



警示

1. 实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2. 当次小组成员成绩只计学号、姓名登录在下表中的。
3. 在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
4. 实验报告文件以 PDF 格式提交。

| | | | | | |
|------|-------------------|----------|----------|-------------------|-----|
| 专业 | 软件工程 | 班 级 | 19 级软件工程 | 组长 | 冼子婷 |
| 学号 | 18338072 | 18346019 | 18322043 | | |
| 学生 | 冼子婷 | 胡文浩 | 廖雨轩 | | |
| 实验分工 | | | | | |
| 冼子婷 | 进行实验，截图，编写和分析实验报告 | | 廖雨轩 | 进行实验，截图，编写和分析实验报告 | |
| 胡文浩 | 进行实验，截图，编写和分析实验报告 | | | | |

【实验题目】静态路由实验

【实验目的】掌握静态路由的配置和使用方法，熟悉交换机端口镜像的方法以及如何用于监视端口。

【实验内容】

- (1) 阅读教材 P190-192 关于端口镜像的内容
- (2) 阅读教材 P233 实例 7-1
- (3) 阅读教材 P29，熟悉 Packet Tracer 使用实例
- (4) 完成教材 P273 习题 15

【实验记录】P233 实例 7-1

一、在如图下所示的拓扑结构中配置 PC1 到 PC2 之间的静态路由并检查 PC1 与 PC2 的连通性。按顺序完成以下要求：

实验拓扑图：

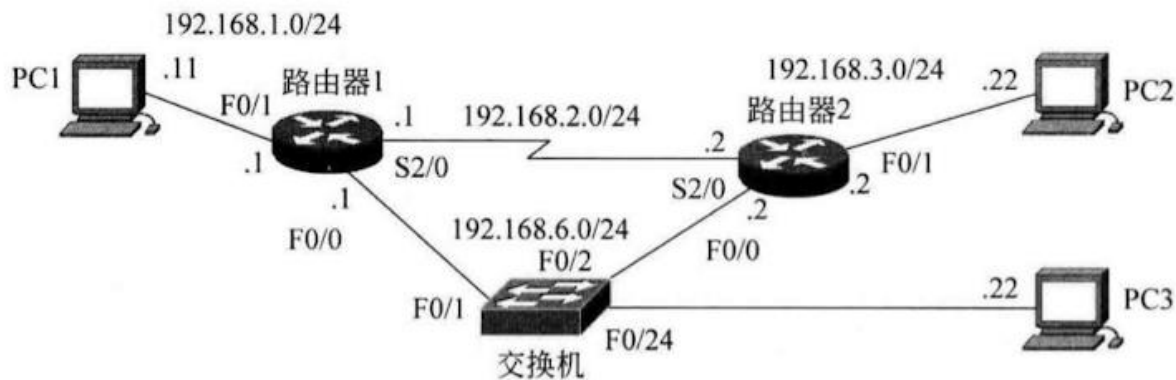


图 7-36 第 15 题拓扑结构

(0) IP 及路由器配置：

1) 首先根据上图的拓扑结构进行连线，并设置 PC1，PC2，PC3 的 IP 地址，如下：

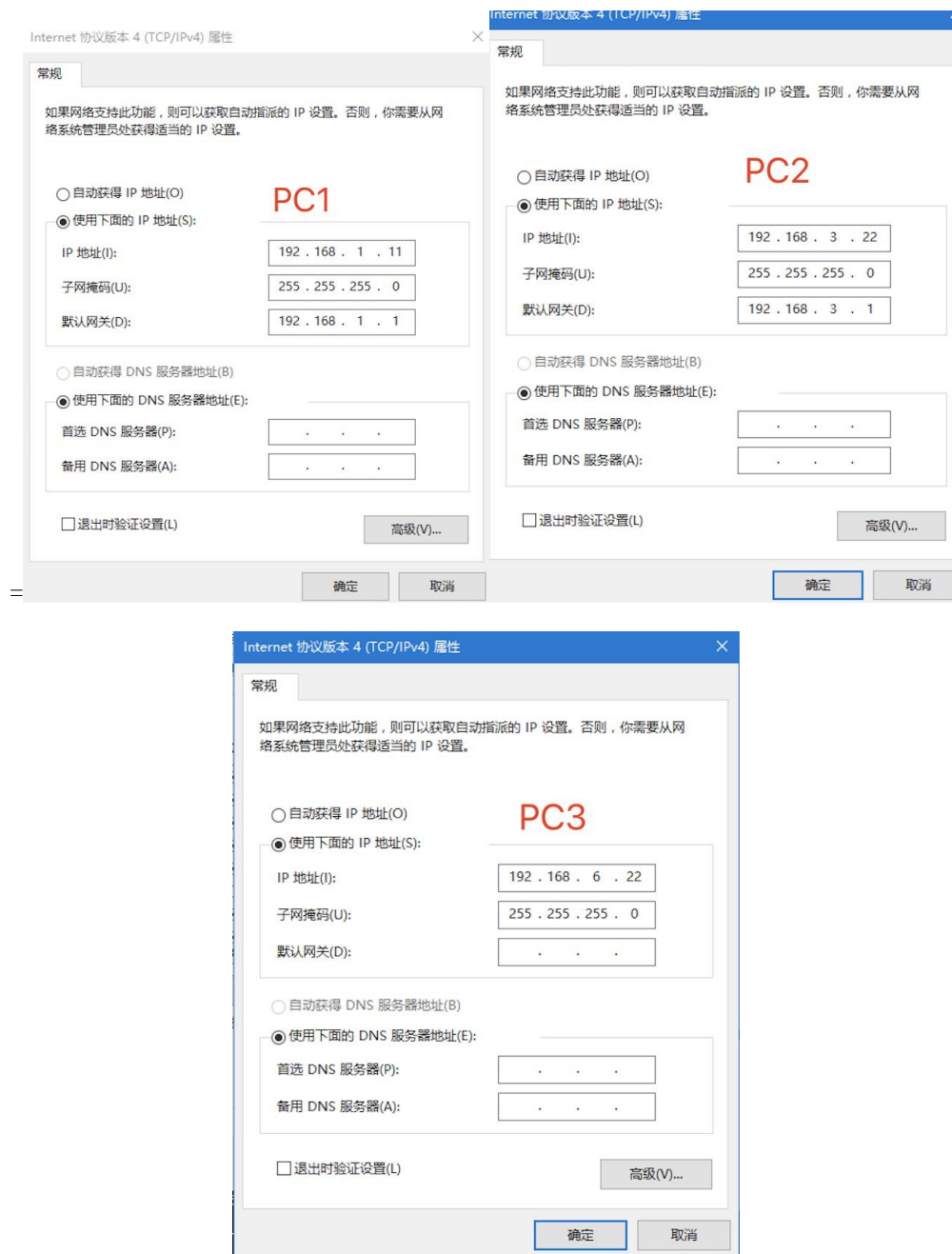


图 1：设置 PC1、PC2、PC3 的 IP 地址。

2) 配置路由器的端口 IP

在路由器 Router1 上设置以太网端口 0/1 和串行端口 2/0 的 IP 地址和子网掩码：

```
11-Router1(config)#hostname Router1
Router1(config)#interface giga
Router1(config)#interface gigabitEthernet 0/1
Router1(config-if-GigabitEthernet 0/1)#ip address 192.168.1.1 255.255.255.0
Router1(config-if-GigabitEthernet 0/1)#no shutdown
Router1(config-if-GigabitEthernet 0/1)#exite
% Unknown command.

Router1(config-if-GigabitEthernet 0/1)#exit
Router1(config)#interface serial 2/0
Router1(config-if-Serial 2/0)#ip address 192.168.2.1 255.255.255.0
Router1(config-if-Serial 2/0)#no shutdown
Router1(config-if-Serial 2/0)#exit
```

设置端口 IP

图 2：配置路由器 1 的端口 IP

设置好路由器端口的 IP 地址后，查看路由器的端口配置：



```
Router1(config)#show ip interface brief
Interface                               IP-Address(Pri)    IP-Address(Sec)    Status    Protocol
Serial 2/0                             192.168.2.1/24     no address          up        up
SIC-3G-WCDMA 3/0                       no address         no address          up        down
GigabitEthernet 0/0                    no address         no address          up        down
GigabitEthernet 0/1                    192.168.1.1/24     no address          up        up
VLAN 1                                  no address         no address          up        down
```

图 4：显示路由器 1 的端口配置

在路由器 Router2 上设置以太网端口 0/1 和串行口端口 2/0 的 IP 地址和子网掩码：

```
Enter configuration commands, one per line. End with CNTL/Z.
11-RSR20-1(config)#hostname Router2
Router2(config)#inte
Router2(config)#interface giga
Router2(config)#interface gigabitEthernet 0/1
Router2(config-if-GigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Router2(config-if-GigabitEthernet 0/1)#no shutdown
% Unknown command.

Router2(config-if-GigabitEthernet 0/1)#no shutdown
Router2(config-if-GigabitEthernet 0/1)#exit
Router2(config)#interface se
Router2(config)#interface serial 2/0
Router2(config-if-Serial 2/0)#ip address 192.168.2.2 255.255.255.0
Router2(config-if-Serial 2/0)#no shutdown
Router2(config-if-Serial 2/0)#exit
Router2(config)#
```

图 5：配置路由器 2 的端口 IP

设置好路由器端口的 IP 地址后，查看路由器的端口配置

```
Router2(config)#show ip interface brief
Interface                               IP-Address(Pri)    IP-Address(Sec)    Status    Protocol
Serial 2/0                             192.168.2.2/24     no address          up        up
SIC-3G-WCDMA 3/0                       no address         no address          up        down
GigabitEthernet 0/0                    no address         no address          up        down
GigabitEthernet 0/1                    192.168.3.1/24     no address          up        up
VLAN 1                                  no address         no address          up        down
Router2(config)#
```

图 6：显示路由器 2 的端口配置

(1) 记录 2 台路由器的路由表：

配置路由器 R1 中 PC1 到 PC2 之间的静态路由后，并查看路由器的路由表如下所示，其中以 C 开头表示直连的路由信息，S 为配置的静态路由：

```
Router1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
Router1(config)#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C 192.168.1.0/24 is directly connected, GigabitEthernet 0/1
C 192.168.1.1/32 is local host.
C 192.168.2.0/24 is directly connected, Serial 2/0
C 192.168.2.1/32 is local host.
S 192.168.3.0/24 [1/0] via 192.168.2.2
```

添加的静态路由项

配置的静态路由项

图 7：配置路由器 1 的静态路由

即路由器 R1 通过下一跳的地址 192.168.2.2 到达目的网段 192.168.3.0/24

配置路由器 R2 中 PC1 到 PC2 之间的静态路由后，并查看路由器的路由表如下所示，其中以 C 开头表



示直连的路由信息，S 为配置的静态路由：

```
Router2(config)#  
Router2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1  
Router2(config)#show ip route  
  
Codes: C - connected, S - static, R - RIP, B - BGP  
O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, * - candidate default  
  
Gateway of last resort is no set  
S 192.168.1.0/24 [1/0] via 192.168.2.1  
C 192.168.2.0/24 is directly connected, Serial 2/0  
C 192.168.2.2/32 is local host.  
C 192.168.3.0/24 is directly connected, GigabitEthernet 0/1  
C 192.168.3.1/32 is local host.  
Router2(config)#
```

图 8：配置路由器 2 的静态路由

即路由器 R2 通过下一跳的地址 192.168.2.1 到达目的网段 192.168.1.0/24

(2) 用 PC1 ping PC2，记录交换机的 MAC 地址表

配置好静态路由并且禁用校园网后(或使用参数 -S srcaddr 使用源地址走静态路由)，使用 PC1 ping PC2，结果如图所示：

```
管理员: 命令提示符  
Microsoft Windows [版本 10.0.14393]  
(c) 2016 Microsoft Corporation。保留所有权利。  
  
C:\windows\system32>ping 192.168.3.22  
  
正在 Ping 192.168.3.22 具有 32 字节的数据:  
来自 192.168.3.22 的回复: 字节=32 时间=36ms TTL=62  
来自 192.168.3.22 的回复: 字节=32 时间=38ms TTL=62  
来自 192.168.3.22 的回复: 字节=32 时间=39ms TTL=62  
来自 192.168.3.22 的回复: 字节=32 时间=39ms TTL=62  
  
192.168.3.22 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 = 36ms, 最长 = 39ms, 平均 = 38ms
```

图 9：PC1 ping PC2

可以发现 PC1 和 PC2 处于不同的网段，在不同网段的情况下是无法直接互联互通的，但是在配置好相对应的路由器端口和路由器的静态路由后，可以实现不同网段之间的主机互相访问。

此时查看交换机的 MAC 地址表，结果如图所示：

```
11-S5750-2(config)#show mac-address-table  
Vlan      MAC Address      Type      Interface  
-----  
1         4433.4c0e.ab7a   DYNAMIC   GigabitEthernet 0/24
```

图 10：交换机的 MAC 地址表

此时交换机的 MAC 地址只有连接 PC3 的 MAC 地址，因为在第(0)，(1)步中在配置静态路由时，只配置了一条通路，也即 192.168.1.0/24 网段与 192.168.3.0/24 网段的互联，是经过 192.168.2.0/24 中的静态路由，而不会经过 192.168.6.0/24 网段，所以交换机并不会接收到路由器 1 和路由器 2 之间传输的数据包。因此 MAC 地址表中也只会 0/24 号端口，PC3 的 MAC 信息。



(3) 清除 MAC 地址表, 启动 Wireshark 捕获, 用 PC1 ping PC2, 查看 PC3 是否可以捕获到 ARP 包、Echo 请求包和 Echo 响应包。记录交换机的 MAC 地址表。

PC1 ping PC2 的结果如下:

```
C:\windows\system32>ping 192.168.3.22

正在 Ping 192.168.3.22 具有 32 字节的数据:
来自 192.168.3.22 的回复: 字节=32 时间=36ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=38ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=39ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=39ms TTL=62

192.168.3.22 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 = 36ms, 最长 = 39ms, 平均 = 38ms
```

图 11: PC1 ping PC2

此时在 PC3 上打开 Wireshark 进行数据包的捕捉, 如下:

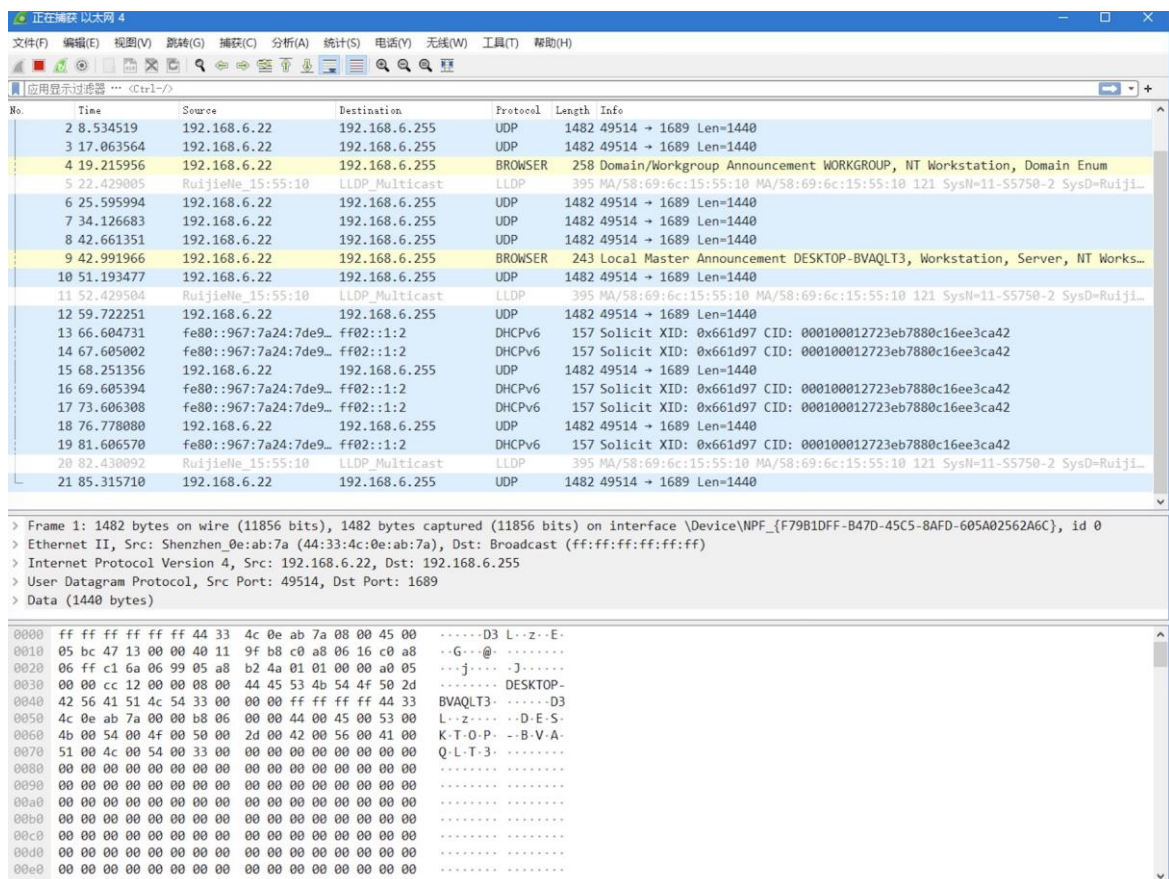


图 12: PC3 上 Wireshark 截图

由于还未设置端口镜像, 此时 PC3 无法收到 PC1 ping PC2 的 ICMP 数据包, 并且由于在该拓扑结构中, 当设置好各机的 IP 后, 只有该 PC 到路由器的 ARP 包, PC3 不会收到 ARP 包。

此时查看交换机的 MAC 地址表如下所示:

```
11-S5750-2(config)#show mac-address-table
Vlan          MAC Address           Type           Interface
-----
1             4433.4c0e.ab7a        DYNAMIC        GigabitEthernet 0/24
```



图 13: 交换机 MAC 地址表

因为在配置静态路由时，只配置了一条 PC1 与 PC2 之间的通路，也即 192.168.1.0/24 与 192.168.3.0/24 网段之间的互联，其通过静态路由网段 192.168.2.0/24，而不会经过 192.168.6.0/24，所以交换机并不会接收到路由器 1 和路由器 2 之间传输的数据包。因此 MAC 地址表中也只会 0/24 号端口，PC3 的 MAC 信息。

(4)重新启动 Wireshark 捕获,用 PC2 ping PC1,查看是否可以捕获到 ARP 包、Echo 请求包和 Echo 响应包。如果有则对捕获的包截屏。查看并记录（截屏）PC1 的 ARP 缓冲区。最后，对结果进行分析。

此时用 PC2 ping PC1:

```
C:\Users\Administrator>ping 192.168.1.11

正在 Ping 192.168.1.11 具有 32 字节的数据:
来自 192.168.1.11 的回复: 字节=32 时间=38ms TTL=62
来自 192.168.1.11 的回复: 字节=32 时间=40ms TTL=62
来自 192.168.1.11 的回复: 字节=32 时间=40ms TTL=62
来自 192.168.1.11 的回复: 字节=32 时间=37ms TTL=62

192.168.1.11 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 = 37ms, 最长 = 40ms, 平均 = 38ms
```

图 14: PC1 ping PC2

在 PC3 上开启 Wireshark 捕获数据包，结果如下图所示：

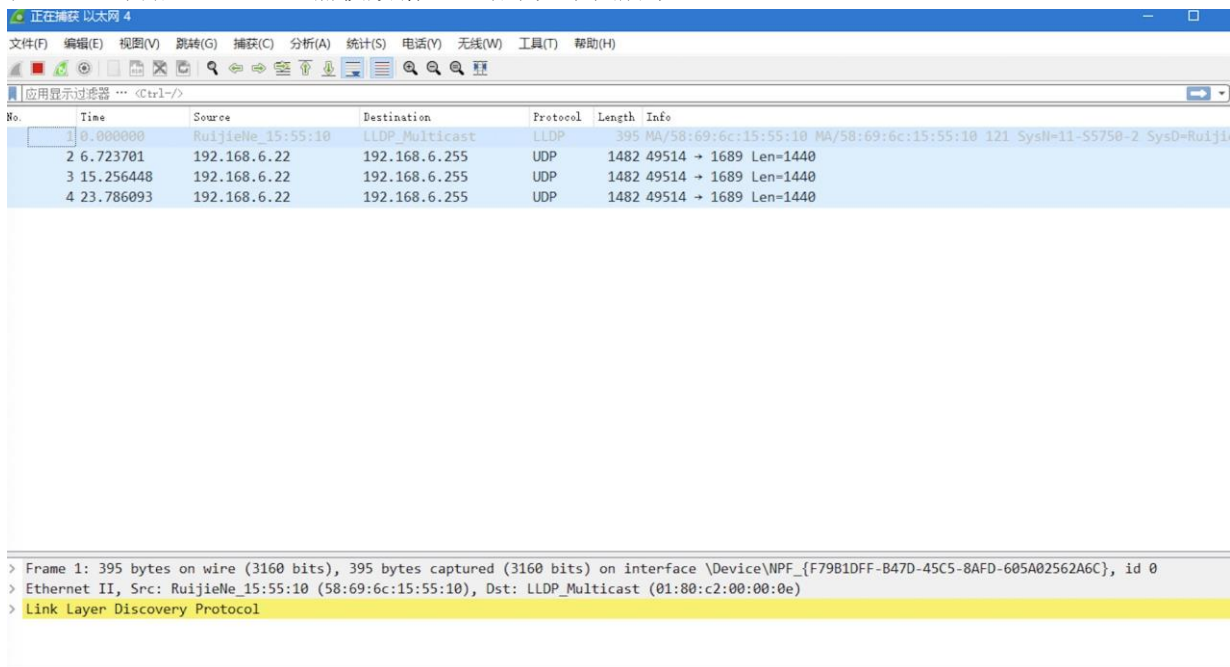


图 15: PC3 Wireshark 截图

由于还未设置端口镜像，此时 PC3 无法收到 PC2 ping PC1 的 ICMP 数据包，并且由于在该拓扑结构中，当设置好各机的 IP 后，只有该 PC 到路由器的 ARP 包，PC3 不会收到 ARP 包。

可以看到抓捕到的数据包中只有本网段的相关数据包(UDP 广播包、链路层发现协议 LLDP)等包。



```
C:\Users\Administrator>arp -d  
  
C:\Users\Administrator>arp -a  
  
接口: 192.168.1.11 --- 0x6  
Internet 地址      物理地址      类型  
192.168.1.255      ff-ff-ff-ff-ff-ff 静态  
224.0.0.22         01-00-5e-00-00-16 静态
```

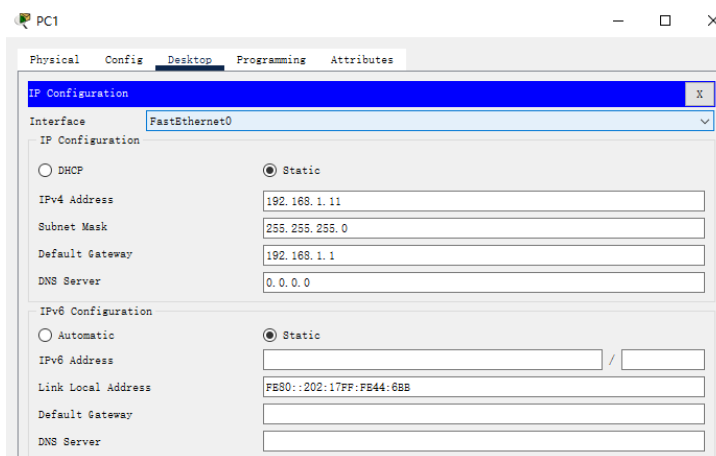
图 16: PC1 arp 缓冲区 (ping 之前)

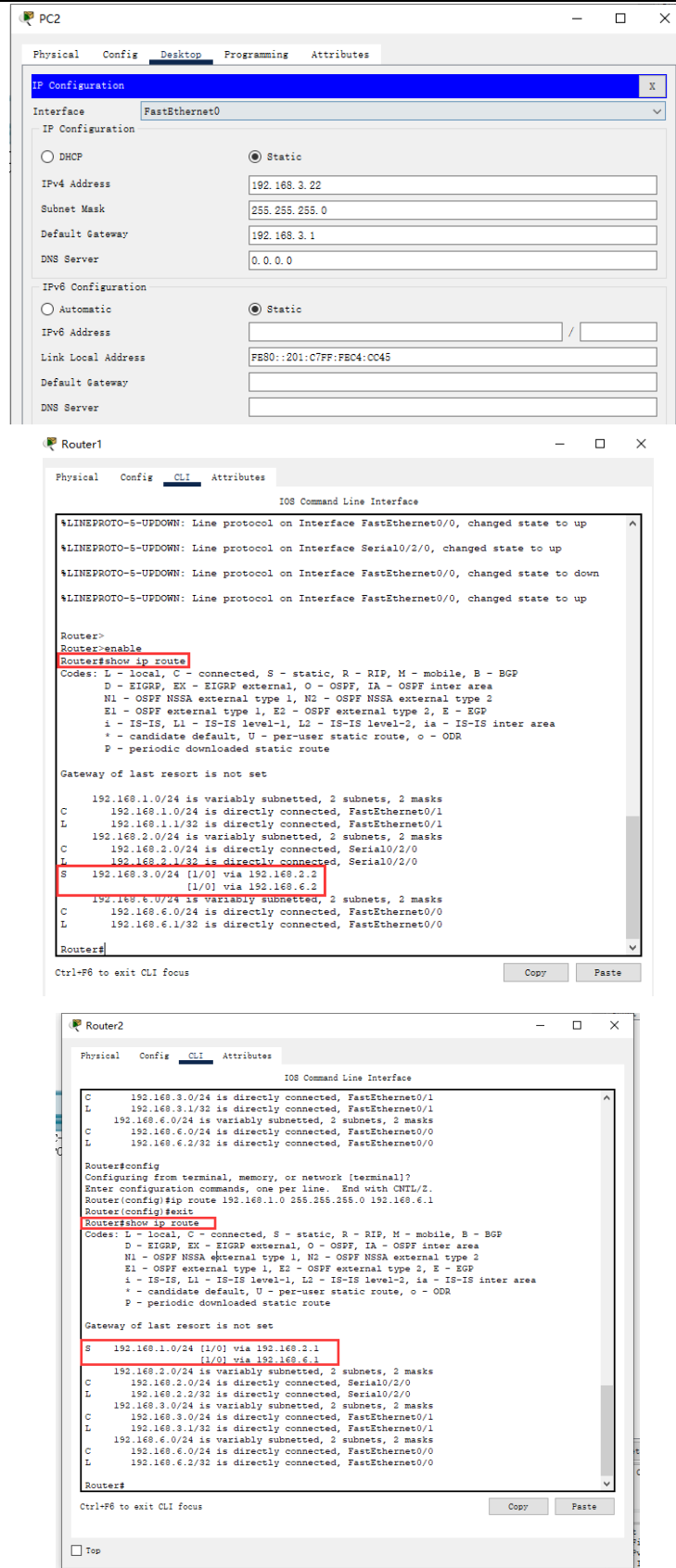
```
C:\Users\Administrator>arp -a  
  
接口: 192.168.1.11 --- 0x6  
Internet 地址      物理地址      类型  
192.168.1.1        58-69-6c-27-c1-9a 动态  
192.168.1.255      ff-ff-ff-ff-ff-ff 静态  
224.0.0.22         01-00-5e-00-00-16 静态  
  
C:\Users\Administrator>
```

图 17: PC1 arp 缓冲区 (ping 之后)

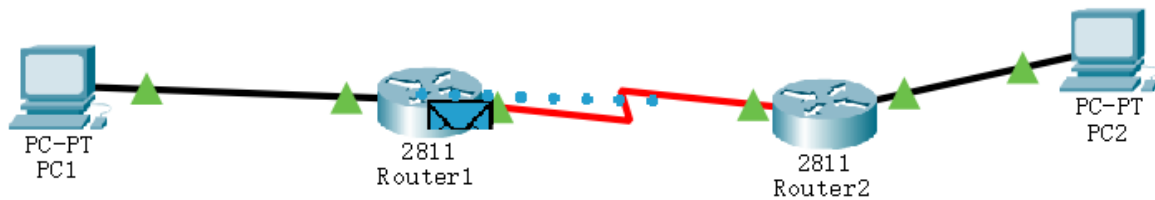
此时 PC1 中的 ARP 缓冲区的地址在 ping 通之间只有本网段的广播地址 192.168.1.255 与预留的组播地址 224.0.0.22, 而在 ping 通之后, 新增了 PC1 的默认网关地址 192.168.1.1。

(5) 利用 Packet Tracer 数据包的 Flash 动画功能, 在模拟模式下, 展示 PC1 与 PC2 间的数据包流动情况。





在 Packet Tracer 中配置 PC1 和 PC2 与路由器 R1, R2 如上图所示, 其中要在路由器 2811 中加入串行口 WIC-1T, 此时用 PC1 ping PC2, 发现可以 PC1 与 PC2 互通:



(6) 把交换机的端口 F0/2 镜像到端口 F0/24, 再用 PC1 ping PC2。查看 PC3 是否可以捕获到 ARP 包、Echo 请求包和 Echo 响应包, 如果可以捕捉到, 则记录结果(截屏)。查看并记录此时交换机的 MAC 地址表。对结果进行解释说明。

为了使 PC1 ping PC2 的数据包经过交换机网段, 需要在路由器 R1 和 R2 上实现交换机到目的网段的静态路由:

```
Router1(config)#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.1.1/32 is local host.
C    192.168.2.0/24 is directly connected, Serial 2/0
C    192.168.2.1/32 is local host.
S    192.168.3.0/24 [1/0] via 192.168.2.2
                                     [1/0] via 192.168.6.2
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.6.1/32 is local host.
Router1(config)#
```

```
Router2(config)#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
S    192.168.1.0/24 [1/0] via 192.168.2.1
                                     [1/0] via 192.168.6.1
C    192.168.2.0/24 is directly connected, Serial 2/0
C    192.168.2.2/32 is local host.
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.3.1/32 is local host.
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.6.2/32 is local host.
Router2(config)#
```

把交换机的端口 F0/2 镜像到端口 F0/24 的指令如下图所示:

图 18: 端口镜像指令操作图



```
11-S5750-2#conf
11-S5750-2#configure
Enter configuration commands, one per line. End with CNTL/Z.
11-S5750-2(config)#host
11-S5750-2(config)#hostname switch2
switch2(config)#mo
switch2(config)#monitor se
switch2(config)#monitor session 1 sou
switch2(config)#monitor session 1 source inte
switch2(config)#monitor session 1 source interface giga
switch2(config)#monitor session 1 source interface gigabitEthernet 0/2
switch2(config)#moni
switch2(config)#monitor ses
switch2(config)#monitor session 1 des
switch2(config)#monitor session 1 destination inte
switch2(config)#monitor session 1 destination interface gi
switch2(config)#monitor session 1 destination interface gigabitEthernet 0/24
switch2(config)#show moni
switch2(config)#show monitor
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
GigabitEthernet 0/2          frame-type Both
dest-intf:
GigabitEthernet 0/24
switch2(config)#
```

配置完毕后，再使用 PC1 ping PC2:

```
C:\Users\Administrator>ping 192.168.3.22

正在 Ping 192.168.3.22 具有 32 字节的数据:
来自 192.168.3.22 的回复: 字节=32 时间=38ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=39ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=39ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=39ms TTL=62

192.168.3.22 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 = 38ms, 最长 = 39ms, 平均 = 38ms

C:\Users\Administrator>
```

图 19: PC1 ping PC2 图

同时在 PC3 上打开 Wireshark，可以捕获到 Echo 请求包 和 Echo 响应包，但捕获不到 ARP 包，如下所示：



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------------|----------------|----------|--------|---|
| 1 | 0.000000 | 192.168.1.11 | 192.168.3.22 | ICMP | 84 | Echo (ping) request id=0x0001, seq=1/256, ttl=63 (reply in 2) |
| 2 | 0.000307 | 192.168.3.22 | 192.168.1.11 | ICMP | 78 | Echo (ping) reply id=0x0001, seq=1/256, ttl=63 (request in 1) |
| 3 | 0.487849 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 4 | 1.002323 | 192.168.1.11 | 192.168.3.22 | ICMP | 82 | Echo (ping) request id=0x0001, seq=2/512, ttl=63 (reply in 5) |
| 5 | 1.002640 | 192.168.3.22 | 192.168.1.11 | ICMP | 78 | Echo (ping) reply id=0x0001, seq=2/512, ttl=63 (request in 4) |
| 6 | 2.007897 | 192.168.1.11 | 192.168.3.22 | ICMP | 82 | Echo (ping) request id=0x0001, seq=3/768, ttl=63 (reply in 7) |
| 7 | 2.008248 | 192.168.3.22 | 192.168.1.11 | ICMP | 78 | Echo (ping) reply id=0x0001, seq=3/768, ttl=63 (request in 6) |
| 8 | 3.013564 | 192.168.1.11 | 192.168.3.22 | ICMP | 82 | Echo (ping) request id=0x0001, seq=4/1024, ttl=63 (reply in 9) |
| 9 | 3.013805 | 192.168.3.22 | 192.168.1.11 | ICMP | 78 | Echo (ping) reply id=0x0001, seq=4/1024, ttl=63 (request in 8) |
| 10 | 9.017609 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 11 | 17.547641 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 12 | 21.664857 | RuijieNe_15:55:10 | LLDP_Multicast | LLDP | 248 | MA/58:69:6c:15:55:10 IN/Gi0/2 121 SysN-switch SysD=Ruijie Layer 3 FULL Gigabit Intelligent Switch(S5750-28GT-12P) |
| 13 | 26.080075 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 14 | 34.613734 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 15 | 39.078473 | 192.168.1.11 | 192.168.3.22 | ICMP | 82 | Echo (ping) request id=0x0001, seq=5/1280, ttl=63 (reply in 16) |
| 16 | 39.078716 | 192.168.3.22 | 192.168.1.11 | ICMP | 78 | Echo (ping) reply id=0x0001, seq=5/1280, ttl=63 (request in 15) |
| 17 | 40.080818 | 192.168.1.11 | 192.168.3.22 | ICMP | 82 | Echo (ping) request id=0x0001, seq=6/1536, ttl=63 (reply in 18) |
| 18 | 40.081184 | 192.168.3.22 | 192.168.1.11 | ICMP | 78 | Echo (ping) reply id=0x0001, seq=6/1536, ttl=63 (request in 17) |
| 19 | 41.086305 | 192.168.1.11 | 192.168.3.22 | ICMP | 82 | Echo (ping) request id=0x0001, seq=7/1792, ttl=63 (reply in 20) |
| 20 | 41.086547 | 192.168.3.22 | 192.168.1.11 | ICMP | 78 | Echo (ping) reply id=0x0001, seq=7/1792, ttl=63 (request in 19) |
| 21 | 42.089232 | 192.168.1.11 | 192.168.3.22 | ICMP | 82 | Echo (ping) request id=0x0001, seq=8/2048, ttl=63 (reply in 22) |
| 22 | 42.089373 | 192.168.3.22 | 192.168.1.11 | ICMP | 78 | Echo (ping) reply id=0x0001, seq=8/2048, ttl=63 (request in 21) |
| 23 | 43.145605 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 24 | 51.665408 | RuijieNe_15:55:10 | LLDP_Multicast | LLDP | 248 | MA/58:69:6c:15:55:10 IN/Gi0/2 121 SysN-switch SysD=Ruijie Layer 3 FULL Gigabit Intelligent Switch(S5750-28GT-12P) |
| 25 | 51.675628 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 26 | 60.205697 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 27 | 68.736231 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 28 | 77.270770 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 29 | 81.666038 | RuijieNe_15:55:10 | LLDP_Multicast | LLDP | 248 | MA/58:69:6c:15:55:10 IN/Gi0/2 121 SysN-switch SysD=Ruijie Layer 3 FULL Gigabit Intelligent Switch(S5750-28GT-12P) |
| 30 | 85.798811 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |

图 20: Echo 请求包和 Echo 响应包

在 ping 之前查看并记录交换机的 MAC 地址表，如下所示：

```
switch2#clear mac-address-table dynamic
switch2#show mac-address-table
Vlan          MAC Address          Type          Interface
-----
switch2#
```

图 21: ping 之前交换机的 MAC 地址表

完成 ping 操作后重新查看交换机的 MAC 地址表，如下所示：

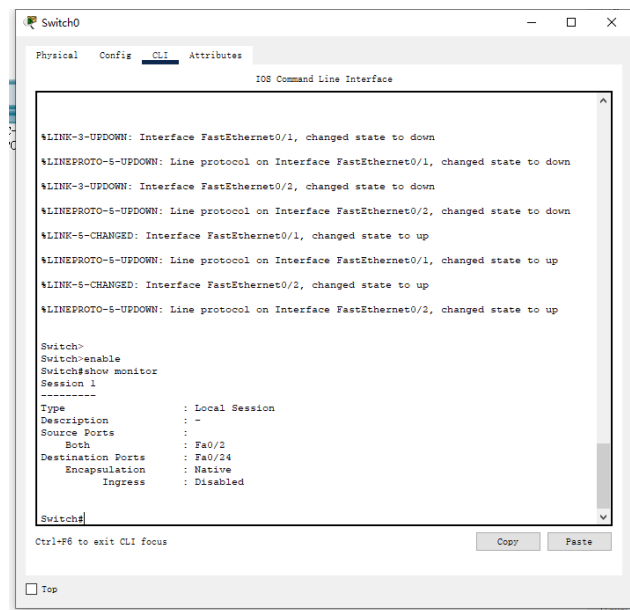
```
switch2#show mac-address-table
Vlan          MAC Address          Type          Interface
-----
1             5869.6c27.c199       DYNAMIC       GigabitEthernet 0/1
1             5869.6c27.c431       DYNAMIC       GigabitEthernet 0/2
switch2#
```

图 22: ping 之后交换机的 MAC 地址表

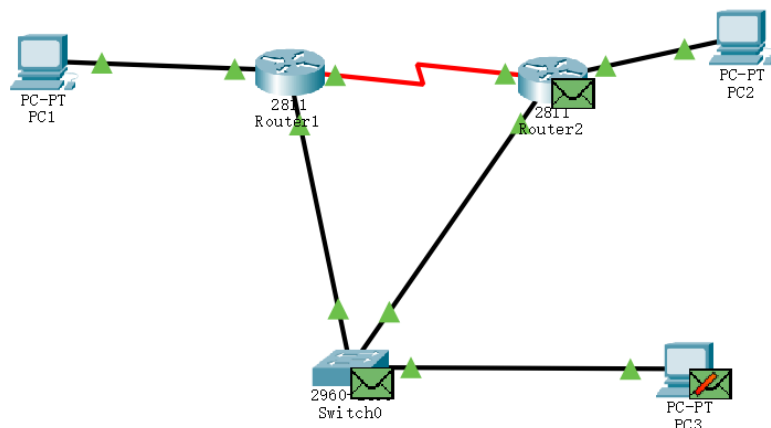
在完成 ping 操作后，再次查看交换机的 MAC 地址表发现，出现了 0/1，0/2 端口的信息，由交换机的 MAC 地址表的学习可以知道，为了使得 PC1 ping PC2 的数据包从交换机的端口 0/2 复制到目的端口 0/24，所以需要在路由器 R1 中添加通过下一跳地址 192.168.6.2 到目的网段 192.168.3.0/24 的静态路由以及在路由器 R2 中添加通过下一跳地址 192.168.6.1 到目的网段 192.168.1.0/24 的静态路由。所以 PC1 ping PC2 的数据包会通过交换机的端口 1 与端口 2，故交换机的 MAC 地址表中端口 0/1 和端口 0/2 的 MAC 地址分别为路由器 R1 和路由器 R2 的以太网口 0/0 的 MAC 地址。

(7) 将 (5) 重做一遍。

配置 Packet Tracer 中的交换机的端口镜像：



同时按照拓扑结构连接后，此时使用 PC1 ping PC2 发现 PC1 ping PC2 的包被镜像到 PC3，并且不仅有 ICMP 包，如果为第一次配置拓扑结构，还会存在 ARP 包：



(8) PC1 运行 `ping -r 6 -l 200 192.168.3.22` 和 `ping -s 4 -l 200 192.168.3.22`（分别带路径和时间戳 ping PC2），在 PC3 上用 Wireshark 进行观察。找出 Echo 请求分组、Echo 响应分组、Timestamp 请求分组、Timestamp 响应分组进行展开并分别截屏。

在 PC1 运行指令 `ping -r 6 -l 200 192.168.3.22`，如下所示：

```
C:\Users\Administrator>ping -r 6 -l 200 192.168.3.22
```

```
正在 Ping 192.168.3.22 具有 200 字节的数据:
```

```
来自 192.168.3.22 的回复: 字节=200 时间<1ms TTL=62
```

```
来自 192.168.3.22 的回复: 字节=200 时间<1ms TTL=62
```

```
来自 192.168.3.22 的回复: 字节=200 时间<1ms TTL=62
```

```
来自 192.168.3.22 的回复: 字节=200 时间<1ms TTL=62
```

```
192.168.3.22 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
```

```
C:\Users\Administrator>
```

图 23: PC1 运行 `ping -r 6 -l 200 192.168.3.22`



此时打开 Wireshark 捕捉数据包，可以捕捉到 Echo 请求包和 Echo 响应包。

使用 ping 参数 -r 6 记录计数跃点的路由，最多记录 6 个路由信息，在 PC1 和 2 之间数据包最多只会经过一个路由器，故这里只有一条路由信息 192.168.6.1

Echo 请求包

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|------------------------|----------------|----------|--------|--|
| 1 | 0.000000 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 2 | 0.435709 | 192.168.1.11 | 192.168.3.22 | ICMP | 278 | Echo (ping) request id=0x0001, seq=89/22784, ttl=63 (reply in 3) |
| 3 | 0.435984 | 192.168.3.22 | 192.168.1.11 | ICMP | 246 | Echo (ping) reply id=0x0001, seq=89/22784, ttl=63 (request in 2) |
| 4 | 1.437657 | 192.168.1.11 | 192.168.3.22 | ICMP | 278 | Echo (ping) request id=0x0001, seq=90/23040, ttl=63 (reply in 5) |
| 5 | 1.437819 | 192.168.3.22 | 192.168.1.11 | ICMP | 246 | Echo (ping) reply id=0x0001, seq=90/23040, ttl=63 (request in 4) |
| 6 | 2.442655 | 192.168.1.11 | 192.168.3.22 | ICMP | 278 | Echo (ping) request id=0x0001, seq=91/23296, ttl=63 (reply in 7) |
| 7 | 2.442848 | 192.168.3.22 | 192.168.1.11 | ICMP | 246 | Echo (ping) reply id=0x0001, seq=91/23296, ttl=63 (request in 6) |
| 8 | 3.445704 | 192.168.1.11 | 192.168.3.22 | ICMP | 278 | Echo (ping) request id=0x0001, seq=92/23552, ttl=63 (reply in 9) |
| 9 | 3.446036 | 192.168.3.22 | 192.168.1.11 | ICMP | 246 | Echo (ping) reply id=0x0001, seq=92/23552, ttl=63 (request in 8) |
| 10 | 8.524346 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 11 | 12.169088 | RuijieNe_15:55:10 | LLDP_Multicast | LLDP | 248 | MA/58:69:6c:15:55:10 IN/Gi0/2 121 SysM=switch SysD=Ruijie Layer 3 FULL |
| 12 | 13.488608 | fe80::967:7a24:7de9... | ff02::1:2 | DHCPv6 | 157 | Solicit XID: 0xa3964e CID: 0001000 2723eb7880c16ee3ca42 |
| 13 | 17.058223 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 14 | 25.590578 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 15 | 34.124503 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 16 | 42.169612 | RuijieNe_15:55:10 | LLDP_Multicast | LLDP | 248 | MA/58:69:6c:15:55:10 IN/Gi0/2 121 SysM=switch SysD=Ruijie Layer 3 FULL |
| 17 | 42.652953 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |

Echo 响应包

Flags: 0x00
Fragment Offset: 0
Time to Live: 63
Protocol: ICMP (1)
Header Checksum: 0xc1f8 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.11
Destination Address: 192.168.3.22
Options: (28 bytes), Record Route
 > IP Option - Record Route (27 bytes)
 > IP Option - End of Options List (EOL)
 > Type: 0
Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xbd62 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 90 (0x005a)

Options: (28 bytes), Record Route
 > IP Option - Record Route (27 bytes)
 > Type: 7
 Length: 27
 Pointer: 8
 Recorded Route: 192.168.6.1
 Empty Route: 0.0.0.0 <- (next)
 Empty Route: 0.0.0.0
 Empty Route: 0.0.0.0
 Empty Route: 0.0.0.0
 Empty Route: 0.0.0.0
 Empty Route: 0.0.0.0
 > IP Option - End of Options List (EOL)

图 24: PC3 捕捉 ping -r 6 -l 200 192.168.3.22 指令数据包图

在 PC1 运行指令 ping -s 4 -l 200 192.168.3.22，如下所示：



```
C:\Users\Administrator>ping -s 4 -l 200 192.168.3.22

正在 Ping 192.168.3.22 具有 200 字节的数据:
来自 192.168.3.22 的回复: 字节=200 时间<1ms TTL=62
来自 192.168.3.22 的回复: 字节=200 时间<1ms TTL=62
来自 192.168.3.22 的回复: 字节=200 时间<1ms TTL=62
来自 192.168.3.22 的回复: 字节=200 时间<1ms TTL=62

192.168.3.22 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

C:\Users\Administrator>
```

图 25: PC1 运行 ping -s 4 -l 200 192.168.3.22

使用 ping -s 参数计数跃点的时间戳:

The image shows a Wireshark packet capture of a ping operation. The packet list shows four ICMP Echo (ping) packets. The first two are requests, and the next two are replies. The packet details pane for the selected packet (packet 3, an ICMP Echo (ping) request) shows the following fields:

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-Set)
- Total Length: 268
- Identification: 0x73bf (29631)
- Flags: 0x00
- Fragment Offset: 0
- Time to Live: 63
- Protocol: ICMP (1)
- Header Checksum: 0xd3f5 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.1.11
- Destination Address: 192.168.3.22
- Options: (40 bytes) **Time Stamp**
- > IP Option - Time Stamp (36 bytes)
- > IP Option - End of Options List (EOL)
- > Type: 0

Red arrows point to the 'Time Stamp' field in the packet details pane for both the request (packet 3) and the reply (packet 4). The text 'Time Stamp 请求分组' (Time Stamp request packet) is written next to the arrow pointing to the request packet's Time Stamp field, and 'Time Stamp 响应分组' (Time Stamp response packet) is written next to the arrow pointing to the reply packet's Time Stamp field.



```

    Options: (40 bytes), Time Stamp
    IP Option - Time Stamp (36 bytes)
    Type: 68
    0... .... = Copy on fragmentation: No
    .10. .... = Class: Debugging and measurement (2)
    ...0 0100 = Number: Time stamp (4)
    Length: 36
    Pointer: 13
    0000 .... = Overflow: 0
    .... 0001 = Flag: Time stamp and address (0x1)
    Address: 192.168.6.1
    Time stamp: 33769000
    Address: -
    Time stamp: 0
    Address: -
    Time stamp: 0
    Address: -
    Time stamp: 0
    IP Option - End of Options List (EOL)
    Type: 0
    0... .... = Copy on fragmentation: No
    .00. .... = Class: Control (0)
    ...0 0000 = Number: End of Option List (EOL) (0)
  
```

图 26: PC3 捕捉 ping -s 4 -l 200 192.168.3.22 指令数据包图

(9) 删除路由器 1 上的静态路由，并增加默认路由指向路由器 2 的以太网端口。PC1 ping PC2，用 Wireshark 进行观察并截屏。

删除路由器 1 上的静态路由并增加默认路由指令如下：

```

Router2(config)#no ip route 192.168.1.0 255.255.255.0 192.168.2.1
Router2(config)#no ip route 192.168.1.0 255.255.255.0 192.168.6.1
Router2(config)#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.2.0/24 is directly connected, Serial 2/0
C    192.168.2.2/32 is local host.
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.3.1/32 is local host.
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.6.2/32 is local host.

Router2(config)#ip add
Router2(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.1
Router2(config)#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 192.168.2.1 to network 0.0.0.0
S*   0.0.0.0/0 [1/0] via 192.168.2.1
C    192.168.2.0/24 is directly connected, Serial 2/0
C    192.168.2.2/32 is local host.
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.3.1/32 is local host.
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.6.2/32 is local host.
  
```

删除静态路由指令

增加默认路由指令

图 27: 删除路由器 1 的静态路由，增加默认路由。

在 PC1 ping PC2，如下所示，发现 ping 的延迟大幅增加：



```
C:\windows\system32>ping 192.168.3.22

正在 Ping 192.168.3.22 具有 32 字节的数据:
来自 192.168.3.22 的回复: 字节=32 时间=2142ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=2135ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=2093ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=2250ms TTL=62

192.168.3.22 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 = 2093ms, 最长 = 2250ms, 平均 = 2155ms
```

图 28: PC1 ping PC2 图。

此时在 PC3 打开 Wireshark 截图, 如下所示, 只能抓到 ICMP 的 Echo 的应答数据包, 由分析知, 之前路由器 1 是有 2 条静态路由记录的, 删除对应记录并设置对应的默认路由后, PC1 发往 PC2 的数据包会通过路由器 1 的默认路由, 即经过 192.168.2.0/24 网段, 而不会经过 192.168.6.0/24。所以连接交换机的 PC3 并不会接收到 PC1 发往 PC2 的数据包, 但是此时路由器 2 尚有 2 条静态路由记录, 因此 PC2 发往 PC1 的数据包经过 192.168.6.0/24 网段, 且由于交换机端口镜像监控了端口 0/2 的双向数据流, 所以连接交换机的 PC3 会收到 PC2 发往 PC1 的数据包, 即 ICMP 的 Echo 应答数据包。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------------|---------------|----------|--------|---|
| 1 | 0.000000 | 192.168.3.22 | 192.168.1.11 | ICMP | 246 | Echo (ping) reply id=0x0001, seq=42/10752, ttl=63 |
| 2 | 1.004080 | 192.168.3.22 | 192.168.1.11 | ICMP | 246 | Echo (ping) reply id=0x0001, seq=43/11008, ttl=63 |
| 3 | 2.008163 | 192.168.3.22 | 192.168.1.11 | ICMP | 246 | Echo (ping) reply id=0x0001, seq=44/11264, ttl=63 |
| 4 | 2.520757 | RuijieNe_15:55:10 | 192.168.1.11 | LLDP | 248 | MA/58:69:60:15:55:10 IN/G10/2 121 SysN=switch SysD=Ruijie Layer 3 |
| 5 | 3.012206 | 192.168.3.22 | 192.168.1.11 | ICMP | 246 | Echo (ping) reply id=0x0001, seq=45/11520, ttl=63 |
| 6 | 4.176790 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 7 | 12.710508 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 8 | 21.243930 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |
| 9 | 29.773745 | 192.168.6.22 | 192.168.6.255 | UDP | 1482 | 59514 → 1689 Len=1440 |

图 29: PC3 开 Wireshark 捕获数据包图

删除路由器 2 上的静态路由, 并增加默认路由指向路由器 1 的以太网端口。PC1 ping PC2, 用 Wireshark 进行观察并截屏。

删除路由器 2 上的静态路由操作如下所示因为我们前面分别设置了两条路由路径, 这里我们使用 no 删除对应静态路由, 并加入默认路由, 让默认路由指向 192.168.2.1。

```
Router2(config)#no ip route 192.168.1.0 255.255.255.0 192.168.2.1
Router2(config)#no ip route 192.168.1.0 255.255.255.0 192.168.6.1
Router2(config)#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.2.0/24 is directly connected, Serial 2/0
C    192.168.2.2/32 is local host.
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.3.1/32 is local host.
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.6.2/32 is local host
Router2(config)#ip add
Router2(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

删除静态路由

增加默认路由

图 30: 删除路由器 2 的静态路由, 增加默认路由。



此时 PC1 ping PC2，如下图所示：

```
C:\windows\system32>ping 192.168.3.22

正在 Ping 192.168.3.22 具有 32 字节的数据:
来自 192.168.3.22 的回复: 字节=32 时间=2590ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=2637ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=2681ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=2589ms TTL=62

192.168.3.22 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 = 2589ms, 最长 = 2681ms, 平均 = 2624ms
```

图 31: PC1 ping PC2 图。

此时在 PC3 打开 Wireshark，如下所示，无法捕获到 PC1 到 PC2 之间的数据包了。这是因为，配置好路由器 1、2 的默认路由并删除原先的静态路由后，此时只配置了一条通路，也即 192.168.1.0/24 与 192.168.3.0/24 的互联是经过 192.168.2.0/24 网段跳转，而不会经过 192.168.6.0/24，所以交换机并不会接收到路由器 1 和路由器 2 之间传输的数据包，交换机端口 0/2 不能监控到数据包流动，PC3 上无法抓到对应的数据包。

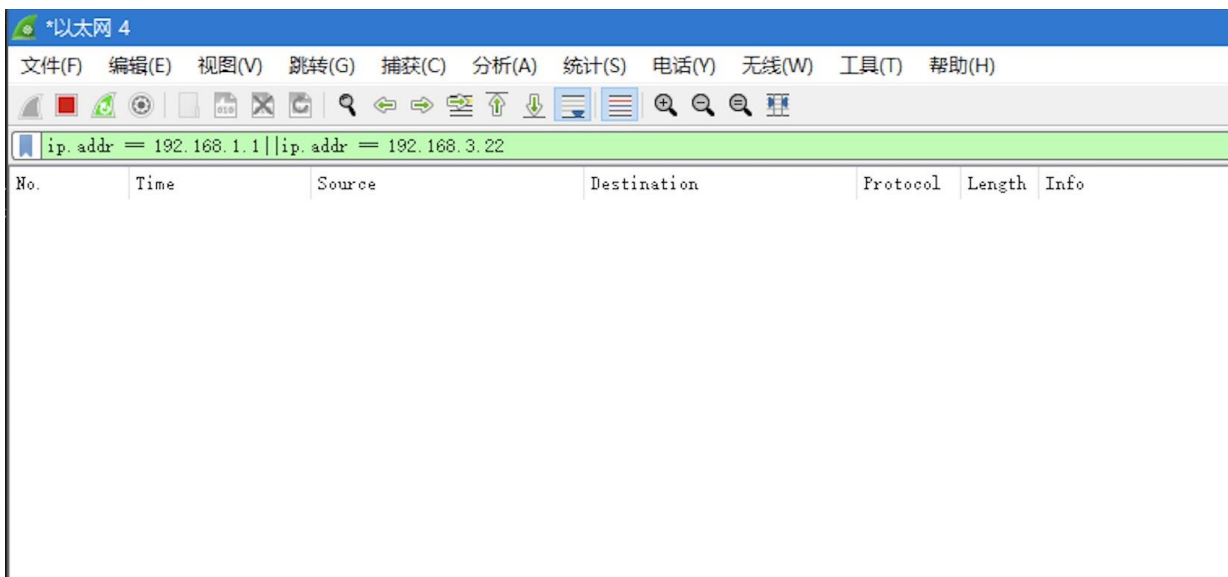


图 32: PC3 开 Wireshark 捕获数据包图

(10) PC1 ping 一个本拓扑结构外的 IP 地址，用 Wireshark 观察流量并截屏，对结果进行分析。使用 PC1 ping 一个本拓扑结构外的 IP，如下所示，我们发现 PC1 无法访问目标网

```
C:\windows\system32>ping www.baidu.com

正在 Ping www.a.shifen.com [183.232.231.172] 具有 32 字节的数据:
来自 192.168.6.2 的回复: 无法访问目标网。
来自 192.168.6.2 的回复: 无法访问目标网。
来自 192.168.6.2 的回复: 无法访问目标网。
来自 192.168.6.2 的回复: 无法访问目标网。

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

图 33: PC1 ping 本拓扑结构外的 IP 图



让 PC1 去 ping 一个本拓扑结构外的 IP，如下所示，可以看到有大量的 ICMP 数据包 Destination unreachable，因为其 IP 地址在拓扑结构外，所以路由的路由表里并没有该 IP 地址，但是路由器配置了默认路由，路由器会将该数据包发往默认路由，因此路由器 1 通过默认路由发给路由器 2，路由器 2 通过默认路由发给路由器 1，所以最终在环路里被不断传播直到超时。

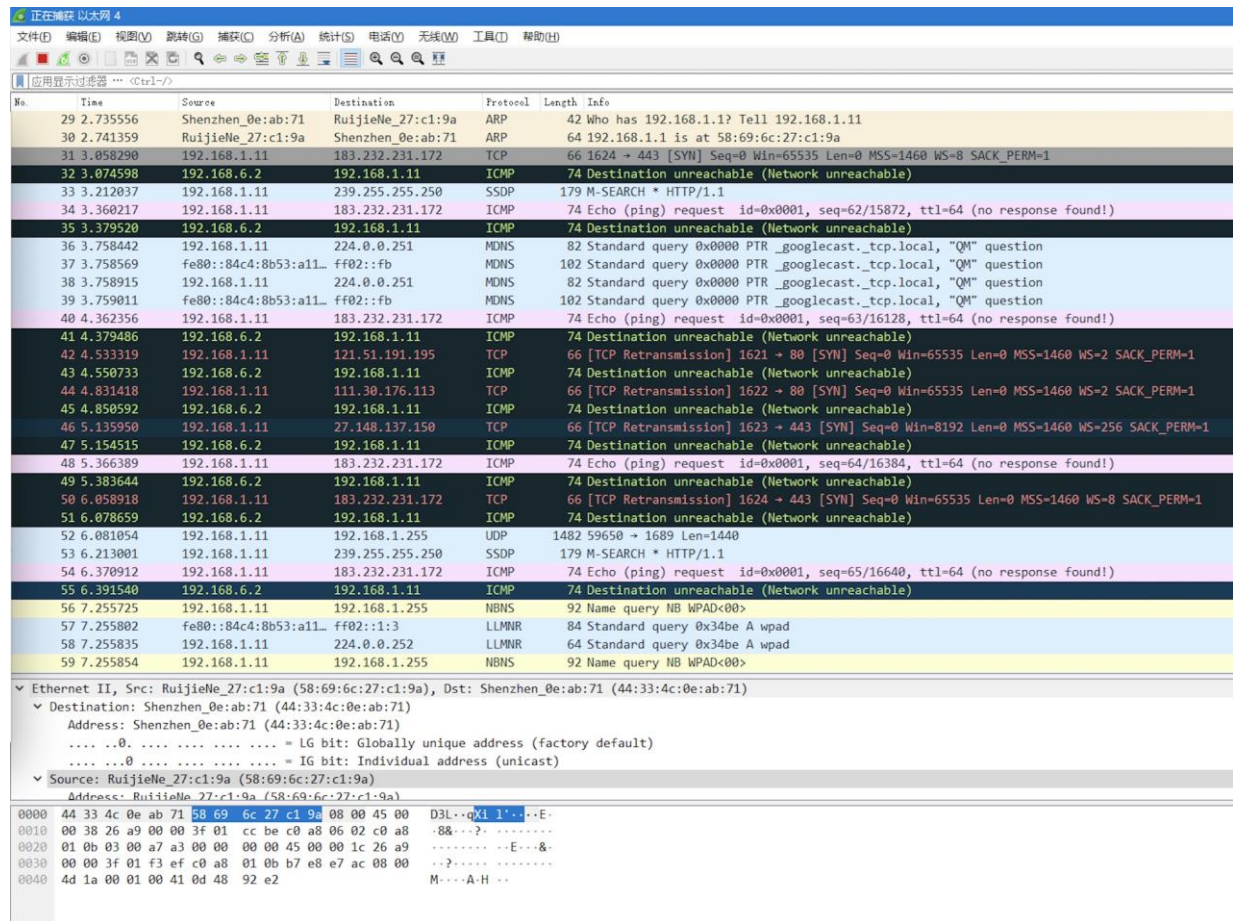


图 34: PC1 开 Wireshark 捕获数据包。

本次实验完成后，请根据组员在实验中的贡献，请实事求是，自评在实验中应得的分数。（按百分制）

| 学号 | 学生 | 自评分 |
|----------|-----|-----|
| 18338072 | 冼子婷 | 98 |
| 18322043 | 廖雨轩 | 98 |
| 18346019 | 胡文浩 | 98 |
| | | |
| | | |

【交实验报告】

上传实验报告：<ftp://222.200.180.109/>

上传包括两个文件：

截止日期（不迟于）：1 周之内



计算机网络实验报告

(1) 小组实验报告。上传文件名格式：小组号_Ftp 协议分析实验.pdf （由组长负责上传）

例如：文件名“10_Ftp 协议分析实验.pdf”表示第 10 组的 Ftp 协议分析实验报告

(2) 小组成员实验体会。每个同学单独交一份只填写了实验体会的实验报告。只需填写自己的学号和姓名。

文件名格式：小组号_学号_姓名_Ftp 协议分析实验.pdf （由组员自行上传）

例如：文件名“10_05373092_张三_Ftp 协议分析实验.pdf”表示第 10 组的 Ftp 协议分析实验报告。

注意：不要打包上传！