计算机网络综合实验报告

易凯
人工智能与机器人研究所
西安交通大学软件学院
yikai2015@stu.xjtu.edu.cn

Abstract

中文摘要：这篇实验报告是 2018 年春季《计算机网络实验》的七次实验综合总结，该系列实验旨在从理解掌握计算机基础理论的基础之上，对计算机网络核心部分的交换机和路由器进行掌握，从软硬件协同的角度对网络进一步深入理解。该系列实验由七个不同实验构成，分别为组网与接入认证，VLAN 配置与协议分析，ARP 协议分析与欺骗防范，TCP 协议分析，RIP 协议分析，OSPF 路由协议分析和 IPv6。其实验的基本范式是首先根据制定的实验任务完成网络拓扑结构的搭建，然后在此基础上对交换机、路由器等网络设备进行配置，最后则是针对特定任务捕获报文并对报文进行分析。通过系列实验，掌握了相关基础理论，为之后的进一步学习奠定了基础。

Abstract: This experimental report is a comprehensive summary of the seven experiments in the computer network experiment in spring 2018. The series of experiments are designed to grasp the switches and routers in the core part of the computer network and understand the network further from the perspective of hardware and software collaboration from the basis of understanding and mastering the basic computer theory. The series of experiments are composed of seven different experiments, which are networking and access authentication, VLAN configuration and protocol analysis, ARP protocol analysis and deception prevention, TCP protocol analysis, RIP protocol analysis, OSPF routing protocol analysis and IPv6. The basic paradigm of the experiment is to complete the construction of network topology based on the experimental task, and then configure the network equipment such as switches and routers on this basis, and finally to capture messages for specific tasks and analyze the message. Through a series of experiments, we have grasped the relevant basic theories and laid the foundation for further study.

该实验报告作者为西安交通大学 2015 级本科生易凯，学号为 2151601053，研究方向为受脑认知启发的人工智能，机器视觉，机器学习基础理论与计算心理学。

目录

图

表

1 基本说明

1.1 实验概述

该实验报告为《计算机网络专题实验》系列实验整合报告书，实验时间为 2018 年 5 月 29 日–2018 年 7 月 7 日，实验地点为西安交通大学兴庆校区西一楼电信学院 201。

1.2 实验目标

该系列实验的实验目标为在理解与掌握计算机网络基础理论的基础之上，学会网络组件中交换机与路由器的多种使用，从而以实践为根基提升对网络的深入理解，从而对计算机网络有着更加深入地掌握，在软硬件协同的角度，为之后的进一步学习打下基础。

1.3 实验的一般化流程

1. 基于实验室硬件资源按照拓扑结构对网络进行搭建；

2. 针对不同实验的基本情况对交换机与路由器进行配置；

3. 对特定实验的报文数据进行捕获并进行分析。

2 组网与接入认证

2.1 实验目的

A. 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。

B. 网络接入安全方案设计与实现。

2.2 实验内容

A. 使用路由器和交换机进行组网，实现各 PC 间的互联互通。

B. 802.1x [1] 认证服务器的构建。

C. 设计实现接入终端的认证。

D. 讨论接入认证的安全问题。

2.3 实验环境与拓扑结构

2.3.1 实验环境

该实验要求四人一组，分配 DCR2626 路由器 [2] 一台，交换机两台。

2.3.2 拓扑结构

该实验的拓扑结构如图 1 所示：

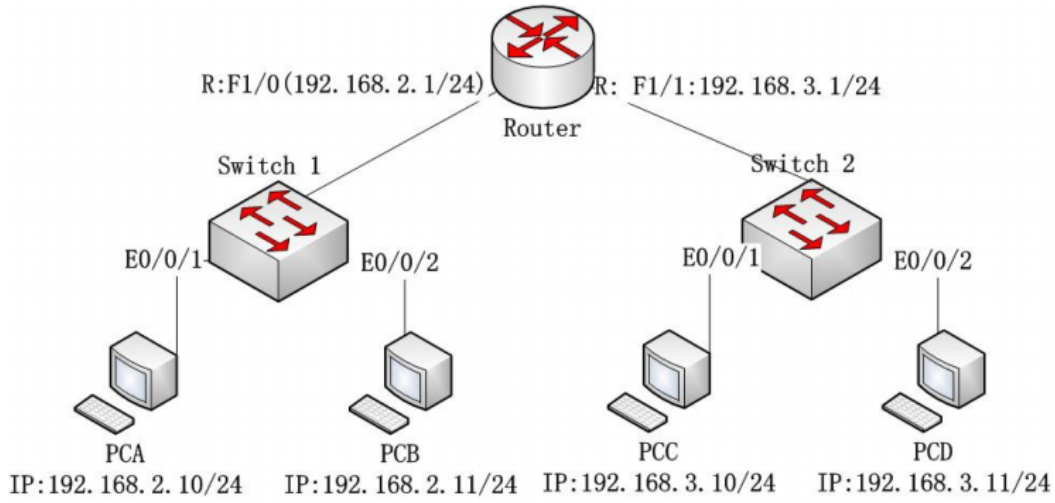

图 1: 实验一网络拓扑结构

2.4 实验步骤与结果

2.4.1 终端互通检验

A. 按照拓扑图搭建网络，设置各 PC 的 IP 地址与默认网关，如图 2 所示。

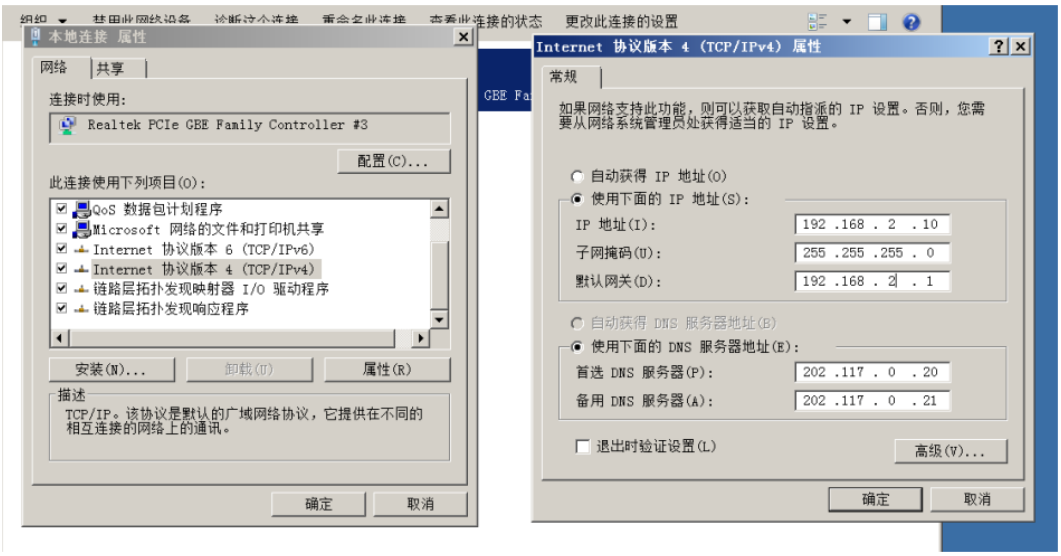

图 2: IP 地址与默认网关分配

B. 配置路由器 Router 的接口 IP 地址，f0/0 接口的配置命令如下：

```
Router>enable
```

表 1: 网络连通情况测试

		命令	能够 Ping 通
同一网段中	PCA ping PCB	ping 192.168.2.11	能
同一网段中	PCC ping PCD	ping 192.168.3.11	能
不同网段中	PCB ping PCC	ping 192.168.3.10	能
不同网段中	PCD ping PCA	ping 192.168.2.10	能

```
Router#config
Router_config#interface f0/0
Router_config_f0/0#ip address 192.168.2.1 255.255.255.0
Router_config_f0/0#no shutdown
Router#show interface f0/0
```

C. 在各台 PC 上使用 ping 命令检查网络连接情况，并记录结果如表 **??** 所示。

3 是实验的部分截图。

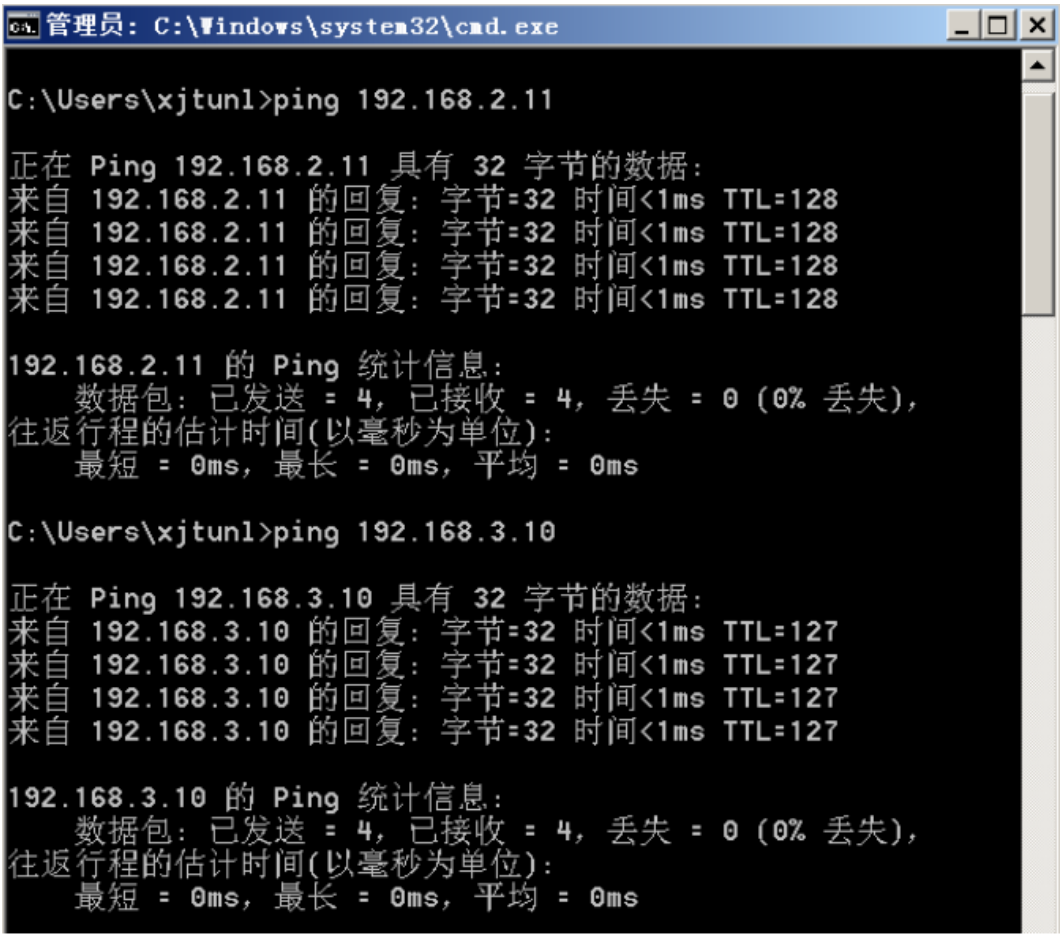

图 3: 网络连通情况测试实验截图

D. 查看路由器路由表，实验结果如图 4。

```
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      192.168.2.0/24[0]    is directly connected, FastEthernet0/0[0]
C      192.168.3.0/24[0]    is directly connected, FastEthernet0/3[0]
Router_config_f0/3#
```

图 4: 路由器路由表信息

其中，由于路由表中存在两个网络之间的路由信息，所以数据可以通过路由器进行跨网段的转发，不同网段也可以互通。

2.4.2 802.1x 接入安全认证

A. 构建 802.1x 认证服务器：将 WinRadius14.zip 解压

B. 配置访问认证数据库连接。

a) 在认证服务器上打开 WinRadius，配置 ODBC、生成 ODBC 连接

b) 添加认证账户

c) 更改认证服务器的密钥

C. 使用如下命令配置认证交换机。

```
DCRS-5650(config)#interface vlan 1
DCRS-5650(config-if-vlan1)#ip address 192.168.2.111 255.255.255.0
DCRS-5650(config-if-vlan1)#no shutdown
DCRS-5650(config)#radius-server authentication host 192.168.2.11
DCRS-5650(config)#radius-server key WinRadius
DCRS-5650(config)#aaa enable
DCRS-5650(config)#dot1x enable
DCRS-5650(config)#interface ethernet0/0/1
DCRS-5650(config-ethernet0/0/1)#dot1x enable
DCRS-5650(config-ethernet0/0/1)#dot1x port-control auto
DCRS-5650(config-ethernet0/0/1)#dot1x port-method portbased
DCRS-5650(config-ethernet0/0/1)#show run
```

D. 配置认证客户端，并使用 2 中设置的用户名和密码登录。

E. 登陆后确保已经认证，此后即可 ping 通其他终端 PC。

2.5 实验小结

通过组网与用户认证的实验，我们对于网络基本连接的访问以及 802.1x 接入认证有了较为深入的认识。总体说来，本次实验是后续实验的基础，虽然配置 802.1x 接入认证的认证服务器数据库上花费了较大精力，但是总体而言还是为之后的进一步学习买下了伏笔。

3 VLAN 配置与协议分析

3.1 实验目的

A. 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。

B. 掌握镜像端口的配置方法，了解 VLAN 数据帧的格式、VLAN 标记添加和删除的过程。

3.2 实验内容

A. 在一台交换机上划分 VLAN，用 ping 命令测试连通性。

B. 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。

C. 配置端口镜像，截获 VLAN 数据帧，分析 VLAN 数据帧的格式和 VLAN 标记添加和删除的过程。

3.3 实验环境与拓扑结构

3.3.1 实验环境

4 人一组，DCRS-5650 交换机 2 台。

3.3.2 拓扑结构

该实验拓扑结构分为同一交换设备上配置 VLAN 以及利用 Trunk 端口 [3] 在两台设备上配置 VLAN 构成，其拓扑结构分别如 5, 6 所示。

3.4 实验步骤与结果

3.4.1 同一交换设备上配置 VLAN

A. 按照图 5 连接好设备，设置交换机划分 VLAN，其中 VLAN2 的命令如下：

```
switch(Config)#vlan 2
```

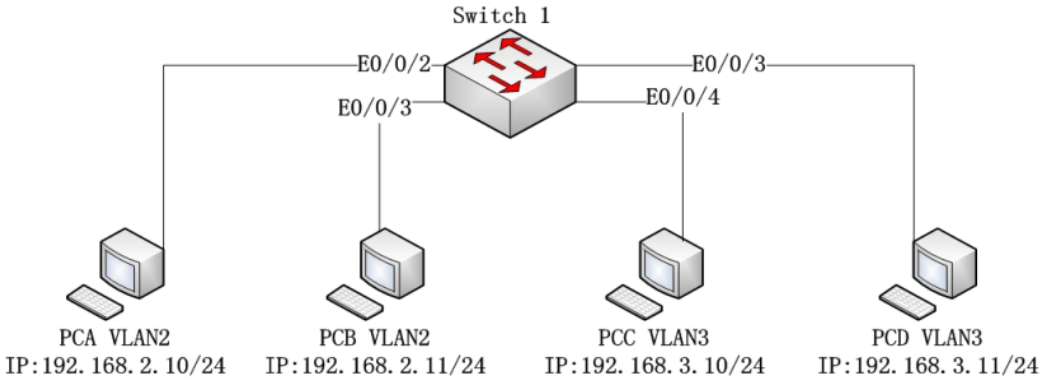

图 5: 同一交换设备上配置 VLAN

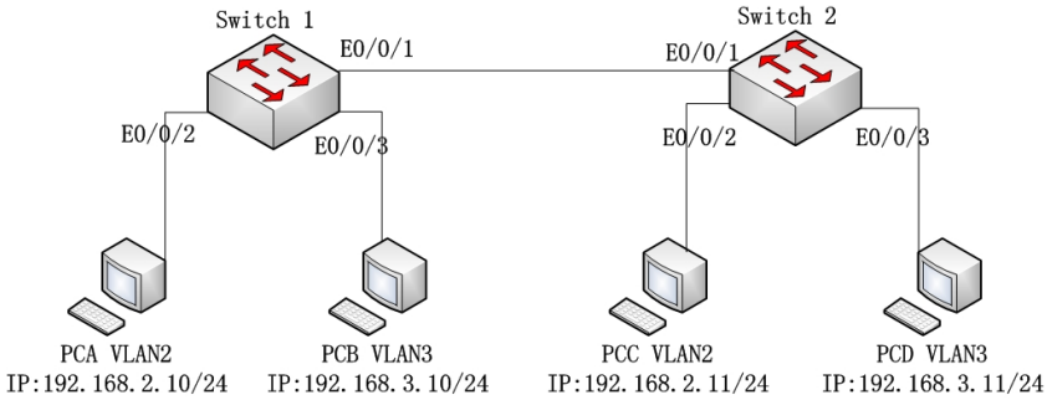

图 6: 利用 Trunk 端口在两台设备上配置 VLAN

```
switch(Config-vlan2)#switchport interface Ethernet 0/0/2-3
switch(Config-vlan2)#exit
switch#show vlan
```

B. 按照图 5 设置各 PC 的 IP 地址。

C. 用 ping 命令验证同一 VLAN 和不同 VLAN 间的计算机能否通信。

结果表明，相同 VLAN 之间可以进行通信，而不同 VLAN 之间不能够进行通信，原因是没有两个 VLAN 之间的路由信息。

实验的截图如 7 所示。

3.4.2 利用 **Trunk** 端口在两台设备上配置 **VLAN**

A. 按照图 5 连接设备，配置各台计算机的 IP 地址。为交换机 S1 和 S2 划分 vlan 2 和 vlan 3。

B. 验证各 PC 间是否能 ping 通。

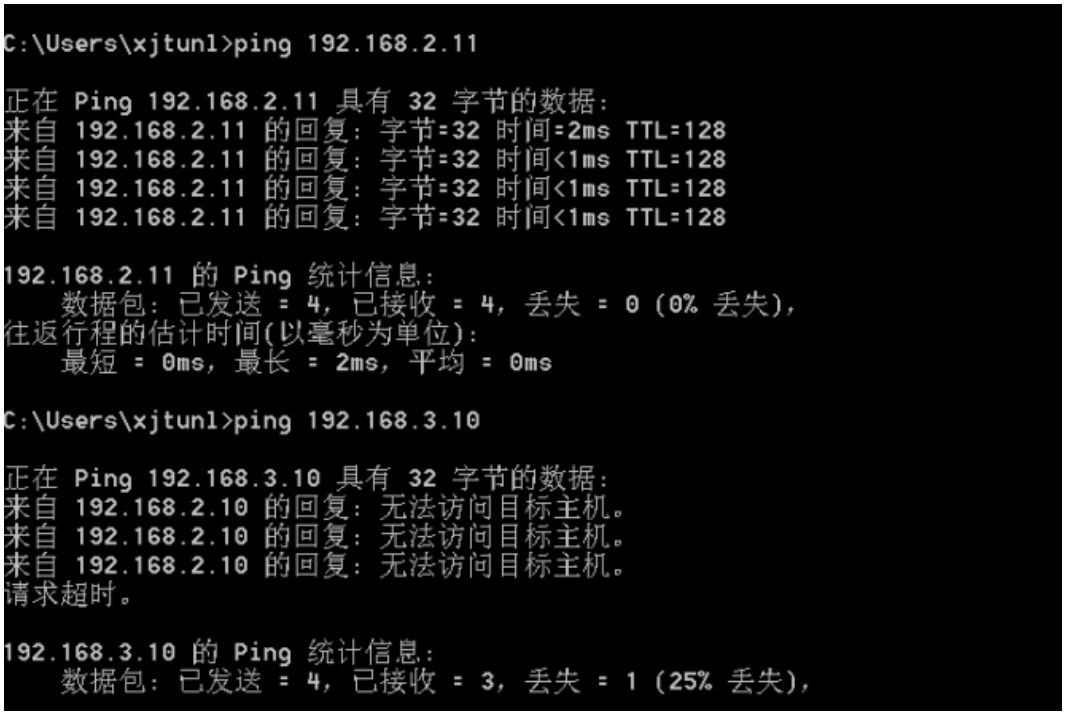

图 7: VLAN 通信的实验截图

实验结果表明，任意两个 PC 之间均无法 ping 通。其原因主要为同一 VLAN 下无法构成交换机间的连接而无法 ping 通，而不同 VLAN 下则是由于没有不同 VLAN 之下的路由转发信息而无法 ping 通。

C. 在 2 个交换机上配置 trunk 端口，并将 trunk 端口加入 vlan 2 和 vlan 3。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
```

D. 测试相同 VLAN 和不同 VLAN 之间是否可以 ping 通。

实验结果表明，相同 VLAN 之间可以 ping 通，原因是设置 trunk 后两个交换机的信息可以共享，而不同 VLAN 之间仍然不能 ping 通，原因是此处仍然没有两个 VLAN 之间的路由信息。实验的截图如图 8 所示。

E. 在交换机 S1 上设置端口镜像，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
```

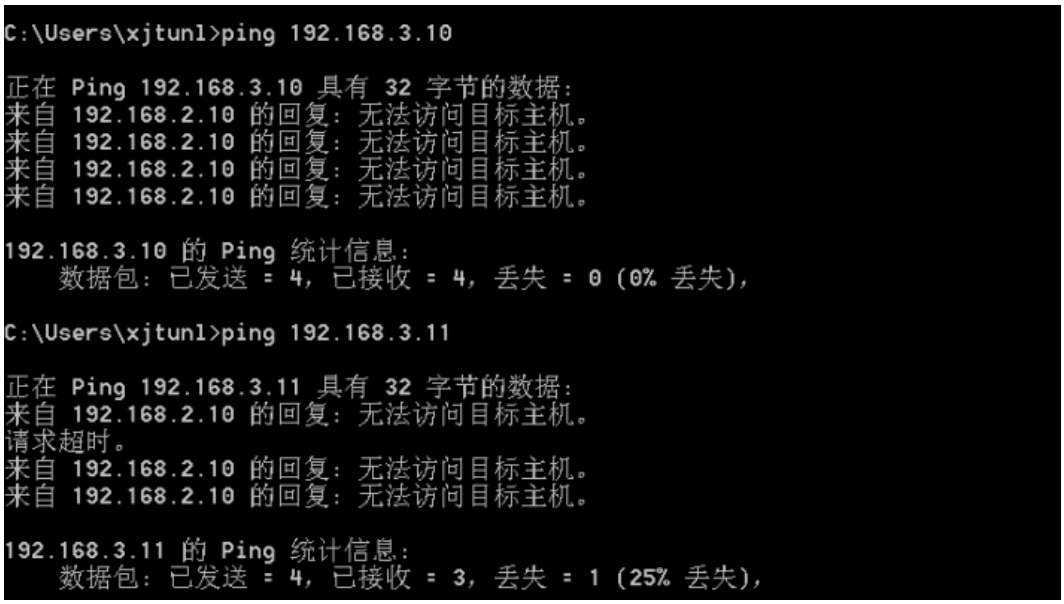

图 8: 使用 Trunk 的 VLAN 连通性测试

表 2: VLAN 包转发过程以及对应 VLAN 标记值

转发过程与方向	VLAN 标记值	标记出现与否的原因
PCA <- S1	无	经过交换机会进行解封装操作
S1 <- S2	8100	交换机之间进行信息交流会封装 Tag
S2 <- PCC	无	主机发出的帧不带 Tag

F. 在 4 台 PC 上捕获报文，验证 PCA ping PCC 是否能 ping 通。在 PCB 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。

实验结果表明，PCA ping PCC 可以 ping 通。转发过程以及对应 VLAN 的标记值如表 **??** 所示

3.4.3 VLAN 之间通信

A. 在交换机 S1 上配置 VLAN2 和 VLAN3 的接口 IP 地址，VLAN2 的 IP 地址为 192.168.2.1/24，VLAN3 的接口 IP 地址为 192.168.3.1/24。VLAN2 配置参考命令如下所示：

```
switch(Config)#interface vlan 2
switch(Config-If-Vlan2)#ip address 192.168.2.1 255.255.255.0
switch(Config-If-Vlan2)#no shutdown
switch(Config-If-Vlan2)#exit
```

B. 配置 PCA 和 PCC 网关为 192.168.2.1，配置 PCB 和 PCD 的网关为 192.168.3.1。执行 PCC ping PCD，观察能否 ping 通，说明原因。

实验结果表明，PCC ping PCD 可以 ping 通，原因是在设置 VLAN 接口的 IP 地址后，交换机在网络层建立了 VLAN 间的路由信息，从而使得不同网段下可以通信。

3.5 实验小结

通过本次实验，对于 VLAN 的基本配置以及不同网络 IP 对应的相关信息有了进一步较为深入的认识，对 IP 划分的实践以及 VLAN 之间的通信方法有了进一步的理解，为之后的进一步学习奠定了基础。

4 ARP 协议分析与欺骗防范

4.1 实验目的

A. 分析 ARP [4] 协议报文首部格式。

B. 分析 ARP 协议在同一网段内和不同网段间的解析过程。

C. 分析 ARP 欺骗的基础和防范手段。

4.2 实验内容

A. 分析 ARP 协议报文首部格式。

B. 分析 ARP 协议在同一网段内和不同网段间的解析过程。

C. 分析 ARP 欺骗的基础和防范手段。

4.3 实验环境与拓扑结构

4.3.1 实验环境

2 人一组，3 层交换机一台（Cisco3560）

4.3.2 拓扑结构

实验的拓扑结构分在在同一网段之下以及在不同网段之下两个部分构成, 拓扑结构的图分别如 9, 10 所示。

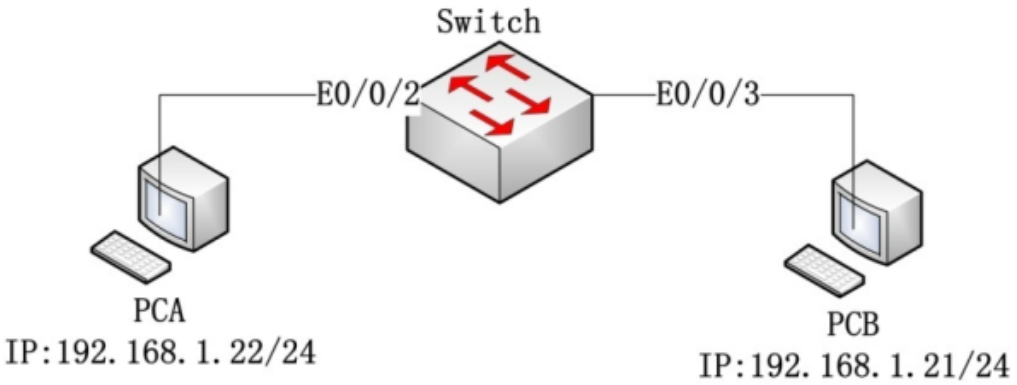

图 9: 同一网段之下的 ARP 组网图

4.4 实验步骤与结果

4.4.1 同一网段 ARP 协议分析

A. 按照图 9 连接设备，配置对应的 IP 信息；

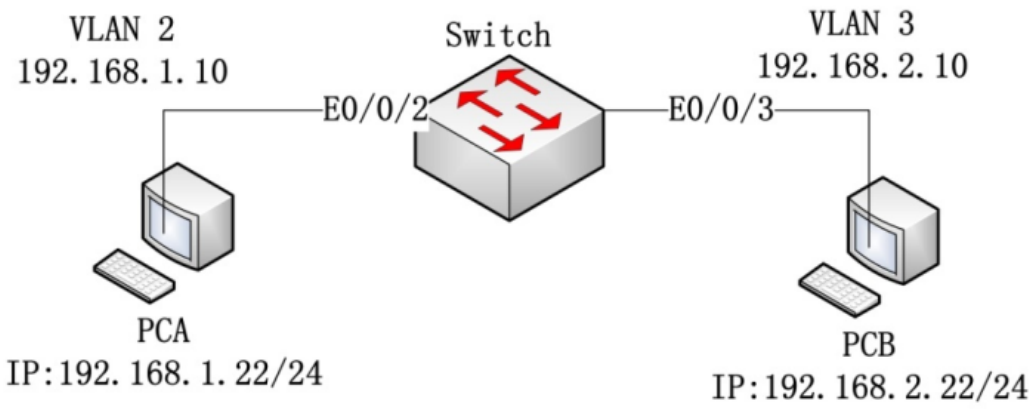

图 10: 不同网段之下的 ARP 组网图

B. 在 PCA 和 PCB 的命令行窗口均执行如下命令：

```
arp –a  查看 arp 缓存
arp –d  清除 arp 缓存
```

C. 在 PCA 执行 ping PCB，执行 arp -a，记录结果

```
Internet 地址    物理地址              类型
192.168.1.21   xx–xx–xx–xx–xx–xx   动态
```

4.4.2 不同网段 ARP 协议分析

A. 按照图 10 连接设备，同时为交换机划分 VLAN 如下：

```
Switch#show vlan
Switch#config
Switch(Config)#vlan 2
Switch(Config)#vlan 3
Switch(Config)#interface fa0/2
Switch(Config–if)#switchport access vlan 2
Switch(Config)#interface vlan 2
Switch(Config–if)#ip address 192.168.1.10 255.255.255.0
Switch(Config)#ip routing
Switch#show ip route
```

B. 执行 arp -d 命令，在 PCA 和 PCB 上截获报文，在 PCB 上执行 ping PCA。

C. 执行 arp -a 命令，观察结果。

```
Internet 地址  物理地址  类型
192.168.1.10  xx–xx–xx–xx–xx–xx  动态
```

D. 比较 PCA 以及 PCB 捕获到的报文信息如图 11, 12 所示。

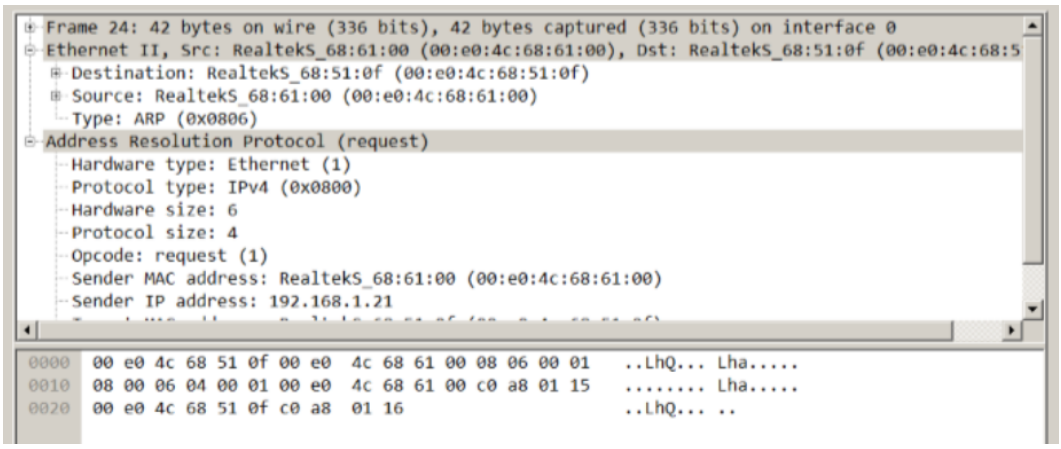

图 11: PCA 捕获到的 ARP 报文

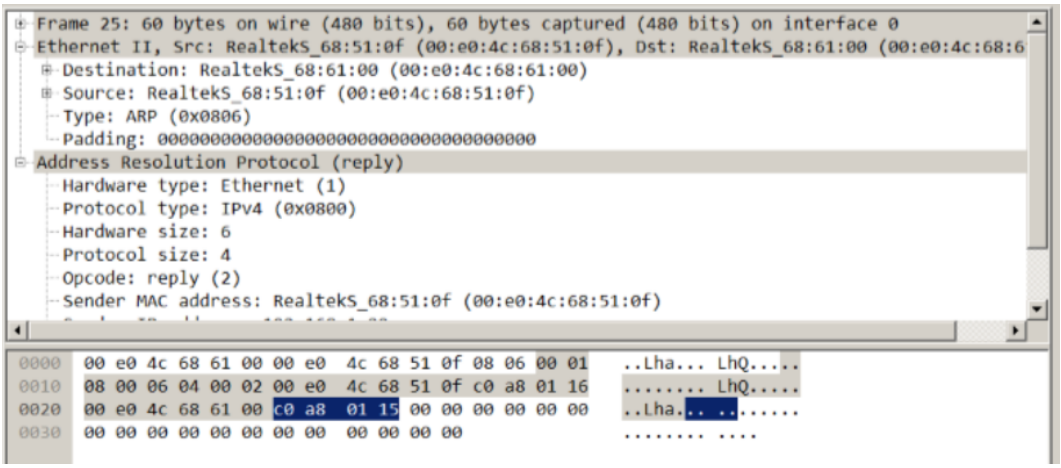

图 12: PCB 捕获到的 ARP 报文

4.4.3 ARP 欺骗与防范

A. 在交换机上进行 MAC 与 IP 的绑定。对应的操作代码如下：

```
// PCA 对应的 MAC 地址访问控制列表
Switch(config)#mac access-list extended mac1
Switch(config-ext-mac1)#permit host xxxx.xxxx.xxxx any
Switch(config-ext-mac1)#permit any host xxxx.xxxx.xxxx

// PCA 对应的 IP 地址访问控制列表
Switch(config)#ip access-list extended ipacc1
Switch(config-ext-nac1)#permit ip 192.168.1.22 0.0.0.0 any
Switch(config-ext-nac1)#permit ip any 192.168.1.22 0.0.0.0

// 启用
Switch(config)#interface fa0/2
```

动作	结果	原因分析
更换 PCA 的 IP 地址，接入端口仍为 fa0/2	不能连通	端口已经固定 IP 地址，会拦截所有发出的
为 vlan 2 添加端口 fa0/1，接入 PCA，IP 地址不变	可以联通	端口 fa0/1 没有任何限制
将其他 PCB 接入 fa0/2，使用 192.168.1.22 地址	不可以联通	端口已经固定 MAC 地址，会拦截所有发出
将其它 PCB 接入 fa0/2，使用 192.168.1.23 地址	不可以联通	端口已经固定 MAC 地址和 IP 地址，会拦截所有

```
Switch(config-if)#mac access-group mac1 in
Switch(config-if)#ip access-group ipacc1 in
Switch#show access-lists
```

B. 进行连通性测试，测试结果以及分析如表 **??** 所示。

4.5 实验小结

本次实验中，通过分析 ARP 协议以及其对应的报文结构，加深了我们对于 ARP 协议的理解，同时 ARP 欺骗以及防范的内容对 ARP 协议进一步有了深入的认识。

5 TCP 协议分析

5.1 实验目的

A. 理解 TCP [5] 报文首部格式和字段的作用。

B. 理解 TCP 连接的建立和释放过程。

C. 理解 TCP 数据传输中的编号和确认的过程。

5.2 实验内容

A. 应用 TCP 程序传输文件，截取 TCP 报文。

B. 分析 TCP 报文首部信息、TCP 连接的建立和释放过程、TCP 数据的编号和确认机制。

5.3 实验环境与拓扑结构

5.3.1 实验环境

2 人一组，DCR-2626 路由器 1 台，DCRS-5650 交换机一台

5.3.2 拓扑结构

TCP 协议的测试组网拓扑结构如图 13 所示。

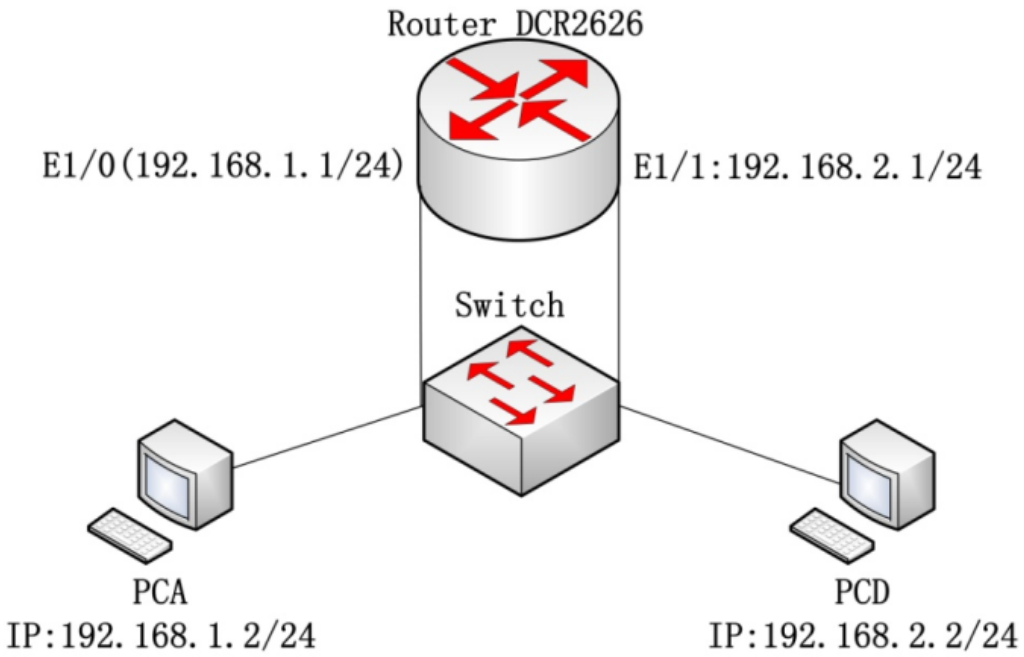

图 13: TCP 协议分析组网图

表 3: TCP 连接建立报文信息

字段名称	第一条报文	第二条报文	第三条报文
报文发出的计算机	192.168.2.2	192.168.1.2	192.168.2.2
捕获的报文序号	4	5	6
Sequence Number	0	0	1
Acknowledgement Number	0	1	1
ACK 标志	0(ACK 值无效)	1(ACK 有效)	1(ACK 有效)
SYN 标志	1(连接建立)	1(连接建立)	0

表 4: TCP 连接撤销报文信息

字段名称	第一条	第二条	第三条	第四条
报文发出计算机	192.168.2.2	192.168.1.2	192.168.1.2	192.168.2.2
捕获的报文序号	748	749	750	751
Sequence Number	485761	1	1	485762
Acknowledgement Number	1	485762	485762	2
ACK 标志	1	1	1	1
FIN 标志	1	0	1	0

5.4 实验步骤与结果

A. 连接设备，配置计算机的 IP。配置路由器 IP，e1/0 接口对应命令如下：

```
Router#config
Router_config#interface e1/0
Router_config_e1/0#ip address 192.168.2.1 255.255.255.0
Router#show interface e1/0
```

B. 在 PCA 以及 PCB 上进行报文截获。

C. 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（PCB -> PCA）。文件传输完成后，停止报文截获。

D. 观察报文，从 PCA 的角度填写完成以下表格 3, 4, 5。

E. 解答以下问题：

a) 如何确定哪条捕获的报文已经被确认?

对于一条确认报文，只要其确认号（ACK）大于发送报文的序号（seq）即可以认为这条报文已经被确认。

b) 窗口值何时何因由谁调整?

表 5: TCP 数据传送阶段前 8 个报文, 其中实际窗口大小为填写窗口大小 × 256

捕获报文序号	报文种类	序号	确认号	数据长度	确认到哪一条报文	窗口大小
11	发送	1	1	1460		256
12	发送	1461	1	540		256
13	确认	1	2001	0	12	256
14	发送	2001	1	1460		256
15	发送	3461	1	540		256
16	发送	4001	1	1460		256
17	确认	1	5461	0	16	256
18	发送	5461	1	540		256

窗口值大小由接收端的数据量以及数据送往应用层是否发生阻塞两个因素由接收端进行调整。

5.5 实验小结

通过本次关于 TCP 的连接机制以及对应的连接报文的分析，我们对 TCP 连接的建立、传输以及撤销过程有了更加深入的认识与理解。

6 RIP 协议分析

6.1 实验目的

A. 理解路由协议的分类，掌握静态路由和 RIP [6] 协议的配置方法。

B. 分析掌握 RIP 报文结构及各字段的含义。

C. 分析两个路由设备之间 RIP 报文的交换以及路由表的构建过程。

6.2 实验内容

A. 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 命令测试网络的联通性。

B. 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。

C. 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。

6.3 实验环境与拓扑结构

6.3.1 实验环境

2 人一组，DCR-5650 交换机 1 台，DCR-2626 路由器 1 台，Cisco-3560 交换机 1 台。

6.3.2 拓扑结构

该实验的拓扑结构如图 **??** 所示。

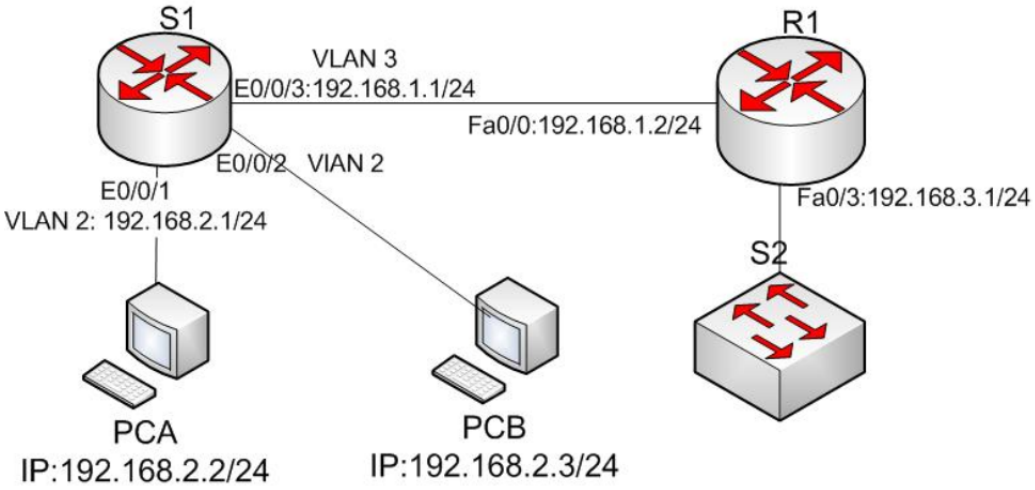

图 14: RIP 协议配置组网拓扑图

6.4 实验步骤与结果

6.4.1 RIP 协议配置

A. 连接设备，配置 IP 地址，配置交换机和路由器各接口的 IP 地址，相关代码如下：

```
// S1
switch(Config)#vlan 2
switch(Config-vlan2)#switchport interface Ethernet 0/0/1-2
switch(Config-vlan2)#exit
switch(Config)#interface vlan 2
switch(Config-If-Vlan2)#ip address 192.168.2.1 255.255.255.0
// R1
Router_config#interface f0/0
Router_config_fa0/0#ip address 192.168.1.2 255.255.255.0
Router_config#interface f0/3
Router_config_fa0/3#ip address 192.168.3.1 255.255.255.0
```

R1 ping 各台 PC 的结果以及分析如下:

```
R1 ping 192.168.2.2: fail
R1 ping 192.168.2.3: fail
```

R1 路由表如下:

```
C 192.168.1.0/24[0] is directly connected, Fast Ethernet 0/0[0]
C 192.168.3.0/24[0] is directly connected, Fast Ethernet 0/3[0]
```

通过 R1 的路由表我们可以看到，由于该路由表上没有到达 192.168.2.0 的路由信息，因此无法 ping 通。

B. 在 R1 上配置静态路由, 命令如下：

```
Router_config#ip route 192.168.2.0 255.255.255.0 192.168.1.1
```

R1 ping 各台 PC 的结果以及分析如下：

```
R1 ping 192.168.2.2: success
R1 ping 192.168.2.3: success
```

R1 路由表见下：

```
C 192.168.1.0/24[0] is directly connected, Fast Ethernet 0/0[0]
S 192.168.2.0/24[0] [1,0] via 192.168.1.1 (on Fast Ethernet 0/0[0])
C 192.168.3.0/24[0] is directly connected, Fast Ethernet 0/3[0]
```

在 R1 上添加了静态路由之后的路由表可以看到，由于该表上存在 192.168.2.0 的路由信息，因此可以 ping 通。

C. 删除 B 中设置的静态路由。

D. 在 S1 和 R1 分别启动 RIP 协议，命令如下:

```
// S1
switch(Config)#router rip
switch(Config-router)#version 2
switch(Config-router)#network vlan3
switch(Config-router)#network vlan2
// R1
Router_config#router rip
Router_config_rip#version 2
Router_config_rip#network 192.168.1.0 255.255.255.0
Router_config_rip#network 192.168.3.0 255.255.255.0
```

接下来对其连通性进行测试, 相关测试结果如下：

```
R1 ping 192.168.2.2: success
R1 ping 192.168.2.3: success
```

表 6: 添加 RIP 协议的 R1 路由表基本信息

设备	Destination/ Mask	Protocol	Pref	Cost	Nexthop	Interface
S1	192.168.1.0/24	connected				VLAN3
S1	192.168.2.0/24	connected				VLAN2
S1	192.168.3.0/24	RIP	120	2	192.168.1.2	VLAN3
R1	192.168.1.0/24	connected				fa 0/0
R1	192.168.2.0/24	RIP	120	1	192.168.1.1	fa 0/0
R1	192.168.3.0/24	connected				fa 0/3

表 7: RIP 协议应答报文

观察点	字段	值	含义
IP	目的地址	244.0.0.9	RIPv2 使用的组播地址
UDP	端口号	520	RIP 协议默认端口
RIP 头部	命令字段	02	RIP 应答
RIP 头部	版本号	02	版本 2
RIP 路由信息	地址族标识	2	携带地址类型为 IP 地址
RIP 路由信息	网络地址	192.168.1.0	IP 地址
RIP 路由信息	跳数	1	表示到网络地址的跳数

而得到的路由表信息如图 6 所示：

RIP 协议报文分析:

a) 将交换机 S1 上与 R 相连的端口镜像到 E0/0/1 端口;

b) 停止交换机 S1 上的 RIP 协议；

c) 在 PCA 上截获报文，在 S1 上启动 RIP 协议。观察截获的请求报文和应答报文。

应答报文如图 7

6.5 实验小结

本次实验，我们对 RIP 协议的组织形式以及报文结构有了较为深入的认识，进而加深了对 RIP 路由协议的理解，通过对路由器配置 RIP 协议以及相关使用的过程实践，对 RIP 协议有了更深层次的掌握。

7 OSPF 路由协议分析

7.1 实验目的

A. 详细分析 OSPF 的 5 种报文结构。

B. 掌握 OSPF 邻居建立及报文交换过程。

7.2 实验内容

A. 在路由器上启用 OSPF [7] 协议；

B. 在计算机截取报文，分析 OSPF 邻居建立以及报文交换的过程。

7.3 实验环境与拓扑结构

7.3.1 实验环境

4 人一组，DCR-2626 路由器 2 台，DCRS-5650 交换机 1 台。

7.3.2 拓扑结构

OSPF 邻居建立与报文交换过程组网图如 15 所示。

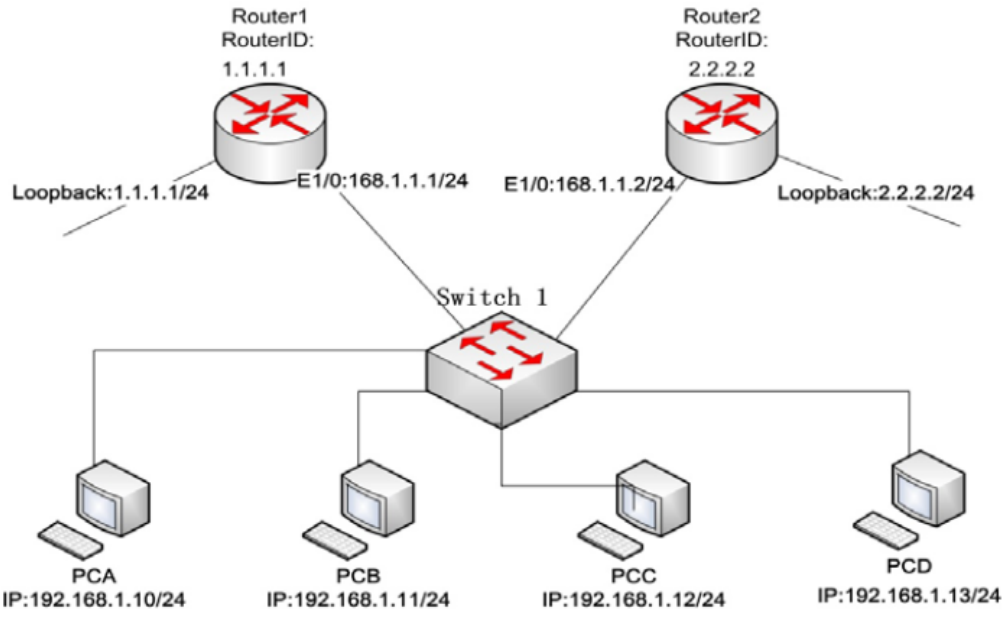

图 15: OSPF 邻居建立与报文交换过程组网图

7.4 实验步骤与结果

A. 根据实验拓扑图 15 连接实验设备，配置 IP 地址。

B. 将交换机上连接路由器的端口镜像到一台 PC（PCA）连接的端口上。使用如下命令完成操作：

```
switch(Config)#monitor session 1 source interface ethernet 0/0/5-6 both
switch(Config)#monitor session 1 destination interface ethernet 0/0/1
```

C. 运行 Wireshark 软件，截获报文。

D. 配置路由器，启动 OSPF 协议，并在接口上指定响应的 OSPF 区域。以下为 R1 配置命令:

```
Router_config#interface lookback0
Router_config_10#ip address 1.1.1.1 255.255.255.0
Router_config#interface e1/0
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
Router_config_ospf_1#network 168.1.1.0 255.255.255.0 area 0
Router_config_ospf_1#network 1.1.1.0 255.255.255.0 area 0
```

E. 查看对应路由表如下：

```
                // R1
C(直连) 1.1.1.0/24[0] is directly connected, Loopback0[0](回环
端口)
O(OSPF) 2.2.2.2/32[0] [110,11](优先级, cost) via 168.1.1.2 (on
Async 0/0[0])(OSPF 协议默认使用异步串行端口)
C(直连) 168.1.1.0/24[0] is directly connected, Ethernet 1/0[0]
// R2
O 1.1.1.1/32[0] [110,11] via 168.1.1.1 (on Async 0/0[0])
C 2.2.2.0/24[0] is directly connected, Loopback0[0]
C 168.1.1.0/24[0] is directly connected, Ethernet 1/0[0]
```

F. 分析截获的报文，找出 OSPF 的 5 种协议报文，描述 OSPF 协议邻居建立和数据库同步的过程。

截取的报文根据镜像机与非镜像机有两类，其中镜像机有五种报文，非镜像机有三种报文（除了 DD 报文以及 LSR 报文）

截取的报文示例如下：DD 报文如图 16, Hello 报文如图 17, LSR 报文如图 18, LSU 报文如图 19, LSAck 报文如图 20。

通过上述分析，可以得到：

a) 邻居建立过程：每 10s 发送 Hello 报文宣告自身存在-> 发现 active neighbor -> 数据库同步-> 邻接

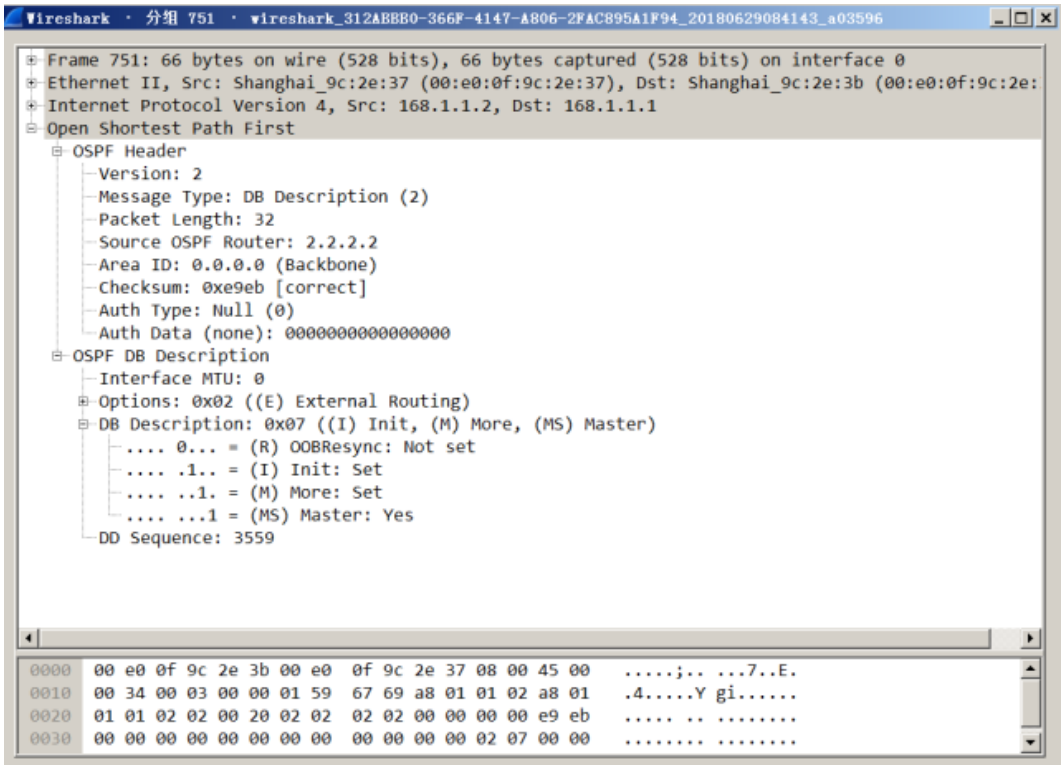

图 16: DD 报文

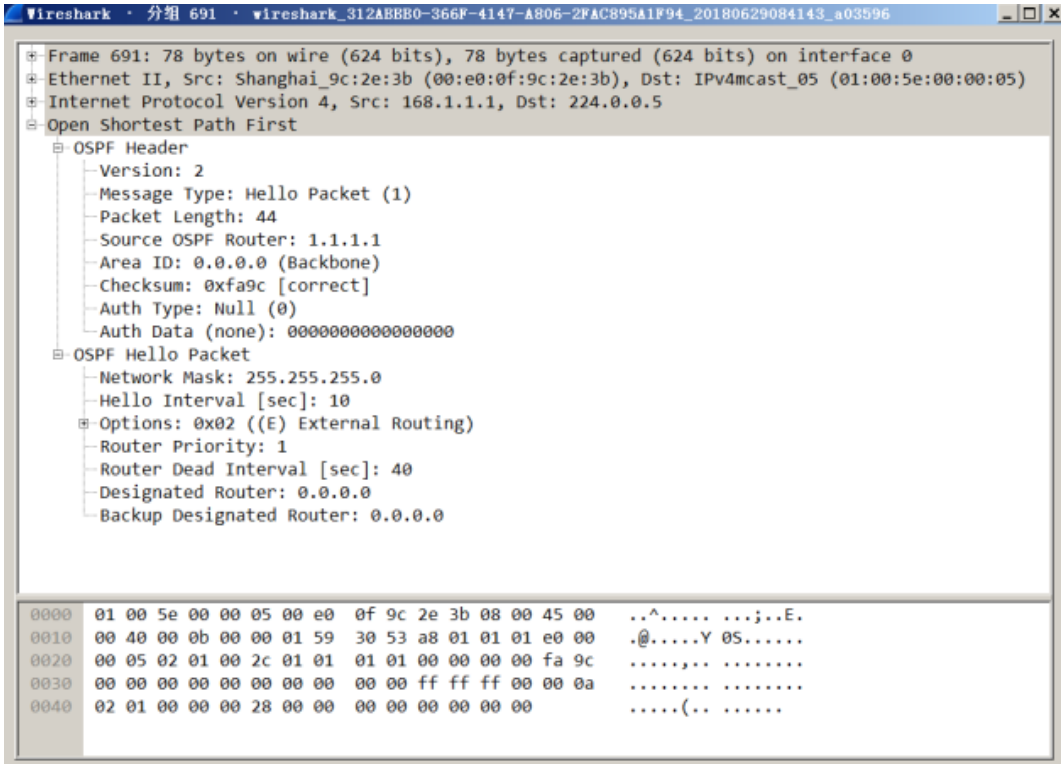

图 17: Hello 报文

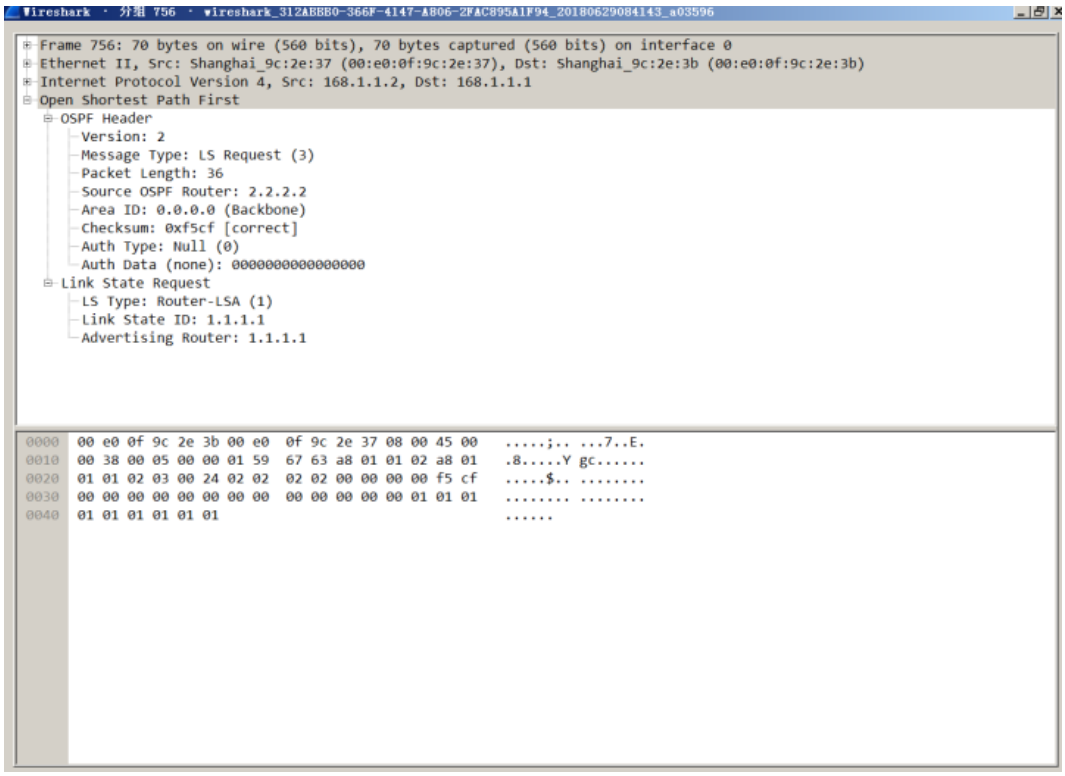

图 18: LSR 报文

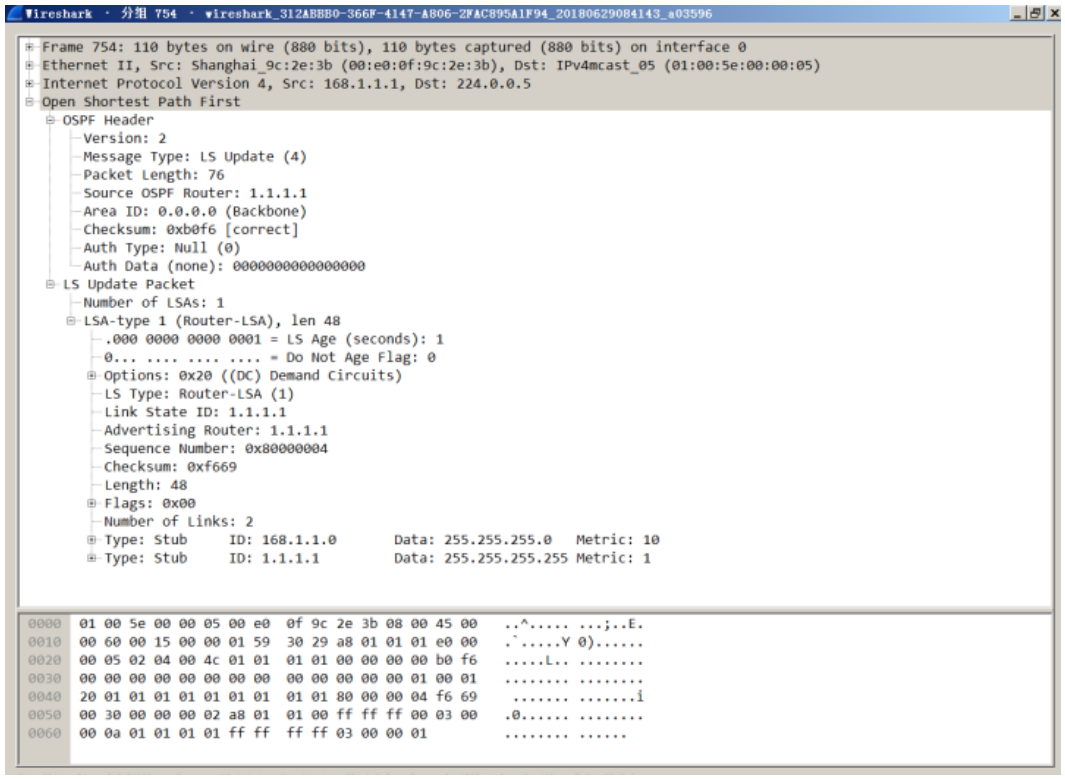

图 19: LSU 报文

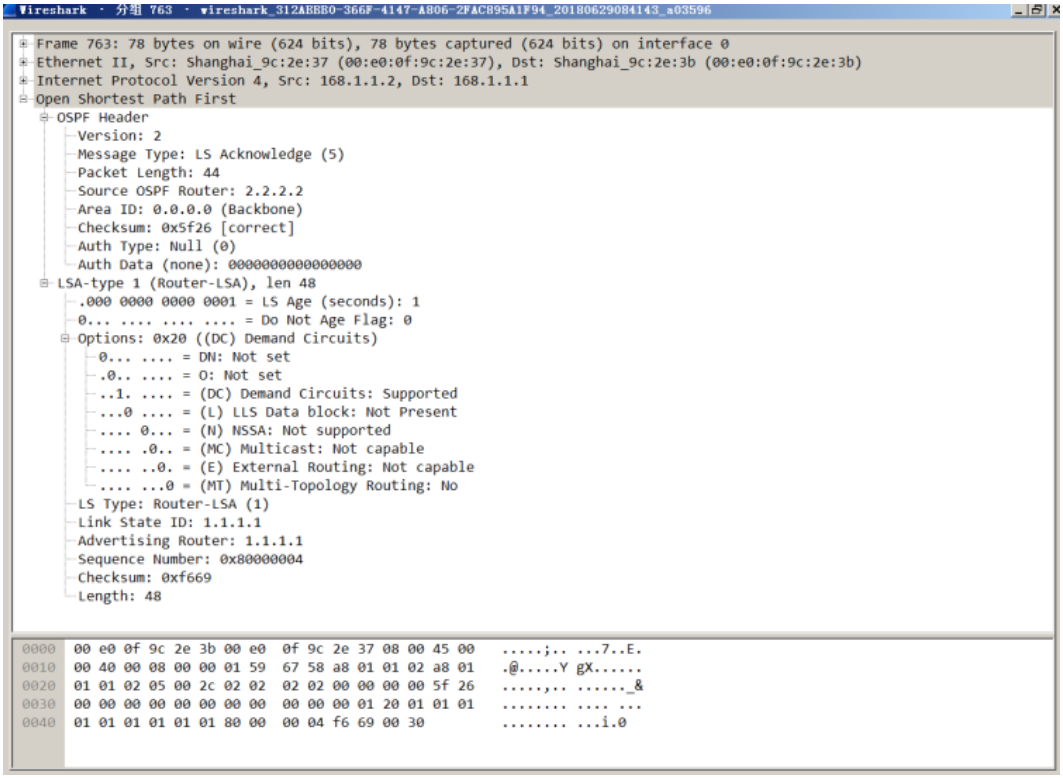

图 20: LSAck 报文

b) 数据库同步过程：双方发送 DD 报文，确认主从关系 -> 双方发送 DD 报文，介绍自身 LSA -> 发送 LSR 报文，要求提供缺失部分 -> 双方发送 LSU 报文响应-> 发送 LSAck 报文响应

Router-LSA 各字段的含义和作用：

取 LSU 报文中的 LSA 信息：

LS Age: 1 (该 LSA 产生时间)

LS Type: 1 (Router–LSA)

Link State ID: 1.1.1.1 (生成 LSA 的路由器 ID)

Advertising Router: 1.1.1.1 (通告路由器)

Number of Links: 2 (连接信息)

Link ID: 168.1.1.0

Link Data: 255.255.255.0 (子网掩码)

Link Type: 3 (终端网络)

Number of Metrics: 0 (TOS 标记)

0 Metric: 10 (cost = 10)

7.5 实验小结

本次实验的完成，我们对 OSPF 协议报文的机构以及其对应的保证形式有了较为深入的认识，同时通过对路由器 OSPF 协议的学习实践我们对网络路由协议有了更为冷静的思考以及明确了未来的发展方向。

8 IPv6 实验

8.1 实验目的

A. 理解 IPV6 地址结构。

B. 掌握路由器 IPV6 地址、静态路由配置方法。

C. 掌握 RIPing 配置方法与基本原理。

8.2 实验内容

IPV6 基本配置与简要分析

8.3 实验环境与拓扑结构

8.3.1 实验环境

4 人一组，DCRS-5650 交换机 2 台

8.3.2 拓扑结构

IPv6 实验组网的拓扑结构如图 21 所示。

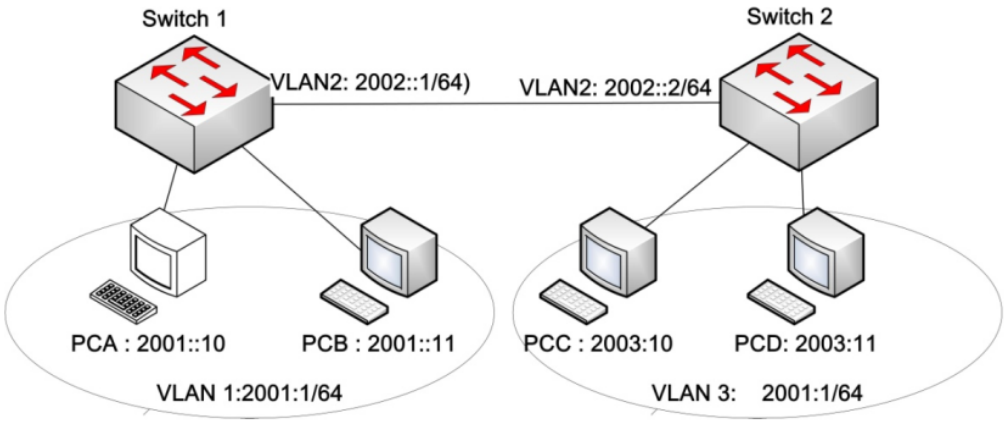

图 21: IPv6 实验组网

8.4 实验步骤与结果

A. 按照网络拓扑图 21 为两个交换机分配 VLAN；

B. 在交换机上使能 IPv6，并为 VLAN 端口配置 IPV6 地址。交换机 S1 配置命令如下：

```
switch(Config)#ipv6 enable
switch(Config)#interface vlan 2
switch(Config-If-Vlan2)#ipv6 address 2002::1/64
switch(Config-If-Vlan2)#no ipv6 nd suppress-ra
switch(Config)#interface vlan 1
switch(Config-If-Vlan1)#ipv6 address 2001::1/64
switch(Config-If-Vlan1)#no ipv6 nd suppress-ra
```

C. 为 PC 机配置 IPv6 地址。

D. 在交换机 S1 和 S2 上配置静态路由：

```
// S1
switch(Config)#ipv6 route 2003::/64 2002::2
// S2
switch(Config)#ipv6 route 2001::/64 2002::1
```

E. 测试 IPv6 网络连通性，测试结果如下：

```
PCA ping PCB: OK
PCA ping PCC: OK
PCA ping PCD: OK
```

由于 IPv6 具有不同 VLAN 之间的路由信息，因此其跨路由器的通信仍然可以 ping 通。

F. 去掉设置的静态路由，相关操作如下：

```
switch(Config)#no ipv6 route 2003::/64 2002::2
```

G. 为交换机配置 RIPng 协议：首先全局启动 RIPng 协议，然后在各 VLAN 上使能 RIPng。

```
// S1 交换机
switch(Config)#router ipv6 rip
switch(Config)#interface vlan 2
switch(Config-If-Vlan2)#ipv6 router rip
switch(Config-If-Vlan2)#exit
switch(Config)#vlan 1
switch(Config-If-Vlan1)#ipv6 router rip
```

H. 查看路由表并分析，22 是运行的基本截图。

对其基本的分析如下：

```
DCRS-5650-28(config)#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP
Timers: Uptime

C    ::1/128 via ::, Loopback, 01:18:25
C    2001::/64 via ::, Vlan1, 00:25:48
C    2002::/64 via ::, Vlan2, 00:23:15
R    2003::/64 [120/2] via fe80::212:cfff:fe50:cd00, Vlan2, 00:01:36

DCRS-5650-28(config)#
```

图 22: 配置路由表基本信息

- R：基于 RIP 协议获得该表项
- 2003::/64：网络 IP 地址

120/2 ：[优先级（取决于协议）/cost]

- via xxxxxx，VLAN 2：经过的端口（交换机端口 IP）
- 00:01:36：该表项存在的时间

I. 将 S1 上链接 S2 的端口镜像到 PCB，在 PCA、PCB 和 PCC 上捕获 PCA ping6 PCC 的报文，分析与 IPV4 的 ICMP 报文有哪些区别？

捕获的报文种类为：

- PCA: ICMP request, ICMP reply, Neighbor Solicitation, Neighbor Advertisement
- PCB: ICMP reply, Neighbor Solicitation, Neighbor Advertisement
- PCC: ICMP request, ICMP reply, Neighbor Solicitation, Neighbor Advertisement

No.	Time	Source	Destination	Protocol	Length	Info
3	1.949005	fe80::212:cfff:fe50:ca20	fe80::940:8c1b:55aa:312e	ICMPv6	86	Neighbor Solicitation for fe80::940:8
4	1.949221	fe80::940:8c1b:55aa:312e	ff02::1:ff50:ca20	ICMPv6	86	Neighbor Solicitation for fe80::212:c
5	1.950889	fe80::212:cfff:fe50:ca20	fe80::940:8c1b:55aa:312e	ICMPv6	86	Neighbor Advertisement fe80::212:cfff
6	1.950939	fe80::940:8c1b:55aa:312e	fe80::212:cfff:fe50:ca20	ICMPv6	86	Neighbor Advertisement fe80::940:8c1b
9	3.457682	2003::11	2001::54fb:49eb:37de:af0a	ICMPv6	94	Echo (ping) reply id=0x0001, seq=9, h
10	4.454163	2003::11	2001::54fb:49eb:37de:af0a	ICMPv6	94	Echo (ping) reply id=0x0001, seq=10,
13	5.457492	2003::11	2001::54fb:49eb:37de:af0a	ICMPv6	94	Echo (ping) reply id=0x0001, seq=11,
16	6.450945	2003::11	2001::54fb:49eb:37de:af0a	ICMPv6	94	Echo (ping) reply id=0x0001, seq=12,

图 23: PCB 捕获的报文

IPv6 下 ICMP 报文与 IPv4 下 ICMP 报文区别：

- Type 的编码不同：ipv6 下 request/reply 的编码为 128/129，而 ipv4 下为 8/0

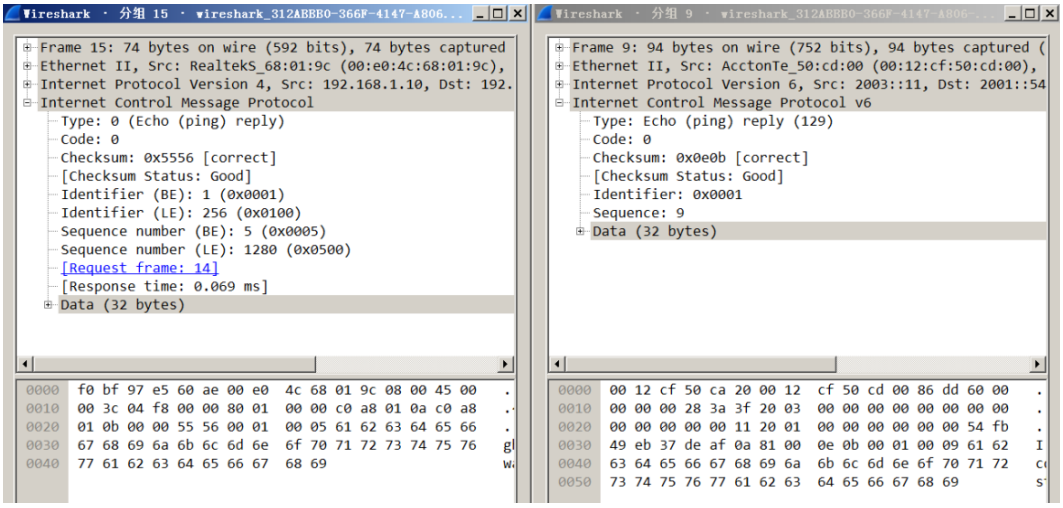

图 24: IPv6 下 ICMP 报文与 IPv4 下 ICMP 报文比较

- 在 IPv4 下报文中，Identifier 和 Sequence number 由于系统不同，存在 BE 和 LE 两组表示方式，而在 IPv6 中，这两个字段得到统一。
- IPv4 中的 ARP 报文被 IPv6 中的 Neighbor Solicitation（邻居建立）, Neighbor Advertisement（邻居告知）报文取代。

8.5 实验小结

在本次试验中，通过对 IPv6 自带协议的分析，以及 IPv6 报文与 IPv4 报文之间的比较，对于报文一些协议本身有了更为深入的认识与理解，为之后的进一步发展奠定了基础。

9 回顾与总结

计算机网络的系列实验，让我从计算机网络中如交换机、路由器等的基础配置到基于其的软硬件协同实验有了较为深入的认识与理解，在这个过程中，对接下来进一步发展的方向进行了明确。相对而言，之前的硬件以及网络基础相对薄弱，有很多环节之前并没有顾忌到，而且，由于实验刚开始的那段时间自己在国外的缘故，之前的几次实验并没有参加，因此为之后的学习造成了不小的障碍。好在得到了老师以及很多同学的帮助，在大家的配合之下最终完成了实验。

致谢

感谢魏老师循循善诱的指导，感谢同学们在实验过程中给予的帮助，感谢小伙伴们齐心协力完成了本次实验，感谢开源社区对遇到了问题提供的正向反馈。

参考文献

[1] A Mishra. An initial security analysis of the ieee 802.1x standard. 2002.

[2] P V Sreelakshmi and Shibily Joseph. Dcr based route request flooding prevention in manet. *Advances in Dental Research*, 24(2):27–27, 2015.

[3] Shiri Kadambi and Shekhar Ambe. Method for sending packets between trunk ports of network switches, 2000.

[4] M Laubach. Classical ip and arp over atm. *Rfc*, 11(3):82–89, 1994.

[5] J Padhye. Modeling tcp throughput : a simple model and empirical validation. *Acm Sigcomm98 September*, 28(4):303–314, 1998.

[6] D. Pei, D. Massey, and L. Zhang. Detection of invalid routing announcements in rip protocol. In *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*, pages 1450–1455 vol.3, 2004.

[7] J Moi. Ospf version 2. *Rfc*, 1998.