



東南大學
SOUTHEAST UNIVERSITY

计算机网络课程 实验报告

学 号 _____ 09021227

姓 名 _____ 金桥

东南大学计算机科学与工程学院

二 0 二三 年 十二 月

目录

1 实验 1.1 物理连通实验	4
1.1 实验内容	4
1.2 实验过程	4
1.3 实验结果分析	4
1.4 实验思考	4
2 实验 2.1 2 台 PC 直连组网	4
2.1 实验内容	4
2.2 实验过程	4
2.2.1 xcap 发包	4
2.2.2 目的 MAC 设置为广播 MAC	5
2.2.3 目的 MAC 设置为对端 PC 机 MAC	5
2.2.4 目的 MAC 设置为未知的 MAC	5
2.3 实验结果分析	5
2.4 实验思考	5
3 实验 2.2 多 PC 通过集线器 HUB 组网	6
3.1 实验内容	6
3.2 实验过程	6
3.3 实验结果分析	6
3.4 实验思考	6
4 实验 2.3 多 PC 通过交换机组网	7
4.1 实验内容	7
4.2 实验过程	7
4.2.1 交换机启动 MAC 学习	7
4.2.2 3 台 PC 机静态配置 IP 地址	7
4.2.3 3 台 PC 间互相 ping, 观察连通性	7
4.3 实验结果分析	7
4.4 实验思考	7
5 实验 2.4 使用交换机 +VLAN 组网	10
5.1 实验内容	10
5.2 实验过程	10
5.2.1 配置 Switch 3 的 VLAN	10
5.3 实验结果分析	10
5.4 实验思考	10
6 实验 3.1 使用 L2 交换机 +L3 交换机组网	12
6.1 实验内容	12
6.2 实验过程	12
6.2.1 配置 Switch 2 的 VLAN	12
6.2.2 配置 Switch 3 的 VLAN	12
6.3 实验结果分析	13

6.4	实验思考	13
7	实验 3.2 路由器/L3 交换机静态路由组网	14
7.1	实验内容	14
7.2	实验过程	14
7.2.1	配置 Switch 3 的 VLAN	14
7.2.2	配置路由器静态路由	14
7.2.3	配置 Switch 3 的静态路由	15
7.3	实验结果分析	15
7.4	实验思考	16
8	实验 3.3 路由器/L3 交换机 OSPF 组网	16
8.1	实验内容	16
8.2	实验过程	16
8.2.1	配置 Switch 3 OSPF	16
8.2.2	配置路由器 OSPF	17
8.3	实验结果分析	17
8.4	实验思考	17

1 实验 1.1 物理连通实验

1.1 实验内容

- 制作一根传输速率为 Gbit/s 的以太网线，作为后续实验链路
- 网线分为直通网线 (Straight through cable) 和交叉网线 (Crossover cable) 两种，当前绝大部分网卡/设备都支持自适应线序，本实验只需要制作直通网线

1.2 实验过程

- 使用网线钳剪下约一米长的网线，并使用剥线钳拨开约 1.5 厘米长的外皮。
- 按照 T568B 线序理线，颜色依次是橙白、橙色、绿白、蓝色、蓝白、绿色、棕白、棕色。
- 使用网线钳减去头部线缆，使其对齐。
- 将线缆插入水晶头并确保线缆插到底部。
- 将水晶头伸入网线钳用力压紧。
- 同样的方法制作网线另一端。



1.3 实验结果分析

采用测线仪对制作的网线进行检测，确认 8 根线缆均已联通。

1.4 实验思考

根据实验所用线材判断，应为双绞线与非屏蔽线。接线器为 RJ45 连接器。

2 实验 2.1 2 台 PC 直连组网

2.1 实验内容

- PC 使用 xcap 模拟发送以太报文 (设置为非 IP 包，例如用 IPX 协议)
 - 目的 MAC 设置为广播 MAC
 - 目的 MAC 设置为对端 PC 机 MAC
 - 目的 MAC 设置为未知的 MAC

2.2 实验过程

使用实验 1.1 中制作的网线连接两台电脑（分别为 A 与 B）的网口。

2.2.1 xcap 发包

- 启动 xcap，右键左侧 Interfaces 中有线网卡对应的 Interface，点击 Start Interface.
- 右键左侧 Packet group 并新建一个分组，命名为 ipx.
- 在右侧空白区域右键添加 Packet，命名为 ipx.
- 在上方选择刚才启动的 Interface，并勾选下方的分组。
- 点击左侧的按钮即可开始发包。

2.2.2 目的 MAC 设置为广播 MAC

- 右键更改分组属性，将目的 MAC 设置为广播 MAC，即 `ff:ff:ff:ff:ff:ff`。
- 在主机 A 上启动发包，在主机 B 上启动 Wireshark 进行观察。

2.2.3 目的 MAC 设置为对端 PC 机 MAC

- 在主机 B 上打开系统设置，查看 MAC 地址。
- 右键更改分组属性，将目的 MAC 设置为对端 PC 机 MAC。
- 在主机 A 上启动发包，在主机 B 上启动 Wireshark 进行观察。

2.2.4 目的 MAC 设置为未知的 MAC

- 右键更改分组属性，将目的 MAC 设置为随机的一个 MAC 地址。
- 在主机 A 上启动发包，在主机 B 上启动 Wireshark 进行观察。

2.3 实验结果分析

实验结果如图 1, 2, 3 所示：

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Xerox_00:00:33	Broadcast	IPX	60	[Malformed Packet]
2	0.989983	Xerox_00:00:33	Broadcast	IPX	60	[Malformed Packet]
3	1.992726	Xerox_00:00:33	Broadcast	IPX	60	[Malformed Packet]
4	2.997821	Xerox_00:00:33	Broadcast	IPX	60	[Malformed Packet]
5	3.987576	Xerox_00:00:33	Broadcast	IPX	60	[Malformed Packet]
6	5.001862	Xerox_00:00:33	Broadcast	IPX	60	[Malformed Packet]
7	5.988107	Xerox_00:00:33	Broadcast	IPX	60	[Malformed Packet]
8	6.992251	Xerox_00:00:33	Broadcast	IPX	60	[Malformed Packet]
9	8.000880	Xerox_00:00:33	Broadcast	IPX	60	[Malformed Packet]
10	8.996729	Xerox_00:00:33	Broadcast	IPX	60	[Malformed Packet]

图 1: 目的 MAC 设置为广播 MAC。可以看到，分组的目的地为 Broadcast，也就是广播地址。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Dell_43:6f:f5	ASUSTekCOMPU_d3...	IPX	60	[Malformed Packet]
2	1.010240	Dell_43:6f:f5	ASUSTekCOMPU_d3...	IPX	60	[Malformed Packet]
3	2.008599	Dell_43:6f:f5	ASUSTekCOMPU_d3...	IPX	60	[Malformed Packet]
4	3.008621	Dell_43:6f:f5	ASUSTekCOMPU_d3...	IPX	60	[Malformed Packet]
5	4.008000	Dell_43:6f:f5	ASUSTekCOMPU_d3...	IPX	60	[Malformed Packet]
6	5.004740	Dell_43:6f:f5	ASUSTekCOMPU_d3...	IPX	60	[Malformed Packet]
7	6.018859	Dell_43:6f:f5	ASUSTekCOMPU_d3...	IPX	60	[Malformed Packet]
8	7.005534	Dell_43:6f:f5	ASUSTekCOMPU_d3...	IPX	60	[Malformed Packet]
9	8.006978	Dell_43:6f:f5	ASUSTekCOMPU_d3...	IPX	60	[Malformed Packet]
10	8.993278	Dell_43:6f:f5	ASUSTekCOMPU_d3...	IPX	60	[Malformed Packet]

图 2: 目的 MAC 设置为对端 PC 机 MAC。可以看到，分组的目的地被替换为主机 B 名称。

2.4 实验思考

1. 抓包看到的以太网帧，与物理链路上传输的数据，有哪些差异？

根据查阅的资料，抓包时看到的以太网帧，与物理链路上传输的数据，主要的差异在于物理层的一些细节，如前导序列、帧间隔、错误检测和物理编码等，这些都是在网卡和硬件中处理的，通常在抓包时是看不到的。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	169.254.247.91	224.0.0.251	MDNS	355	Standard query response 0x0000 TXT, cache
2	0.148248	169.254.198.108	224.0.0.251	MDNS	356	Standard query response 0x0000 TXT, cache
3	0.220142	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x851fff60
4	1.019542	Xerox_00:00:33	7a:7a:c0:a8:c8:...	IPX	60	[Malformed Packet]
5	2.024258	Xerox_00:00:33	7a:7a:c0:a8:c8:...	IPX	60	[Malformed Packet]
6	3.038138	Xerox_00:00:33	7a:7a:c0:a8:c8:...	IPX	60	[Malformed Packet]
7	4.029274	Xerox_00:00:33	7a:7a:c0:a8:c8:...	IPX	60	[Malformed Packet]
8	5.019668	Xerox_00:00:33	7a:7a:c0:a8:c8:...	IPX	60	[Malformed Packet]
9	6.021255	Xerox_00:00:33	7a:7a:c0:a8:c8:...	IPX	60	[Malformed Packet]
10	7.033568	Xerox_00:00:33	7a:7a:c0:a8:c8:...	IPX	60	[Malformed Packet]

图 3: 目的 MAC 设置为未知的 MAC。可以看到, 分组的目的地为设置的 MAC 地址。

3 实验 2.2 多 PC 通过集线器 HUB 组网

3.1 实验内容

- 交换机关闭 MAC 学习, 广播转发, 用来模拟 HUB。
- PC 机间使用网线连接集线器 HUB, 实现互连。
- PC 间使用 xcap 模拟发送以太报文 (可以设置为非 IP 包)

3.2 实验过程

- 将三台电脑连接至设置好的 HUB 上, 分别为 A,B,C。
- 在主机 A 上启动 xcap 发包, 目的 MAC 设置为主机 C 的 MAC 地址。
- 在主机 B 上观察 Wireshark 抓包。

3.3 实验结果分析

实验结果如图 4 所示:

No.	Time	Source	Destination	Protocol	Length	Info
35	26.976987	Dell_43:6f:f5	ASIXElectron_81:25:34	IPX	60	[Malformed Packet]
36	27.969872	Dell_43:6f:f5	ASIXElectron_81:25:34	IPX	60	[Malformed Packet]
37	28.268490	ASIXElectron_81...	Broadcast	ARP	60	Who has 169.254.255.255? Tell 169.2
38	28.821588	HuaweiTechno_bd...	Spanning-tree-(for-bri...	STP	119	MST. Root = 32768/0/8c:68:3a:bd:2e:
39	28.956314	Dell_43:6f:f5	ASIXElectron_81:25:34	IPX	60	[Malformed Packet]
40	29.289367	ASIXElectron_81...	Broadcast	ARP	60	Who has 169.254.255.255? Tell 169.2
41	29.582413	HuaweiTechno_bd...	LLDP_Multicast	LLDP	515	MA/8c:68:3a:bd:2e:42 IN/GigabitEthe
42	29.965864	Dell_43:6f:f5	ASIXElectron_81:25:34	IPX	60	[Malformed Packet]
43	30.712366	HuaweiTechno_bd...	Broadcast	0x9998	60	Ethernet II
44	30.830819	HuaweiTechno_bd...	Spanning-tree-(for-bri...	STP	119	MST. Root = 32768/0/8c:68:3a:bd:2e:

图 4: 主机 B 上 Wireshark 截图。主机 A 为 Dell, 主机 B 为 ASUSTek, 主机 C 为 ASIXElectron。可以看到, 主机 B 观察到了主机 A 发送给主机 C 的数据, 说明 HUB 组网存在隐私问题。

3.4 实验思考

1. PC 机 MAC 地址是怎样分配的? 保存在哪里?

MAC 地址的分配遵循 IEEE 的规定, 由两部分组成: 组织唯一标识符 (OUI) 与扩展标识符。MAC 地址通常是由设备制造商在生产过程中分配并写入到网络接口控制器 (NIC, 也就是网卡) 的固件或硬件中的。

2. 网卡收到其它 PC 的帧，怎样确定是否要继续处理？

当网卡收到一个网络帧时，首先会检查该帧的目标 MAC 地址。网卡会将这个目标 MAC 地址与自己的 MAC 地址进行比较，以确定是否需要继续处理这个帧。

4 实验 2.3 多 PC 通过交换机组网

4.1 实验内容

- 交换机启动 MAC 学习。
- 3 台 PC 机使用 IP 协议，静态配置 IP 地址。
- PC 机使用有线网卡，使用网线，接入临近交换机。
- 3 台 PC 间互相 ping，观察连通性。

4.2 实验过程

4.2.1 交换机启动 MAC 学习

- 用线缆连接交换机 CONSOLE 接口与 PC 机 USB 接口。
- 打开 MobaXterm, 新建会话，选择 Serial, 端口 9600。
- 输入用户名与密码，进入管理平台，依次键入以下命令启动 MAC 学习：
 - `system-view`
 - `vlan 1`
 - `undo mac-address learning disable`

4.2.2 3 台 PC 机静态配置 IP 地址

3 台 PC 机分别配置 IP 地址为：

- 主机 A (本机): 192.168.1.2
- 主机 B: 192.168.1.3
- 主机 C: 192.168.1.4

4.2.3 3 台 PC 间互相 ping, 观察连通性

在终端中分别执行 `ping 192.168.1.3` 与 `ping 192.168.1.4`，观察执行结果。

4.3 实验结果分析

实验结果如图 5, 6, 7, 8 所示。

4.4 实验思考

1. MAC 学习会学习哪几个关键 key？

会学习 MAC 地址与对应的端口，除此以外还有相应的 VLAN 信息。

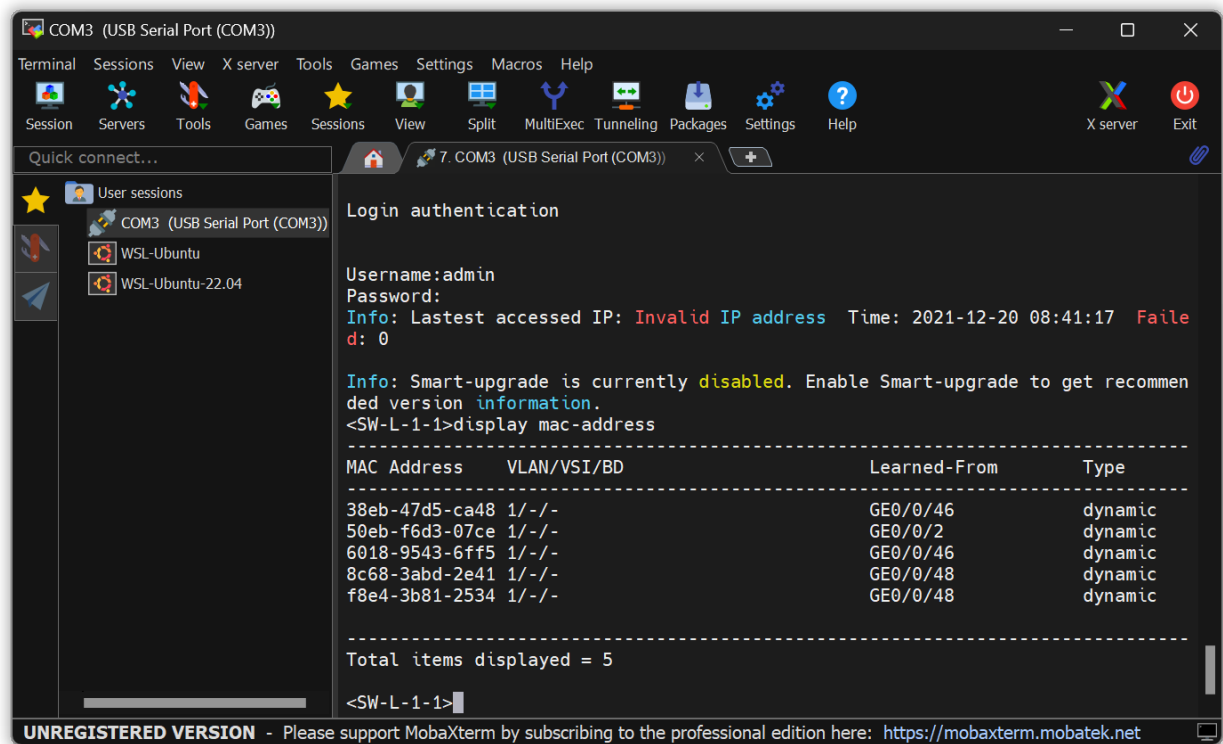


图 5: 启用交换机 MAC 学习。图中为启用 MAC 学习之后显示 MAC 地址表。可以看到有 5 个 MAC 地址，分别为其他两台交换机以及三台 PC 机。

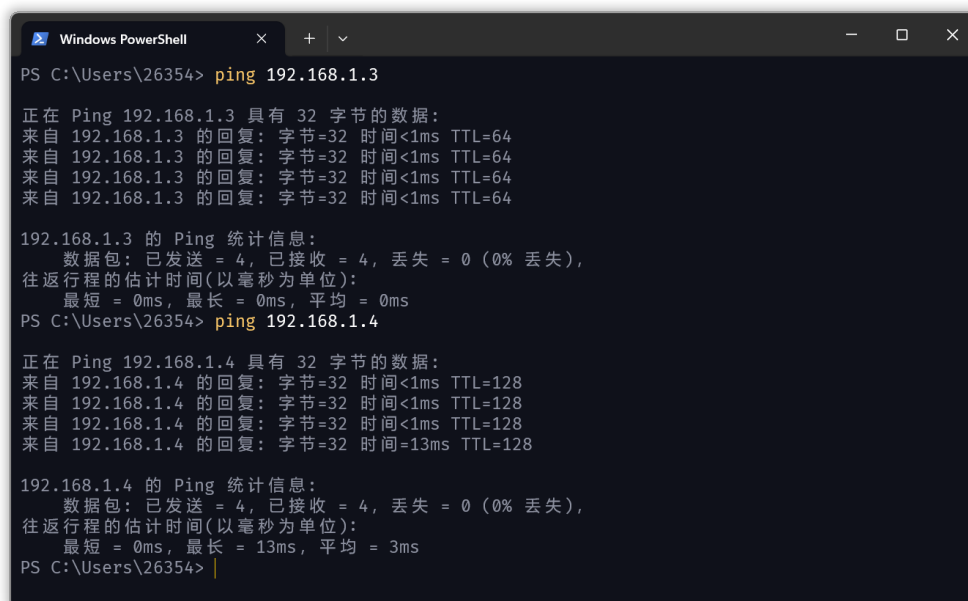


图 6: PC 间相互 ping 输出。主机 A 尝试 ping B, C. 结果均为联通。

arp						
No.	Time	Source	Destination	Protocol	Length	Info
2	0.075240	ASUSTekCOMPU_d3...	Broadcast	ARP	42	Who has 192.168.1.2? (ARP Probe)
4	1.084748	ASUSTekCOMPU_d3...	Broadcast	ARP	42	Who has 192.168.1.2? (ARP Probe)
6	2.082941	ASUSTekCOMPU_d3...	Broadcast	ARP	42	Who has 192.168.1.2? (ARP Probe)
10	3.082148	ASUSTekCOMPU_d3...	Broadcast	ARP	42	ARP Announcement for 192.168.1.2
28	5.086689	ASUSTekCOMPU_d3...	Broadcast	ARP	42	ARP Announcement for 192.168.1.2
84	11.862327	ASUSTekCOMPU_d3...	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.2
85	11.862506	Dell_43:6f:f5	ASUSTekCOMPU_d3:07:ce	ARP	60	192.168.1.4 is at 60:18:95:43:6f:f5
114	16.693269	Dell_43:6f:f5	ASUSTekCOMPU_d3:07:ce	ARP	60	Who has 192.168.1.2? Tell 192.168.1.4
115	16.693288	ASUSTekCOMPU_d3...	Dell_43:6f:f5	ARP	42	192.168.1.2 is at 50:eb:f6:d3:07:ce
305	67.304706	ASUSTekCOMPU_d3...	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.2
306	67.304938	ASIXElectron_81...	ASUSTekCOMPU_d3:07:ce	ARP	60	192.168.1.3 is at f8:e4:3b:81:25:34
336	74.063007	ASIXElectron_81...	Broadcast	ARP	60	Who has 192.168.1.4? Tell 192.168.1.3
393	88.576548	ASUSTekCOMPU_d3...	ASIXElectron_81:25:34	ARP	42	Who has 192.168.1.3? Tell 192.168.1.2
394	88.577040	ASIXElectron_81...	ASUSTekCOMPU_d3:07:ce	ARP	60	192.168.1.3 is at f8:e4:3b:81:25:34
421	92.573819	ASUSTekCOMPU_d3...	Dell_43:6f:f5	ARP	42	Who has 192.168.1.4? Tell 192.168.1.2
422	92.574146	Dell_43:6f:f5	ASUSTekCOMPU_d3:07:ce	ARP	60	192.168.1.4 is at 60:18:95:43:6f:f5
424	92.685611	Dell_43:6f:f5	ASUSTekCOMPU_d3:07:ce	ARP	60	Who has 192.168.1.2? Tell 192.168.1.4
425	92.685628	ASUSTekCOMPU_d3...	Dell_43:6f:f5	ARP	42	192.168.1.2 is at 50:eb:f6:d3:07:ce

图 7: 主机 A 收到的 ARP 报文。由于 ARP 报文均为广播，所以可以收到 B 与 C 的 ARP 报文。

icmp and ip.src==192.168.1.3						
No.	Time	Source	Destination	Protocol	Length	Info
304	67.304555	192.168.1.3	192.168.1.2	ICMP	98	Echo (ping) request id=0xf567, seq=0/0, ttl=64 (reply in 307)
309	68.309572	192.168.1.3	192.168.1.2	ICMP	98	Echo (ping) request id=0xf567, seq=1/256, ttl=64 (reply in 310)
318	69.314102	192.168.1.3	192.168.1.2	ICMP	98	Echo (ping) request id=0xf567, seq=2/512, ttl=64 (reply in 319)
321	70.319490	192.168.1.3	192.168.1.2	ICMP	98	Echo (ping) request id=0xf567, seq=3/768, ttl=64 (reply in 322)
330	71.322762	192.168.1.3	192.168.1.2	ICMP	98	Echo (ping) request id=0xf567, seq=4/1024, ttl=64 (reply in 331)
366	80.738008	192.168.1.3	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=59/15104, ttl=64 (request in 365)
368	81.744384	192.168.1.3	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=60/15360, ttl=64 (request in 367)
371	82.758769	192.168.1.3	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=61/15616, ttl=64 (request in 370)
380	83.772448	192.168.1.3	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=62/15872, ttl=64 (request in 379)

icmp and ip.src==192.168.1.4						
No.	Time	Source	Destination	Protocol	Length	Info
87	11.862731	192.168.1.4	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=55/14080, ttl=128 (request in 86)
94	12.879693	192.168.1.4	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=56/14336, ttl=128 (request in 93)
101	13.890786	192.168.1.4	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=57/14592, ttl=128 (request in 100)
104	14.902650	192.168.1.4	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=58/14848, ttl=128 (request in 103)
391	87.917231	192.168.1.4	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=63/16128, ttl=128 (request in 390)
402	88.927505	192.168.1.4	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=64/16384, ttl=128 (request in 401)
404	89.942778	192.168.1.4	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=65/16640, ttl=128 (request in 403)
407	90.954666	192.168.1.4	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=66/16896, ttl=128 (request in 406)

图 8: 主机 A 收到主机 B 与 C 的 ping 报文。但这里并没有主机 B 与主机 C 之间 ping 的报文，因为交换机按目的 MAC 转发，将其过滤掉了。

2. 为什么学习到的 MAC 地址会老化？不老化有什么问题？

老化机制可以帮助交换机删除那些不再有效的 MAC 地址信息，从而保持 MAC 地址表的准确性。并且交换机的 MAC 地址表的大小是有限的。通过定期删除老化的条目，交换机可以释放存储空间，为新的设备和新的 MAC 地址留出空间。

如果不老化可能会导致 MAC 地址表满了，新的设备无法加入网络，因为交换机无法为它们分配新的 MAC 地址条目。并且如果 MAC 地址表中包含了很多无效的条目，那么在查找目标 MAC 地址时可能需要更多的时间，会降低网络的性能。

5 实验 2.4 使用交换机 +VLAN 组网

5.1 实验内容

- 3 台 PC 机使用 IP 协议，静态配置 IP 地址。
- PC 机使用有线网卡，使用网线，接入临近交换机。
- 交换机间通过网线互联，相互连通。
- 研发 PC 1/PC 2 分配 VLAN 10，财务 PC 3 分配 VLAN 20。
- PC 2 变更为财务部 PC，接入到 Switch 1 上，进行实验。

5.2 实验过程

5.2.1 配置 Switch 3 的 VLAN

- 登录到 Switch 3 交换机的管理平台上，依次键入如下命令创建对应拓扑的 VLAN(Switch 1 连接在 46 网口，Switch 2 连接在 48 网口):
 - `vlan 10`
 - `interface gigabitethernet 0/0/46`
 - `port link-type trunk`
 - `port trunk allow-pass vlan 10`
 - `vlan 20`
 - `interface gigabitethernet 0/0/48`
 - `port link-type trunk`
 - `port trunk allow-pass vlan 20`

5.3 实验结果分析

实验结果如图 9, 10 所示。

5.4 实验思考

1. Access/Trunk 两种 Link Type 的差别

一个 Access 端口只能属于一个 VLAN. 当数据帧从 Access 端口发送出去时，VLAN 信息会被去除；而一个 Trunk 端口可以携带来自多个 VLAN 的数据帧。这些帧在传输时会保留其 VLAN 信息，

2. VLAN 与物理接口的关系

在 VLAN 中，每个物理接口可以被配置为属于一个或多个 VLAN。这个配置决定了通过这个接口的数据帧将被认为是来自哪个 VLAN，以及应该被发送到哪个 VLAN。

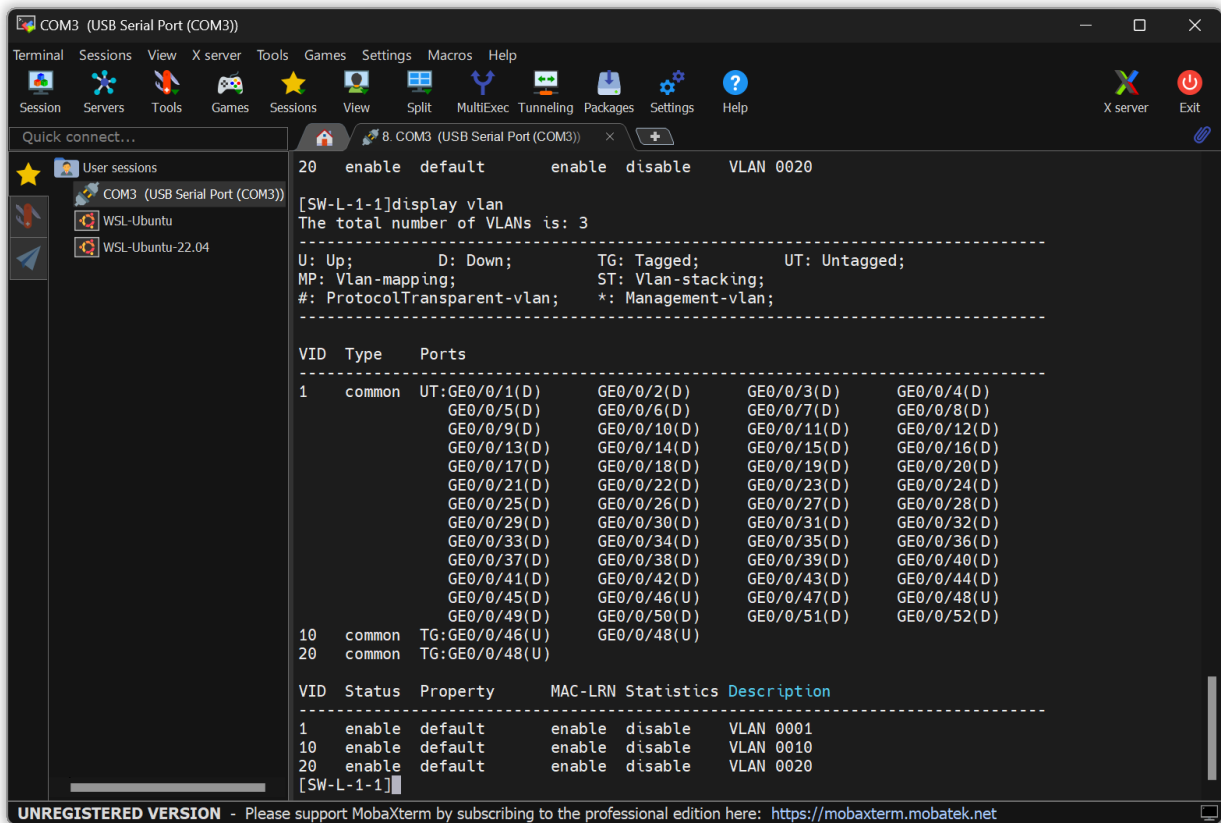


图 9: Switch 3 配置完 VLAN 的界面。可以看到下方有三个 VLAN，分别为 VLAN 1, VLAN 10 与 VLAN 20。

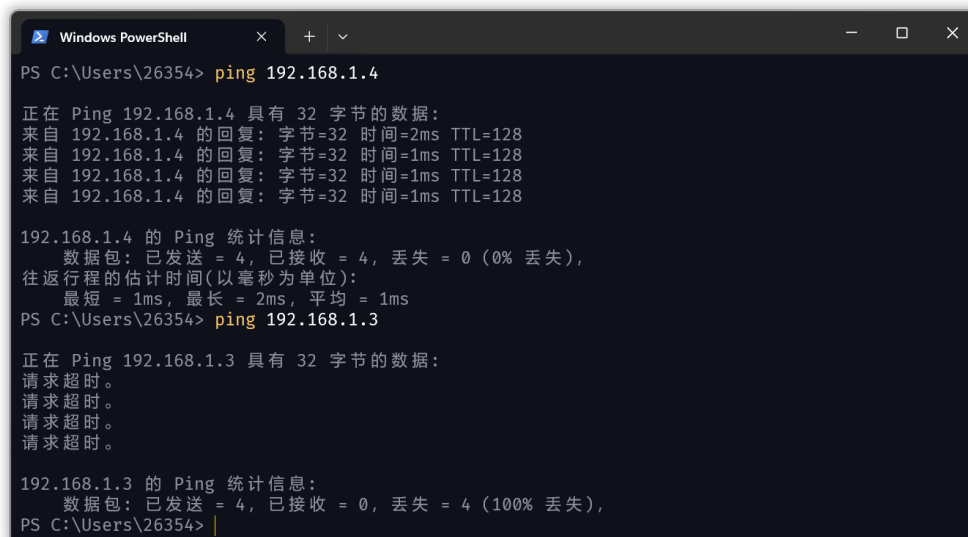


图 10: 配置完网络后，PC 2 尝试 ping PC 1 与 PC 3。可以看到 PC 1 可以 ping 通而 PC 3 则无法 PING 通。而如果将 PC 2 变为 VLAN 20 后插到 Switch 1 上则都无法 ping 通。

3. 所有接口都配置成 Access 口，会出现怎样的情况？

如果所有的接口都是 Access 端口，那么 VLAN 信息将无法传播。因为在 Access 端口发送数据帧时，VLAN 信息会被去除，在接收数据帧时，会根据接口的 VLAN 配置添加 VLAN 信息。

6 实验 3.1 使用 L2 交换机 + L3 交换机组网

6.1 实验内容

- 3 台 PC 机使用 IP 协议，DHCP 动态分配 IP 地址。
- PC 机使用有线网卡，使用网线，接入临近 L2 交换机。
- L2 交换机间通过 L3 交换机互联。
- L3 交换机配置 VLANIF，做 PC 机网关，并启用 DHCP server 为 PC 机分配地址。

6.2 实验过程

6.2.1 配置 Switch 2 的 VLAN

- 登录到 Switch 2 交换机的管理平台上，依次键入如下命令创建对应拓扑的 VLAN(PC 2 连接在 14 网口，PC 3 连接在 10 网口，Switch 3 连接在 4 网口):
 - `vlan 10`
 - `interface gigabitethernet 0/0/14`
 - `port link-type access`
 - `port default vlan 10`
 - `vlan 20`
 - `interface gigabitethernet 0/0/10`
 - `port link-type access`
 - `port default vlan 20`
 - `quit`
 - `interface gigabitethernet 0/0/4`
 - `port link-type trunk`
 - `port trunk allow-pass vlan 10 20`

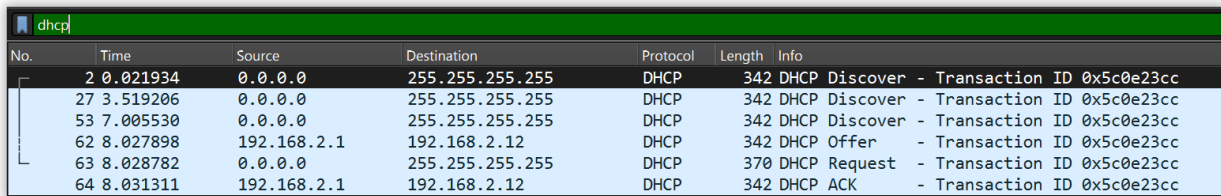
6.2.2 配置 Switch 3 的 VLAN

- 登录到 Switch 3 交换机的管理平台上，依次键入如下命令创建对应拓扑的 VLAN(Switch 1 连接在 2 网口，Switch 2 连接在 24 网口):
 - `vlan 10`
 - `vlan 20`
 - `dhcp enable`
 - `interface GigabitEthernet 0/0/2`
 - `port link-type trunk`
 - `port trunk allow-pass vlan 10`
 - `interface GigabitEthernet 0/0/24`
 - `port link-type trunk`
 - `port trunk allow-pass vlan 10 20`
 - `interface Vlanif 10`
 - `ip address 192.168.102.1 24`
 - `dhcp select interface`
 - `dhcp server dns-list 1.2.4.8`
 - `interface Vlanif 20`
 - `ip address 192.168.103.1 24`
 - `dhcp select interface`

- dhcp server dns-list 1.2.4.8

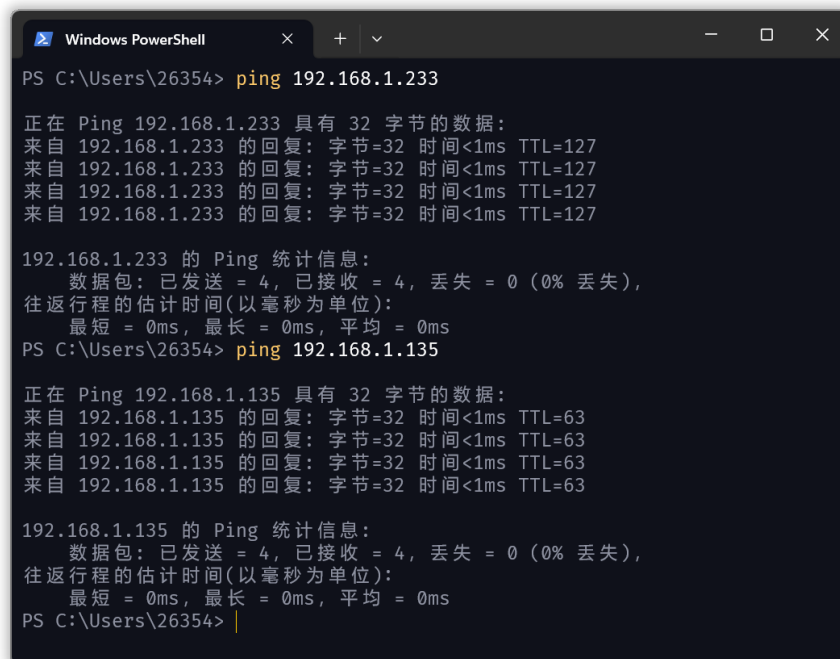
6.3 实验结果分析

实验结果如图 11, 12, 13 所示。



No.	Time	Source	Destination	Protocol	Length	Info
2	0.021934	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5c0e23cc
27	3.519206	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5c0e23cc
53	7.005530	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5c0e23cc
62	8.027898	192.168.2.1	192.168.2.12	DHCP	342	DHCP Offer - Transaction ID 0x5c0e23cc
63	8.028782	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x5c0e23cc
64	8.031311	192.168.2.1	192.168.2.12	DHCP	342	DHCP ACK - Transaction ID 0x5c0e23cc

图 11: PC 3 收到的 DHCP 报文。可以看到, PC 3 发现了 DHCP 服务器并向其发送 DHCP Request 请求, 获取到了 IP 地址。



```

Windows PowerShell
PS C:\Users\26354> ping 192.168.1.233

正在 Ping 192.168.1.233 具有 32 字节的数据:
来自 192.168.1.233 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.1.233 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.1.233 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.1.233 的回复: 字节=32 时间<1ms TTL=127

192.168.1.233 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
PS C:\Users\26354> ping 192.168.1.135

正在 Ping 192.168.1.135 具有 32 字节的数据:
来自 192.168.1.135 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.1.135 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.1.135 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.1.135 的回复: 字节=32 时间<1ms TTL=63

192.168.1.135 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
PS C:\Users\26354>
  
```

图 12: 主机 3 成功 ping 通主机 1 与主机 2。

6.4 实验思考

1. VLANIF 与 VLAN 的关系如何?

每个 VLANIF 与一个 VLAN 关联, 用于在该 VLAN 上执行 IP 层的操作。

2. VLANIF 与物理接口有什么关系?

物理接口上的数据流可以根据其 VLAN 标签被路由到与该 VLAN 关联的 VLANIF, 然后由 VLANIF 进行 IP 层的处理。

```
[SWITCH-3-Vlanif20]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
Destinations : 6      Routes : 6

Destination/Mask    Proto  Pre  Cost    Flags NextHop         Interface
-----
127.0.0.0/8         Direct  0    0        D  127.0.0.1         InLoopBack0
127.0.0.1/32        Direct  0    0        D  127.0.0.1         InLoopBack0
192.168.1.0/24       Direct  0    0        D  192.168.1.1       Vlanif10
192.168.1.1/32       Direct  0    0        D  127.0.0.1         Vlanif10
192.168.2.0/24       Direct  0    0        D  192.168.2.1       Vlanif20
192.168.2.1/32       Direct  0    0        D  127.0.0.1         Vlanif20

[SWITCH-3-Vlanif20]
```

图 13: 配置完成后, Switch 3 上的 route table.

3. 同一 L3 交换机 VLANIF 10 和 VLANIF 20 可以配置相同的网段吗?

不可以。如果两个 VLANIF 配置了相同的 IP 网络段, 那么交换机将无法正确地进行 IP 路由, 因为它无法确定一个给定的 IP 地址应该路由到哪个 VLAN。

7 实验 3.2 路由器/L3 交换机静态路由组网

7.1 实验内容

- 同实验 3.1
- 同一岛内两小组的路由器通过网线互联。
- 路由器使用主接口配置 IP 地址。
- L3 交换机/路由器部署静态路由协议。

7.2 实验过程

Switch 2 无需配置, 保持与上一个实验一致。

7.2.1 配置 Switch 3 的 VLAN

- 登录到 Switch 3 交换机的管理平台上, 依次键入如下命令创建对应拓扑的 VLAN:
 - vlan 30
 - interface GigabitEthernet 0/0/4
 - port link-type access
 - port default vlan 30
 - interface Vlanif 30
 - ip address 10.100.100.0 31

7.2.2 配置路由器静态路由

- 登录到路由器的管理平台上, 依次键入如下命令创建静态路由:
 - interface GigabitEthernet 0/0/6
 - undo portswitch
 - ip address 10.100.100.1 31
 - ip route-static 192.168.102.0 23 10.100.100.0
 - interface GigabitEthernet 0/0/2
 - ip address 10.100.100.2 31
 - ip route-static 192.168.100.0 23 10.100.100.3

7.2.3 配置 Switch 3 的静态路由

- 登录到 Switch 3 交换机的管理平台上，依次键入如下命令创建对应的静态路由：
 - ip route-static 192.168.100.0 23 10.100.100.1

7.3 实验结果分析

实验结果如图 14, 15, 16 所示。

```
[R-L-5-7]display ip routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance
-----
Routing Tables: Public
      Destinations : 13          Routes : 13
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.100.100.0/31	Direct	0	0	D	10.100.100.1	GigabitEthernet0/0/6
10.100.100.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/6
10.100.100.2/31	Direct	0	0	D	10.100.100.2	GigabitEthernet0/0/2
10.100.100.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/2
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
192.168.1.0/24	Direct	0	0	D	192.168.1.1	Vlanif1
192.168.1.1/32	Direct	0	0	D	127.0.0.1	Vlanif1
192.168.1.255/32	Direct	0	0	D	127.0.0.1	Vlanif1
192.168.100.0/23	Static	60	0	RD	10.100.100.3	GigabitEthernet0/0/2
192.168.102.0/23	Static	60	0	RD	10.100.100.0	GigabitEthernet0/0/6
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

图 14: 配置完成后其中一台三层交换机的路由表。

```
Windows PowerShell
PS C:\Users\26354> ping 192.168.103.157

正在 Ping 192.168.103.157 具有 32 字节的数据:
来自 192.168.103.157 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.103.157 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.103.157 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.103.157 的回复: 字节=32 时间<1ms TTL=63

192.168.103.157 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
PS C:\Users\26354> ping 192.168.100.76

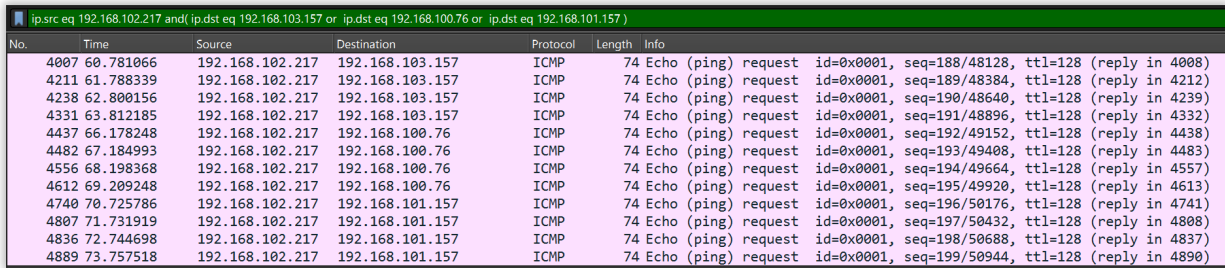
正在 Ping 192.168.100.76 具有 32 字节的数据:
来自 192.168.100.76 的回复: 字节=32 时间<1ms TTL=124
来自 192.168.100.76 的回复: 字节=32 时间<1ms TTL=124
来自 192.168.100.76 的回复: 字节=32 时间<1ms TTL=124
来自 192.168.100.76 的回复: 字节=32 时间<1ms TTL=124

192.168.100.76 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
PS C:\Users\26354> ping 192.168.101.157

正在 Ping 192.168.101.157 具有 32 字节的数据:
来自 192.168.101.157 的回复: 字节=32 时间=7ms TTL=124
来自 192.168.101.157 的回复: 字节=32 时间<1ms TTL=124
来自 192.168.101.157 的回复: 字节=32 时间<1ms TTL=124
来自 192.168.101.157 的回复: 字节=32 时间=1ms TTL=124

192.168.101.157 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 = 7ms, 平均 = 2ms
PS C:\Users\26354>
```

图 15: 配置完成后，可以 ping 通另一个小组的 PC 机。



No.	Time	Source	Destination	Protocol	Length	Info
4007	60.781066	192.168.102.217	192.168.103.157	ICMP	74	Echo (ping) request id=0x0001, seq=188/48128, ttl=128 (reply in 4008)
4211	61.788339	192.168.102.217	192.168.103.157	ICMP	74	Echo (ping) request id=0x0001, seq=189/48384, ttl=128 (reply in 4212)
4238	62.800156	192.168.102.217	192.168.103.157	ICMP	74	Echo (ping) request id=0x0001, seq=190/48640, ttl=128 (reply in 4239)
4331	63.812185	192.168.102.217	192.168.103.157	ICMP	74	Echo (ping) request id=0x0001, seq=191/48896, ttl=128 (reply in 4332)
4437	66.178248	192.168.102.217	192.168.100.76	ICMP	74	Echo (ping) request id=0x0001, seq=192/49152, ttl=128 (reply in 4438)
4482	67.184993	192.168.102.217	192.168.100.76	ICMP	74	Echo (ping) request id=0x0001, seq=193/49408, ttl=128 (reply in 4483)
4556	68.198368	192.168.102.217	192.168.100.76	ICMP	74	Echo (ping) request id=0x0001, seq=194/49664, ttl=128 (reply in 4557)
4612	69.209248	192.168.102.217	192.168.100.76	ICMP	74	Echo (ping) request id=0x0001, seq=195/49920, ttl=128 (reply in 4613)
4740	70.725786	192.168.102.217	192.168.101.157	ICMP	74	Echo (ping) request id=0x0001, seq=196/50176, ttl=128 (reply in 4741)
4807	71.731919	192.168.102.217	192.168.101.157	ICMP	74	Echo (ping) request id=0x0001, seq=197/50432, ttl=128 (reply in 4808)
4836	72.744698	192.168.102.217	192.168.101.157	ICMP	74	Echo (ping) request id=0x0001, seq=198/50688, ttl=128 (reply in 4837)
4889	73.757518	192.168.102.217	192.168.101.157	ICMP	74	Echo (ping) request id=0x0001, seq=199/50944, ttl=128 (reply in 4890)

图 16: 配置完成后, 可以 ping 通另一个小组的 PC 机对应的报文。

7.4 实验思考

1. 路由器间接口网段需要使用多少位掩码?

30 位。因为对于两个路由器之间的点对点连接只需要两个可用的 IP 地址

2. 查看路由表中, 有几个字段, 各什么含义?

- **Destination/Mask:** 目的网段与掩码。
- **Proto:** 路由协议, 分为直连路由 (direct), 静态路由 (static) 等。
- **Pre:** 路由协议优先级。
- **Cost:** 路由开销。
- **Flags:** 路由标记。
- **NextHop:** 路由的下一跳地址。
- **Interface:** 路由的出接口。

3. 拔掉 Switch 3 至 Switch 1 接口, 网络中网关 1 路由还在吗?

没了。直连路由拔掉就没了。

4. 拔掉 PC 1 接口, 网络中网关 1 路由还在吗?

还有。交换机还连着。

8 实验 3.3 路由器/L3 交换机 OSPF 组网

8.1 实验内容

- 同实验 3.2
- 同一岛内两小组的路由器通过网线互联
- 同一岛内两小组的交换机增加三层互联
- L3 交换机/路由器部署 OSPF 路由协议

8.2 实验过程

8.2.1 配置 Switch 3 OSPF

- 登录到 Switch 3 的管理平台上, 依次键入如下命令创建 OSPF:
 - interface GigabitEthernet 0/0/10

- port link-type trunk
- port trunk allow-pass vlan 40
- ospf 1 router-id 192.168.102.1
- area 0
- network 192.168.0.0 0.0.255.255
- network 10.100.100.0 0.0.0.255

8.2.2 配置路由器 OSPF

- 登录到路由器的管理平台上，依次键入如下命令创建 OSPF:
 - ospf 1 router-id 10.100.100.1
 - area 0
 - network 192.168.0.0 0.0.255.255
 - network 10.100.100.0 0.0.0.255

8.3 实验结果分析

实验结果如图 17, 18 所示。

```
[R-L-5-7]display ip routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance
-----
Routing Tables: Public
Destinations : 18      Routes : 18
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.100.100.0/31	Direct	0	0	D	10.100.100.1	GigabitEthernet0/0/6
10.100.100.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/6
10.100.100.2/31	Direct	0	0	D	10.100.100.2	GigabitEthernet0/0/2
10.100.100.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/2
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
192.168.1.0/24	Direct	0	0	D	192.168.1.1	Vlanif1
192.168.1.1/32	Direct	0	0	D	127.0.0.1	Vlanif1
192.168.1.255/32	Direct	0	0	D	127.0.0.1	Vlanif1
192.168.100.0/23	Static	60	0	RD	10.100.100.3	GigabitEthernet0/0/2
192.168.100.0/24	OSPF	10	3	D	10.100.100.3	GigabitEthernet0/0/2
192.168.101.0/24	OSPF	10	3	D	10.100.100.3	GigabitEthernet0/0/2
192.168.102.0/23	Static	60	0	RD	10.100.100.0	GigabitEthernet0/0/6
192.168.102.0/24	OSPF	10	2	D	10.100.100.0	GigabitEthernet0/0/6
192.168.103.0/24	OSPF	10	2	D	10.100.100.0	GigabitEthernet0/0/6
192.168.106.0/24	OSPF	10	2	D	10.100.100.3	GigabitEthernet0/0/2
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

```
[R-L-5-7]
```

图 17: 配置完成后，路由器上的路由表。

8.4 实验思考

1. Router-ID 的作用

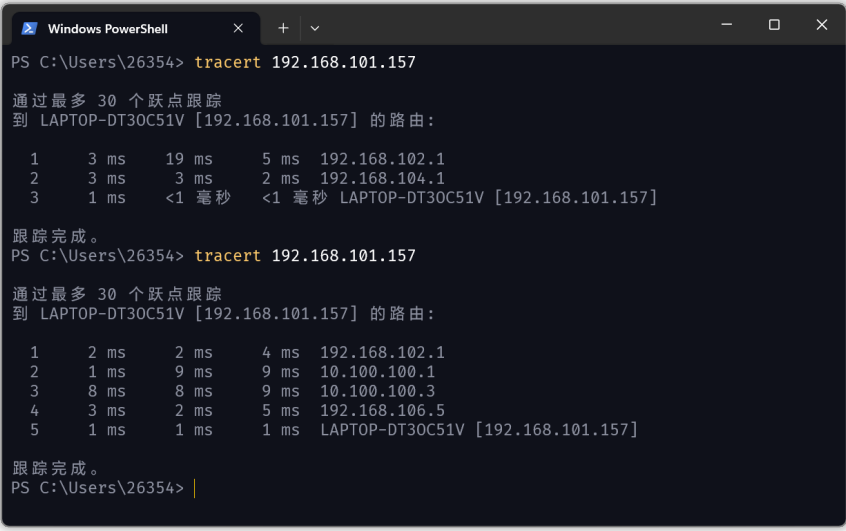
用于作为路由器的身份标示。

2. 每个路由器 OSPF 有哪些链路状态？

有 Down、Attempt、Init、2-Way、Exstart、Exchange、Loading 和 Full 共 8 个状态。

3. 同时配置了静态路由和 OSPF，如何选择最优的路由？

路由器选择最优路由的过程通常基于路由表中的路由的优先级。一般静态路由的优先级会比较高，大部分情况是走静态路由。



```
Windows PowerShell
PS C:\Users\26354> tracert 192.168.101.157

通过最多 30 个跃点跟踪
到 LAPTOP-DT30C51V [192.168.101.157] 的路由:

  1   3 ms   19 ms   5 ms  192.168.102.1
  2   3 ms    3 ms   2 ms  192.168.104.1
  3   1 ms   <1 毫秒 <1 毫秒 LAPTOP-DT30C51V [192.168.101.157]

跟踪完成。
PS C:\Users\26354> tracert 192.168.101.157

通过最多 30 个跃点跟踪
到 LAPTOP-DT30C51V [192.168.101.157] 的路由:

  1   2 ms   2 ms   4 ms  192.168.102.1
  2   1 ms   9 ms   9 ms  10.100.100.1
  3   8 ms   8 ms   9 ms  10.100.100.3
  4   3 ms   2 ms   5 ms  192.168.106.5
  5   1 ms   1 ms   1 ms  LAPTOP-DT30C51V [192.168.101.157]

跟踪完成。
PS C:\Users\26354> |
```

图 18: 配置完成后, 对比拔掉交换机间三层互联接口前后的 `tracert` 执行结果. 可以看到, 拔掉之前直接走互联接口, 拔掉之后走 OSPF 组网。