

# 计算机网络实验报告

姓名：白思雨

学号：2186123935

日期：2021.1.13

# 实验一：组网与接入认证

## 一、概述

### 1.1 时间

2020.11.25 早上 8 点到 12 点

### 1.2 地点

西一楼网络专题实验室 A201

### 1.3 试验任务

- (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) 802.1x 认证服务器的构建；
- (3) 设计实现接入终端的认证；
- (4) 讨论接入认证的安全问题。

### 1.4 结果综述

- 1、使用路由器和交换机进行组网，实现了个 PC 之间的互联互通。
- 2、构建 802.1x 服务器，实现接入终端认证。在交换机上启动 802.1x 认证后，认证终端没有回答认证质询前，认证终端 PC 与相同网段 PC 可以 ping 通
- 3、在交换机上启动 802.1x 认证后，认证终端完成认证质询后，认证终端 PC 与不同网段 PC 可以 ping 通。

## 二、实验过程及结果

### 2.1 目的

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；  
网络接入安全方案设计与实现。

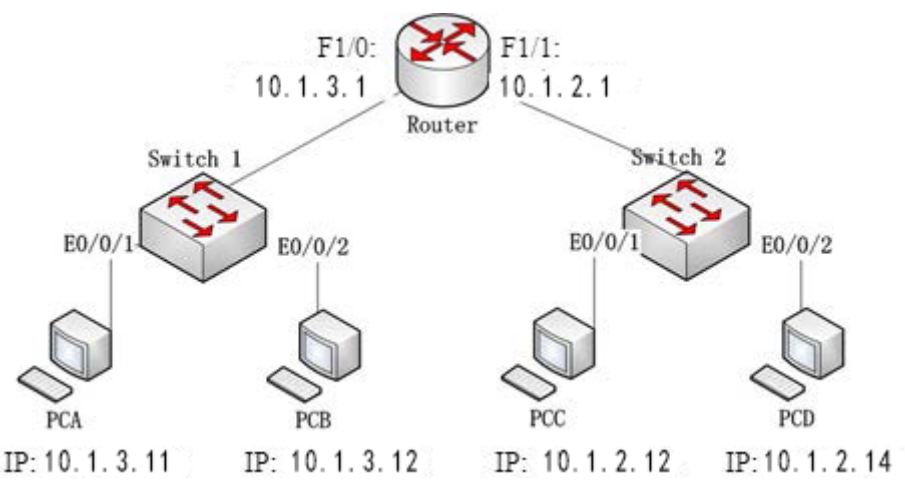
2.2 使用设备及软件

路由器 1 台（DCR2626-1），交换机 2 台，PC4 台

2.3 组网实验过程简述

组网试验：

步骤 1: 按照图示连接好设备，设置各 PC 的 IP 地址和默认网关；



图中 IP 即为我们自行分配的 IP 地址

步骤 2: 将交换机恢复为出厂设置。

步骤 3: 配置路由器 Router 的接口 IP 地址

2.4 实验结果描述

1) 在各台 PC 上使用 ping 命令检查网络连通情况，按表要求记录结果。

网络连通测试结果：

		所用命令	能否 ping 通
同一网段中	PCA ping PCB	ping 10.1.3.12	能
	PCB ping PCA	ping 10.1.3.11	能
不同网段中	PCA ping PCC	ping 10.1.2.12	能
	PCA ping PCD	ping 10.1.2.14	能

网络连通测试截图：

```
C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 10.1.3.11

正在 Ping 10.1.3.11 具有 32 字节的数据:
来自 10.1.3.11 的回复: 字节=32 时间=1ms TTL=128
来自 10.1.3.11 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.3.11 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.3.11 的回复: 字节=32 时间<1ms TTL=128

10.1.3.11 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms

C:\Users\Administrator>ping 10.1.3.12

正在 Ping 10.1.3.12 具有 32 字节的数据:
来自 10.1.3.12 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.3.12 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.3.12 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.3.12 的回复: 字节=32 时间<1ms TTL=128

10.1.3.12 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

同一网段连通测试

```
C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 10.1.2.14

正在 Ping 10.1.2.14 具有 32 字节的数据:
来自 10.1.2.14 的回复: 字节=32 时间=1ms TTL=127
来自 10.1.2.14 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.2.14 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.2.14 的回复: 字节=32 时间<1ms TTL=127

10.1.2.14 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms

C:\Users\Administrator>ping 10.1.2.12

正在 Ping 10.1.2.12 具有 32 字节的数据:
来自 10.1.2.12 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.2.12 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.2.12 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.2.12 的回复: 字节=32 时间<1ms TTL=127

10.1.2.12 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

不同网段连通测试

路由表:

```

Router_config_f0/3#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
        D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
        ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
        OE1 - OSPF external type 1, OE2 - OSPF external type 2
        DHCP - DHCP type

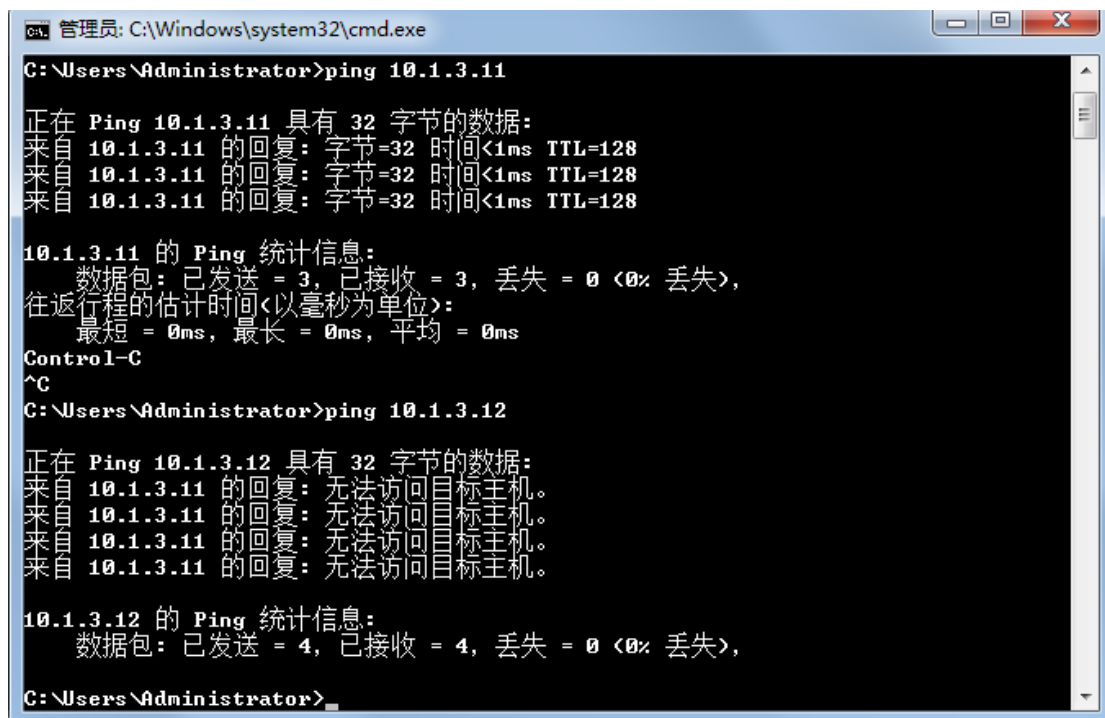
VRF ID: 0

C       10.1.2.0/24[0]         is directly connected, FastEthernet0/0[0]
C       10.1.3.0/24[0]         is directly connected, FastEthernet0/3[0]

```

路由器 R1 的路由表

测试启动 802.1x 认证后，认证终端回答认证质询前，同一网段 PC 能否互相 ping 通：



```

C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 10.1.3.11

正在 Ping 10.1.3.11 具有 32 字节的数据:
来自 10.1.3.11 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.3.11 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.3.11 的回复: 字节=32 时间<1ms TTL=128

10.1.3.11 的 Ping 统计信息:
    数据包: 已发送 = 3, 已接收 = 3, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
Control-C
^C
C:\Users\Administrator>ping 10.1.3.12

正在 Ping 10.1.3.12 具有 32 字节的数据:
来自 10.1.3.11 的回复: 无法访问目标主机。
来自 10.1.3.11 的回复: 无法访问目标主机。
来自 10.1.3.11 的回复: 无法访问目标主机。
来自 10.1.3.11 的回复: 无法访问目标主机。

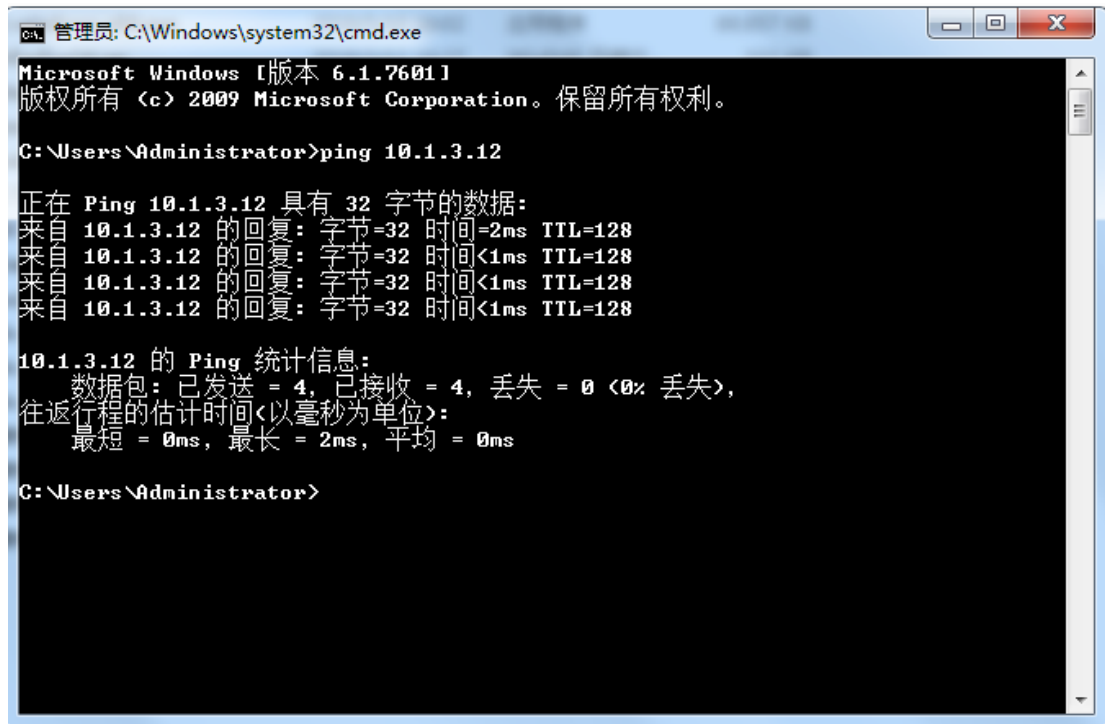
10.1.3.12 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

C:\Users\Administrator>

```

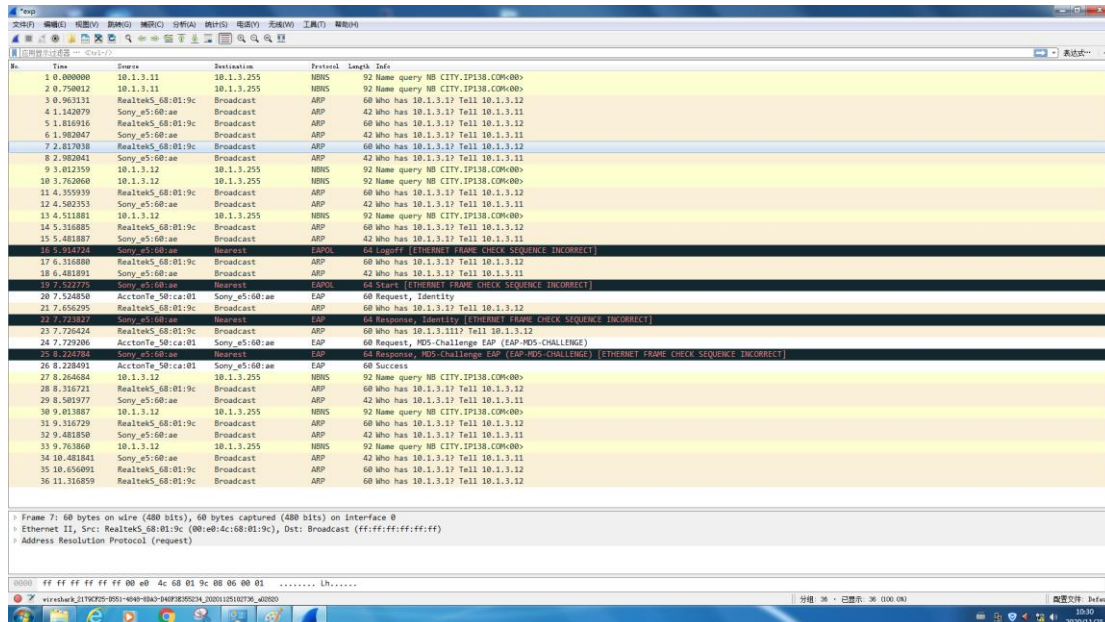
Ping 不通

测试启动 802.1x 认证后，认证终端回答认证质询后，同一网段 PC 能否互相 ping 通：



Ping 得通

Wireshark 捕获到的包：



2) 用 show ip route 查看 R1 的路由表，分析不同网段互通的原因，体会网关的作用？

原因：两个不同的交换机由路由器连接，可以实现不同网段的互通。

网关作用：将两个使用不同传输协议的网络段连接在一起。

## **2.5 遇到的问题及处理**

按书上步骤进行，较为顺利。

## **三、总结与体会**

此次实验为第一次实验，各种操作比较不熟悉，但还是比较成功的。掌握了路由器、交换机进行简单组网的方法，理解交换机、路由器的工作原理和网络接入安全方案设计与实现。

## 实验二：VLAN 的配置与协议分析

### 一、概述

#### 1.1 时间

2020.12.2 早上 8 点到 12 点

#### 1.2 地点

西一楼网络专题实验室 A201

#### 1.3 试验任务

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。

#### 1.4 结果综述

同一 VLAN 的两台计算机可以通信，不同 VLAN 之间的计算机不能通信。

完成 Trunk 端口配置后，同一 VLAN 之间计算机可以互通，不同 VLAN 之间计算机不能互通。

完成步骤 10 后不同 VLAN 间可以互相通信。

### 二、实验过程及结果

#### 2.1 目的

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。

#### 2.2 使用设备及软件



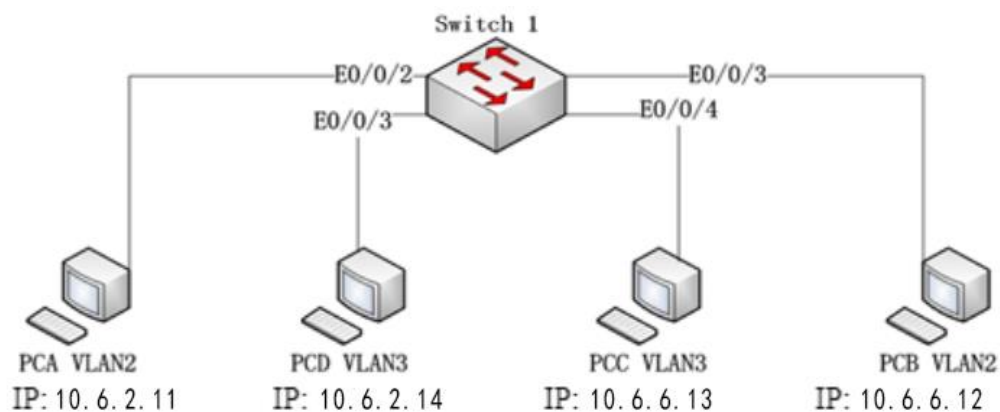
DCRS-5650 交换机 2 台

## 2.3 实验过程简述

### 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：按照下图连接好交换机和设备，并按照下图配置每个设备的 IP 地址；



图中 IP 即为我们自行分配的 IP 地址

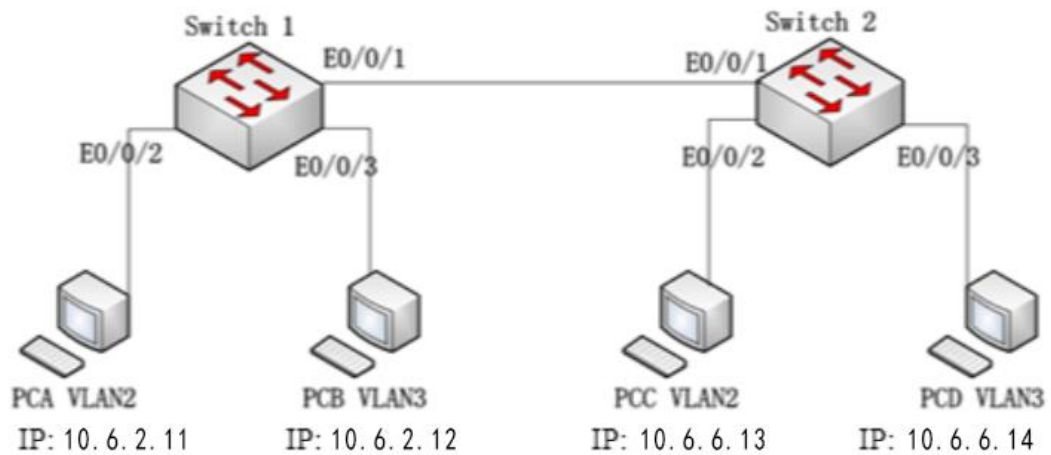
为交换机划分 VLAN

步骤 2：设置各 PC 的 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

步骤 4：按照如图所示更改设备的连接方式，配置各台计算机的 IP 地址，为交换机 S1、S2。各自划分 VLAN2 和 VLAN3；



图中 IP 即为我们自行分配的 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。

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。

### 3) VLAN tag 标记的分析

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

在 4 台 PC 上捕获报文，验证 PCA ping PCC 能否 ping 通。在 PCB 和 PCD 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。

### 4) 网卡注册表的修改（若可以捕获到可以不做）

如果在 windows 下无法捕获到含有 802.1q 标记的报文，就需要修改网卡 exp 的注册表项（确认网卡类型是 Realtek PCIe GBE Family Controller）。步骤

如下：

(1) 运行 regedit 程序。

(2) 在这个项目（网卡接口 exp 的对应注册表配置）下进行修改（添加）：

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Class{4D36E972-E325-11CE-BFC1-08002BE10318}\00nn 【注意：一般是 0011/12/13/14 之一】

MonitorModeEnabled: 1

MonitorMode: 1

PriorityVLANTag: 0

SkDisableVlanStrip: 1

(3) 修改完毕后关闭 regedit，把网卡 exp 禁用后重新启用。重启 wireshark 。

(4) 打开 wireshark 捕获 PCA ping PCC 的测试报文；

(5) 分析 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。

## 5) VLAN 间通信

步骤 8：在 4 台计算机上都运行 Ethereal 截获报文，执行 PCC ping PCD，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

步骤 10：配置 PCA 和 PCC 的网关为 10.6.2.1，配置 PCB 和 PCD 的网关为 10.6.3.1。同时，在 PCB 上用 Wireshark 监听捕获报文；执行 PCC ping PCD；观察能否 ping 通，说明原因。（如果 ping 不通，检查 S2 上镜像有没有关闭。）

2.4 实验结果描述

在配置好 VLAN 后，各机的连通情况如图：

		VLAN2		VLAN3	
		PCA	PCD	PCC	PCB
VLAN2	PCA	√	√	×	×
	PCD	√	√	×	×
VLAN3	PCC	×	×	√	√
	PCB	×	×	√	√

由此可见，划分 VLAN 后，相同 VLAN 间可以通信，不同 VLAN 间不能通信。

配置好 Trunk 端口后，各机联通情况如图：

		VLAN2		VLAN3	
		PCA	PCD	PCC	PCB
VLAN2	PCA	√	√	√	√
	PCD	√	√	√	×
VLAN3	PCC	√	√	√	√
	PCB	√	√	√	√

由此可见，在交换机之间的不同 VLAN 可以通过 trunk 端口联通。

步骤 8 中捕获到的报文：

转发过程及方向	VLAN 标记	原因
PCA-S1		收发不带 tag 的帧
S1-S2	802.1Q	Trunk 端口收发其他所有 VLAN 都带 tag
S2-PCC		收发本 VLAN 不带 tag 的帧

在完成步骤 10 后，由于对 VLAN2 和 VLAN3 配置了 IP，三层交换机就可以实现 VLAN 间的路由功能。

## 2.5 遇到的问题及处理

经过网卡注册表的修改后依旧只有一台 PC 能够捕获到 802.1Q 报文。

## 三、总结体会与建议

在实验中有部分机器的原因导致无法截获报文，其他情况比较顺利。了解了 VLAN 的作用，掌握了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。掌握了镜像端口和 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。

# 实验三：ARP 协议分析与欺骗防范

## 一、概述

### 1.1 时间

2020.12.9 早上 8 点到 12 点

### 1.2 地点

西一楼网络专题实验室 A201

### 1.3 试验任务

- (1) 采用三层交换机分别搭建图 3-1 和图 3-2 网络拓扑结构。
- (2) 通过在位于同一网段和不同网段的主机之间执行 ping 命令，截获报文，分析 ARP 协议报文结构，并分析 ARP 协议在同一网段和不同网段间的解析过程。
- (3) 分析 ARP 欺骗的手段，在 Cisco3560 三层交换机上构建基本防范能。

### 1.4 结果综述

分析同一网段的 ARP 包格式，不同网段的 ARP 请求和响应报文  
进行连通性测试分析原因  
见实验结果

## 二、实验过程及结果

### 2.1 目的

分析 ARP 协议报文首部格式，分析 ARP 协议在同一网段内和不同网段间的解析过程。分析 ARP 欺骗的基础和防范手段。

### 2.2 使用设备及软件

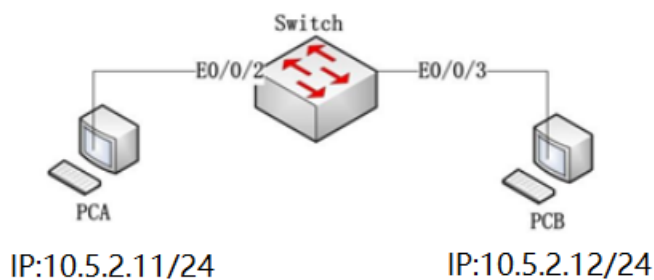
Cisco 3560 三层交换机 1 台

## 2.3 实验过程简述

### 1. ARP 协议分析

#### ○同一网段的 ARP 协议分析

步骤 1：按照图所示连接设备，配置计算机的 IP 地址。



步骤 2：在 PCA、PCB 的命令行窗口执行命令：

执行“arp -a”观察 arp 缓存；

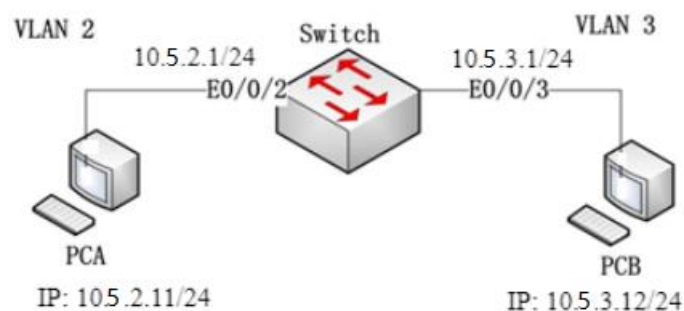
执行“arp -d”命令清空 arp 缓存。

步骤 3：在 PCA、PCB 上运行 Ethereal 截获报文；在 PCA 的命令行窗口执行“ping 10.5.2.12”。执行完之后，停止 PCA、PCB 上报文截获。分析截获的报文。

步骤 4：在命令行窗口执行“arp -a”，记录结果。

#### ○不同网段的 ARP 协议分析

步骤 5：按照图 3-2 所示连接设备，为交换机划分 VLAN，为 PC 机配置 IP 地址和网关。



## Cisco3560 交换机配置

### PCA 与 PCB 应能互通

步骤 6：首先执行“arp -d”清空缓存。在 PCA、PCB 上运行 Ethereal 捕获报文，执行命令“ping 10.5.2.22”。

步骤 7：执行“arp -a”命令，记录结果。

步骤 8：比较 PCA 和 PBB 捕获的报文进行比较。在自己一端捕获的报文中选中第一条 ARP 请求报文和第一条应答报文，填写表。

步骤 9：比较 ARP 协议在不同网段和相同网段内解析过程的异同。

## 2. MAC 与 IP 绑定实验

步骤 1：在图 3-2 基础上，定义与 PCA 对应的 MAC 地址访问控制列表 mac1。

步骤 2：定义与 PCA 对应的 IP 地址访问控制列表 ipac1。

步骤 3：在 fa0/2 端口启用 MAC 的访问列表 mac1 和 IP 访问列表 ipac1

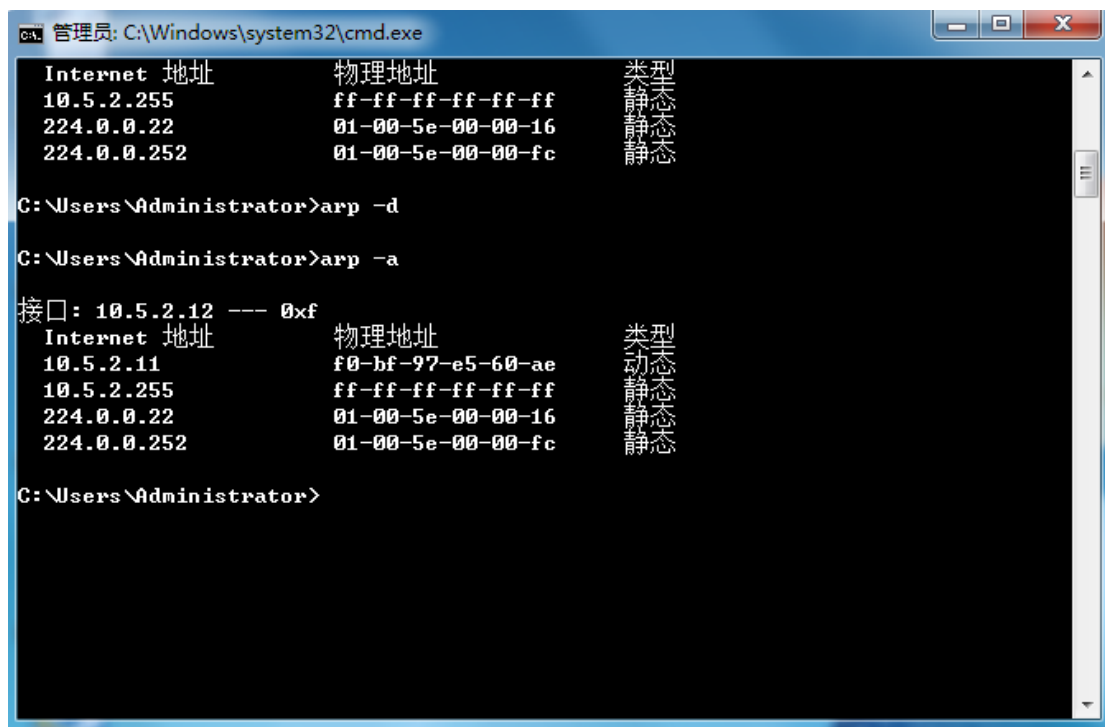
步骤 4：进行如下连通性测试，通过报文分析原因，记录结果。

- (1) 更换 PCA 的 IP 地址，如 10.5.2.13，接入端口仍为 fa0/2；
- (2) 为 Vlan2 添加端口 fa0/1，接入 PCA，IP 地址不变，即 10.5.2.11；
- (3) 将 PCC 替换 PCA 接入 fa0/2，使用 10.5.2.11 地址；
- (4) 将 PCC 替换 PCA 接入 fa0/2，使用 10.5.2.13 地址。

## 2.4 实验结果描述

1) 记录步骤 4 中“arp -a”的结果，写出其含义。



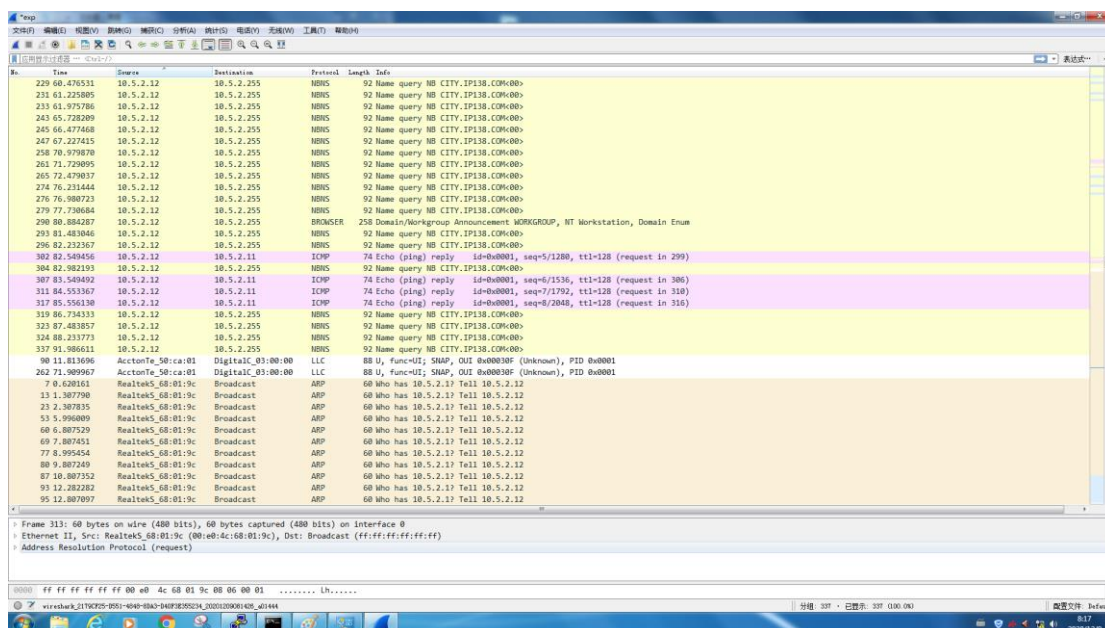


本电脑 IP 为 10.5.2.12，有 2 个 MAC 缓存

一个是 10.5.2.11，物理地址为 00-e0-4c-68-1e-0a，为动态地址

一个是 10.5.2.255，物理地址为 ff-ff-ff-ff-ff-ff，为静态地址

2) 观察同一网段的 arp 包格式，记录结果。



捕获到的 arp 包

字段	请求报文	应答报文
以太网链路层 Destination 项	ff:ff:ff:ff:ff:ff	00:e0:4c:68:01:9c
以太网链路层 Source 项	00:e0:4c:68:01:9c	f0:bf:97:e5:60:ae
ARP 报文发送者硬件地址	00:e0:4c:68:01:9c	f0:bf:97:e5:60:ae
ARP 报文发送者 IP	10.5.2.11	10.5.2.12
ARP 报文目标硬件地址	00:00:00:00:00:00	00:e0:4c:68:01:9c
ARP 报文目标 IP	10.5.2.12	10.5.2.11

3)完成步骤 7 后，分析不同网段的 ARP 请求和响应报文，填写下表。

```

C:\Windows\system32\cmd.exe
C:\Users\Administrator>arp -d
C:\Users\Administrator>arp -a
接口: 10.5.2.12 --- 0xf
Internet 地址      物理地址      类型
10.5.2.11          f0-bf-97-e5-60-ae 动态
10.5.2.255         ff-ff-ff-ff-ff-ff 静态
224.0.0.22         01-00-5e-00-00-16 静态
224.0.0.252        01-00-5e-00-00-fc 静态
C:\Users\Administrator>ping 10.5.2.11
正在 Ping 10.5.2.11 具有 32 字节的数据:
来自 10.5.2.11 的回复: 字节=32 时间<1ms TTL=127
来自 10.5.2.11 的回复: 字节=32 时间=1ms TTL=127
来自 10.5.2.11 的回复: 字节=32 时间=1ms TTL=127
来自 10.5.2.11 的回复: 字节=32 时间<1ms TTL=127

10.5.2.11 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 1ms, 平均 = 0ms
C:\Users\Administrator>

```

运行 arp -a 后的结果

字段	请求报文	应答报文
以太网链路层 Destination 项	ff:ff:ff:ff:ff:ff	00:e0:4c:68:01:9c
以太网链路层 Source 项	00:e0:4c:68:01:9c	00:12:cf:50:ca:00
ARP 报文发送者硬件地址	00:e0:4c:68:01:9c	00:12:cf:50:ca:00
ARP 报文发送者 IP	10.5.3.12	10.5.2.11
ARP 报文目标硬件地址	00:00:00:00:00:00	00:e0:4c:68:01:9c
ARP 报文目标 IP	10.5.2.11	10.5.3.12

4) 完成 3.10 节步骤 4 后，测试结果及原因是：

(1) 更换 PCA 的 IP 地址，如 10.5.2.13，接入端口仍为 fa0/2；

不连通，IP 与 MAC 地址不匹配。

(2) 为 Vlan2 添加端口 fa0/1，接入 PCA，IP 地址不变，即 10.5.2.11；

连通，IP 与 MAC 地址匹配，端口 fa0/1 没有加入映射表。

(3) 将 PCC 替换 PCA 接入 fa0/2，使用 10.5.2.11 地址；

不连通，IP 与 MAC 地址不匹配。

(4) 将 PCC 替换 PCA 接入 fa0/2，使用 10.5.2.13 地址。

不连通，IP 与 MAC 地址不匹配。

## 2.5 遇到的问题及处理

在实验过程中填写表格时有的数据抄错造成错误。

### 三、总结体会与建议

在获取和分析数据是要更用心。了解了 ARP 协议报文首部格式，分析了 ARP 协议在同一网段内和不同网段间的解析过程。了解了 ARP 欺骗的基础和防范手段。

## 实验四：TCP 协议分析

### 1.1 时间

2020.12.16 早上 8 点到 12 点

### 1.2 地点

西一楼网络专题实验室 A201

### 1.3 试验任务

应用 TCP 应用程序传输文件，截取 TCP 报文，分析 TCP 报文首部信息、TCP 连接的建立和释放过程、TCP 数据的编号与确认机制。

## 二、实验过程及结果

### 2.1 目的

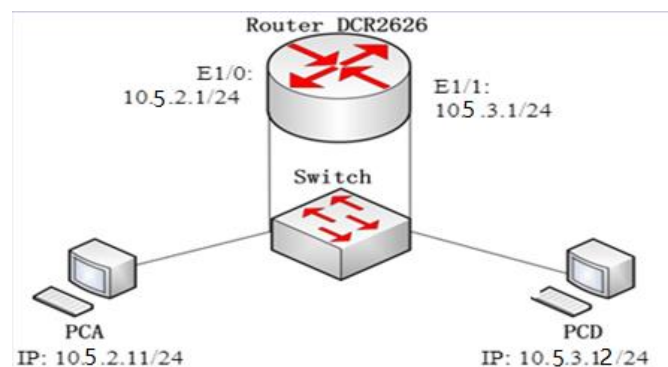
理解 TCP 报文首部格式和字段的作用，TCP 连接的建立和释放过程，TCP 数据传输中的编号与确认的过程。

### 2.2 使用设备及软件

路由器 1 台，交换机 1 台，PC 2 台，TCP 协议测试软件和报文捕获软件

### 2.3 实验过程简述

步骤 1：按图所示连接设备，为 PC 和路由器接口配置 IP。



本次实验中两台 PC 的 IP 地址配置分别为：10.5.2.11/24；10.5.3.12/24。

步骤 2：在 PCA 和 PCB 上开始截获报文。

步骤 3：在 PCA 和 PCB 上分别运行 TCP 协议测试软件，发送和接收一个约 300KB 的文件。文件传输完成后，停止报文截获。

步骤 4：观察截获的报文，分析 TCP 协议的建立过程的三个报文并填表

步骤 5：分析 TCP 连接的释放过程，选择 TCP 连接撤销的四个报文并填表

步骤 6：分析 TCP 数据传送阶段的报文，填表

步骤 7：TCPDebug 软件，调整发送时间间隔等参数，“发送缓冲长度”不得小于 2000，使得接收方的窗口有明显变化。

步骤 8：观察数据发送方和接收方的报文数据长度，推测原因。

步骤 9：在交换机上设置端口镜像，用 Wireshark 捕获报文进行分析，确定双方 TCP 数据长度不同的原因所在。

步骤 10：修改发送方的 Realtek PCIe GBE 网卡（如果是其他网卡，则作为接收方），网卡属性-> 配置->高级 ->“大量发送减负”为“关闭”。重新发送。

## **2.4 实验结果描述**

路由器配置结果：

```
192.168.1.50 - PuTTY

Router_config_e1/0#exit
Router_config#show interface e1/0
Ethernet1/0 is up, line protocol is up
address is 00e0.0f9c.2e57
MTU 1500 bytes, BW 10000 kbit, DLY 100 usec
Interface address is 10.5.2.1/24
Encapsulation ARPA, loopback not set
Keepalive not set
ARP type: ARPA, ARP timeout 00:03:00
60 second input rate 2904 bits/sec, 3 packets/sec!
60 second output rate 13 bits/sec, 0 packets/sec!
Half-duplex, 10Mb/s, 10BaseTX, 4162 Interrupt
4084 packets input, 355717 bytes, 100 rx_freebuf
Received 212 unicasts, 0 lowmark, 4084 ri, 0 rx_busy
0 input errors, 0 CRC, 0 framing, 0 overrun
0 long, 0 collisions, 0 discard, 0 no buffer
33 packets output, 1774 bytes, 50 tx_freebd, 0 underruns
0 output errors, 0 collisions, 0 late collisions
0 lost carrier, 0 output buffer failures

Router_config#show interface e1/1
Ethernet1/1 is up, line protocol is up
address is 00e0.0f9c.2e56
MTU 1500 bytes, BW 10000 kbit, DLY 100 usec
Interface address is 10.5.3.1/24
Encapsulation ARPA, loopback not set
Keepalive not set
ARP type: ARPA, ARP timeout 00:03:00
60 second input rate 2404 bits/sec, 2 packets/sec!
60 second output rate 59 bits/sec, 0 packets/sec!
Half-duplex, 10Mb/s, 10BaseTX, 3086 Interrupt
3029 packets input, 259525 bytes, 100 rx_freebuf
Received 195 unicasts, 0 lowmark, 3029 ri, 0 rx_busy
0 input errors, 0 CRC, 0 framing, 0 overrun
0 long, 0 collisions, 0 discard, 0 no buffer
38 packets output, 2004 bytes, 50 tx_freebd, 0 underruns
0 output errors, 0 collisions, 0 late collisions
0 lost carrier, 0 output buffer failures

Router_config#
```

## TCP 确认:

9 2.410791	10.5.3.12	10.5.2.11	TCP	66 49915 → 6005 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
10 2.411754	10.5.2.11	10.5.3.12	TCP	66 6005 → 49915 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11 2.411799	10.5.3.12	10.5.2.11	TCP	54 49915 → 6005 [ACK] Seq=1 Ack=1 Win=65536 Len=0

## TCP 撤销:

The image shows a Wireshark packet capture of a network interface. The packet list on the left shows several TCP segments and a NetBIOS name service request. The packet details pane on the right shows the structure of the selected packet (Frame 20), which is a NetBIOS name service request. The packet structure is as follows:

- Frame 20: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
- Ethernet II, Src: Sonys\_a5:60:ae (08:0f:97:e5:60:ae), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: Sonys\_a5:60:ae (08:0f:97:e5:60:ae)
- Type: IPv4 (0x0080)
- Internet Protocol Version 4, Src: 10.5.3.12, Dst: 10.5.3.255
- User Datagram Protocol, Src Port: 137, Dst Port: 137
- NetBIOS Name Service

The packet data is shown in hexadecimal and ASCII at the bottom of the packet details pane.

TCP 传送：

26	9.199407	10.5.3.12	10.5.2.11	TCP	1514 49915 → 6005 [ACK] Seq=1 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
27	9.199417	10.5.3.12	10.5.2.11	TCP	594 49915 → 6005 [PSH, ACK] Seq=1461 Ack=1 Win=65536 Len=540 [TCP segment of a reassembled PDU]
28	9.204076	10.5.2.11	10.5.3.12	TCP	60 6005 → 49915 [ACK] Seq=1 Ack=2001 Win=65536 Len=0
29	9.310285	10.5.3.12	10.5.2.11	TCP	1514 49915 → 6005 [ACK] Seq=2001 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
30	9.310295	10.5.3.12	10.5.2.11	TCP	594 49915 → 6005 [PSH, ACK] Seq=3461 Ack=1 Win=65536 Len=540 [TCP segment of a reassembled PDU]
31	9.314543	10.5.2.11	10.5.3.12	TCP	60 6005 → 49915 [ACK] Seq=1 Ack=4001 Win=65536 Len=0
32	9.420384	10.5.3.12	10.5.2.11	TCP	1514 49915 → 6005 [ACK] Seq=4001 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
33	9.420389	10.5.3.12	10.5.2.11	TCP	594 49915 → 6005 [PSH, ACK] Seq=5461 Ack=1 Win=65536 Len=540 [TCP segment of a reassembled PDU]
34	9.424451	10.5.2.11	10.5.3.12	TCP	60 6005 → 49915 [ACK] Seq=1 Ack=6001 Win=65536 Len=0
35	9.530280	10.5.3.12	10.5.2.11	TCP	1514 49915 → 6005 [ACK] Seq=6001 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
36	9.530290	10.5.3.12	10.5.2.11	TCP	594 49915 → 6005 [PSH, ACK] Seq=7461 Ack=1 Win=65536 Len=540 [TCP segment of a reassembled PDU]
37	9.534567	10.5.2.11	10.5.3.12	TCP	60 6005 → 49915 [ACK] Seq=1 Ack=8001 Win=65536 Len=0
38	9.640423	10.5.3.12	10.5.2.11	TCP	1514 49915 → 6005 [ACK] Seq=8001 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
39	9.640432	10.5.3.12	10.5.2.11	TCP	594 49915 → 6005 [PSH, ACK] Seq=9461 Ack=1 Win=65536 Len=540 [TCP segment of a reassembled PDU]
40	9.644793	10.5.2.11	10.5.3.12	TCP	60 6005 → 49915 [ACK] Seq=1 Ack=10001 Win=65536 Len=0

1) 分析截获的报文，记录 TCP 连接建立过程的三个报文和连接撤销过程的四个报文。

TCP 连接建立报文信息：

报文捕获计算机：

字段名称	第 1 条报文值及含义	第二条报文值及含义	第三条报文值及含义
报文发出计算机	10.5.3.12	10.5.2.11	10.5.3.12
捕获的报文序号	9	10	11
Sequence Number	0	0	1
Acknowledgement Number	0	1	1
ACK 标志	0	1	1
SYN 标志	1	1	0

TCP 连接撤销报文信息：

报文捕获计算机：



字段名称	第一条报文值及含义	第二条报文值及含义	第三条报文值及含义	第四条报文值及含义
报文发出计算机	10.5.3.12	10.5.2.11	10.5.2.11	10.5.3.12
捕获的报文序号	506	507	508	509
Sequence Number	303102	1	1	303103
Acknowledgement Number	1	303103	303103	2
ACK 标志	1	1	1	1
FIN 标志	1	0	1	0

2) 记录 TCP 数据传送阶段的前 12 个报文。

报文序号	报文种类 (数据/确认)	序号字段 Seq Number	确认号 Ack Number	数据 长度	确认到哪条 报文 (填序号)	窗口 大小
25	数据	1	1	1460		65536
26	数据	1461	1	540		65536
27	确认	1	2001	0	26	65536
28	数据	2001	1	1460		65536
29	数据	3461	1	540		65536
30	数据	1	4001	0	29	65536
31	数据	4001	1	1460		65536
32	确认	5461	1	540	32	65536

33	数据	1	6001	0		65536
34	数据	6001	1	1460		65536
35	数据	7461	1	540		65536
36	确认	1	8001	0	35	65536

3) 如何确定那条捕获的报文已被确认? 窗口值大小何时、何因由谁调整?

当确认号大小等于该报文的 Seq+Len 时, 该捕获的报文被确认。报文被捕获时, 窗口的大小改变。接收方因为缓冲区大小不足以及时完全接受发送方发来的数据, 接收端窗口变小, 告诉发送端一个信号, 使数据发送更慢。

## 2.5 遇到的问题及处理

在捕获 TCP 传输报文时, 发现发送几个数据报后才有一条应答报文, 原因是网络连接不畅通, 因为无法进行处理, 所以按照实验事实填写报告。

## 三、总结与体会

理解了 TCP 报文首部格式和字段的作用, TCP 连接的建立和释放过程, TCP 数据传输中的编号与确认的过程。

# 实验五：RIP 协议分析

## 一、概述

### 1.1 时间

2020.12.23 早上 8 点到 12 点

### 1.2 地点

西一楼网络专题实验室 A201

### 1.3 试验任务

- 1) 在路由器、三层交换机上依次配置静态路由、缺省路由和 RIP 协议，然后分别用 ping 命令测试网络的连通性。
- 2) 在路由器和三层交换机上配置 RIP 协议，在计算机上使用报文分析软件截获 RIP 报文，分析 RIP 报文各字段的含义。
- 3) 采用镜像技术，捕获两个路由设备之间交换的 RIP 报文，分析两个设备中路由表的构建情况。

### 1.4 结果综述

步骤 1 后在 R1 上不能 ping 通，步骤 2 后在 R1 上能 ping 通，步骤 4 之后能 ping 通。

## 二、实验过程及结果

### 2.1 目的

- 1) 理解路由协议的分类，掌握静态路由和 RIP 协议的配置方法；
- 2) 分析掌握 RIP 报文结构及各字段的含义；
- 3) 分析两个路由设备之间 RIP 报文的交换及路由表的构建过程。

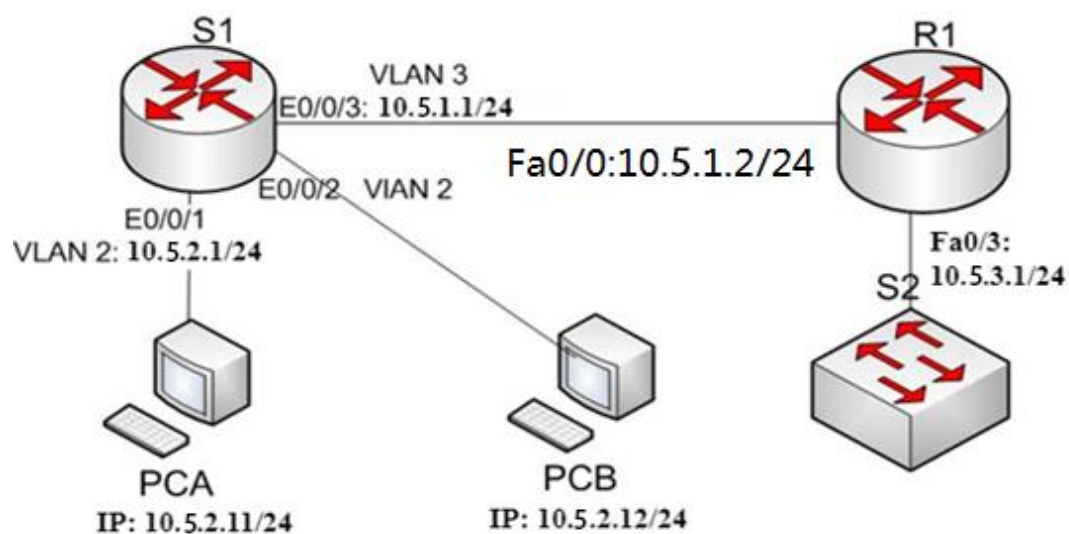
### 2.2 使用设备及软件

DCRS-5650 三层交换机 1 台（简称 S1），DCR2626 路由器 1 台（简称 R1），其他交换设备 1 台（简称 S2），PC 2 个。

## 2.3 实验过程简述

### 1) RIP 启动与路由分析

步骤 1：按照图 5-1 所示连接好设备，配置各 PC 的 IP 地址、子网掩码和网关。



配置交换机和路由器各接口的 IP 地址。

步骤 2：在 R1 上配置 10.5.2.0/24 的静态路由。

在 R1 上 ping 各 PC 看能否 ping 通，查看路由表，分析原因。

步骤 3：删除步骤 2 配置的静态路由

步骤 4：在 S1 和 R1 分别启动 RIP 协议。

测试连通性，查看 S1 和 R1 的路由表信息，将路由表信息填入检查单的表中，分析原因，回答相关问题。

### 2) RIP 报文捕获及结果分析

步骤 1：按照图 5-1 完成配置；

步骤 2：将交换机 S1 上与 R 相连接端口镜像到 E0/0/1 端口；

步骤 3：停止交换机 S1 上的 RIP 协议；

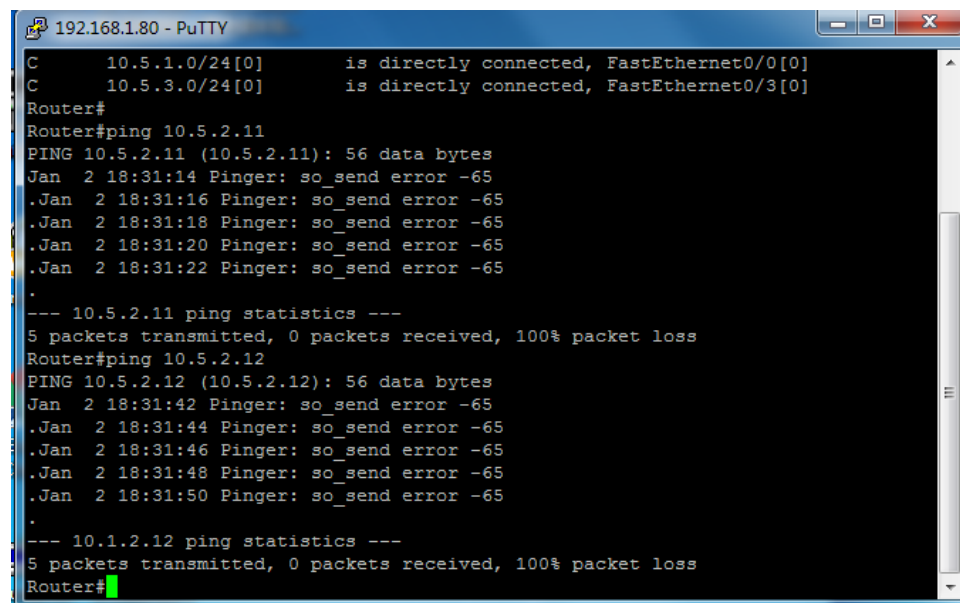
switch(Config)#no router rip

步骤 4：在 PCA 上运行 Ethereal 截获报文，然后在 S1 上启动 RIP 协议

观察截获 的请求报文和应答报文，选择一条 RIP 应答报文填写在表 5-2 中并理解其含义。

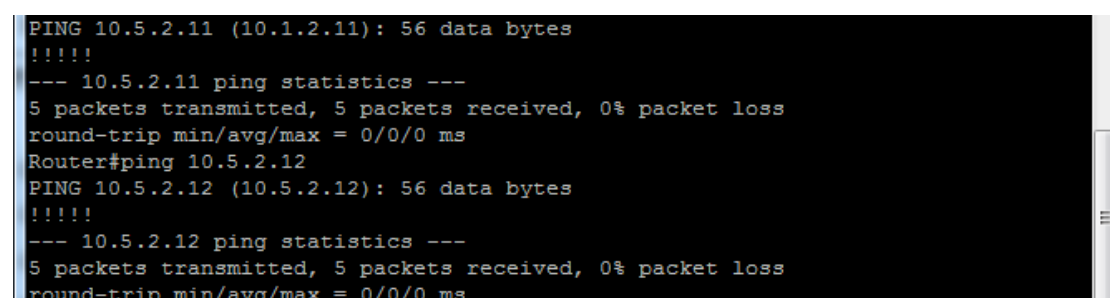
## 2.4 实验结果描述

1) 步骤 1 之后在 R1 上 ping 各台 PC，看能否 ping 通，分析路由表写出原因。



不能 ping 通， PCA， PCB 不在路由器所在子网中

2) 步骤 2 之后在 R1 上 ping 各台 PC，看能否 ping 通，分析路由表写出原因。



能 ping 通，访问 10.5.2.12 时，被转发到了交换机 10.5.2.1，而这个交换机链接

子网 10.5.2.0/24，可以找到 10.5.2.x 的路由。PCA，PCB 在路由器所在子网中。

3) 步骤 4 之后。

(a) 测试连通性（在 R1 上 ping 各台 PC，看能否 ping 通），记录连通性结果，写出原因。

```
Router#ping 10.5.2.11
PING 10.5.2.11 (10. .2.11): 56 data bytes
!!!!
--- 10.5.2.11 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/2/10 ms
Router#ping 10.5.2.12
PING 10.5.2.12 (10.5.2.12): 56 data bytes
!!!!
--- 10.5.2.12 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

启动 RIP 协议后，RIP 在 520 号端口上接收来自远程路由器的路由修改信息，并对本地的路由表做相应的修改，同时通知其他路由器。

(b) 填写 5-1

设备	Destination/Mask	Protocol	Pref	Cost	Nexthop	Interface
R1	10.5.2.0/24[0]	RIP	120	1	10.5.3.1	Ethernet1/0[0]
R1	10.5.3.0/24[0]	Connected				Ethernet1/0[0]
R1	10.5.4.0/24[0]	Connected				Ethernet1/0[0]
S1	10.5.2.0/24	Connected				Vlan2
S1	10.5.4.0/24	Connected				Vlan3
S1	10.5.4.0/24	RIP	120	2	10.5.3.2	Vlan3

4) 完成 7.8 节步骤 4 之后，分析所截获的报文，理解所截获的请求报文和应答报文的含义，将应答报文之一的各字段值填入表 5-2：

观察点:		字段	值	含义
IP		目的地址	224.0.0.9	报文目的地址
UDP		端口号	520	协议通信所使用的端口号
RIP	头部	命令字段	Response(2)	RIP 应答报文
		版本号	RIPv2(2)	RIP 版本号 2
	路由 信息	地址族标识	IP(2)	目的地址为 IP 地址
		网络地址	10.5.3.0	该字段描述的是 10.5.3.0 的路由
		跳数	1	该网络路由的所需跳数

## 2.5 遇到的问题及处理

网络拓扑结构连接错误导致无法 ping 通，修改连接后解决

## 三、总结体会与建议

理解了路由协议的分类，掌握静态路由和 RIP 协议的配置方法，分析掌握 RIP 报文结构及各字段的含义，分析两个路由设备之间 RIP 报文的交换及路由表的构建过程。

# 实验六：OSPF 路由协议分析

## 一、概述

### 1.1 时间

2020.12.30 早上 8 点到 12 点

### 1.2 地点

西一楼网络实验室 A201

### 1.3 实验任务

在路由器上启动 OSPF 协议，同时在计算机上运行 Ethereal 截获报文，详细分析 OSPF 的 5 种报文结构，掌握 OSPF 邻居建立及报文交换过程。

### 1.4 结果综述

OSPF 有 5 种报文结构，较为详细地描述了 OSPF 邻居建立以及报文交换的过程。

## 二、实验过程及结果

### 2.1 目的

详细分析 OSPF 的 5 种报文结构，掌握 OSPF 邻居建立及报文交换过程。

### 2.2 使用设备及软件

DCR-2626 路由器 2 台，DCR-5650 交换机 1 台，PC 4 台

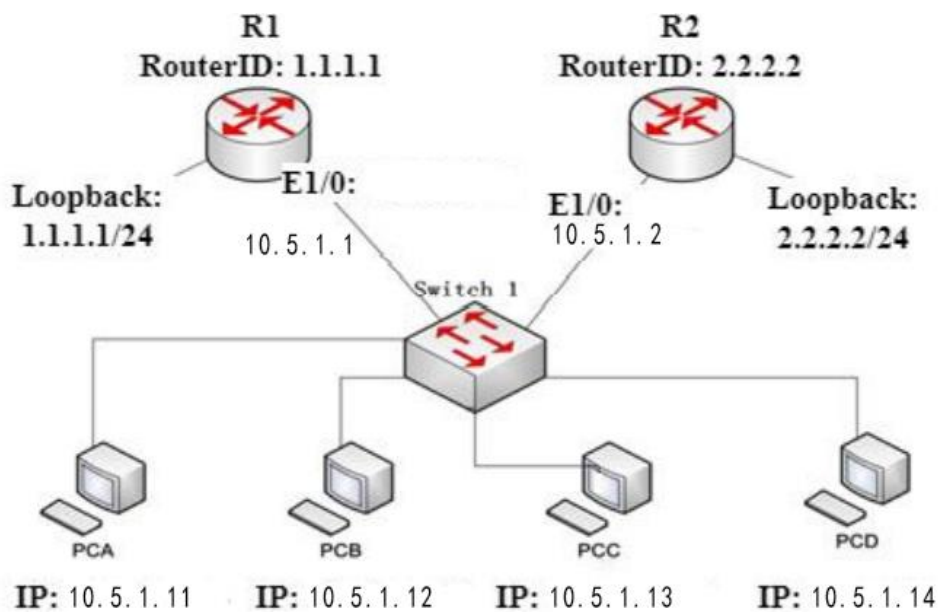
### 2.3 实验过程简述

步骤 1：按图连接好各实验设备，配置 IP 地址；交换机不用划分 VLAN，各端口 都在一个 VLAN 中。各台 PC 的 IP 地址分别是：10.5.2.11, 10.5.2.12, 10.5.2.13, 10.5.2.14。

交换机不用划分 VLAN，各端口都在一个 VLAN 中。各台 PC 的 IP 地址分别是：

10.5.1.10, 10.5.1.11, 10.5.1.12, 10.5.1.13。





步骤 2：将交换机上连接两个路由器的端口镜像到其中一台 PC 连接的端口上。例：若两个路由器连接到交换机的 25、26 口，PCA 连接在交换机的 1 口，将 25、26 口的流量镜像到 1 端口的命令如下：

```
switch(Config)#monitor session 1 source interface Ethernet 0/0/25-26 both
switch(Config)#monitor session 1 destination interface Ethernet 0/0/1
```

步骤 3：在每台 PC 上运行 Ethereal 软件，开始截获报文。

步骤 4：配置两台路由器，启动 OSPF 协议，并在接口上指定相应的 OSPF 区域，路由器 R1 配置的参考命令如下：

```
Router_config#interface loopback0 !配置环回接口
Router_config_l0#ip address 1.1.1.1 255.255.255.0
Router_config#interface e1/0 !配置 Ethernet0 接口
Router_config_e1/0#ip address 168.1.1.1 255.255.255.0
Router_config_e1/0#no shutdown
Router_config#router ospf 1 !启动 ospf 进程，进程号为 1
Router_config_ospf_1#network 168.1.1.0 255.255.255.0 area 0 ! 指定 OSPF 区
```

域

Router\_config\_ospf\_1#network 1.1.1.0 255.255.255.0 area 0

同理配置 R2 路由器。

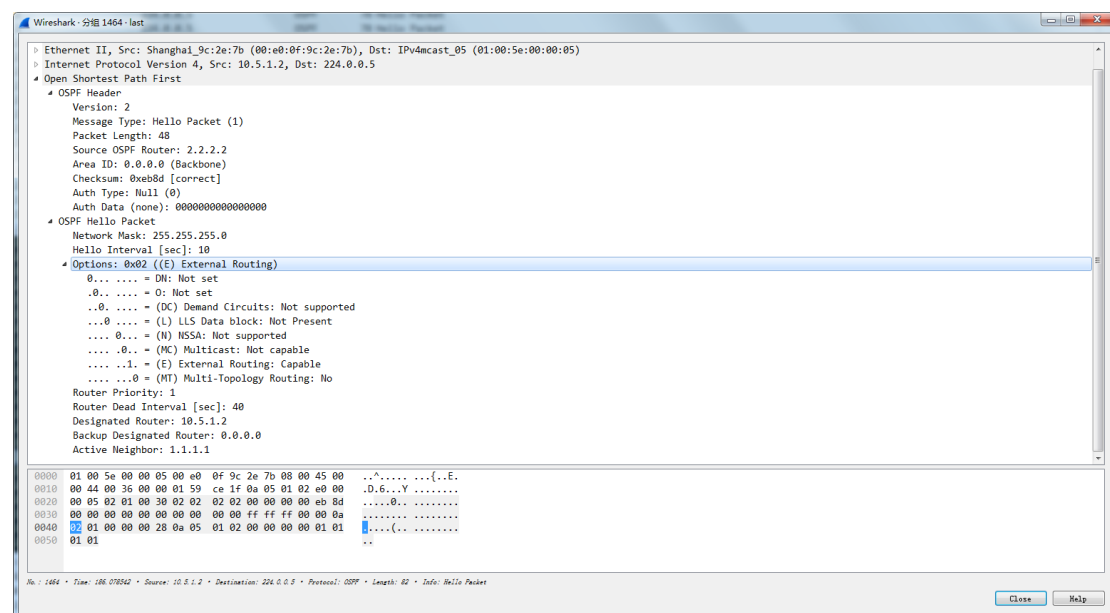
步骤 5：“show ip route”查看路由表，如果出现了 ospf 路由，则说明两台路由器成功建立了邻居关系并交换了路由信息。在 PC 上停止报文截获。

## 2.4 实验结果描述

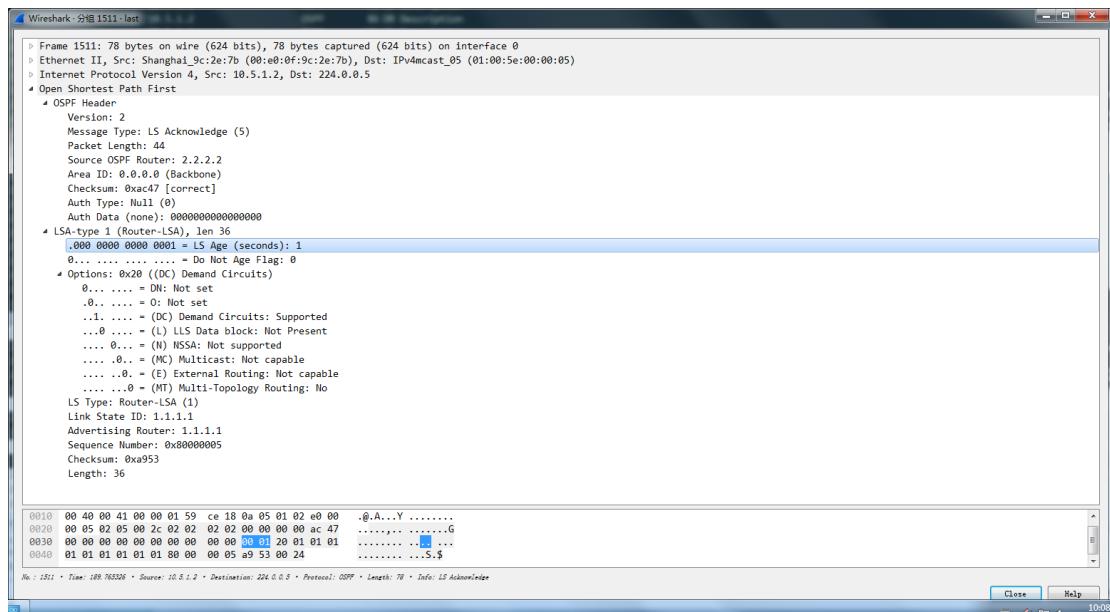
1) 针对自己截获的报文，写出其包含的 ospf 报文的含义（每类挑选一条）；

结合实验获得的报文，简要描述 ospf 协议邻居建立和数据库同步的过程。

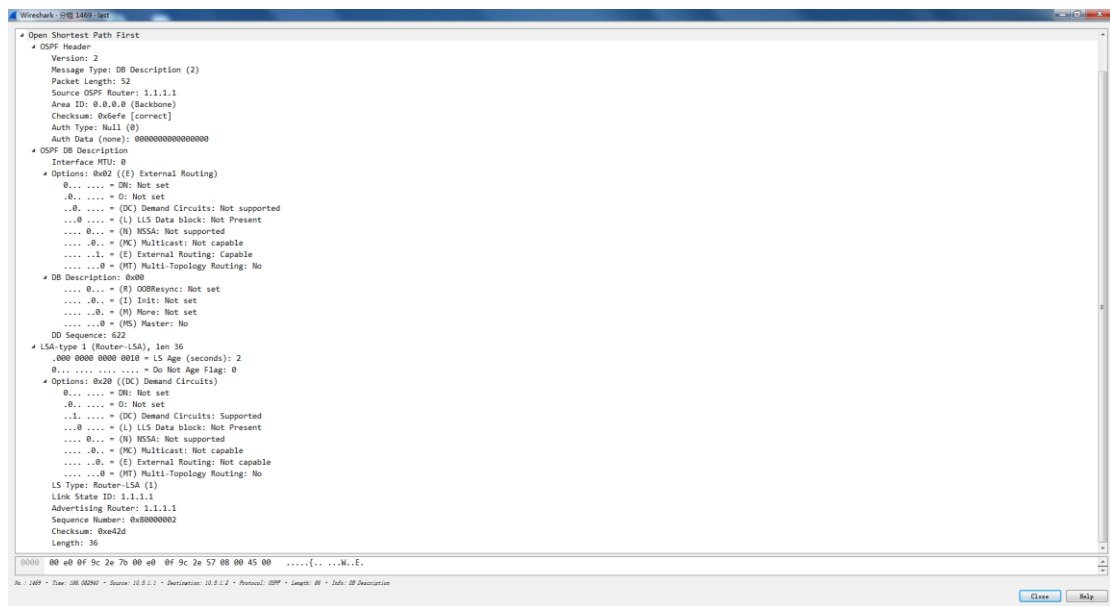
截获的报文：



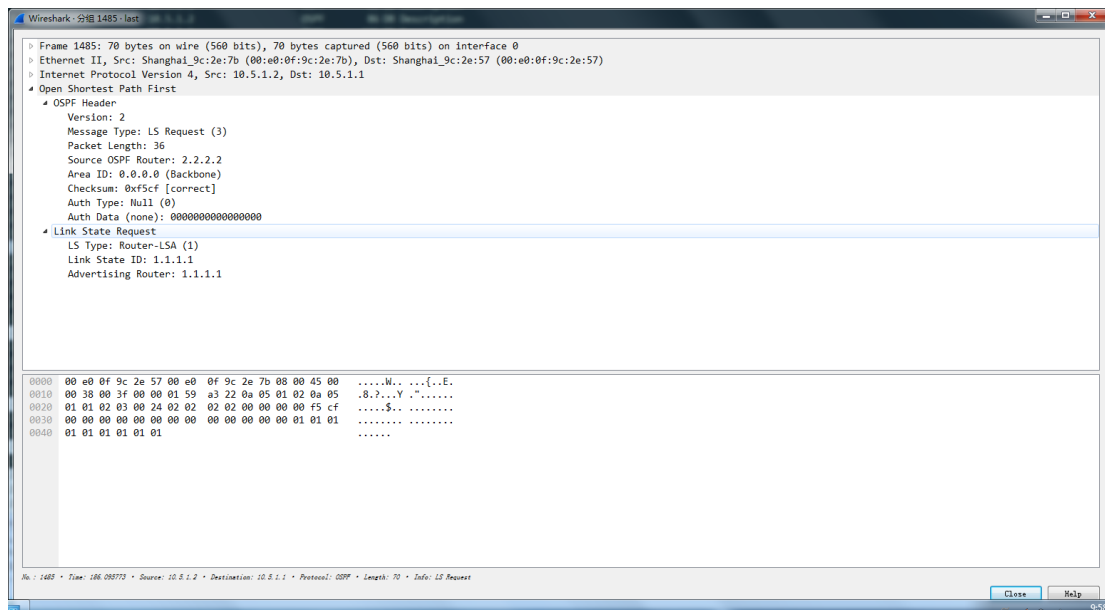
Hello 报文



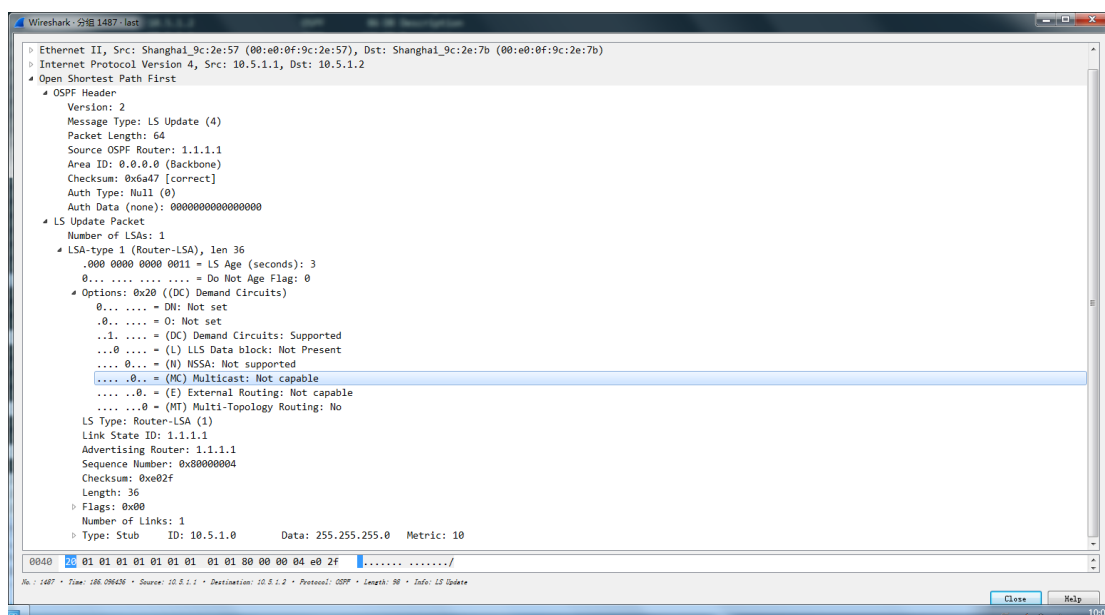
## LsAck 报文



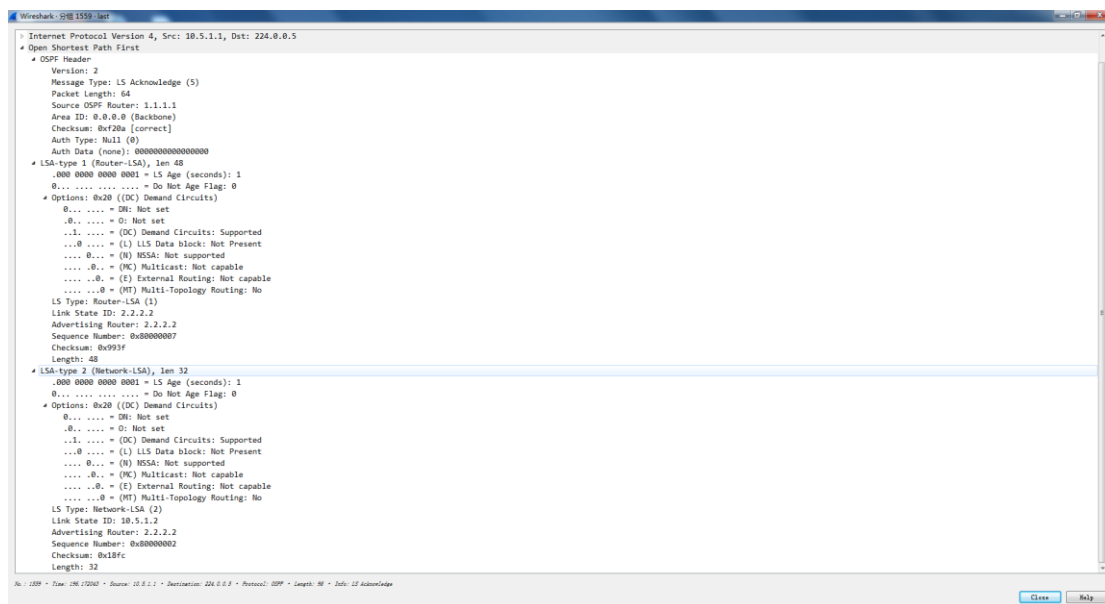
## LsDD 报文



## LsRequest 报文



## LsUpdate 报文



## R-Lsa 报文

2) 说明路由器 R1、R2 中产生的 OSPF 路由表项的含义？

R2 路由器的路由表项及含义：

路由表项： O 1.1.1.1/32[0] [110, 11] via 10.5.1.1 (on Asy010[0])  
 含义： 使用 OSPF 传输，目标 1.1.1.1，优先级 110，cost 为 11

路由表项： C 2.2.2.0/24[0] is directly connected Loopback 0[0]  
 含义： 目标 2.2.2.0 直连，端口为 Loopback 0[0]

路由表项： C 10.5.1.0/24[0] is directly connected Ethernet 1/0[0]  
 含义： 目标 10.5.1.0 直连，端口为 Ethernet 1/0[0]

## 2.5 遇到的问题及处理

经常敲错命令导致一直达不到想要的结果，经常检查就可以解决。

## 三、总结体会与建议

详细分析了 OSPF 的 5 种报文结构，掌握了 OSPF 邻居建立及报文交换过程。