

实验五 路由器与交换机的联网实验

5.1 实验目的

1. 掌握路由器、交换机进行简单组网的方法，理解交换机、路由器的工作原理
2. 了解 VLAN 的作用，掌握在一台交换机上划分 VLAN 的方法和跨交换机的 VLAN 的配置方法。掌握镜像端口和 Trunk 端口的配置方法，了解 VLAN 数据帧的格式、VLAN 标记添加和删除的过程。

5.2 实验内容

- (1) 使用路由器和交换机进行组网，实现各 PC 间的互联互通。
- (2) 首先在一台交换机上划分 VLAN，用 ping 命令测试连通性。然后在交换机上配置 Trunk 端口，测试在同一 VLAN 和不同 VLAN 中设备的连通性。配置端口镜像，截获 VLAN 数据帧，分析 VLAN 数据帧的格式和 VLAN 标记添加与删除的过程。

5.3 实验原理

5.3.1 路由器和交换机

以太网交换机实际是一个基于网桥技术的多端口第二层网络设备，它为数据帧从一个端口到另一个任意端口的转发提供了低时延、低开销的通路。而交换机技术的发展，还出现了集成了三层路由功能的三层交换机，这时交换机又“变成”了一个路由器。交换机工作在数据链路层，可以用来隔离冲突域，按 MAC 地址寻址。交换机通过自学习来建造一个 MAC 地址和端口的对照表（知道某个 MAC 在哪个端口上连着），通过这张表进行数据帧的转发。

路由器是网络层中的分组交换设备，基本功能是把 IP 报文传送到正确的网络，包括：

1. IP 数据报的转发，包括数据报的寻径和传送；

2. 子网隔离，抑制广播风暴；
3. 维护路由表，并与其他路由器交换路由信息，这是 IP 报文转发的基础。
4. IP 数据报的差错处理及简单的拥塞控制；
5. 实现对 IP 数据报的过滤和记帐。

路由器的 IP 数据报转发是通过路由表进行的，寻址的依据是目标 IP 地址。而路由表的建造是通过路由协议自动完成，或管理员的人工设置。

5.3.2 采用 VLAN 强化网络管理和网络安全

VLAN 即虚拟局域网，通过将局域网划分为虚拟网络 VLAN 网段，可以强化网络管理和网络安全，控制不必要的数据广播，网络中工作组可以突破共享网络中的地理位置限制，而根据管理功能来划分子网。不同厂商的交换机对 VLAN 的支持能力不同，支持 VLAN 的数量也不同。

以太网交换机在数据链路层上基于端口进行数据转发，使得冲突域被缩小到交换机的每一个端口。但是交换机的所有端口都在同一个广播域，当网络内主机数量急剧增加时，大量的广播报文将引起网络性能恶化。为了将大的广播域隔离成多个较小的广播域，引入了 VLAN 技术。在 VLAN 技术中规定，凡是具有 VLAN 功能的交换机在转发数据报文时，都需要确认该报文属于某一个 VLAN，并且该报文只能被转发到属于同一个 VLAN 的端口或主机，不同 VLAN 间在链路层不能直接通信。VLAN 的划分有很多种：按照 IP 地址来划分，按照端口来划分、按照 MAC 地址划分或者按照协议来划分。其中基于端口划分的方法是最普遍使用的，也是目前所有交换机都支持的一种划分方法。

5.3.3 802.1q 协议与三层交换

交换机可分为二层交换机、三层交换级和多层交换机。二层交换机按照接入设备的 MAC 地址进行数据帧的过滤和转发。802.1q 协议定义了基于端口的 VLAN 模型。802.1q 规范使第 2 层交换具有以优先级区分信息流的能力，完成动态多播过滤。802.1q 标准主要用来解决如何将大型网络划分为多个小网络，如此广播和组播流量就不会占据更多带宽的问题。此外 802.1q 标准还提供更高的网络段间安全性。

三层交换机就是具有部分路由器功能的交换机，在同一个交换机划分的 VLAN 之间能够做到“一次路由，多次转发”。对路由信息更新、路由表维护、路由计算、路由确定等功能都由软件实现。三层交换技术就是二层交换技术+三层转发技术。三层交换机都支持 802.1q 标准。

1) 802.1q 以太网帧格式

802.1Q 标记过程修改原始的以太网帧。一个称为标记字段的 4 字节字段被插入原始的以太网帧中,并且原始帧的 FCS(检验和)也根据这些变化而重新计算。插入 4 字节字段后以太网帧格式如下:

所占位	48	48	16	3	1	12	16		32
域名	目的地址	源地址	8100	Priority	CFI	VLAN	类型	数据	FCS

进行标记的目的是帮助其相连的交换机将帧置于源 VLAN 之中,插入得 4 字节包含以下字段:

8100: 16 位恒定值域,指明这个帧包含 802.1q 标签。

Priority: 3 位,可定义 8 种用户优先级。支持 802.1q 规范的交换机可以使每一个输出端口具有使用多缓冲器排列能力,该能力可以选择信息传输的优先次序。该字段支持将数据包分组为各种流量种类。流量种类也可以定义为第二层服务质量(QoS)或服务类(CoS),并且在网络适配器和交换机上实现,而不需要任何预留设置。

CFI: 规范格式指示,在以太网交换机中规范格式指示器总被设置为 0。

VLAN: 该字段为 12 位。支持 4096 个 VLAN 的识别。

2) 以太网端口的三种链路类型

目前的主机都不支持带有 tag 域的帧,因此交换机要对连接主机的端口上的数据包执行封装和去封装操作。根据交换机处理 VLAN 数据帧的不同,可以将交换机端口分为三类:

(1) Access 类型的端口

该类型的端口只能属于 1 个 VLAN,一般用于连接计算机的端口。进入端口的数据,端口根据自己的缺省 VLAN ID 对帧进行封装,从 Access 端口转发出去的数据帧将它去掉封装,变成普通的以太网数据帧。

(2) Trunk 类型的端口

该类型的端口可以属于多个 VLAN,可以接收和发送多个不同 VLAN 的报文,一般用于连接两个交换机。进入 Trunk 端口的数据帧,对于已经携带 tag 域的数据,端口直接进行转发,而普通数据帧,端口用自己的缺省 VLAN ID 进行封装后再转发。

(3) Hybrid 类型的端口

该类型的端口可以属于多个 VLAN,可以接收和发送多个不同 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。

5.3.4 三层交换机实现 VLAN 之间的互通

三层交换机可以实现 VLAN 之间的互通，VLAN 之间的互通是通过实现一个虚拟 VLAN 接口来实现的，即针对每个 VLAN，交换机内部维护了一个与该 VLAN 对应的接口，该接口对外是不可见的，是一个虚拟的接口，但该接口有所有物理接口所具有的特性，比如有 MAC 地址，可配置 IP 地址、最大传输单元和传输的以太网帧类型等。当交换机接收到一个数据帧时，判断是不是发给自己的 VLAN，判断的依据便是查看该 MAC 地址是不是针对接收数据帧所在 VLAN 的接口 MAC 地址，如果是，则进行三层处理，若不是，则进行二层处理。

5.3.5 端口镜像 (port Mirroring)技术

以太网交换机在数据链路层上基于端口进行数据转发，使得冲突域被缩小到交换机的每一个端口。一般情况下，交换机每个端口只能得到与自己相关的数据包。

在网络数据包检测和安全监控中，就需要交换机把某一个端口接收或发送的数据帧完全相同的复制给另一个端口。其中被复制的端口称为镜像源端口，复制的端口称为镜像目的端口，镜像目的端口不能再传输数据。

端口镜像在不同的产品中通常有以下几种别名：

Port Mirroring；Monitoring Port ；Spanning Port ；SPAN port ；Link Mode port 。

5.4 路由器和交换机的组网实验

5.4.1 实验环境与分组

路由器 1 台（DCR2626-1），交换机 2 台；
每组 4 名同学，每人一台 PC，协同进行实验。

5.4.2 实验拓扑结构

图 5-1 给出了本实验的组网实验示意图，鼓励各小组灵活自定义 IP 分配。

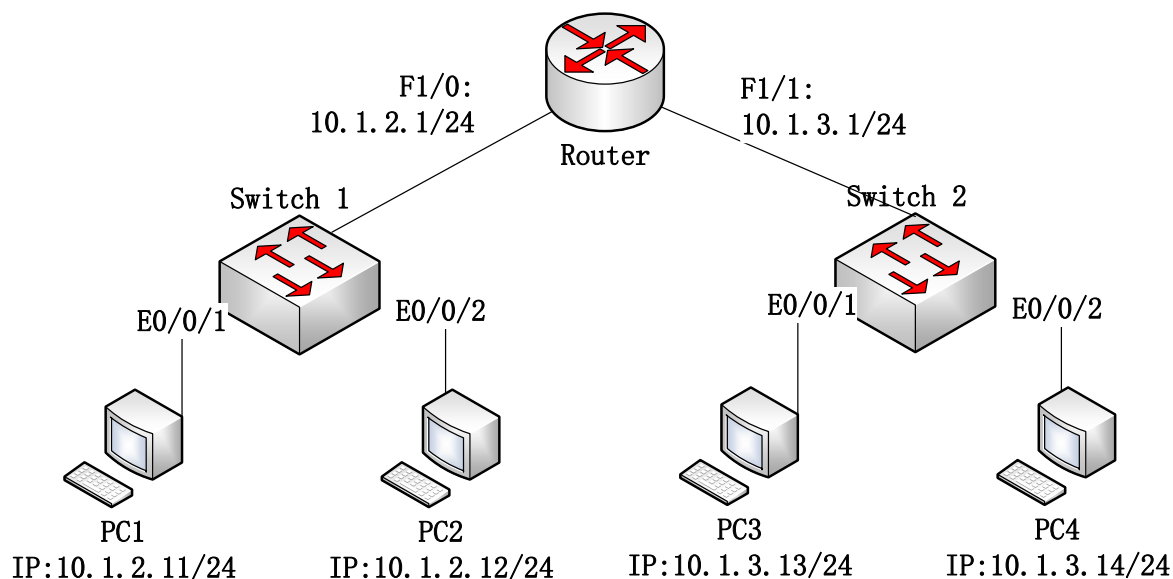


图 5-1 组网实验示意图

5.4.3 组网实验步骤

步骤 1: 按照图 5-1 连接好设备, 设置各 PC 的 IP 地址和默认网关。

步骤 2: 将交换机、路由器恢复为出厂设置, 参考命令如下:

交换机:

switch> enable !进入特权用户模式

switch# set default !启动初始化

Are you sure? [Y/N] = y ! 确认初始化, 显示初始化信息

switch# write ! 写入初始化信息到启动文件

switch# reload ! 重新启动交换机

路由器:

Router>enable ! 进入特权用户配置模式

Router#delete !恢复出厂设置

Router#reboot !重启路由设备

switch# reload ! 重新启动交换机

步骤 3: 配置路由器 Router 的接口 IP 地址, f1/0 接口的配置命令如下:

```
Router#config
Router(Config)#interface f1/0
Router(Config-if)#ip address 10.1.2.1 255.255.255.0
Router(Config-if)#no shutdown
Router#show interface f1/0
```

参照 f1/0 接口的配置命令配置 f1/1 接口的 IP 地址 10.1.3.1。

5.4.4 组网实验结果及分析

- 1) 在实验 1 的现场检查单上画出实验拓扑图，标明使用的设备（如 1#DCR2626-1）及设置的接口及 IP。
- 2) 在各台 PC 上使用 ping 命令检查网络连通情况，在现场检查单中按表 5-1 要求记录结果。

表 5-1 路由器和交换机的组网实验测试结果

		所用命令	能否 ping 通
同一网段中	PC1 ping PC2		
	PC3 ping PC4		
不同网段中	PC2 ping PC3		
	PC4 ping PC1		

- 3) 用 show ip route 查看 R1 的路由表，分析不同网段互通原因，体会网关的作用？
- 4) 在 PC1 上用 tracert -d 10.1.3.14，查看 PC1-PC4 的路由连通路径。

5.5 VLAN 的组网实验

5.5.1 实验环境与分组

DCRS-5650 交换机 2 台，每 4 人一组，共同配置 2 台交换机。

5.5.2 实验网络拓扑

图 5-2 是在 1 个交换机上配置 2 个 VLAN 的组网图，图 5-3 是在 2 个交换机上配置 2 个 VLAN 的组网图。图中参数只作为参考，鼓励各小组灵活自定义 IP 等参数。

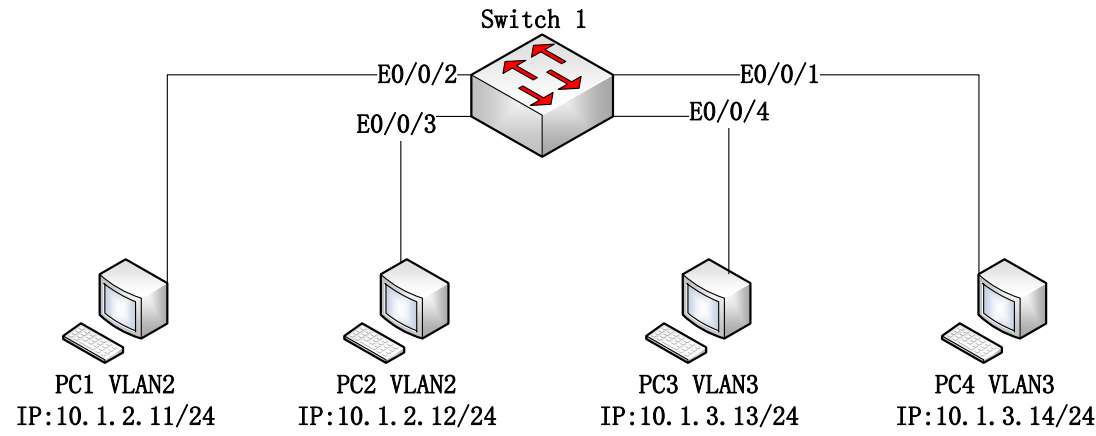


图 5-2 同一交换设备上配置 Vlan

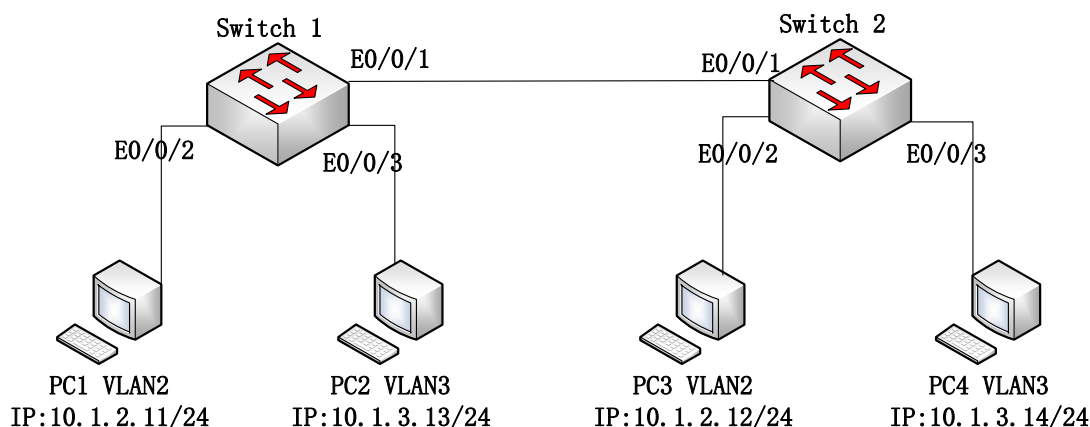


图 5-3 利用 trunk 端口在 2 台设备上配置 Vlan

5.5.3 实验过程及结果分析

清除电脑原本的 IP 地址设置，根据本组的网络拓扑设计配置 exp 网卡 IP 地址，连接设备，用 Putty 登录设备进行配置（详细步骤请参考《设备配置方式》）。

1) VLAN 的基本配置

首先将交换机恢复为出厂设置，然后按如下步骤进行实验。

步骤 1：按图 5-2 所示连接好设备，为交换机划分 VLAN，vlan 2 的配置参考命令如下：

```
switch> enable
switch# config ! 进入全局配置模式
switch(Config)#vlan 2
switch(Config-vlan2)#switchport interface Ethernet 0/0/2-3
switch(Config-vlan2)#exit
switch#show vlan ! 查看 vlan 配置信息
```

同理配置 vlan 3。

步骤 2：设置各 PC 的 exp 网卡 IP 地址。

步骤 3：用 ping 命令验证同一 VLAN 的两台计算机能否通信，不同 VLAN 之间的计算机能否通信，记录结果。

2) Trunk 端口配置

将交换机恢复为出厂设置，然后按如下步骤进行实验。

步骤 4：按照图 5-3 连接好设备，配置各台计算机的 exp 网卡 IP 地址。为交换机 S1、S2 各自划分 VLAN2 和 VLAN3。配置命令同上。

步骤 5：验证各 PC 机之间能否 ping 通。

步骤 6: 分别在两台交换机上配置 Trunk 端口, 并且将 trunk 端口加入 VLAN2 和 VLAN3 中。参考配置命令如下:

```
switch(Config)#interface ethernet 0/0/1
switch(Config-Ethernet0/0/1)#switchport mode trunk
switch(Config-Ethernet0/0/1)#switchport trunk allowed vlan all
switch(Config-Ethernet0/0/1)#exit
switch#show vlan
```

测试交换机 S1、S2 上相同 VLAN 和不同 VLAN 之间是否可以 ping 通, 记录结果, 分析原因。在 PC1 上用 `tracert -d 10.1.3.14`, 查看 PC1-PC4 的路由连通路径。

步骤 7: 分别在交换机 S1 和 S2 上配置端口镜像, 将 E0/0/1 端口镜像到端口 E0/0/3, 配置命令如下:

```
switch(Config)#monitor session 1 source interface ethernet 0/0/1 both
switch(Config)#monitor session 1 destination interface ethernet 0/0/3
```

在 4 台 PC 上捕获报文, 验证 PC1 ping PC3 能否 ping 通。在 PC2 和 PC4 上截获含有 802.1q 标记的报文, 对各 PC 上截获的报文进行比较分析, 记录结果, 并分析原因。(注: 新网卡默认过滤掉了 802.1q, 如果抓不到报文, 如实记录即可, 下表不用再分析)。

表 5-2 跨交换机 VLAN 实验 (PC1 ping PC3)

转发过程及方向	VLAN 标记值 (只填写观察到的值)	标记出现与否的原因
PC1 - S1		
S1 - S2		
S2 - PC3		

No.	Time	Source	Destination	Protocol	Length	Info
9	1.192539	10.2.3.13	10.2.2.14	ICMP	78	Echo (ping) request id=0x0001, seq=9/2304, ttl=127 (reply in 10)
10	1.193170	10.2.2.14	10.2.3.13	ICMP	78	Echo (ping) reply id=0x0001, seq=9/2304, ttl=127 (request in 9)
15	2.194659	10.2.3.13	10.2.2.14	ICMP	78	Echo (ping) request id=0x0001, seq=10/2560, ttl=127 (reply in 16)
16	2.195427	10.2.2.14	10.2.3.13	ICMP	78	Echo (ping) reply id=0x0001, seq=10/2560, ttl=127 (request in 15)
20	3.198582	10.2.3.13	10.2.2.14	ICMP	78	Echo (ping) request id=0x0001, seq=11/2816, ttl=127 (reply in 21)
21	3.199238	10.2.2.14	10.2.3.13	ICMP	78	Echo (ping) reply id=0x0001, seq=11/2816, ttl=127 (request in 20)
26	4.201356	10.2.3.13	10.2.2.14	ICMP	78	Echo (ping) request id=0x0001, seq=12/3072, ttl=127 (reply in 27)
27	4.201969	10.2.2.14	10.2.3.13	ICMP	78	Echo (ping) reply id=0x0001, seq=12/3072, ttl=127 (request in 26)

Frame 9: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
 Ethernet II, Src: DigitalC_0b:7b:4a (00:03:0f:0b:7b:4a), Dst: RealtekS_01:90:95 (00:e0:4c:01:90:95)
 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2
 000. = Priority: Best Effort (default) (0)
 ...0 = DEI: Ineligible
 0000 0000 0010 = ID: 2
 Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 10.2.3.13, Dst: 10.2.2.14
 Internet Control Message Protocol

3) VLAN 间通信

步骤 8: 在 4 台计算机上都运行 Wireshark 截获报文, 执行 PC3 ping PC4,

观察能否 ping 通，对各计算机截获的报文进行综合分析，说明原因。

步骤 9: 在交换机 S1 上配置 VLAN2 和 VLAN3 的接口 IP 地址，VLAN2 的 IP 为 10.1.2.1/24，VLAN3 接口的 IP 为 10.1.3.1/24。VLAN2 的 IP 配置参考命令如下：

```
switch(Config)#interface vlan 2
switch(Config-If-Vlan2)#ip address 10.1.2.1 255.255.255.0
switch(Config-If-Vlan2)#no shutdown
switch(Config-If-Vlan2)#exit
```

同理配置 VLAN3 的 IP 地址。

关闭 S2 上的镜像，配置参考命令如下：

```
switch(Config)# no monitor session 1 source interface ethernet 0/0/1
switch(Config)# no monitor session 1 destination interface ethernet 0/0/3
```

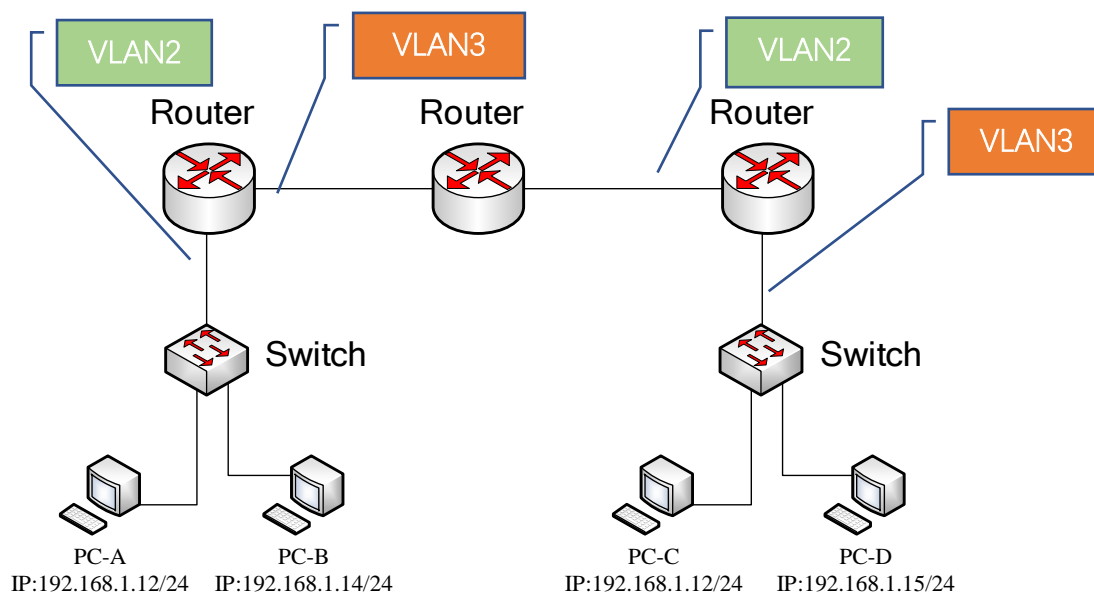
步骤 10: 配置 PC1 和 PC3 的网关为 10.1.2.1，配置 PC2 和 PC4 的网关为 10.1.3.1。同时，在 PC2 上用 Wireshark 监听捕获报文；执行 PC3 ping PC4；观察能否 ping 通，说明原因。

如果 ping 不通： 1、检查 PC 机和交换机的 IP 地址、子网掩码和网关设置是否正确，设备接口连接是否与拓扑图相符； 2、删除 out 网卡的默认路由，只保留 exp 网卡的默认路由。

5.6 互动讨论主题

- 1) 分析不同 LAN 中 PC 互通的原因及跨越的链路；
- 2) 理解网关的目的及作用；
- 3) 路由表的形成及使用。

5.7 进阶自设计



5.8 互动讨论主题

- (1) 交换设备与 Vlan 配置；
- (2) 交换设备端口类型与镜像口；
- (3) 路由表生成方法；
- (4) 路由表的使用。