端口绑定大致有以下两步：

（1） 禁止端口的学习功能；

（2） 添加静态表项。

[SwitchA]interface e1/0/1

[SwitchA –Ethernet1/0/1]mac-address max-mac-count 0

[SwitchA –Ethernet1/0/1]interface e1/0/2

[SwitchA –Ethernet1/0/2]mac-address max-mac-count 0

[SwitchA –Ethernet1/0/2]interface e1/0/3

[SwitchA –Ethernet1/0/3]mac-address max-mac-count 0

[SwitchA –Ethernet1/0/3]quit

//在这里只是禁止了端口 Ethernet1/0/1- Ethernet1/0/3 的 MAC 地址学习功能

[SwitchA] mac-address static 0013-4677-8ce9 interface ethernet1/0/1 vlan 1

//添加PC1网卡的静态表项

然后进入VLAN接口视图：

[SwitchA] vlan 1

//进入vlan 1

[SwitchA-Vlan1] int vlan 1

//进入vlan 1的虚接口

[SwitchA-Vlan-interface1] ip address 192.168.0.1 255.255.255.0

//设置vlan 1的虚接口IP地址，即管理用IP地址：

7、测试验证

在交换机上输入ping 192.168.0.150，测试和PC1是否可以连通。如果可以连通，将PC1连接到交换机的另外一个端口Ethernet1/0/2，使用Ping命令看是否可以连通。显示MAC表，看有什么变化。将PC1连接到交换机的端口Ethernet1/0/10，使用Ping命令看是否可以连通，为什么？

可以将PC2连接到交换机上，使用Ping命令，查看是否可以与PC1或交换机连通，使用命令查看MAC表，看有何变化。

如果要取消对以太网端口最多可以学习到的MAC地址数的限制，使用命令undo mac-address max-mac-count。

2.3.2 端口汇聚

端口汇聚是将多个端口汇聚在一起形成1个汇聚组，以实现出/入负荷在各成员端口中的分担，同时也提供了更高的连接可靠性。本实验以华为S2100二层交换机和S3900三层交换机为例进行实验。二层和三层交换机各自的命令配置不同。另外需要注意的是，二层交换机只有相邻端口才能汇聚，且汇聚端口必须属于同一组，即1～8端口，9～16端口，17～24端口。

1、软硬件要求：交换机2台（三层交换机1台，二层交换机1台），计算机2台，Console线2根，网线若干。

2、网络拓扑图：

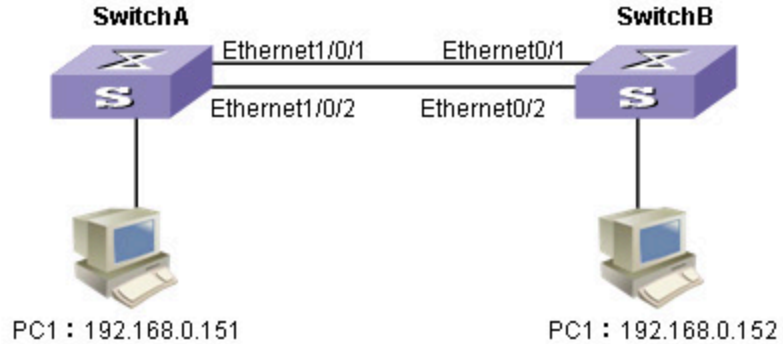

图2-5 端口汇聚实验

3、连接设备

交换机SwitchA和SwitchB通过以太网口实现互连。SwitchA用于互连的端口为Ethernet1/0/1和Ethernet1/0/2，SwitchB用于互连的端口为Ethernet1/0/1和Ethernet1/0/2。PC1连接在SwitchA除汇聚端口以外的任意以太网端口。PC2连接在SwitchB除汇聚端口

以外的任意以太网端口。

PC1 和 PC2 的 IP 地址分别为 192.168.0.151 和 192.168.0.152，子网掩码同为 255.255.255.0。

4、观察

经过一定时间可以观察到两台交换机相连的端口快速闪动，即在未启动生成树协议及端口汇聚功能未打开时,交换机陷入非正常状态。用 Ping 命令进行连通性测试，可以发现两台 PC 不通或丢包现象很严重。

5、SwitchA 端口汇聚配置（三层交换机）

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname SwitchA
//设置名称为 SwitchA
[SwitchA] link-aggregation group 1 mode manual
//创建手工汇聚组 1
[SwitchA]interface Ethernet 1/0/1
//进入端口 Ethernet1/0/1
[SwitchA-Ethernet1/0/1]duplex full
//端口设置为全双工模式
[SwitchA-Ethernet1/0/1]speed 100
//设置端口速率
[SwitchA -Ethernet1/0/1] port link-aggregation group 1
//将以太网端口 Ethernet1/0/1 加入汇聚组 1

[SwitchA-Ethernet1/0/1]interface Ethernet 1/0/2
[SwitchA-Ethernet1/0/2]duplex full
[SwitchA-Ethernet1/0/2]speed 100

[SwitchA -Ethernet1/0/2] port link-aggregation group 1
//将以太网端口 Ethernet1/0/2 加入汇聚组 1
```

6、SwitchB 端口汇聚配置（二层交换机）

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname SwitchB
//设置名称为 SwitchB
[SwitchB]interface Ethernet 0/1
//进入端口 Ethernet 0/1
[SwitchB-Ethernet 0/1]duplex full
//端口设置为全双工模式
[SwitchB-Ethernet 0/1]speed 100
//设置端口速率
[SwitchB-Ethernet 0/1]interface Ethernet 0/2
//进入端口 Ethernet 0/2
[SwitchB-Ethernet 0/2]duplex full
```

//端口设置为全双工模式
[SwitchB-Ethernet 0/2]speed 100
//设置端口速率
[SwitchB] link-aggregation Ethernet 0/1 to Ethernet 0/2 both
//将以太网端口 Ethernet 0/1 和 Ethernet 0/2 汇聚在一起。

7、测试验证

用 Ping 命令进行连通性测试，PC1 和 PC2 可以互相 Ping 通。使用命令 display link-aggregation summary 查看聚合组情况。将以太网端口退出汇聚组的命令是 undo port link-aggregation group。二层交换机删除端口汇聚命令为 undo link-aggregation all；三层交换机删除端口汇聚命令为 undo link-aggregation group 1。

2.3.3 端口镜像

端口镜像就是将被镜像端口上的数据复制到指定的镜像端口，对数据进行分析和监视。以太网交换机支持多对一的镜像，即将多个端口的报文复制到一个镜像端口上进行监控。需要注意的是二层交换机设置镜像端口和被镜像端口必须属于同一组，即端口号限制在 1－8 或 9－16 或 17－24 之内；三层交换机不存在此问题。但设端口时，二层交换机和三层交换机都要先设镜像端口，再设被镜像端口，删除时与此相反。

1、软硬件要求：交换机 1 台，计算机 4 台，Console 线 1 根，网线若干。协议分析软件。

2、网络拓扑图：

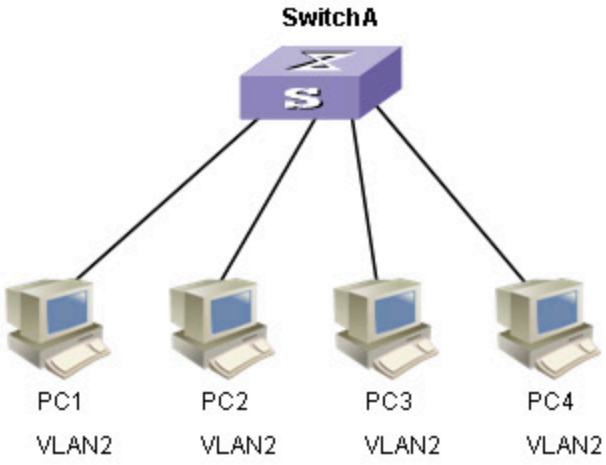

图 2-6 端口镜像实验

3、连接设备

按照图 2-6 连接设备。其中 PC1-PC4 接在交换机端口 Ethernet1/0/2- Ethernet1/0/5，端口 Ethernet1/0/2- Ethernet1/0/5 设置到 VLAN2。PC1-PC4 分别配置同一网段 IP 地址。

4、配置端口镜像

三层交换机使用华为 3900 系列交换机，配置过程如下：

<Quidway> system-view
//进入系统视图
[Quidway] sysname SwitchA
//设置名称为 SwitchA

[SwitchA]vlan 2
//创建（进入）vlan2
[SwitchA-vlan2]port ethernet 1/0/2 to ethernet 1/0/5
//将端口 Ethernet1/0/2- Ethernet1/0/5 加入到 vlan2

[SwitchA-vlan2]int ethernet1/0/2
//进入端口 Ethernet1/0/2 视图
[SwitchA-Ethernet1/0/2] monitor-port
// 将 Ethernet1/0/2 设置为监控端口

[SwitchA-Ethernet1/0/2]int ethernet1/0/3
//进入端口 Ethernet1/0/3 视图
[SwitchA-Ethernet1/0/3]mirroring-port both
//将 Ethernet1/0/3 设置为被监控端口
[SwitchA-Ethernet1/0/3]int ethernet1/0/4
[SwitchA-Ethernet1/0/4]mirroring-port both
//将 Ethernet1/0/4 设置为被监控端口
[SwitchA-Ethernet1/0/4]int ethernet1/0/5
[SwitchA-Ethernet1/0/5]mirroring-port both
//将 Ethernet1/0/5 设置为被监控端口

二层交换机使用华为 2100 系列交换机，配置过程如下：
<Quidway> system-view
//进入系统视图
[Quidway] sysname SwitchA
//设置名称为 SwitchA
[SwitchA]vlan 2
//创建（进入）vlan2
[SwitchA-vlan2]port ethernet 0/2 to ethernet 0/5
//将端口 Ethernet1/0/2- Ethernet1/0/5 加入到 vlan2
[SwitchA-vlan2]quit
[SwitchA] monitor-port Ethernet 0/2 no-filt
//端口 Ethernet 0/2 定义为镜像端口（即监控端口），no-filt 表示监控所有报文。
[SwitchA] mirroring-port Ethernet 0/3 both
[SwitchA] mirroring-port Ethernet 0/4 both
[SwitchA] mirroring-port Ethernet 0/5 both
//将 Ethernet0/3- Ethernet0/5 设置为被监控端口

5、测试验证

查看 MAC 地址表。在 PC1 上使用协议分析软件抓包，分析。删除监控端口命令 undo monitor-port。删除当前被监控端口的命令是 undo mirroring-port。

2.3.4 端口隔离

通过端口隔离特性，用户可以将需要进行控制的端口加入到一个隔离组中，实现端口之间二层、三层数据的隔离，既增强了网络的安全性，也提供了灵活的组网方案。

1、软硬件要求：交换机 1 台，计算机 4 台，Console 线 1 根，网线若干。

2、网络拓扑图：

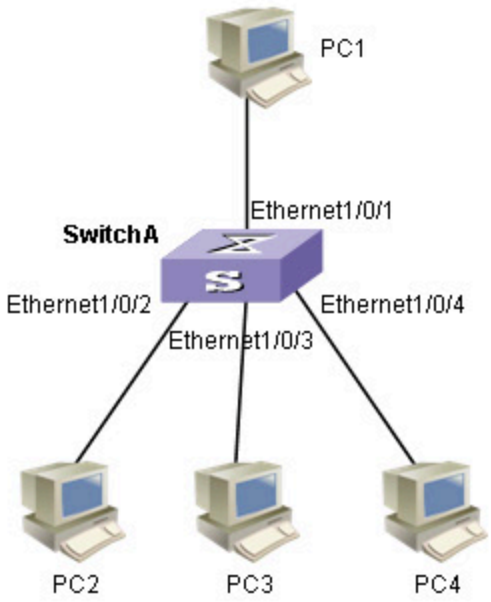

图 2-7 端口隔离实验

3、连接设备

按照图 2-7 连接设备。其中 PC1-PC4 分别与交换机的以太网端口 Ethernet1/0/1-Ethernet1/0/4 相连。PC1-PC4 分别配置同一网段 IP 地址。

4、观察

PC1、PC2、PC3 和 PC4 之间能够相互 Ping 通。查看 MAC 表，有 4 个网卡所对应的表项。

5、配置端口隔离

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname SwitchA
//修改系统名称
[SwitchA] interface ethernet1/0/2
[SwitchA-Ethernet1/0/2] port isolate
//将以太网端口 Ethernet1/0/2 加入隔离组
[SwitchA-Ethernet1/0/2] interface ethernet1/0/3
[SwitchA-Ethernet1/0/3] port isolate
//将以太网端口 Ethernet1/0/3 加入隔离组
[SwitchA-Ethernet1/0/3] interface ethernet1/0/4
[SwitchA-Ethernet1/0/4] port isolate
//将以太网端口 Ethernet1/0/4 加入隔离组
```

6、测试验证

用 Ping 命令进行连通性测试，PC2、PC3 和 PC4 之间不能互通。PC1 可以与其它 PC 通信。使用命令 display isolate port 显示隔离组中的端口信息。

2.4 思考题

（1） 写出以太网交换机工作机制。
（2） 写出 MAC 帧格式。
（3） 解释交换机 MAC 表项的含义。
（4） 端口汇聚的作用是什么？
（5） 满足什么条件的端口可以汇聚？
（6） 写出端口镜像的分类以及定义。
（7） 端口隔离有什么作用？

第三章 VLAN 实验

3.1 实验背景知识

3.1.1 VLAN 简介

VLAN（Virtual Local Area Network），虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的技术。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 IEEE 802.1Q 协议标准草案。

VLAN 技术允许网络管理者将一个物理的 LAN 逻辑地划分成不同的广播域（或称虚拟 LAN，即 VLAN），每一个 VLAN 都包含一组有着相同需求的计算机，由于 VLAN 是逻辑地而不是物理地划分，所以同一个 VLAN 内的各个计算机不必被放置在同一个物理空间里，即这些计算机不一定属于同一个物理 LAN 网段。

VLAN 的优势在于 VLAN 内部的广播和单播流量不会被转发到其它 VLAN 中，从而有助于控制网络流量、减少设备投资、简化网络管理、提高网络安全性。

3.1.2 802.1Q

802.1Q 协议，即 Virtual Bridged Local Area Networks 协议，主要规定了 VLAN 的实现。802.1Q 协议规范确定了包含 32 位标签包头，所有 32 位均插入在分组的包头的正常目的地址与源地址之后。

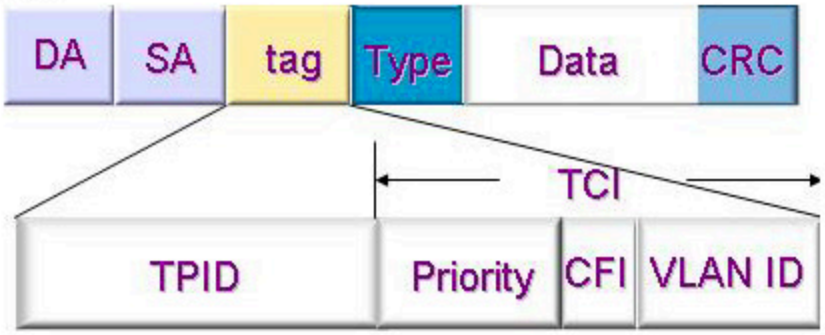

图 3-1 带有 802.1Q 标签头的以太网帧

这 4 个字节的 802.1Q 标签头包含了 2 个字节的 TPID（Tag Protocol Identifier 标签协议标识）和 2 个字节的 TCI（Tag Control Information 标签控制信息），TPID 是 IEEE 定义的新的类型，表明这是一个加了 802.1Q 标签的报文。

在标签头中，TCI 字节中 Priority 字段有 3 个优先位用于指明帧的优先级，一共有 8 种优先级，主要用于当交换机阻塞时，优先发送哪个数据包。802.1Q 的优先位可由桌面系统、服务器、路由器和第三层交换机来设置。

3.2 实验目的

本章节实验共 4 个内容，包括单交换机 VLAN 配置、交换机之间的 VLAN 内互通、公共端口和 VLAN 间互通。通过本章节实验，能够掌握 VLAN 工作原理和交换机 VLAN 的基

本配置方法。

3.3 实验内容

3.3.1 单交换机 VLAN 配置

1、软硬件要求：交换机 1 台，计算机 4 台，Console 线 1 根，网线若干。
2、网络拓扑图：

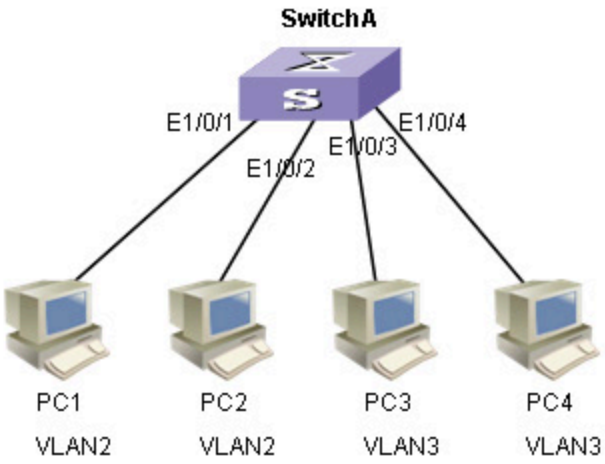

图 3-2 单交换机 VLAN 配置实验

3、连接设备

将 PC1—PC4 分别依次连接到端口 Ethernet1/0/1 ～ Ethernet1/0/4。端口 Ethernet1/0/1 和 Ethernet1/0/2 包含在 VLAN2 中，端口 Ethernet1/0/3 和 Ethernet1/0/4 包含在 VLAN3 中。使用 PC1 连接交换机 Console 口进行配置。PC1-PC4 分别配置同一网段 IP 地址。

4、配置步骤

<Quidway> system-view
//进入系统视图
[Quidway] sysname SwitchA
//修改系统名称
[SwitchA] vlan 2
//创建 VLAN2 并进入其视图
[SwitchA -vlan2] port ethernet1/0/1 ethernet1/0/2
//向 VLAN2 中加入端口 Ethernet1/0/1 和 Ethernet1/0/2
[SwitchA -vlan2] vlan 3
//创建 VLAN3 并进入其视图
[SwitchA -vlan3] port ethernet1/0/3 ethernet1/0/4
//向 VLAN3 中加入端口 Ethernet1/0/3 和 Ethernet1/0/4

缺省情况下所有端口都属于 VLAN 1，并且端口是 access 端口，一个 access 端口只能属于一个 vlan。如果端口是 access 端口，则把端口加入到另外一个 vlan 的同时，系统自动把该端口从原来的 vlan 中删除掉。

5、测试验证

使用命令 display current-configuration 可以看到端口 Ethernet1/0/1 和 Ethernet1/0/2 属于

vlan2，端口 Ethernet1/0/3 和 Ethernet1/0/4 属于 VLAN3。使用 display interface Ethernet 1/0/1 可以看到端口为 access 端口，PVID 为 2。使用 display interface Ethernet 1/0/3 可以看到端口为 access 端口，PVID 为 3。PC1 和 PC2 可以互相 Ping 通，PC3 和 PC4 可以互相 Ping 通，但是分处 2 个 VLAN 的 PC 之间不能互通。

3.3.2 交换机之间的 VLAN 内互通

1、软硬件要求：交换机 2 台，计算机 4 台，Console 线 2 根，网线若干。

2、网络拓扑图：

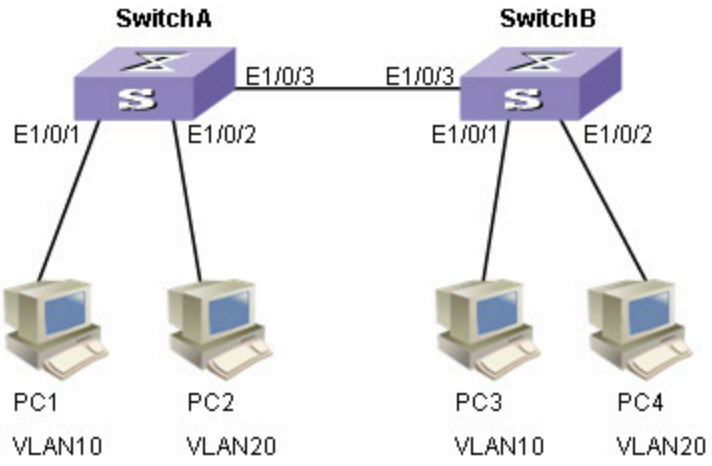

图 3-3 交换机之间的 VLAN 内互通实验

3、连接设备

将 PC1 连接到 SwitchA 端口 Ethernet1/0/1，将 PC2 连接到 SwitchA 端口 Ethernet1/0/2，将 PC3 连接到 SwitchB 端口 Ethernet1/0/1，将 PC4 连接到 SwitchB 端口 Ethernet1/0/2。SwitchA 端口 Ethernet1/0/1 和 SwitchB 端口 Ethernet1/0/1 包含在 VLAN10 中，SwitchA 端口 Ethernet1/0/2 和 SwitchB 端口 Ethernet1/0/2 包含在 VLAN20 中。SwitchA 和 SwitchB 通过端口 Ethernet1/0/3 相连。PC1-PC4 分别配置同一网段 IP 地址。

使用 PC1 连接交换机 SwitchA 的 Console 口进行配置。使用 PC3 连接交换机 SwitchB 的 Console 口进行配置。

4、SwitchA 配置步骤

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname SwitchA
//修改系统名称
[SwitchA] vlan 10
//创建 VLAN10 并进入其视图
[SwitchA –vlan10] port ethernet1/0/1
//向 VLAN10 中加入端口 Ethernet1/0/1
[SwitchA –vlan10] vlan 20
//创建 VLAN20 并进入其视图
[SwitchA –vlan20] port ethernet1/0/2
//向 VLAN20 中加入端口 Ethernet1/0/2
```

[SwitchA –vlan20]int ethernet1/0/3
[SwitchA-Ethernet1/0/3]port link-type trunk
//将上行端口设置成 trunk 属性
[SwitchA-Ethernet1/0/3]port trunk permit vlan all
//允许所有的 vlan 从 E0/3 端口通过

5、SwitchB 配置步骤

<Quidway> system-view
//进入系统视图
[Quidway] sysname SwitchB
//修改系统名称
[SwitchB] vlan 10
//创建 VLAN10 并进入其视图
[SwitchB –vlan10] port ethernet1/0/1
//向 VLAN10 中加入端口 Ethernet1/0/1
[SwitchB –vlan10] vlan 20
//创建 VLAN20 并进入其视图
[SwitchB –vlan20] port ethernet1/0/2
//向 VLAN20 中加入端口 Ethernet1/0/2
[SwitchB –vlan20]int ethernet1/0/3
[SwitchB-Ethernet1/0/3]port link-type trunk
//将上行端口设置成 trunk 属性
[SwitchB-Ethernet1/0/3]port trunk permit vlan all
//允许所有的 vlan 从 E0/3 端口通过

6、测试验证

SwitchA vlan10 内的 PC 可以与 SwitchB vlan10 内的 PC 互通，SwitchA vlan20 内的 PC 可以与 SwitchB vlan20 内的 PC 互通，SwitchA vlan10 内的 PC 不能与 SwitchB vlan20 内的 PC 互通。使用命令查看端口状态。查看 MAC 地址表。

3.3.3 VLAN 间的互通

VLAN 之间互通要使用三层交换机的路由功能，关于路由协议，在第六章有详细介绍。

1、软硬件要求：交换机 2 台，计算机 2 台，Console 线 2 根，网线若干。

2、网络拓扑图：

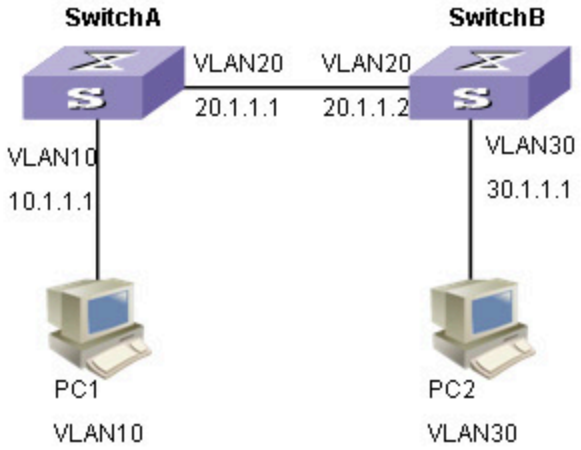

图 3-4 VLAN 间的互通实验

3、连接设备

交换机 SwitchA、SwitchB 实现互连。SwitchA 中 vlan10 虚接口地址 10.1.1.1/8，vlan20 虚接口地址 20.1.1.1/8， vlan20 与 SwitchB vlan20 互连，vlan10 接局域网；SwitchB 中 vlan20 虚接口地址 20.1.1.2/8，vlan30 虚接口地址 30.1.1.1/8，vlan20 与 SwitchA vlan20 互连，vlan30 接局域网；PC1 的 IP 地址是 10.1.1.2/8，网关为 10.1.1.1；PC2 的 IP 地址是 30.1.1.2/8，网关为 30.1.1.1。

使用 PC1 连接交换机 SwitchA 的 Console 口进行配置。使用 PC2 连接交换机 SwitchB 的 Console 口进行配置。

4、SwitchA 配置步骤

<Quidway> system-view
//进入系统视图
[Quidway] sysname SwitchA
//修改系统名称
[SwitchA] vlan 10
//创建 VLAN10 并进入其视图
[SwitchA –vlan10] port ethernet1/0/1
//向 VLAN10 中加入端口 Ethernet1/0/1
[SwitchA –vlan10]int vlan 10
//创建（进入）vlan10 的虚接口
[SwitchA-Vlan-interface10]ip address 10.1.1.1 255.0.0.0
//给 vlan10 的虚接口配置 IP 地址
[SwitchA-Vlan-interface10] vlan 20
//创建 VLAN20 并进入其视图
[SwitchA –vlan20] port ethernet1/0/2
//向 VLAN20 中加入端口 Ethernet1/0/2
[SwitchA]int vlan 20
//创建（进入）vlan20 的虚接口
[SwitchA-Vlan-interface20]ip address 20.1.1.1 255.0.0.0
//给 vlan20 的虚接口配置 IP 地址
[SwitchA-Vlan-interface20]rip
//启动 RIP

[SwitchA-rip]network 10.1.1.0

//从 10.1.1.0 网段的接口发布和接收 RIP 路由信息

[SwitchA-rip]network 20.1.1.0

//从 20.1.1.0 网段的接口发布和接收 RIP 路由信息

5、SwitchB 配置步骤

<Quidway> system-view

//进入系统视图

[Quidway] sysname SwitchB

//修改系统名称

[SwitchB] vlan 30

//创建 VLAN30 并进入其视图

[SwitchB –vlan30] port ethernet1/0/1

//向 VLAN30 中加入端口 Ethernet1/0/1

[SwitchB –vlan30]int vlan 30

//创建（进入）vlan30 的虚接口

[SwitchB-Vlan-interface30]ip address 30.1.1.1 255.0.0.0

//给 vlan30 的虚接口配置 IP 地址

[SwitchB-Vlan-interface30] vlan 20

//创建 VLAN20 并进入其视图

[SwitchB –vlan20] port ethernet1/0/2

//向 VLAN20 中加入端口 Ethernet1/0/2

[SwitchB –vlan20]int vlan 20

//创建（进入）vlan20 的虚接口

[SwitchB-Vlan-interface20]ip address 20.1.1.2 255.0.0.0

//给 vlan20 的虚接口配置 IP 地址

[SwitchB-Vlan-interface20]rip

//启动 RIP

[SwitchB-rip]network 30.1.1.0

//从 10.1.1.0 网段的接口发布和接收 RIP 路由信息

[SwitchB-rip]network 20.1.1.0

//从 20.1.1.0 网段的接口发布和接收 RIP 路由信息

6、测试验证

配置 RIP 路由协议后，PC1 能够 Ping 通 PC2，在交换机上使用命令 display ip routing-table 可以看到各个网段路由信息。

3.4 思考题

（1）简述 VLAN 产生的原因以及作用。

（2）划分 VLAN 有哪些方法？

（3）画出 VLAN 的帧格式。

（4）VLAN 之间如何进行互通？