华中科技大学计算机学院

《计算机通信与网络》实验报告

实验名称 分析 Ethernet II 帧、 分析集线器和交换机工作机理 分析 IP 和 ARP 协议

姓 名	班 级	学 号	得 分

教师评语：

一 实验环境

1. 实验环境：运行 Arch Linux x86_64 位操作系统的 PC 机一台
2. 网络环境：校园网（教育网）
3. IP 地址：10.11.56.37
4. ARP 实验网络环境：电信网，两台主机处于同一子网内，
   A 本机 IP：192.168.1.108，B 主机 IP：192.168.1.103
5. Wireshark 版本：2.6.4
6. PacketTracer 版本：7.0.0.0202

二 实验目的

1. 深入理解 Ethernet II 帧结构。
2. 深入理解 IP 报文结构和工作原理。
3. 深入理解地址解析协议 ARP 的工作原理。
4. 基本掌握使用 Wireshark 分析俘获的踪迹文件的基本技能。
5. 理解 IP 和以太网协议的关系，掌握 IP 地址和 MAC 地址的映射机制，搞清楚 IP 报文是如何利用底层的以太网帧进行传输的。
6. 观察交换机处理广播和单播报文的过程
7. 比较交换机和集线器的工作过程。
8. 掌握使用 PacketTracker 模拟网络场景的基本方法，加深对网络环境，网络设备和网络协议交互过程等方面的理解。

三 实验内容及步骤

3.1 分析踪迹文件中的帧结构

打开 Wireshark 并俘获一组网络分组。如下图所示，选择第 12 号帧（TCP）进行分析。

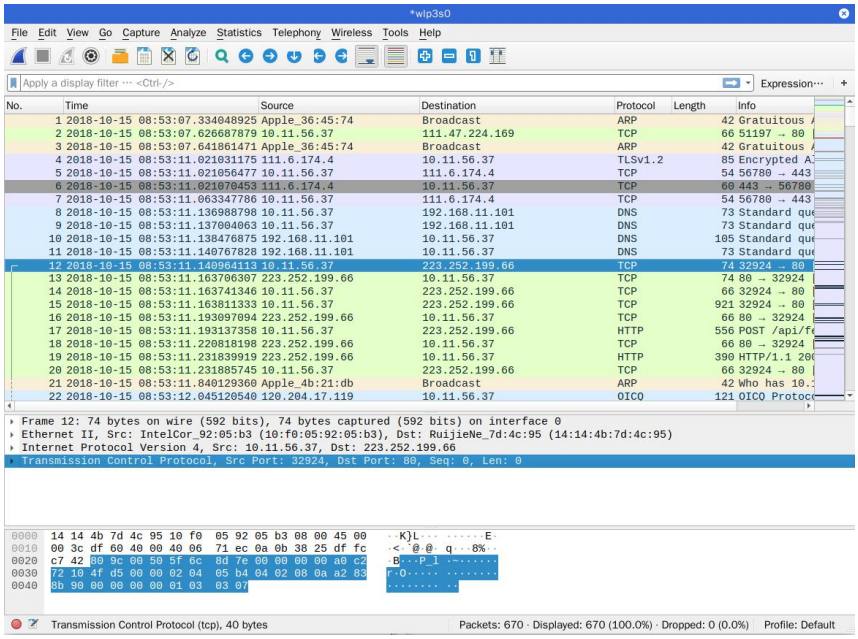

图 1 Wireshark 俘获帧

该帧显示为绿色，表明是一个正常的 TCP 数据包，同时我们可以在下面看到该帧有 Ethernet:IP:TCP 的封装结构。

进一步分析，点击首部细节信息栏中的“Ethernet II”行，可以看到如下的信息：

```
▸ Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▾ Ethernet II, Src: IntelCor_92:05:b3 (10:f0:05:92:05:b3), Dst: RuijieNe_7d:4c:95 (14:14:4b:7d:4c:95)
  ▾ Destination: RuijieNe_7d:4c:95 (14:14:4b:7d:4c:95)
      Address: RuijieNe_7d:4c:95 (14:14:4b:7d:4c:95)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: IntelCor_92:05:b3 (10:f0:05:92:05:b3)
      Address: IntelCor_92:05:b3 (10:f0:05:92:05:b3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.11.56.37, Dst: 223.252.199.66
▸ Transmission Control Protocol, Src Port: 32924, Dst Port: 80, Seq: 0, Len: 0
```

图 2 Ethernet II 详细信息

从上图中我们可以看到如下的信息：

源 MAC 地址：10:f0:05:92:05:b3

目的 MAC 地址：14:14:4b:7d:4c:95

以太网类型字段（Type）：0x0800，表示上层封装的是 IP 数据报

3.2 分析以太帧结构

在终端中执行 ping www.baidu.com，并使用 Wireshark 俘获分组，筛选出 ICMP 报文如下：

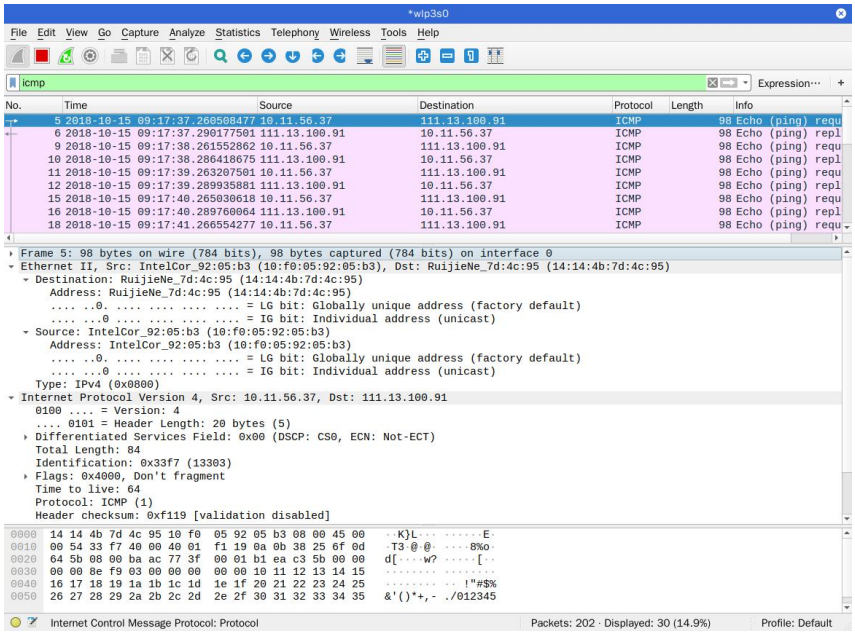

图 3 ping 命令分组俘获

3.3 分析 IP 报文结构

接着使用 5 号帧，并展开其详细信息进行分析，具体见实验结果。

3.4 分析 ARP 协议的工作原理

在终端中执行 ifconfig -a，可以看到设备所有网卡的信息，输出如下：

```
panyue@Saltedfish ~ ifconfig -a
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:58:a5:56:d0  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b0:25:aa:23:1d:69  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 93604  bytes 12291336 (11.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 93604  bytes 12291336 (11.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.11.56.37  netmask 255.255.240.0  broadcast 10.11.63.255
        inet6 fe80::acb3:1d8c:a792:40c4  prefixlen 64  scopeid 0x20<link>
        inet6 2001:250:4000:40df:cb1a:bf15:ccc7:62e5  prefixlen 64  scopeid 0x0<global>
        ether 10:f0:05:92:05:b3  txqueuelen 1000  (Ethernet)
        RX packets 418558  bytes 547348279 (521.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 167825  bytes 17030633 (16.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

图 4 ifconfig -a 命令输出

由输出可知，设备所使用的无线网卡 wlp3s0 的 MAC 地址为 10:f0:05:92:05:b3，IP 地址为 10.11.56.37，子网掩码为 255.255.240.0。

执行 arp -a 命令，可以看到设备的 ARP 表如下：

```
panyue@Saltedfish ~ arp -a
? (10.11.56.55) at 14:14:4b:7d:4c:95 [ether] on wlp3s0
_gateway (10.11.63.254) at 14:14:4b:7d:4c:95 [ether] on wlp3s0
? (10.11.56.58) at 14:14:4b:7d:4c:95 [ether] on wlp3s0
? (10.11.56.45) at e4:47:90:15:a2:73 [ether] on wlp3s0
apollo.archlinux.org (138.201.81.199) at <incomplete> on enp2s0
apollo.archlinux.org (138.201.81.199) at <incomplete> on docker0
```

图 5 arp -a 命令输出

在主机 A 与 B 上分别执行 ARP 表项清除命令，结果如下图：

```
panyue@Saltedfish ~ arp -a
_gateway (192.168.1.1) at f4:83:cd:56:c3:d2 [ether] on wlp3s0
apollo.archlinux.org (138.201.81.199) at <incomplete> on wlp3s0
apollo.archlinux.org (138.201.81.199) at <incomplete> on docker0
apollo.archlinux.org (138.201.81.199) at <incomplete> on enp2s0
panyue@Saltedfish ~
```

图 6 清空主机 A 上的 ARP 表

```
C:\windows\system32>arp -a

接口: 192.168.217.1 --- 0x6
  Internet 地址         物理地址              类型
  224.0.0.22            01-00-5e-00-00-16     静态

接口: 192.168.19.1 --- 0x12
  Internet 地址         物理地址              类型
  224.0.0.22            01-00-5e-00-00-16     静态

接口: 192.168.1.103 --- 0x14
  Internet 地址         物理地址              类型
  192.168.1.1           f4-83-cd-56-c3-d2     动态
  224.0.0.22            01-00-5e-00-00-16     静态
```

图 7 清空主机 B 上的 ARP 表

接着在主机 A 上运行 Wireshark 程序，执行包俘获操作，稍后停止发 Ping 包。分别检查两台主机的 ARP 表。

3.5 分析集线器和交换机工作原理

打开 PacketTracker，构建拓扑如下图：

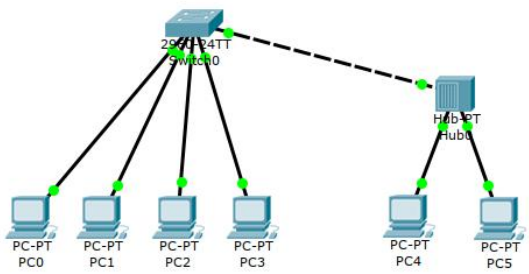

图 8 拓扑构建

接着，为每台 PC 配置自己的 IP 地址，从左到右分别配置为 192.168.1.2~192.168.1.7，子网掩码均设置为 255.255.255.0，如下图：

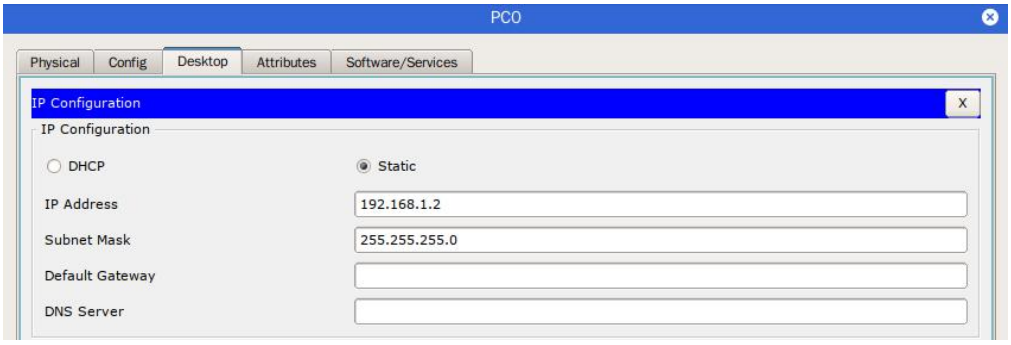

图 9 主机 IP 配置

在实时与模拟模式之间切换 4 次，完成生成树协议，所有链路指示灯变为绿色，最后停留在模拟模式中，就可以开始观察实验了。

四 实验结果

4.1 以太网帧结构分析

任选一个上面俘获到的 ICMP 帧进行分析，这里选择第一个，如下图：

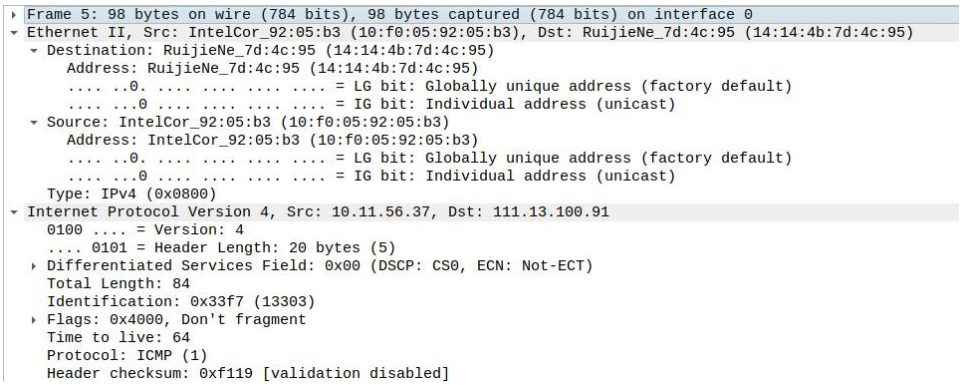

图 10 ICMP 数据帧分析

由上图可以分析，并回答实验提出的如下问题：

（1）本机的 48 比特 MAC 地址是什么？

本机的 MAC 地址即上述报文中的源 MAC 地址 10:f0:05:92:05:b3

（2）以太帧中目的 MAC 地址是什么？它是你选定的远地 Web 服务器的 MAC 地址吗？

目的 MAC 地址为：14:14:4b:7d:4c:95，显然这并不是 Web 服务器的 MAC 地址而是路由器的 MAC 地址。实际上不同的 ICMP 数据帧的目的 MAC 地址并不同，他们是该数据帧应该走向的下一跳设备的 MAC 地址。

（3）给出 2 字节以太类型字段的十六进制的值。它表示该以太帧包含了什么样的协议？上网查找如果其中封装的 IPv6 协议，其值应为多少？

以太帧中的 Type 字段为 0x0800，表示封装的是 IPv4 协议，查找资料知道 IPv6 的 Type 字段值为 0x86dd。

4.2 IP 报文结构分析

选择和上一个实验同样的数据帧，展开其 IP 层详细信息如下：

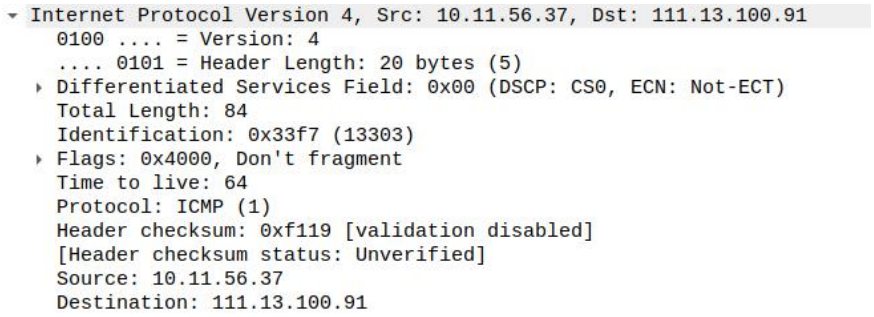

图 11 IP 数据帧分析

由上图可以分析，并回答实验提出的如下问题：

（1）你使用的计算机的 IP 地址是什么？

从源地址中得到我的 IP 地址为 10.11.56.37。

（2）在 IP 数据报首部，较高层协议字段中的值是什么？

高层协议字段 Protocol 为 1，表明是 ICMP 协议。

（3）IP 首部有多少字节？载荷字段有多少字节？

从 Header Length 字段中知道 IP 首部有 20 字节，从 Total Length 字段中知道总长度位 84 字节，所以载荷字段有 64 字节。

（4）该 IP 数据报分段了没有？如何判断该 IP 数据报有没有分段？

没有，从 Flags 字段为 0x4000 可知，标志位为 010，即 DF 字段为 1，表示 Don’t fragment 即不分段。当 DF 字段为 0 时表示分段。

（5）关于高层协议有哪些有用信息？

展开高层协议的信息如下图：

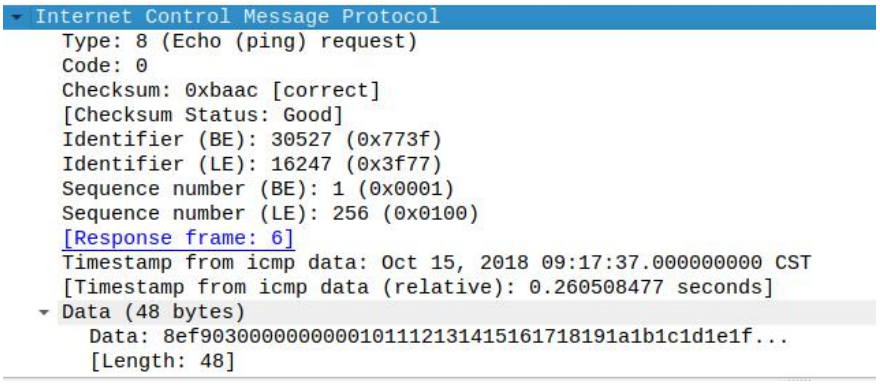

图 12 IP 数据帧分析

从图中可以看出，类型字段 Type 为 8，代码字段 Code 为 0，表示这是一个

ping 回显请求包，校验和为 0xbaac，校验正常，其余为一些表示符和序列号。

4.3 ARP 工作原理分析

停止俘获后，首先，在两台主机上分别查看 ARP 表，发现均多了对方主机的信息。如下图：

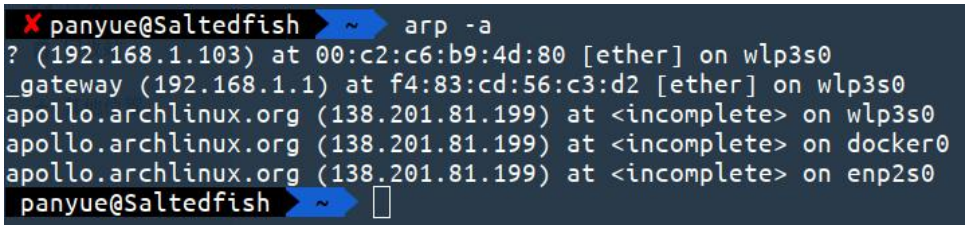

图 13 主机 A 的 ARP 表

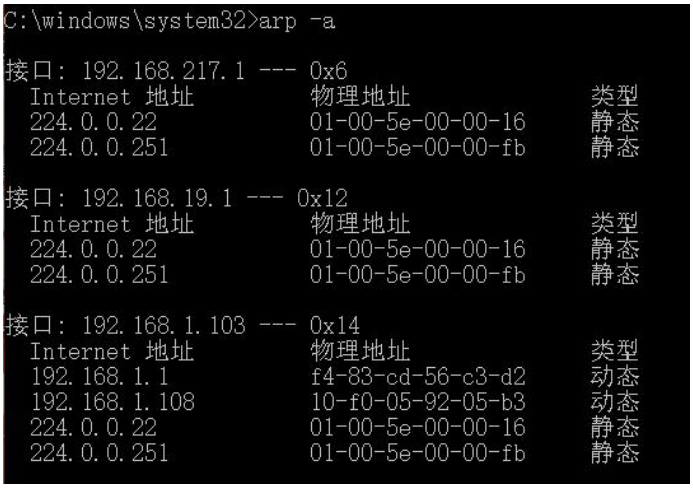

图 14 主机 B 的 ARP 表

在 Wireshark 中筛选出 ARP 和 ICMP 报文，得到：

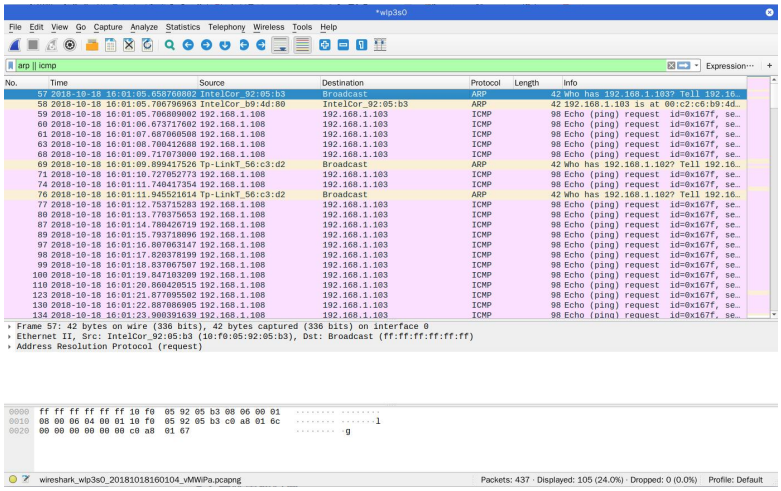

图 15 Wireshark 筛选 ARP 和 ICMP 报文

根据报文，对 ARP 协议执行的全过程如下分析：

1. 主机 A 发送 ARP 广播包，询问谁有 192.168.1.103

2. 主机 B 收到主机 A 的 ARP 请求，在自己的 ARP 表中记录主机 A 的 MAC 地址

3. 主机 B 发送 ARP 应答包，回复自己的 MAC 地址

4. 主机 A 收到主机 B 的 ARP 应答，在自己的 ARP 表中记录主机 B 的 MAC 地址

5. 现在，主机 A 和 B 的 ARP 表中都有了对方的 MAC 地址，于是可以进行正常的 ping 通信了。

4.4 集线器和交换机工作原理分析

首先，使用 Inspect 工具打开 PC 0 和 PC 1 的 ARP 表以及交换机的 MAC 表，结果观察不到任何 ARP 信息和 MAC 信息，将选择箭头移到交换机上，查看交换机端口及其接口 MAC 地址的摘要如下图：

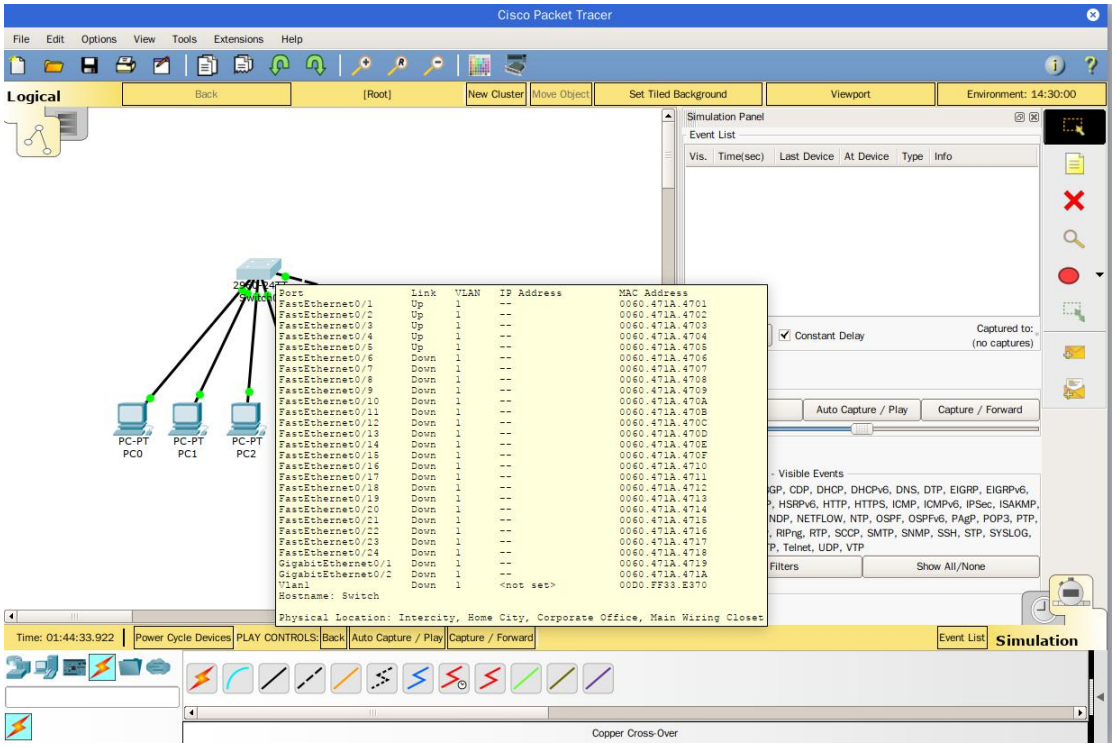

图 16 交换机接口 MAC 地址摘要

点击 Add Simple PDU，从 PC 0 发送一个 ping 到 PC 1 如下图，Event List 中可以看到一个 ICMP 回应和一个 ARP 请求。

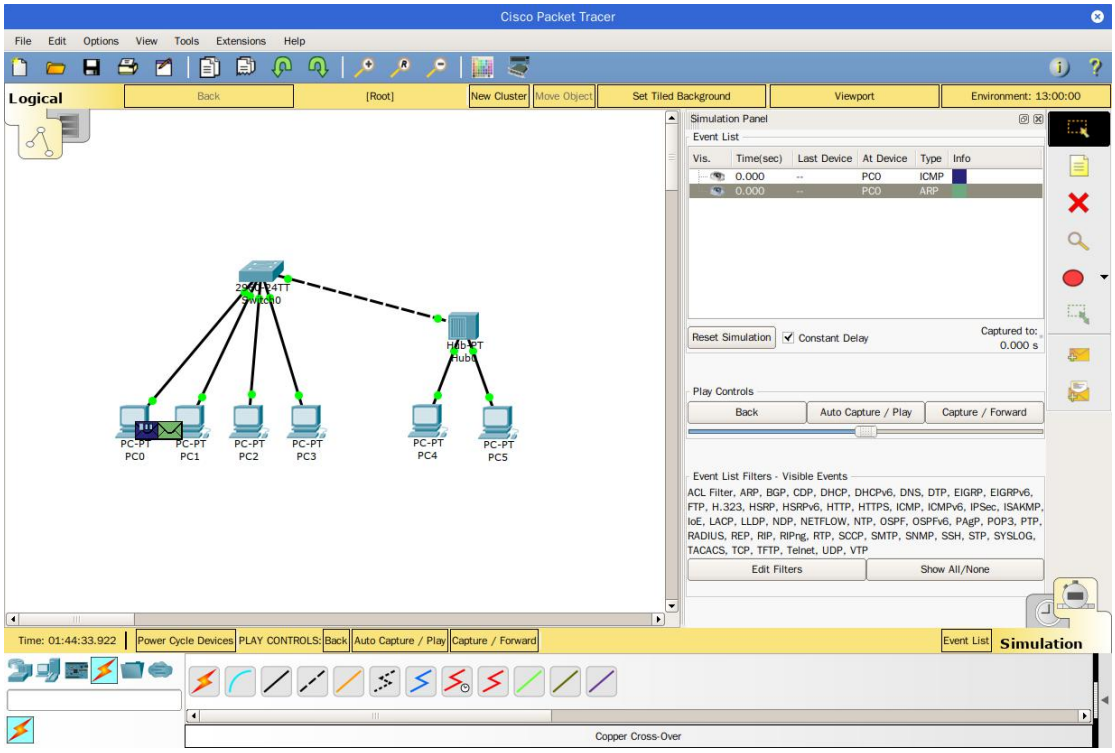

图 17 添加 PDU

开始逐步运行模拟，点击 Capture/Forward 按钮跟踪数据包的最终顺序。

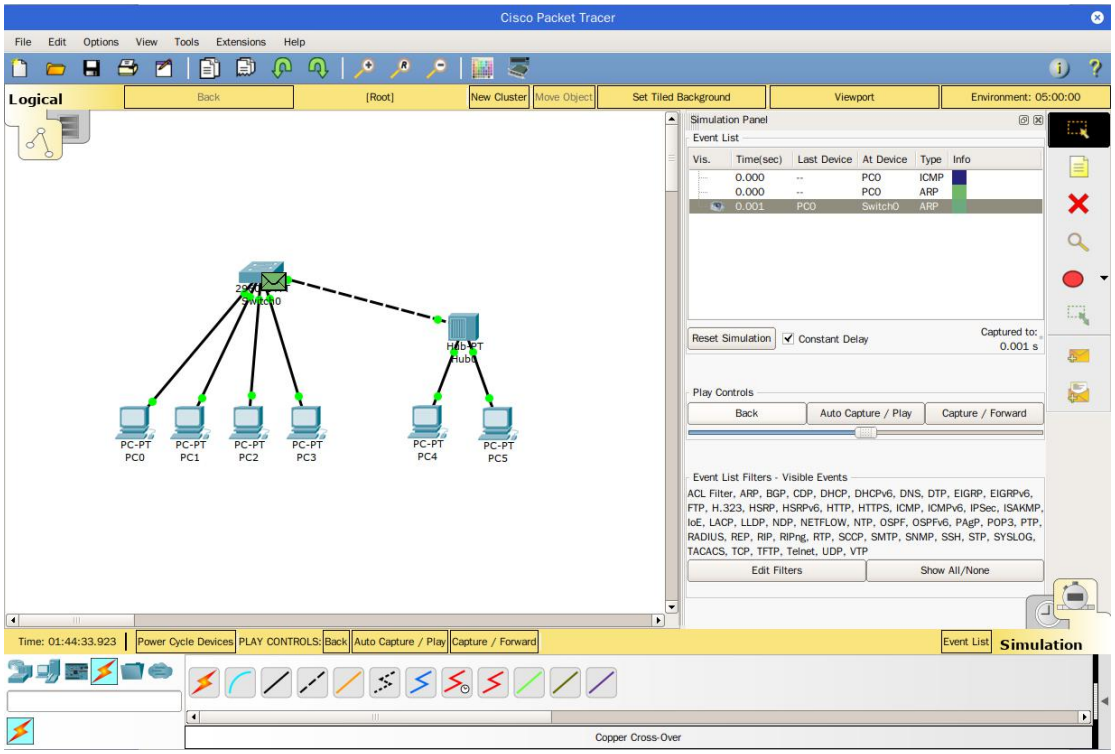

图 18 ARP 发送（一）

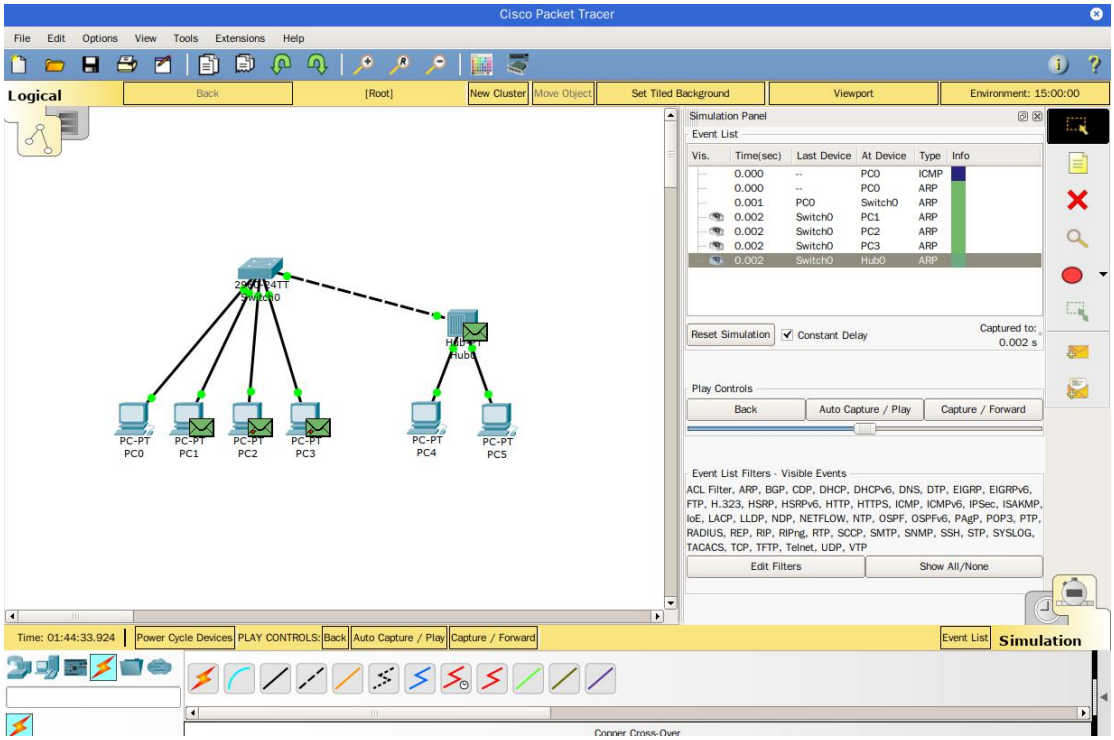

图 19 ARP 发送（二）

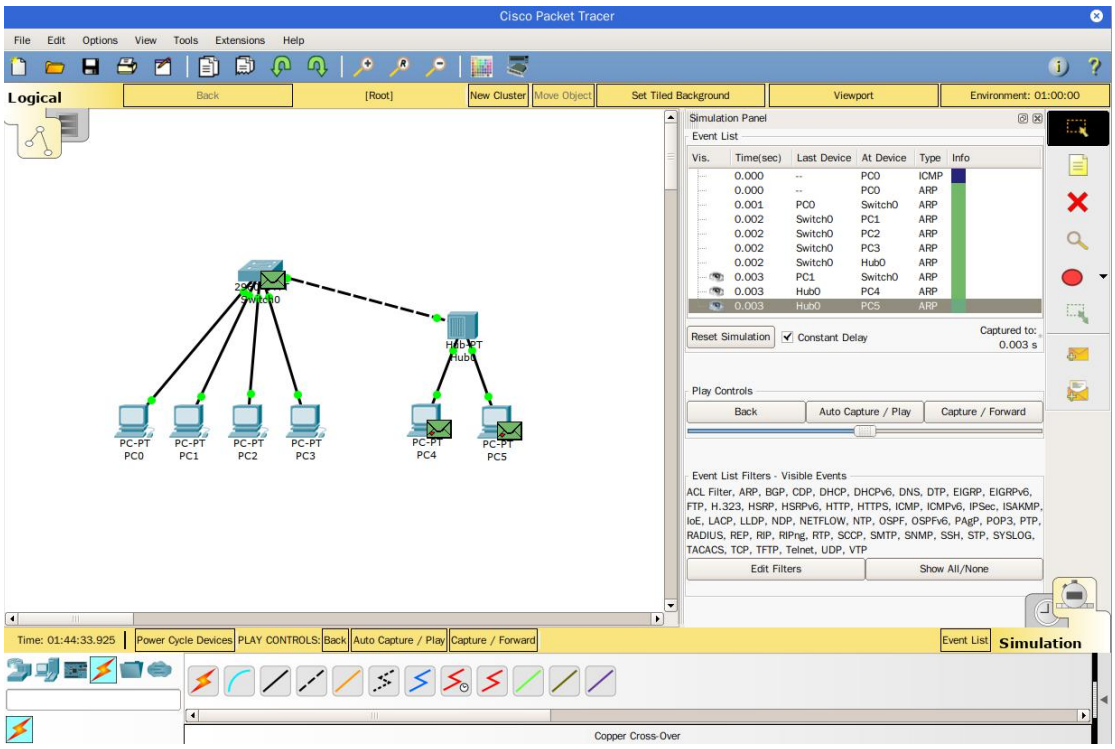

图 20 ARP 发送（三）

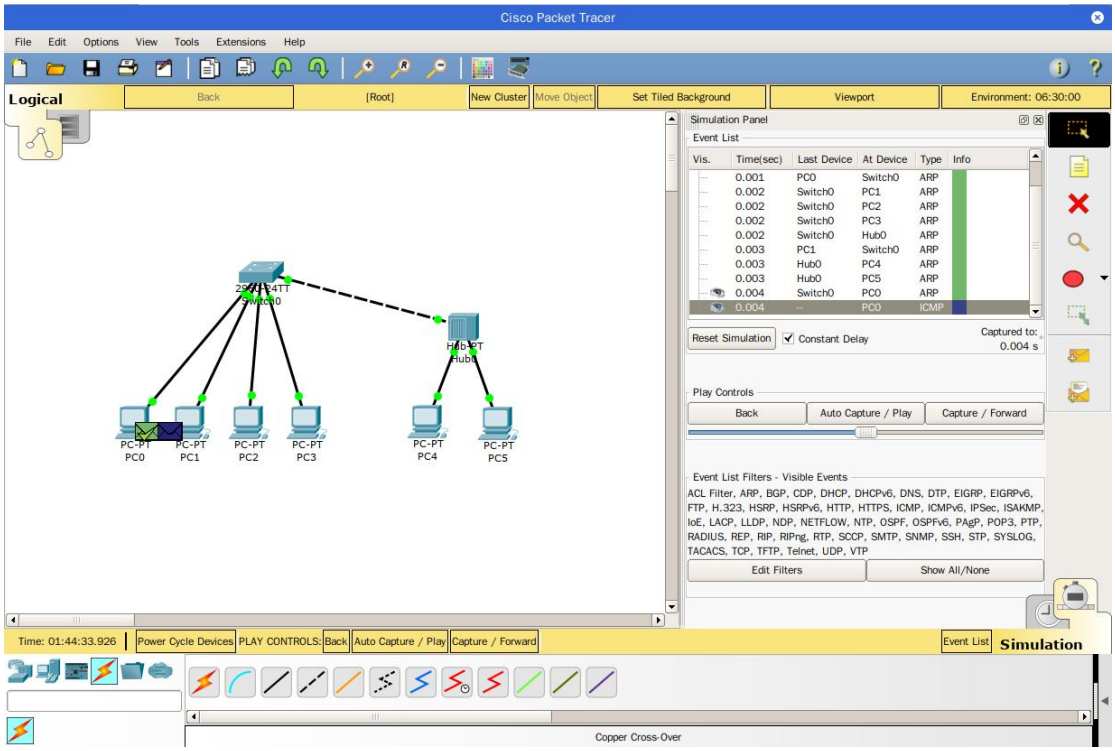

图 21 ARP 发送（四）

经过这四步之后，查看 PC 0 和 PC 1 的 ARP 表，即可看到 ARP 表中已经有了相应表项。

图 22 PC 0 的 ARP 表

图 23 PC 1 的 ARP 表

从这个过程中可以观察到，ARP 请求始终是广播，交换机会将 ARP 请求从所有端口泛洪出去。

接下来观察交换机如何处理未知单播。

点击交换机，点击 CLI 选项卡，按几次 Enter 键，将会显示 Switch>提示。键入 enable 并按 Enter 键，提示会变为 Switch#，此时键入命令 clear mac-address-table dynamic，并按 Enter 键，可以消除交换机的 MAC 表，此时重新发送数据包，可以看到当 ICMP 请求到达交换机时，交换机仍会将其当做广播包广播出去，如下图所示：

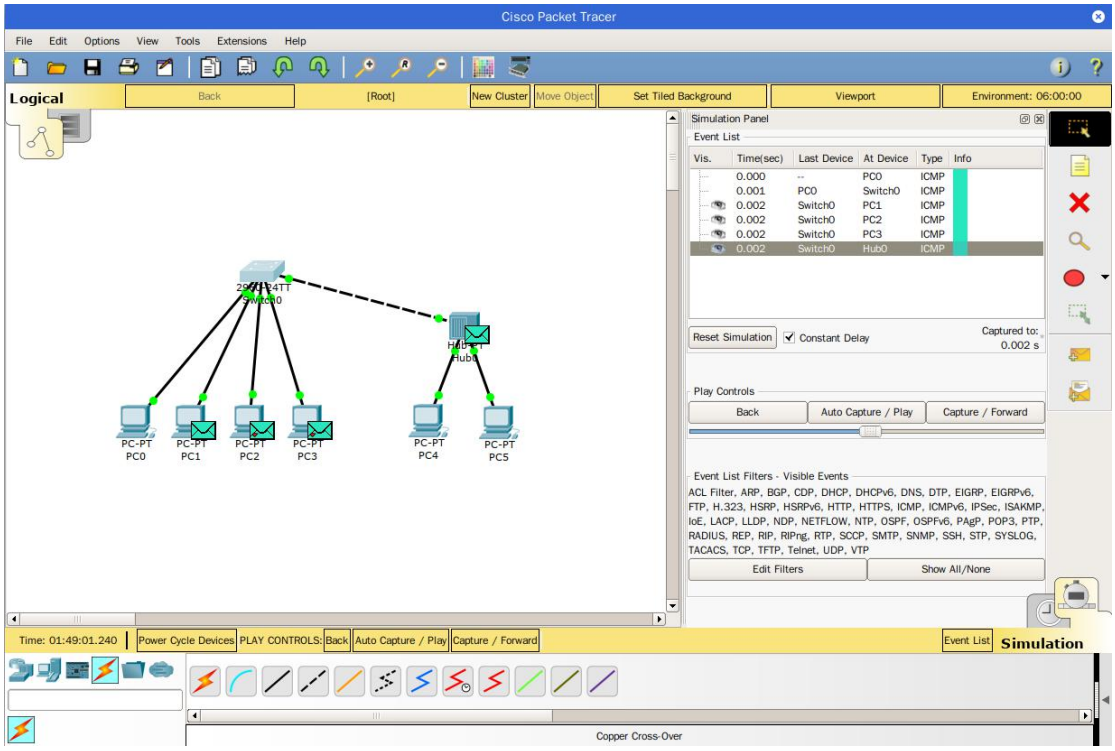

图 24 交换机广播请求

接下来观察集线器如何处理数据包。

点击 Add Simple PDU，从 PC 5 发送一个 ping 到 PC 3，集线器将该数据包从来源以外的地方广播了出去。

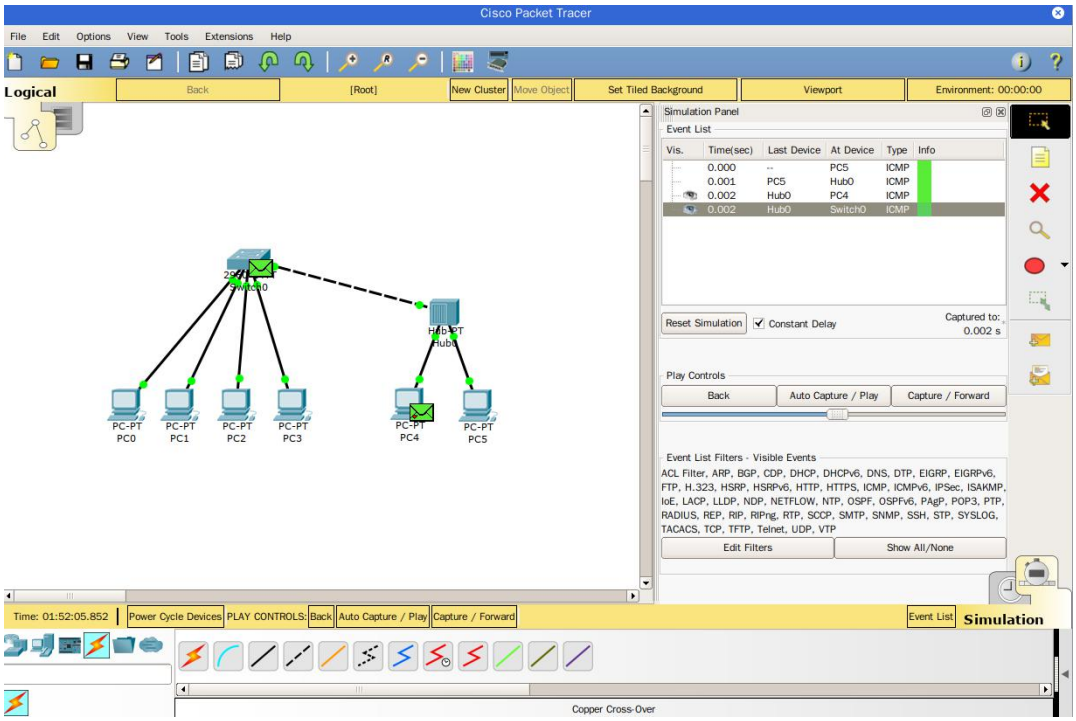

图 25 集线器广播请求

五 实验中的问题及心得

5.1 实验中的问题

为什么在寝室网络环境下做 ARP 实验时，ARP 请求没有经过路由器转发直接在两台主机之间通信了呢？

这是因为路由器的桥接”过程影响了 ARP 请求的传输，但是寝室路由器没有开启这项功能，所以没有途径路由器直接在两台主机间进行了数据的传输，完成了操作。

5.2 实验总结

本次实验需要动手的地方不是特别多，主要是对协议通信过程的分析和思考，通过本次实验，我更加深刻掌握了 ARP 的工作原理，同时也更加熟练地使用 PacketTracker，玩熟了交换机和集线器的配置，为接下来的实验打好了基础同同时也强化了上课学习的知识。