计算机网络实验报告

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。

院系	软件学院	班 级	软工 1 班	组长	崔子潇
学号	19308024	19335040	19335286		
学生	崔子潇	丁维力	郑有为		
实验分工					
崔子潇	操作 PC1，管理路由器 1，搭建实验室路由，收集实验截图，实验分析	丁维力	操作 PC2，管理路由器 2，搭建实验室路由，收集实验截图，实验分析		
郑有为	操作 PC3，使用 Packet Tracer 搭建模拟环境，录制剪辑视频，实验报告编写				

【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】

一、阅读教材 P190-192 关于端口镜像的内容

配置端口镜像的方法：

1. 配置源端口和配置目的端口(目的端口即作为镜像的端口)：

```
Switch enable
Switch# config terminal
Switch(config)# monitor session session_number(端口镜像会话号,例如填 1 ) source/destination(选一) interface type interface-id(例如 fa0/1,指定多个用逗号隔开) [rx/tx/both]
```

2. 取消端口镜像：`no monitor session session_number/all`
3. 查看镜像配置：`show monitor`

二、阅读教材 P233 实例 7-1

静态路由：由管理员创建和维护的固定路由表。

1. 三种接口：局域网接口（f0/1 或 gi0/1），广域网接口（serial 2/0），配置接口（Console 接口）
2. 为路由器设置一条路由条目，里面需要包含的信息：目的 IP 地址、其子网掩码、下一跳地址、转发端口
3. 路由遵循匹配原则（与路由的子网掩码进行捍卫逻辑与）和最长前缀原则

配置静态路由的方法：

1. 路由器上查看路由表信息：`show ip route`；PC 命令行查看路由表信息：`route print`
2. 进入路由器指定端口进行配置（config #模式），如 gi0/1：`interface gi0/1`
3. 配置端口 ip 并开启该端口：

```
ip address 网段 子网掩码
```

```
no shutdown
```

4. 配置静态路由：`ip route` 目的 `ip` 子网掩码 下一跳路由 `ip`

三、阅读教材 P29 熟悉 Packet Tracer 使用实例

四、完成教材 P273 习题 15

15. 在如图 7-36 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：

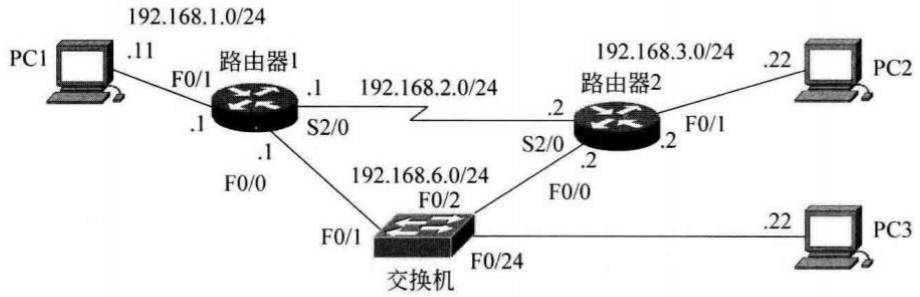


图 7-36 第 15 题拓扑结构

1、记录两台路由器的路由表

如上图，每个路由器的路由表都包含：一条从与其直连的 PC 到另一个路由器的静态路由，和三个端口 IP。

```
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
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.6.1/32 is local host.
```

（路由器 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    192.168.3.2/32 is local host.
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.6.2/32 is local host.
```

（路由器 2）

2、PC1 ping PC2，记录交换机 MAC 地址表

如下图，PC1 ping PC2 可以 ping 通，交换机的 MAC 地址表有两条内容，分别为 Gi0/2 和 Gi0/24。

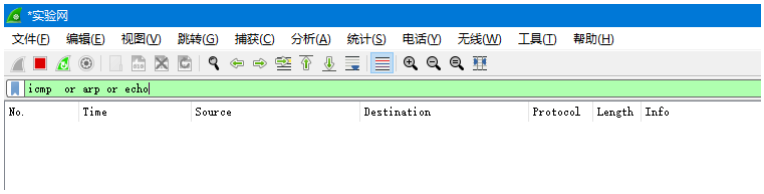
```
C:\Users\Administrator>ping 192.168.3.22

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=37ms 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=38ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=38ms TTL=62
```

```
Switch(config)#show mac-address-table
Vlan        MAC Address          Type      Interface
----------  -------------------- --------  --------------------
   1        0088.9900.1351       DYNAMIC   GigabitEthernet 0/24
   1        5869.6c27.c3ed       DYNAMIC   GigabitEthernet 0/2
```

3、重启 MAC 地址表，启动 Wireshark 捕获，PC1 ping PC2，查看 PC3 是否可以捕获到 ARP 包、Echo 请求包和 Echo 相应包，记录交换机 MAC 地址表。

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

（重启交换机地址表，记录交换机 MAC 地址表）



（PC1 ping PC2，PC3 无法捕获到 ARP 包、Echo 请求包和 Echo 相应包）

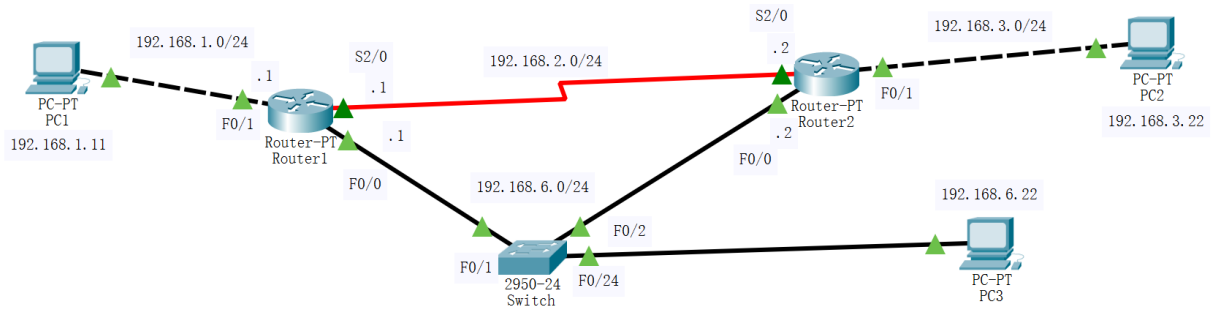
4、重启 Wireshark 捕获，PC2 ping PC1，查看是否可以捕获到 ARP 包、Echo 数据包和 Echo 响应包。有则对捕获的包截屏，查看并记录 PC1 的 ARP 缓冲区，并分析结果

PC3 依然不可以捕获到 ARP 包、Echo 数据包和 Echo 响应包，PC1 的 ARP 缓冲区结果如下：第一行是 PC1 的 IP 地址。

```
C:\Users\Administrator>arp -a

接口: 192.168.1.11 --- 0x5
  Internet 地址         物理地址              类型
  192.168.1.1           58-69-6c-27-bf-a6     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
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
```

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 之间的数据包流动情况

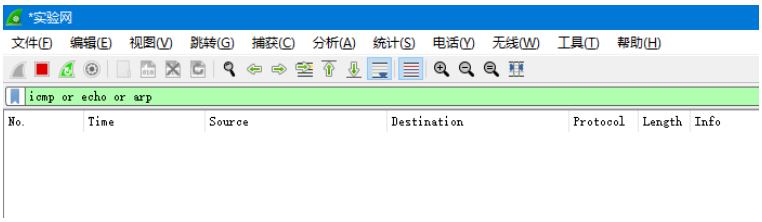
实验视频：5.mp4



6、把交换机的端口 F0/2 镜像到 F0/24，再用 PC1 ping PC2，查看 PC3 是否可以捕获到 ARP 包、Echo 请求、响应包，查看记录此时交换机 MAC 地址表，对其结果进行解释和说明

```
Switch#con
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#monitor session 1 source interface gi 0/2 both
Switch(config)#monitor session 1 destination interface gi 0/24 both
                                                                ^
% Invalid input detected at '^' marker.

Switch(config)#monitor session 1 destination interface gi 0/24
Switch(config)#show monitor
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
GigabitEthernet 0/2          frame-type Both
dest-intf:
GigabitEthernet 0/24
Switch(config)#
```

（端口镜像配置）



PC3 启动 Wireshark，依然没有捕获到 PC1 ping PC2 过程的包，原因是，在 PC1 发送到路由器 1 后，路由器直接经过路由表对其进行转发，不会经过交换机，根据第五题画出的拓扑图我们可以看到，一旦包没有经过交换机，交换机上设置的静态端口就不会起作用，因此端口 F0/24 依然没有检测到任何 ICMP、ARP、echo 包。

7、将（5）重做一次

实验视频已经与（5）的整合在了一起，可以看到结果同（6）相同，数据报不经过交换机，端口镜像无反应。

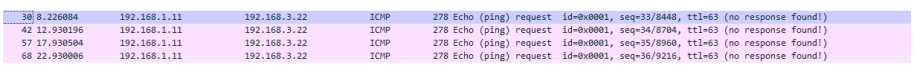
8、PC1 运行 ping -r 6 -l 200 192.168.3.22 和 ping -s 4 -l 200 192.168.3.22（分别带路径和时间戳 ping PC2），PC3 上用 Wireshark 观察，观察 Echo 分组和 Timestamp 分组

无法捕获到相关数据报文，原因同第六问提到的一样。

9、删除路由器 1 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，PC3 用 Wireshark 进行观察

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 192.168.6.2
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 192.168.6.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 192.168.6.2
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.
C     192.168.6.0/24 is directly connected, GigabitEthernet 0/0
C     192.168.6.1/32 is local host.
Router1(config)#
```

（路由器 1 配置过程）



（ping -r 抓包结果）

（ping -s 抓包结果，以捕获时间戳）

```
Protocol: ICMP (1)
Header Checksum: 0xce66 [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: 0xbd9b [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 33 (0x0021)
  Sequence Number (LE): 8448 (0x2100)
  [No response seen]
  Data (200 bytes)
    Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869…
    [Length: 200]
```

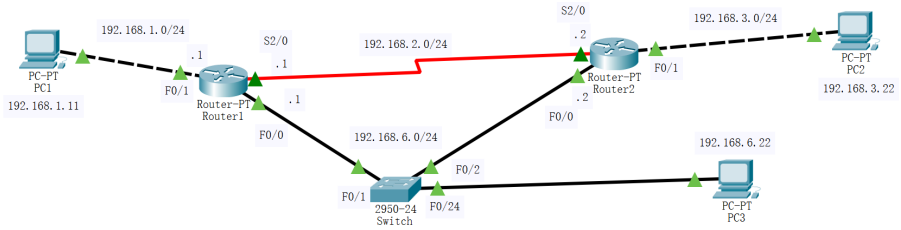
（ICMP 包局部信息）

```
Options: (40 bytes), Time Stamp
  IP Option - Time Stamp (36 bytes)
    Type: 68
    Length: 36
    Pointer: 13
    0000 .... = Overflow: 0
    .... 0001 = Flag: Time stamp and address (0x1)
    Address: 192.168.6.1
    Time stamp: 55736180
    Address: -
    Time stamp: 0
    Address: -
    Time stamp: 0
    Address: -
    Time stamp: 0
  IP Option - End of Options List (EOL)
    Type: 0
```

（Timestamp 请求分组）

从上述两次 ping 中可以看到，每次 PC3 只捕捉到了四个从 PC1 发送到 PC2 的包，但是没有检测到 PC2 返回给 PC1 的数据包，并且此时，PC1 ping 不通 PC2，原因如下：根据下面一张拓扑图进行分析，当静态路断开后（即图中红色的折线），此时默认路由会把 PC1 发到路由器 1 的 ICMP 包发给交换机，一旦发到交换机，PC3 根据端口镜像捕获到 ICMP 包，故有 Wireshark 截屏得到的四个 echo 请求包。

紧接着，交换机会把 ICMP 包发送给 PC2，即 PC2 包的确接收到数据包的，PC2 准备发送 echo 相应包给 PC1，但是由于红线已经断开，有没有设置默认路由，包会停留在路由器 2 而不再往前发送，自然不经过交换机，PC3 检测不到 echo 响应包，PC1 由于收不到 ICMP 返回包，显示 ping 不通。



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，Wireshark 截屏并分析。

```
Router2(config)#ip route 0.0.0.0 0.0.0.0 192.168.6.1
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 192.168.6.1 to network 0.0.0.0
S*    0.0.0.0/0 [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     192.168.3.2/32 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)#
```

（路由器 2 配置过程）

计算机网络实验报告

```
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>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
```

（ping 截屏）

4708	27.665844	192.168.1.11	192.168.3.22	ICMP	278	Echo (ping) request id=0x0001, seq=25/6400, ttl=63 (reply in 4709)
4709	27.665968	192.168.3.22	192.168.1.11	ICMP	246	Echo (ping) reply id=0x0001, seq=25/6400, ttl=63 (request in 4708)
4794	28.668074	192.168.1.11	192.168.3.22	ICMP	278	Echo (ping) request id=0x0001, seq=26/6656, ttl=63 (reply in 4795)
4795	28.668429	192.168.3.22	192.168.1.11	ICMP	246	Echo (ping) reply id=0x0001, seq=26/6656, ttl=63 (request in 4794)
4948	29.673137	192.168.1.11	192.168.3.22	ICMP	278	Echo (ping) request id=0x0001, seq=27/6912, ttl=63 (reply in 4949)
4949	29.673380	192.168.3.22	192.168.1.11	ICMP	246	Echo (ping) reply id=0x0001, seq=27/6912, ttl=63 (request in 4948)
5162	30.678066	192.168.1.11	192.168.3.22	ICMP	278	Echo (ping) request id=0x0001, seq=28/7168, ttl=63 (reply in 5163)
5163	30.678308	192.168.3.22	192.168.1.11	ICMP	246	Echo (ping) reply id=0x0001, seq=28/7168, ttl=63 (request in 5162)

（PC1 ping PC2 通，检测到 ICMP echo 请求包和响应包）

```
> Frame 4708: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface \Device\NPF_{F79B1DFF-B47D-45C5-8AFD-605A02562A6C}, id 0
> Ethernet II, Src: RuijieNe_27:c3:69 (58:69:6c:27:c3:69), Dst: RuijieNe_27:bf:99 (58:69:6c:27:bf:99)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1
v Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.3.22
    0100 .... = Version: 4
    .... 1100 = Header Length: 48 bytes (12)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 256
    Identification: 0x665f (26207)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0xcf4a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.11
    Destination Address: 192.168.3.22
  > Options: (28 bytes), Record Route
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xbda3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 25 (0x0019)
    Sequence Number (LE): 6400 (0x1900)
    [Response frame: 4709]
  v Data (200 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566768696a6b6c6d…
      [Length: 200]
```

（echo 请求分组）

```
> Frame 4709: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits) on interface \Device\NPF_{F79B1DFF-B47D-45C5-8AFD-605A02562A6C}, id 0
> Ethernet II, Src: RuijieNe_27:bf:99 (58:69:6c:27:bf:99), Dst: RuijieNe_27:c3:69 (58:69:6c:27:c3:69)
v Internet Protocol Version 4, Src: 192.168.3.22, Dst: 192.168.1.11
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 228
    Identification: 0x025a (602)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0xf34d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.3.22
    Destination Address: 192.168.1.11
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xc5a3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 25 (0x0019)
    Sequence Number (LE): 6400 (0x1900)
    [Request frame: 4708]
    [Response time: 0.124 ms]
  v Data (200 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566768696a6b6c6d…
      [Length: 200]
```

（echo 响应分组）

```
Destination Address: 192.168.3.22
Options: (40 bytes), Time Stamp
  IP Option - Time Stamp (36 bytes)
    Type: 68
    Length: 36
    Pointer: 13
    0000 .... = Overflow: 0
    .... 0001 = Flag: Time stamp and address (0x1)
    Address: 192.168.6.1
    Time stamp: 54764250
    Address: -
    Time stamp: 0
    Address: -
    Time stamp: 0
    Address: -
    Time stamp: 0
  IP Option - End of Options List (EOL)
    Type: 0
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xbd9f [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 29 (0x001d)
  Sequence Number (LE): 7424 (0x1d00)
  [Response frame: 9670]
```

（Timestamp 请求）

```
Internet Protocol Version 4, Src: 192.168.3.22, Dst: 192.168.1.11
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 228
  Identification: 0x0266 (614)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment Offset: 0
  Time to Live: 63
  Protocol: ICMP (1)
  Header Checksum: 0xf341 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.3.22
  Destination Address: 192.168.1.11
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0xc59e [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 30 (0x001e)
  Sequence Number (LE): 7680 (0x1e00)
  [Request frame: 10025]
  [Response time: 0.300 ms]
```

（响应包没有时间戳信息）

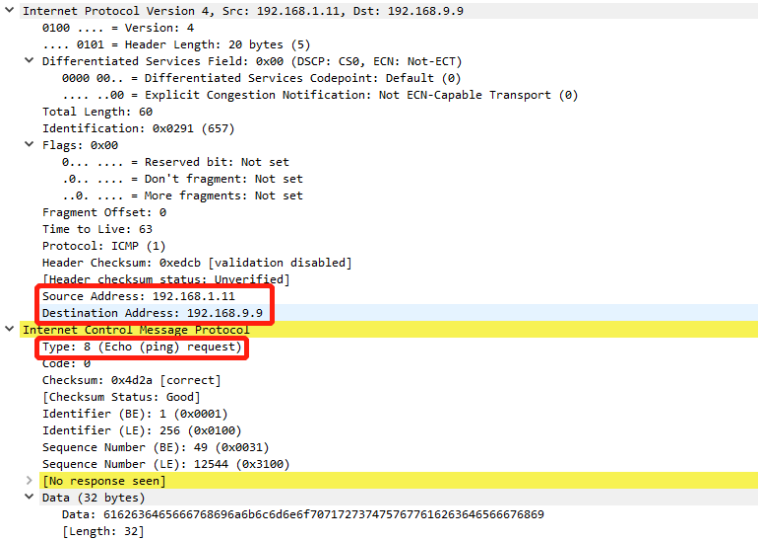
此时 ICMP 请求响应包都能成功通过交换机向另一台 PC 转发，因此端口镜像 PC3 可以捕获到 ping 过程的所有八个包，在抓包过程中没有捕获到 ARP 包，但 ARP 在接线的时候有出现过广播的 ARP 包。

10、PC1 ping 一个本拓扑结构外的 IP，用 Wireshark 观察流量并截屏，对结果进行分析。

我们尝试使用 PC1 ping 一个本拓扑外的 IP，显然 ping 不通，但是依然能检测到四个 Echo 请求包:

54	77.410142	192.168.1.11	192.168.9.9	ICMP	82 Echo (ping) request id=0x0001, seq=49/12544, ttl=63 (no response found!)
67	82.403422	192.168.1.11	192.168.9.9	ICMP	82 Echo (ping) request id=0x0001, seq=50/12800, ttl=63 (no response found!)
77	87.402514	192.168.1.11	192.168.9.9	ICMP	82 Echo (ping) request id=0x0001, seq=51/13056, ttl=63 (no response found!)
88	92.402113	192.168.1.11	192.168.9.9	ICMP	82 Echo (ping) request id=0x0001, seq=52/13312, ttl=63 (no response found!)

(抓包结果)



（echo 请求内容）

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
19308024	崔子潇	100
19335040	丁维力	100
19335286	郑有为	100

【交实验报告】

上传实验报告：ftp://222.200.180.109/　　截止日期（不迟于）：1 周之内

上传包括两个文件：

（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！