# 实验五 路由器与交换机

## 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。

## 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。

## 实验原理

### 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。

### 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VALN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](http://www.qqread.com/z/tech/ip/index.html)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。

### 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，完成动态多波过滤。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](http://baike.baidu.com/view/492256.htm" \t "_blank)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](http://baike.baidu.com/view/1077.htm)就是具有部分[路由器](http://baike.baidu.com/view/1360.htm)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](http://baike.baidu.com/view/18655.htm" \t "_blank)，多次转发” 。对[路由](http://baike.baidu.com/view/18655.htm" \t "_blank)信息更新、[路由表](http://baike.baidu.com/view/149989.htm)维护、路由计算、路由确定等功能都由[软件](http://baike.baidu.com/view/37.htm)实现。[三层交换技术](http://baike.baidu.com/view/802.htm)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。

#### 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。

#### 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。

### 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。

### 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 。

## 路由器和交换机组网实验

### 实验环境与分组

路由器1台（DCR2626-1），交换机2台（DCRS-5650）；

每组4名同学，每人一台PC，协同进行实验。

### 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

### 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 |

步骤3：配置路由器Router的接口IP地址，E1/0接口的配置命令如下：

|  |
| --- |
| Router#config  Router(Config)#interface E1/0  Router(Config-if)#ip address 10.1.2.1 255.255.255.0  Router(Config-if)#no shutdown  Router#show interface E1/0 |

参照f1/0接口的配置命令配置E1/1接口的IP地址10.1.3.1。

### 组网实验结果及分析

1. 在检查单上画出实验拓扑图，标明使用的设备、接口及IP地址等信息。
2. 在各台PC上使用ping命令检查网络连通情况，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 |  |  |

1. 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？
2. 在PC1上用tracert –d 10.1.3.14，查看PC1-PC4的路由连通路径。

## VLAN的组网实验

### 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。

### 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

### 实验过程及结果分析

#### VLAN的基本配置

步骤1：按照图5-2连接好设备，设置各PC的IP地址和默认网关。测试各台PC之间能否ping通，记录结果。

步骤2：为交换机划分VLAN，vlan 2的配置参考命令如下：同理配置vlan 3。

|  |
| --- |
| 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  switch(Config-vlan2)#switchport interface Ethernet 0/0/4  switch(Config-vlan2)#exit  switch#show vlan ！查看vlan配置信息 |

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，记录结果并分析原因。

#### Trunk端口配置

步骤4：按照图5-3连接好设备，设置各PC的IP地址和默认网关。

步骤5：为交换机S2划分VLAN2和VLAN3，配置命令同上。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，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 |

将trunk端口加入VLAN2和VLAN3中。

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。

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 PC2能否ping通，对各PC上截获的ICMP报文进行分析（观测是否含有802.1q标记），记录结果并分析原因。



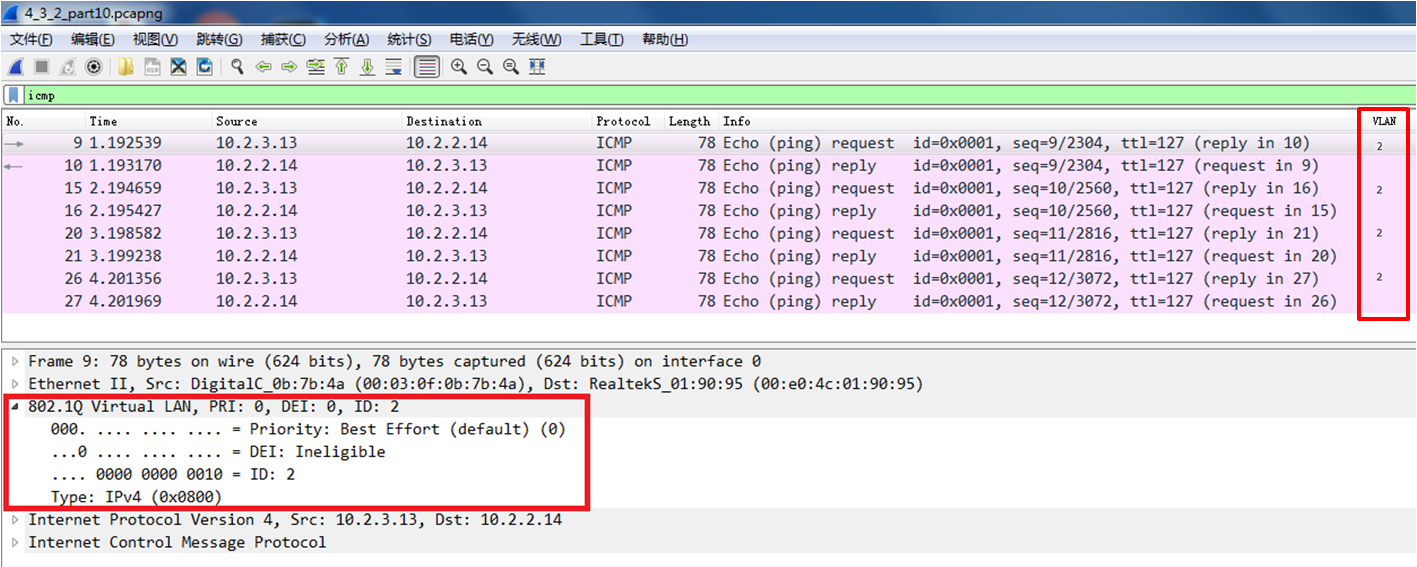
**注：**

**1、新网卡默认过滤掉了802.1q标记，如果抓不到含有标记的报文，如实记录即可，在原因分析中填写预期能观测到的值，分析标记未出现可能的原因；**

**2、结合抓到的报文，尝试分析交换机在处理端口镜像和VLAN标记时的先后顺序。**

表5-2 跨交换机VLAN实验（PC1 ping PC2）

|  |  |  |
| --- | --- | --- |
| 转发过程 | 802.1Q VLAN ID | 标记出现与否的原因分析 |
| PC1 - S1 | Request报文： |  |
| Reply报文： |  |
| S1 - S2 | Request报文： |  |
| Reply报文： |  |
| S2 – PC2 | Request报文： |  |
| Reply报文： |  |



#### VLAN间通信

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8：执行PC2 ping PC4，观察能否ping通，分析原因。

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。

步骤10：在4台PC上捕获报文，验证PC2 ping PC4能否ping通，对各PC上截获的ICMP报文进行分析，填写表5-3，分析观测到的过程和VLAN ID是否与预期相符。

注：如果监听机（PC3）抓不到带标记的报文，在组内另找一台可以抓到的PC，与PC3更换IP配置和连线后，再进行测试。

表5-3 跨VLAN通信（PC2 ping PC4）

|  |  |  |
| --- | --- | --- |
| 转发过程 | 802.1Q VLAN ID | 标记出现与否的原因分析 |
| PC2 -- S2 | Request报文： |  |
| Reply报文： |  |
| S1 -- S2 | Request报文： |  |
| Reply报文： |  |
| S2 -- PC4 | Request报文： |  |
| Reply报文： |  |

**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、断开无线网卡，只保留exp网卡。**

## 互动讨论主题

1. 分析不同网段中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；
4. 交换设备与Vlan配置；
5. 交换设备端口类型与镜像口。

## 进阶自设计



通过配置，使不同网段的PC可以相互访问，各PC都能相互ping通。