

- **E** \*\*\*
- 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	计算机科学与技术		超级计	算方向	组长	林天皓			
学号	18	324034								
学生										
	实验分工									
林天皓		预习并完成实验			<u>朱德鹏</u>	预习并完成实验				
张钺奇		预习并完成实验								

### 【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

### 【实验原理】

本次实验包括配置静态路由使用,以及使用端口镜像观察交换机中的网络数据包,使用 packet tracker 观察网络中数据包的流动情况。

静态路由是由网络管理员手动配置的固定路由表,在不同网段的主机相互连接的过程中,这时数据的传输就需要经过路由器。源主机发送数据包给目标主机,但两台主机又不在同一网段,所以源主机会把数据包发送给本网段的网关路由器,网关路由器接收到数据包后,查看目标 IP 地址再在自己路由表中查找,找到转发路径转发给下一路由器,直到找到并把数据转发给目标主机。

端口镜像 (port Mirroring) 功能通过在交换机或路由器上,将一个或多个源端口的数据流量转发到某一个指定端口来实现对网络的监听,指定端口称之为"镜像端口"或"目的端口",在不严重影响源端口正常吞吐流量的情况下,可以通过镜像端口对网络的流量进行监控分析。在企业中用镜像功能,可以很好地对企业内部的网络数据进行监控管理,在网络出故障的时候,可以快速地定位故障。



Cisco Packet Tracer 是由 Cisco 公司发布的一个辅助学习工具,为学习思科网络课程的初学者去设计、配置、排除网络故障提供了网络模拟环境。 用户可以在软件的图形用户界面上直接使用拖曳方法建立网络拓扑,并可提供数据包在网络中行进的详细处理过程,观察网络实时运行情况。

### 【实验过程和结果】

完成教材 P273 习题 15

本次实验中使用的网络拓扑与实验教材中的一致。如下图。

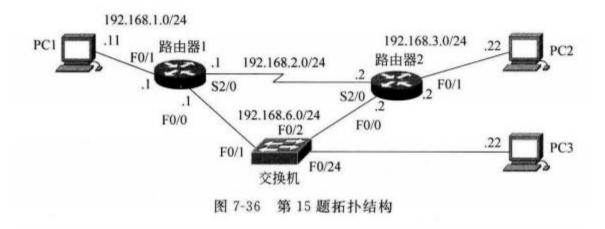


图 1-实验网络拓扑图

首先根据网络拓扑图配置 pc1, pc2, PC3 的 ip 地址

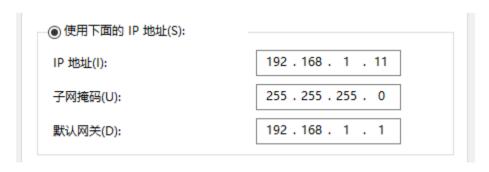


图 2-PC1 设置 IP

PC1, pc2 和 pc3 同理, 不再赘述。

然后配置路由器中的端口 ip 地址。

14-RSR20-1(config)#interface gigabitEthernet 0/1
14-RSR20-1(config-if-GigabitEthernet 0/1)#\$2.168.1.1 255.255.255.0



路由器 1 设置千兆网 1 口地址为 192.168.1.1、子网掩码 255.255.255.0

14-RSR20-1(config-if-GigabitEthernet 0/0)#ip address 192.168.6.1 255.255.255.0

图 4-配置路由器 1 端口 0 IP 地址为 192.168.6.1

路由器 1 设置千兆网 0 口地址为 192.168.6.1, 子网掩码 255.255.255.0

```
14-RSR20-1(config)#interface serial 2/0
14-RSR20-1(config-if-Serial 2/0)#ip address 192.168.2.1 255.255.255.0
```

图 5-配置路由器 1 串口 2 地址

路由器 1 设置串口 2 地址为 192.169.2.1, 子网掩码 255.255.255.0

```
14-RSR20-2(config)#interface gigabitEthernet 0/1
14-RSR20-2(config-if-GigabitEthernet 0/1)#$2.168.3.2 255.255.255.0
14-RSR20-2(config-if-GigabitEthernet 0/1)#interface gig
14-RSR20-2(config)#inter
14-RSR20-2(config)#inter
14-RSR20-2(config)#interface gig
14-RSR20-2(config)#interface gigabitEthernet 0/0
14-RSR20-2(config-if-GigabitEthernet 0/0)#$2.168.6.2 255.255.255.0
14-RSR20-2(config-if-GigabitEthernet 0/0)#exit
14-RSR20-2(config)#interface ser
14-RSR20-2(config)#interface serial 2/0
14-RSR20-2(config)#interface serial 2/0
14-RSR20-2(config-if-Serial 2/0)#ip address 192.168.2.2 255.255.255.0
```

图 6-配置路由器 2 端口 0、1 和串口 2

路由器 2 同理,设置千兆网 1 口地址为 192.168.3.2,子网掩码 255.255.255.0

路由器 2 设置千兆网 0 口地址为 192.168.6.2, 子网掩码 255.255.255.0

路由器 2 设置串口 2 地址为 192.168.2.2, 子网掩码 255.255.255.0

### (1)记录两台路由器的路由表

查看配置结果,查看路由器1与路由器2路由表

```
14-RSR20-1(config-if-Serial 2/0)#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP

0 - 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.

C 192.168.6.0/24 is directly connected, GigabitEthernet 0/0

C 192.168.6.1/32 is local host.
```



### 图 7-查看路由器 1 路由表

在路由器 1 中我们可以查看不同的端口已经被设置为了不同的子网,同时路由器也有三个 localhost 项目。

图 8-查看路由器 2 路由表

在路由器 2 中也拥有了三个子网。192.168.2.0/24, 192.168.3.0/24,192.168.6.0/24

### (2) 用 PC1pingPC2, 记录交换机中的 mac 地址表

```
C:\Users\Administrator>ping 192.168.3.22
正在 Ping 192.168.3.22 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
192.168.3.22 的 Ping 统计信息:
数据包:已发送 = 4,已接收 = 0,丢失 = 4(100% 丢失),
```

图 9-PC1 ping 不通 PC2

一开始 ping 不能联通,使用 tracert 排查故障

```
C:\Users\Administrator>tracert 192.168.3.22
通过最多 30 个跃点跟踪
到 DESKTOP-BVAQLT3 [192.168.3.22] 的路由:
                 <1 臺秒
                            <1 毫秒 172.16.0.1
        1 ms
  2
        2 ms
                  1 ms
                            1 ms 172.18.186.126
                  1 ms
  3
        4 ms
                            4~\mathrm{ms}
                                 10. 44. 185. 201
                 45 ms
       47 ms
                           45 ms
                                  DESKTOP-BVAQLT3 [192.168.3.22]
银踪完成。
```



### 图 10-PC1 tracert PC2

Ping 不同的原因为使用默认路由经过了校园网网关而没有经过我们配置的路由器为网关。

因此我们需要自行手动设置 PC2 中路由表或者拔出校园网卡。

图 10-修改路由表后 PC1 ping 通 PC2

经过拔出校园网后可以PC2 可以ping 通PC1。

然后查看交换机中的 mac 地址表,因为此时我们还没有配置端口镜像,因此我们不能看到 PC1 或者 PC2 的 mac 地址。

图 11-查看交换机 2 的 mac 地址表

经过查看该 mac 地址对应为 PC3 网卡的 mac 地址。

(3) 清楚 mac 地址表,启用 wiresharkk 捕获,用 PC1pingPC2,查看 PC3 是否可以 捕获到 ARP 包,echo 请求包和 echo 响应包





图 12 查看 PC3 捕获数据包

(4) 重新启动 wireshark 捕获,用 PC2pingPC1,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。对结果进行分析。

No.	用显示过滤器 … 《Ctrl- Time	Source	Destination	P1	Length Info
	1 0.000000	192.168.6.22	192.168.6.255	UDP	1482 57143 + 1689 Len=1440
	2 8.529062	192.168.6.22	192.168.6.255	UDP	1482 57143 → 1689 Len=1440
	3 8.850543	RuijieNe 15:57:56	LLDP Multicast	LLDP	395 MA/58:69:6c:15:57:56 MA/58:69:6c:15:57:56 121 SysN=14-S5750-2 SysD=F
L	4 17.058962	192.168.6.22	192.168.6.255	UDP	1482 57143 → 1689 Len=1440

此时我们还没有配置端口镜像,因此我们不能捕获到 ARP 等包。

(5) 利用 packet tracker 数据包的 flash 动画功能,在模拟模式下展示 PC1 与 PC2 间数据包的流动。

在 packet tracker 中使用之前在路由器命令,配置 PC 与交换机

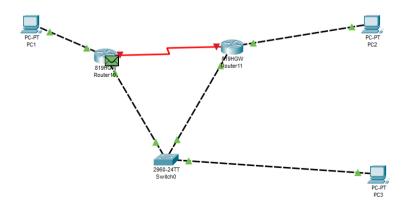


图 13 - packet tracker 模拟模式数据包流动



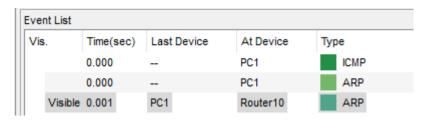


图 14 - acket tracker 查看数据包传递关系

下面我们配置交换机的端口镜像,使得 PC3 可以捕获到 PC1 与 PC2 通信的数据包。

```
14-S5750-2(config)#$urce interface gigabitethernet 0/2 both
14-S5750-2(config)#$stination interface gigabitethernet 0/24
14-S5750-2(config)#show mon
14-S5750-2(config)#show monitor
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
GigabitEthernet 0/2 frame-type Both
dest-intf:
GigabitEthernet 0/24
```

图 15 - 配置交换机 2 的端口镜像

(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,查看此时记录的交换机的 MAC 地址表。对结果进行解释说明。

使用交换机的端口镜像,将交换机端口2的数据包镜像到交换机的24端口上。

然后再使用 PC2pingPC1, 在 PC3 上使用 wireshark 抓包。

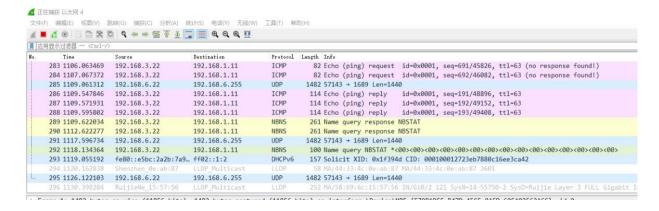


图 16 – PC3 查看 PC1 与 PC2 ping 数据包

可以看到目前在 PC3 上我们可以捕获到 PC1 与 PC2ping 产生的 echo 请求包和 echo 响应包,因此我们的端口镜像配置正常,交换机将 PC1 与 PC2 之间的通信数据包复制到



### 了端口24上。

下面我们再次查看交换机中的 mac 地址表项目,目前我们只能查看到 PC1 和 PC2 的 网卡 mac 地址,不能看到 PC3 的网卡 mac 地址,这是因为端口 24 目前只能接收来自被 镜像端口的数据包,自身不再能发送数据包,因此交换机不再记录该端口的 mac 地址。

```
14-S5750-2#con terminal
14-S5750-2#con terminal
Enter configuration commands, one per line. End with CNTL/Z.
14-S5750-2(config)#show mac-address-table
Vlan MAC Address Type Interface

1 5869.6c27.b81d DYNAMIC GigabitEthernet 0/2
1 5869.6c27.bc35 DYNAMIC GigabitEthernet 0/1
14-S5750-2(config)#
```

图 17 - 再次查看交换机 mac 地址表

### (7) 将(5) 重做一次

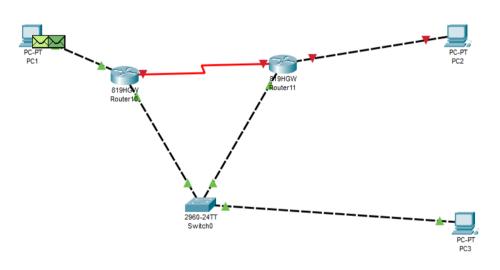


图 18 - 镜像模式后的模拟模式数据包传递图

与上文中不同的是,修改了路由表之后,数据包会被进镜像发往 PC3, PC1 和 PC2 之间的正常通讯也能继续进行。

Vis.	Time(sec)	Last Device	At Device	Туре
	0.000		PC1	ICMP
	0.000		PC1	ARP
	0.881		PC1	ICMP
	0.881		PC1	ICMP
	4 0 4 0		B 1 11	OTD

图 19-镜像模式后的模拟模式数据包传递表



(8) PC1 运行 ping -r 6 -l 200 192.168.3.22 和 ping -s 4 -l 200 192.168.3.44 分别带路径和时间戳 ping PC2,在 PC3 上使用 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析截屏。

	157 381.653436	192.168.1.11	192,168,3,22	NBNS	185 Name query response NBSTAT
	158 386.150177	192.168.1.11	192.168.3.22	ICMP	274 Echo (ping) request id-0x0001, seq-211/54016, ttl-63 (reply in 159)
	159 386.150336	192.168.3.22	192.168.1.11	ICMP	250 Echo (ping) reply id=0x0001, seq=211/54016, ttl=63 (request in 158)
1	160 386.438544	192.168.6.22	192.168.6.255	UDP	1482 57143 → 1689 Len=1440
	161 387.151888	192.168.1.11	192.168.3.22	ICMP	274 Echo (ping) request id=0x0001, seq=212/54272, ttl=63 (reply in 162)
	162 387.152131	192.168.3.22	192.168.1.11	ICMP	250 Echo (ping) reply id=0x0001, seq=212/54272, ttl=63 (request in 161)
	163 388.156474	192.168.1.11	192.168.3.22	ICMP	274 Echo (ping) request id-0x0001, seq-213/54528, ttl-63 (reply in 164)
	164 388.156754	192.168.3.22	192.168.1.11	ICMP	250 Echo (ping) reply id=0x0001, seq=213/54528, ttl=63 (request in 163)
	165 389.161476	192.168.1.11	192.168.3.22	ICMP	274 Echo (ping) request id=0x0001, seq=214/54784, ttl=63 (reply in 166)
-	166 389.161871	192.168.3.22	192.168.1.11	ICMP	250 Echo (ping) reply id=0x0001, seq=214/54784, ttl=63 (request in 165)
	167 390.008472	RuijieNe_15:57:56	LLDP_Multicast	LLDP	252 MA/58:69:6c:15:57:56 IN/Gi0/2 121 SysN=14-S5750-2 SysD=Ruijie Layer 3 FULL Gigabit Intelligent Switch(SS750-28GT-L) By Ruijie Networks
	168 394 969649	192 168 6 22	192 168 6 255	LIDE	1/87 571/3 ± 1689   an=1/1/8

图 20 - 镜像模式后的模拟模式数据包传递表

使用 wireshark 抓包,能看到 echo 请求分组和 echo 响应分组数据包,和 timestamp 请求, timestamp 响应分组数据包。

下面展开 echo 请求分组与 echo 响应分组数据包。查看

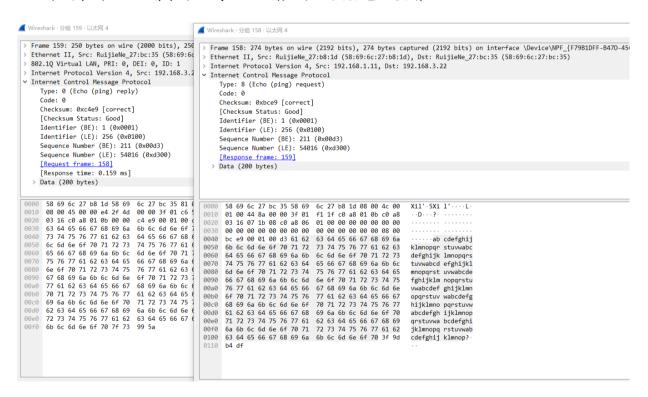


图 21 - echo 请求分组与 echo 响应分组

可见该部分数据包的长度与我们指定的一致,为 200 字节。为从 192.168.1.11 发出,接受方为 192.168.3.22.



```
∨ 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: 5
          0000 .... = Overflow: 0 .... 0001 = Flag: Time stamp and address (0x1)
           Address: -
           Time stamp: 0
           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)

▼ Internet Control Message Protocol

     Type: 8 (Echo (ping) request)
     Code: 0
     Checksum: 0xb677 [correct]
     [Checksum Status: Good]
Identifier (BE): 1 (0x0001)
     Identifier (LE): 256 (0x0100)
Sequence Number (BE): 1861 (0x0745)
     Sequence Number (LE): 17671 (0x4507)
     [Response frame: 56014]
   > Data (200 bytes)
```

图 22 - timestamp 请求分组

```
∨ Flags: 0x00
       0... = Reserved bit: Not set
       .0.. .... = Don't fragment: Not set
       ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x94f3 [validation disabled]
[Header checksum status: Unverified]
     Source Address: 172.18.198.254
    Destination Address: 172.18.198.217
  v Options: (36 bytes), Time Stamp
     IP Option - Time Stamp (36 bytes)
       ∨ Type: 68
            0\dots = 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: 192.168.3.22
         Time stamp: 52784442
         Address:
         Time stamp: 0
         Address:
         Time stamp: 0
          Address: -
         Time stamp: 0

    Internet Control Message Protocol

    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xbe77 [correct]
    [Checksum Status: Good]
     Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
     Sequence Number (BE): 1861 (0x0745)
    Sequence Number (LE): 17671 (0x4507)
     [Request frame: 56012]
     [Response time: 1.475 ms]
  > Data (200 bytes)
```

图 23 - timestamp 响应分组

上述可见 timestamp 请求被放在 IP option 段中, timestamp 回复为 52784442

(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,



### PC1pingPC2, 用 wireshark 进行观察并截屏。

修改路由器中的默认路由

图 24 - 删除路由器 1 原路由, 使用默认路由

图 25 - 删除路由器 2 原路由, 使用默认路由

通过 no 命令删除之前设置的路由表



图 26 - PC1 ping 连接 PC2 正常

结果,通过默认路由 PC1 ping 连接 PC2 正常。

(10) PC1ping 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。

6	正在捕获 以太网 4					- 🗆	$\times$
文件	‡(F) 编辑(E) 视图(V)	跳转(G) 捕获(C) 分析(A)	统计(S) 电话(Y) 无线(W)	工具(T) 報	助(H)		
0		ର   ୧ ⇔ ⇔ ഇ 🕡 🕸	星 🔳 ଭ୍ର୍ର୍ୟ				
I ß	应用显示过滤器 … ⟨Ctrl-/	>					₹.
٥.	Tine	Source	Destination	Protocol	Length Info		
	1323 2599.104364	192.168.1.11	192.168.1.255	NBNS	92 Name query NB WPAD<00>		
	1324 2600.798934	192.168.1.11	183.232.93.211		66 [TCP Retransmission] 2950 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1		
	1325 2600.799042	192.168.1.1	192.168.1.11	ICMP	74 Destination unreachable (Network unreachable)		
	1326 2601.584478	192.168.1.11	192.168.1.255	NBNS	110 Registration NB DESKTOP-BVAQLT3<20>		
	1327 2601.615325	192.168.1.11	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1		
	1328 2602.029404	192.168.1.11	192.168.1.255	UDP	1482 62709 → 1689 Len=1440		
	1329 2603.495103	192.168.1.11	172.18.198.217	TCP	66 2951 → 3389 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1		
	1330 2603.495262	192.168.1.1	192.168.1.11	ICMP	74 Destination unreachable (Network unreachable)		
	1331 2606.496280				66 [TCP Retransmission] 2951 → 3389 [SYN] Seq-0 Win-8192 Len-0 MSS-1460 WS-256 SACK_PERM-1		
	1332 2606.496428	192.168.1.1	192.168.1.11	ICMP	74 Destination unreachable (Network unreachable)		
	1333 2606.799088				62 [TCP Retransmission] 2950 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1		
	1334 2606.799239	192.168.1.1	192.168.1.11	ICMP	74 Destination unreachable (Network unreachable)		
-	1335 2607.818263	192.168.1.11	183.232.93.211	TCP	66 2952 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1		
	1336 2607.818368	192.168.1.1	192.168.1.11	ICMP	74 Destination unreachable (Network unreachable)		
	1337 2608.006016	Shenzhen_0e:ab:7d	RuijieNe_27:b8:1e	ARP	42 Who has 192.168.1.1? Tell 192.168.1.11		
	1338 2608,006754	RuijieNe 27:b8:1e	Shenzhen 0e:ab:7d	ARP	64 192.168.1.1 is at 58:69:6c:27:b8:1e		

图 27 - PC1 ping 192.168.1.17 (不存在的地址)

通过 ping 一个不存在拓扑内的地址,而且不在路由器的路由表中,因此路由器会发回一个网络不可达的数据包通知主机。

### 【实验感想】

本次实验是第一次使用路由器进行配置实验,在实验中,通过手动配置的方式,实现了两台 PC 跨路由器之间的通信,和以前使用的交换机直接就可以通信而通过隔离通信不同,路由器之间都是默认不能连通的,需要配置路由才可以连通,因此我们需要手动配置路由,在本次实验中测试了通过手动控制路由表完成精确选择路由所走的



路线。同时使用端口镜像的过程中,学会了如何在另外的 PC 上查看交换机中的数据包,是一种更加灵活的 debug 方式。使用 packet tracker 的过程中,需要注意思科交换机和实验室中所使用的锐捷交换机的些许区别,例如锐捷交换机一些查看命令在配置模式下也能使用,但是思科交换机只能退出配置模式才能使用等等情况。