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	计算机学院	班 级	行政 1 班	组长	
学号	19335015				
学生	陈恩婷				

【实验题目】**静态路由实验**

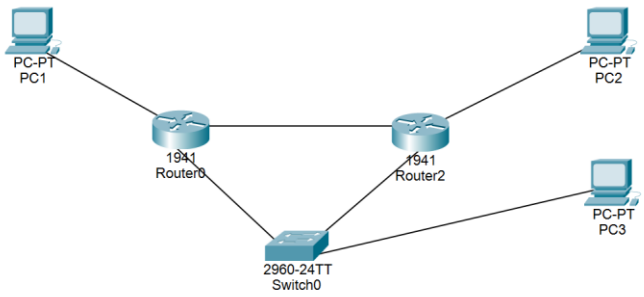
【实验目的】掌握静态路由的配置和使用方法，熟悉交换机端口镜像的方法以及如何用于监视端口。

【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】

在如下图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。



其中路由器 2 的配置结果如下所示：

```
14-RSR20-1(config-if-Serial 2/0)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
14-RSR20-1(config)#show ip int 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        192.168.6.1/24       no address           up                   up
GigabitEthernet 0/1        192.168.1.1/24       no address           up                   up
VLAN 1                     no address           no address           up                   down
```

(1) 记录两台路由器的路由表，如下图所示。

```
14-RSR20-1(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 192.168.6.2
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.6.1/32 is local host.
```

```
14-RSR20-2(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.
```

(2) 用 PC1 ping PC2，记录交换机的 MAC 地址表。

```
C:\Users\Administrator>ping 192.168.3.22 -S 192.168.1.11

正在 Ping 192.168.3.22 从 192.168.1.11 具有 32 字节的数据:
来自 192.168.3.22 的回复: 字节=32 时间=40ms TTL=62
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=37ms TTL=62
来自 192.168.3.22 的回复: 字节=32 时间=40ms 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 = 37ms, 最长 = 40ms, 平均 = 38ms
```

交换机的 MAC 地址表如下：

```
14-S5750-1(config)#show mac-address-table
Vlan        MAC Address          Type      Interface
----------  -------------------- --------  --------------------
   1        0088.9900.1040       DYNAMIC   GigabitEthernet 0/24
   1        1414.4b7b.d9c8       DYNAMIC   GigabitEthernet 0/1
   1        1414.4b7b.e3b4       DYNAMIC   GigabitEthernet 0/2
```

(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。

可以捕获到 ARP 包，不能捕获到 Echo 请求包和响应包。

No.	Time	Source	Destination	Protocol	Length	Info
12	13.261255	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
13	14.400709	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
14	15.261559	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
15	16.261302	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
16	17.400705	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
17	18.261084	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
18	19.261075	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
19	20.833456	192.168.6.22	192.168.6.255	UDP	1482	60951 → 1689 Len=1440
20	23.401487	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
21	24.261046	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
22	25.261213	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
23	29.249191	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
24	29.361512	192.168.6.22	192.168.6.255	UDP	1482	60951 → 1689 Len=1440
25	29.761013	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
26	30.761058	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
27	35.249378	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
28	35.761595	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
29	36.170548	RuijieNe_77:16:94	LLDP_Multicast	LLDP	244	MA/14:14:4b:77:16:94 IN/Gi0/2 121 SysN=14-S5750-1 SysD=Ruijie La
30	36.761682	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
31	37.890903	192.168.6.22	192.168.6.255	UDP	1482	60951 → 1689 Len=1440
32	37.996041	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
33	38.761682	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
34	39.761010	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22

MAC 地址表如下图：

```
14-S5750-1(config)#show mac-address-table
Vlan        MAC Address          Type      Interface
----------  -------------------- --------  --------------------
   1        1414.4b7b.d9c8       DYNAMIC   GigabitEthernet 0/1
   1        1414.4b7b.e3b4       DYNAMIC   GigabitEthernet 0/2
```

(4) 把交换机的端口 gi 0/2 镜像到端口 gi 0/24，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。查看并记录此时交换机的 MAC 地址表。对结果进行解释说明。

可以捕捉到上述数据包。截图如下：

No.	Time	Source	Destination	Protocol	Length	Info
2	0.369454	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=637/32002, ttl=63 (reply in 3)
3	0.369760	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=637/32002, ttl=63 (request in 2)
5	1.374778	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=638/32258, ttl=63 (reply in 6)
6	1.375111	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=638/32258, ttl=63 (request in 5)
9	2.380391	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=639/32514, ttl=63 (reply in 10)
10	2.380671	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=639/32514, ttl=63 (request in 9)
12	3.386037	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=640/32770, ttl=63 (reply in 13)
13	3.386351	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=640/32770, ttl=63 (request in 12)
15	4.391590	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=641/33026, ttl=63 (reply in 16)
16	4.391902	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=641/33026, ttl=63 (request in 15)
17	5.396680	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=642/33282, ttl=63 (reply in 18)
18	5.397048	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=642/33282, ttl=63 (request in 17)
19	6.402193	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=643/33538, ttl=63 (reply in 20)
20	6.402515	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=643/33538, ttl=63 (request in 19)

```
> Frame 154: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{EBC28BE2-6340-4CBB-87CD-F4EB4A236F0F}, id 0
v Ethernet II, Src: RuijieNe_7b:e3:b4 (14:14:4b:7b:e3:b4), Dst: RuijieNe_7b:d9:c8 (14:14:4b:7b:d9:c8)
  > Destination: RuijieNe_7b:d9:c8 (14:14:4b:7b:d9:c8)
  > Source: RuijieNe_7b:e3:b4 (14:14:4b:7b:e3:b4)
    Type: IPv4 (0x0800)
v 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)
    Total Length: 60
    Identification: 0x0343 (835)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0xf30c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.3.22
    Destination Address: 192.168.1.11
> Internet Control Message Protocol
```

如图所示，在 PC3 上捕获到 PC1 ping PC2 的 ICMP 包，其中来自 PC1 的为 Echo 请求包，来自 PC2 的为 Echo 响应包。

(5) 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、Timestamp 请求分组、Timestamp 相应分组进行展开并分别截屏。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=908/35843, ttl=63 (reply in 2)
2	0.000318	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=908/35843, ttl=63 (request in 1)
3	0.150458	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
4	1.004398	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=909/36099, ttl=63 (reply in 5)
5	1.004713	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=909/36099, ttl=63 (request in 4)
6	1.086133	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
7	1.093836	192.168.6.22	192.168.6.255	UDP	1482	60951 → 1689 Len=1440
8	2.009181	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=910/36355, ttl=63 (reply in 9)
9	2.009435	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=910/36355, ttl=63 (request in 8)
10	2.086140	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
11	3.013874	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=911/36611, ttl=63 (reply in 12)
12	3.014187	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=911/36611, ttl=63 (request in 11)
13	3.260605	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
14	4.018656	192.168.1.11	192.168.3.22	ICMP	74	Echo (ping) request id=0x0001, seq=912/36867, ttl=63 (reply in 15)
15	4.018971	192.168.3.22	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=912/36867, ttl=63 (request in 14)
16	4.085831	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22

```
  > Source: RuijieNe_7b:e3:b4 (14:14:4b:7b:e3:b4)
    Type: IPv4 (0x0800)
v 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)
    Total Length: 228
    Identification: 0x04d1 (1233)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0xf0d6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.3.22
    Destination Address: 192.168.1.11
> Internet Control Message Protocol
```

```
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.3.22
    0100 .... = Version: 4
    .... 1111 = Header Length: 60 bytes (15)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 268
    Identification: 0x2734 (10036)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0x2635 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.11
    Destination Address: 192.168.3.22
  > Options: (40 bytes), Time Stamp
> Internet Control Message Protocol
```

如图所示，可见带时间戳的 ping 的 ICMP 包中，有 Optins: (40 bytes), Time Stamp 字样。

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

Ping 运行正常，PC3 能抓到包，如下所示：

```
> Frame 1: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface \Device\NPF_{EBC28BE2-6340-4CBB-87CD-F4EB4A236F0F}, id 0
v Ethernet II, Src: RuijieNe_7b:d9:c8 (14:14:4b:7b:d9:c8), Dst: RuijieNe_7b:e3:b4 (14:14:4b:7b:e3:b4)
  > Destination: RuijieNe_7b:e3:b4 (14:14:4b:7b:e3:b4)
  > Source: RuijieNe_7b:d9:c8 (14:14:4b:7b:d9:c8)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.3.22
    0100 .... = Version: 4
    .... 1111 = Header Length: 60 bytes (15)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 268
    Identification: 0x2734 (10036)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0x2635 [validation disabled]
    [Header checksum status: Unverified]
```

(7) 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。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.11	192.168.7.2	ICMP	74	Echo (ping) request id=0x0001, seq=1275/64260, ttl=63 (no response found!)
2	0.000000	192.168.6.2	192.168.1.11	ICMP	70	Destination unreachable (Network unreachable)
3	0.124088	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
4	0.516985	192.168.1.11	183.192.199.230	UDP	724	57384 → 8000 Len=682
5	0.517300	192.168.6.2	192.168.1.11	ICMP	70	Destination unreachable (Network unreachable)
6	0.859595	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
7	1.004140	192.168.1.11	192.168.7.2	ICMP	74	Echo (ping) request id=0x0001, seq=1276/64516, ttl=63 (no response found!)
8	1.004140	192.168.6.2	192.168.1.11	ICMP	70	Destination unreachable (Network unreachable)
9	1.182020	192.168.6.22	192.168.6.255	UDP	1482	60951 → 1689 Len=1440
10	1.859798	00:88:99:00:10:40	Broadcast	ARP	42	Who has 192.168.6.1? Tell 192.168.6.22
11	2.008773	192.168.1.11	192.168.7.2	ICMP	74	Echo (ping) request id=0x0001, seq=1277/64772, ttl=63 (no response found!)
12	2.008773	192.168.6.2	192.168.1.11	ICMP	70	Destination unreachable (Network unreachable)
13	2.627956	192.168.1.11	183.192.199.230	UDP	724	57384 → 8000 Len=682
14	2.627956	192.168.6.2	192.168.1.11	ICMP	70	Destination unreachable (Network unreachable)
15	3.013551	192.168.1.11	192.168.7.2	ICMP	74	Echo (ping) request id=0x0001, seq=1278/65028, ttl=63 (no response found!)
16	3.013551	192.168.6.2	192.168.1.11	ICMP	70	Destination unreachable (Network unreachable)
17	3.262422	192.168.1.11	183.232.93.211	TCP	62	4689 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
18	3.262422	192.168.6.2	192.168.1.11	ICMP	70	Destination unreachable (Network unreachable)
19	3.300682	RuijieNe_77:16:94	LLDP_Multicast	LLDP	244	MA/14:14:4b:77:16:94 IN/Gi0/2 121 SysN=14-S5750-1 SysD=Ruijie Layer 3 FULL Gigabit Intelligent S
20	4.018987	192.168.1.11	192.168.7.2	ICMP	74	Echo (ping) request id=0x0001, seq=1279/65284, ttl=63 (no response found!)
21	4.018987	192.168.6.2	192.168.1.11	ICMP	70	Destination unreachable (Network unreachable)
22	4.334764	192.168.1.11	183.192.199.230	TCP	66	4691 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
23	4.335083	192.168.6.2	192.168.1.11	ICMP	70	Destination unreachable (Network unreachable)

```
> Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{EBC28BE2-6340-4CBB-87CD-F4EB4A236F0F}, id 0
v Ethernet II, Src: RuijieNe_7b:d9:c8 (14:14:4b:7b:d9:c8), Dst: RuijieNe_7b:e3:b4 (14:14:4b:7b:e3:b4)
  > Destination: RuijieNe_7b:e3:b4 (14:14:4b:7b:e3:b4)
  > Source: RuijieNe_7b:d9:c8 (14:14:4b:7b:d9:c8)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.7.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x3f1d (16157)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0xb346 [validation disabled]
    [Header checksum status: Unverified]
```

如图所示，Ping 一个本拓扑结构外的 IP，会得到路由器返回的 ICMP 包“Destination unreachable”，即目的网不可达。

【实验总结】

在本次实验中，我们成功地在两台交换机之间配置了静态路由与端口镜像，其中也遇到了不少困难，锻炼了在小组内与同学合作、分析问题、解决问题与请教他人的能力，将困难一一解决，体会到了团队协作的快乐和完成实验的成就感。

这次的实验也让我感受到了自己在计算机网络方面的知识在慢慢积累，我希望再接再厉，向老师请教，向同学学习，掌握好这门课程。