ARP 消息分析实验

学生姓名：李俊杰 1850668　　合作学生：无

实验地点：济事楼 330　　实验时间：2020 年 12 月 3 日 78 节

【实验目的】

1.了解和掌握 ARP 消息结构。

2.了解 ARP 工作原理。

3.通过实验再次熟悉相关网络配置操作。

4.利用 Wireshark 软件进行抓包并进行解读。

【实验原理】

1.ARP 背景

地址解析协议（Address Resolution Protocol，ARP），在以太网环境中 ，实际传输的是“帧”，帧里面有目标主机的 MAC 地址，一个主机和另一个主机直接进行通信必须要知道目标主机的 MAC 地址，即数据传输依赖的是 MAC 地址而非 IP 地址，而 ARP 协议就是将已知的 IP 地址转换为 MAC 地址。

2.ARP 映射方式分类

ARP 映射方式主要分为静态映射和动态映射。

静态映射是指手动创建一张 ARP 表，把逻辑（IP）地址和物理地址（MAC）关联起来，这个 ARP 表存储在网络中每一台机器上，机器通过使用目的 IP 地址在 ARP 表中查找对应的物理地址，然后进行帧的发送，这样做有一定的局限性：（1）机器可能更换 NIC（网络接口卡），结果变成一个新的物理地址；（2）在某些局域网中，每当计算机通电时，其物理地址都会进行改变；（3）移动电脑可以从一个物理网络转移到另一个物理网络，这样其物理地址同样会发生改变，而要避免这些问题，必须定期维护更新 ARP 表，而这是分麻烦且会影响网络性能。

动态映射是指每次机器要知道另一台机器的物理地址，就可以使用协议和已知目的逻辑地址找出相对应的物理地址，已经设计出的实现了动态映射的协

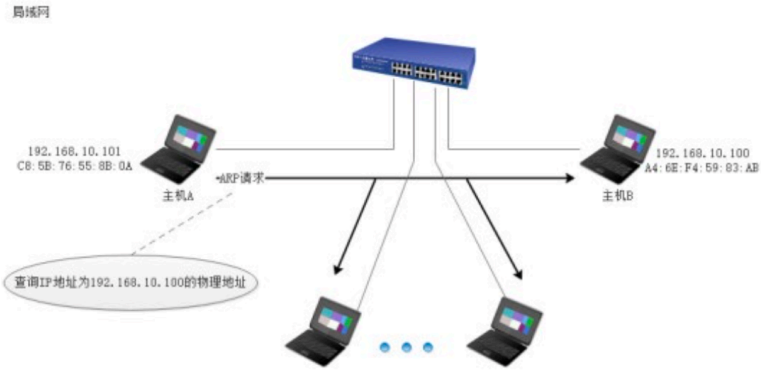
议有 ARP 和 RARP 两种，ARP 把逻辑地址映射为物理地址，RARP 将物理地址映射为逻辑地址。

3.ARP 工作原理（ARP 动态映射）

在任何时候，一台主机有 IP 数据报文发送给另一台主机，都需要知道接收方的逻辑（IP）地址，同时 IP 地址需要被封装到帧中才能通过物理网络传输，这就要求发送方需要知道接收方的物理（MAC）地址，因此需要完成从逻辑地址到物理地址的映射。ARP 协议可以接受来自 IP 协议的逻辑地址，将其映射为对应的物理地址，然后把物理地址递交给数据链路层，即在主机发送帧前将目标 IP 地址转换成 MAC 地址，使得帧能够在实际的物理网络（如以太网）进行传输。

3.1ARP 请求

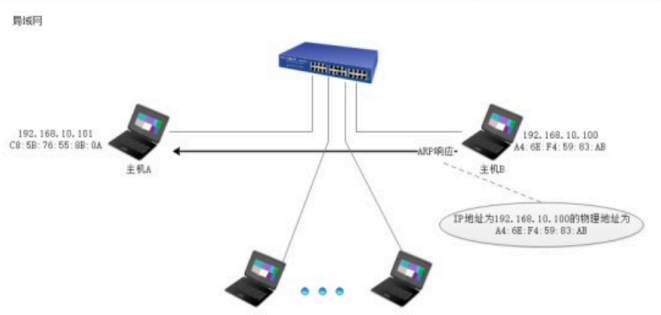
任何时候，当主机需要找出这个网络中另一个主机的物理地址时，就会发送一个 ARP 请求报文，这个报文包含发送方的 MAC 地址和 IP 地址以及接收方的 IP 地址，而接收方的 MAC 地址是空出的（因为不知道），正因如此，这个查询会在网络层中进行**广播**。



(图1) ARP请求广播

3.2ARP 响应

局域网中每一台主机都会接收并处理这个 ARP 请求报文，然后进行验证，查看接收方的 IP 地址是不是自己的地址，只有验证成功的主机才会返回一个 ARP 响应报文，这个报文包含接收方的 IP 地址和物理地址，同时这个报文利用接收到的 ARP 请求报文中的请求方物理地址以单播方式直接发送 ARP 响应报文给请求方。



4.ARP 协议报文字段

4.1 报文格式如图所示

硬件类型		协议类型
硬件长度	协议长度	操作码（请求为1，响应为2）
源硬件地址		
源逻辑地址		
目的硬件地址		
目的逻辑地址		

硬件类型：16 位字段，用来定义运行 ARP 的网络类型，每个局域网基于其类型被指派一个整数，如以太网的类型为 1，ARP 可用在任何物理网络上。

协议类型：16 位字段，用来定义使用的协议，如 IPv4 协议字段使用 0800，ARP 可用于任何高层协议。

硬件长度：8 位字段，用来定义物理地址的长度，以字节为单位，如以太网值位 6（48 位 MAC 地址）。

协议长度 ：8 位字段，用来定义逻辑地址的长度，以字节为单位单位，如 IPv4 协议的值为 4（32 位 IP 地址）。

操作码：16 位字段，用来定义报文的类型，已定义的分组类型有两种，ARP 请求（1）和 ARP 响应（2）。

源硬件地址：这是一个可变长度字段，用来定义发送方的物理地址，如以太网这个字段的长度为 6 个字节。

目的逻辑地址：这是一个可变长度字段，用来定义发送方的逻辑（IP）地址，如 IP 协议这个字段的长度为 4 字节。

目的硬件地址：这是一个可变长度字段，用来定义目标的物理地址，如以太网这个字段的长度为 6 个字节。对于 ARP 请求报文，这个字段为全 0，因为发送方不知道目标的硬件地址。

目的逻辑地址：这是一个可变长度字段，用来定义发送方的逻辑（IP）地址，如 IP 协议这个字段的长度为 4 字节。

4.2ARP 报文总长度

ARP 报文总长度为 64 字节，帧是在数据链路层传输的数据格式，如以太网 2、以太网 IEEE802.3 和 PPP 等，所以 Wireshark 抓取的帧是包含帧头的，即包含以太网 V2 的帧头长 14bytes；而 ARP 数据包的长度固定为 28bytes。

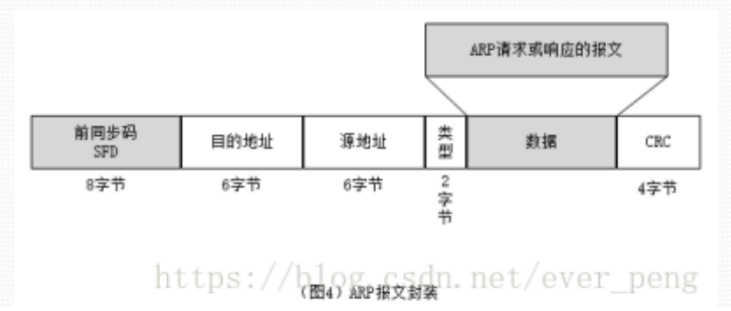
帧的总长度=帧头+网络层包头+传输层报文头+应用数据。

而 ARP 请求中 ARP 包已经是最高层，之上没有传输层和应用层，所以总长度=帧头+ARP 包头=14+28=42bytes。在真正发送帧时，为了保证以太网帧的最小帧长为 64bytes，会在报文里添加一个 padding 字段，用来填充数据包大小（64bytes）。

在使用 Wireshark 抓包时，抓到的包为 60bytes，比以太网帧的最小帧长少了 4bytes，原因是 Wireshark 抓包时不能抓到数据包最后的 CRC 字段（CRC 字段是为了校验以太网帧的正确性，在数据包填充完成后，通过算法计算一个值放到数据包的 CRC 字段，当接收方收到数据包后，会同样使用算法计算一个值，然后和 CRC 字段进行对比，查看是否相同，如果不同则证明数据包被更改，如果相同则证明数据包并未被更改）。

4.3 报文封装

ARP 报文直接封装在数据链路层的帧中，如图所示：



（图4）ARP报文封装

ARP 被封装在以太网的帧中，帧中类型字段指出此帧所携带的数据是 ARP 报文。

【实验设备】

1.一台运行 Windows 系统的计算机。

2.网络终端模拟仿真软件 Cisco Packet Tracer。

3.网络抓包软件 WireShark。

【实验步骤】

1.首先进行相应的 DHCP 配置。

路由器左边网络 DHPC 配置：

ip dhcp excluded-address 192.168.1.0 192.168.1.10

ip dhcp pool myleftnet

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

option 150 ip 192.168.1.3

dns-server 192.168.1.2

路由器右边网络 DHPC 配置：

ip dhcp excluded-address 192.168.2.0 192.168.2.10

ip dhcp pool myrightnet

network 192.168.2.0 255.255.255.0

default-router 192.168.2.1

option 150 ip 192.168.2.3

dns-server 192.168.2.2

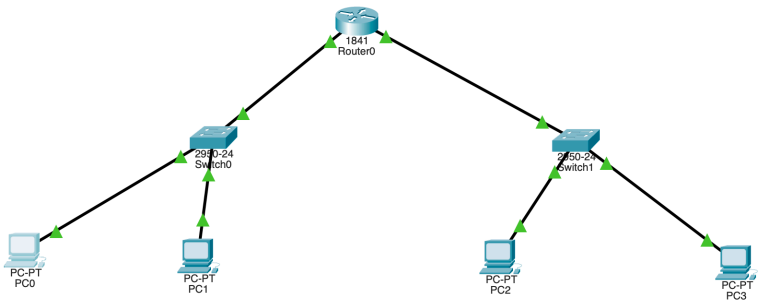
2.清空相关 PC 的 ARP，命令为 arp -d。

路由器相关命令为 clear arp-cache。

3.使用 Packert Tracert 抓取分析 ARP 报文。

【实验现象】

1.网络拓扑图如图所示，DHCP 已配置好。



2.清空 ARP 表。

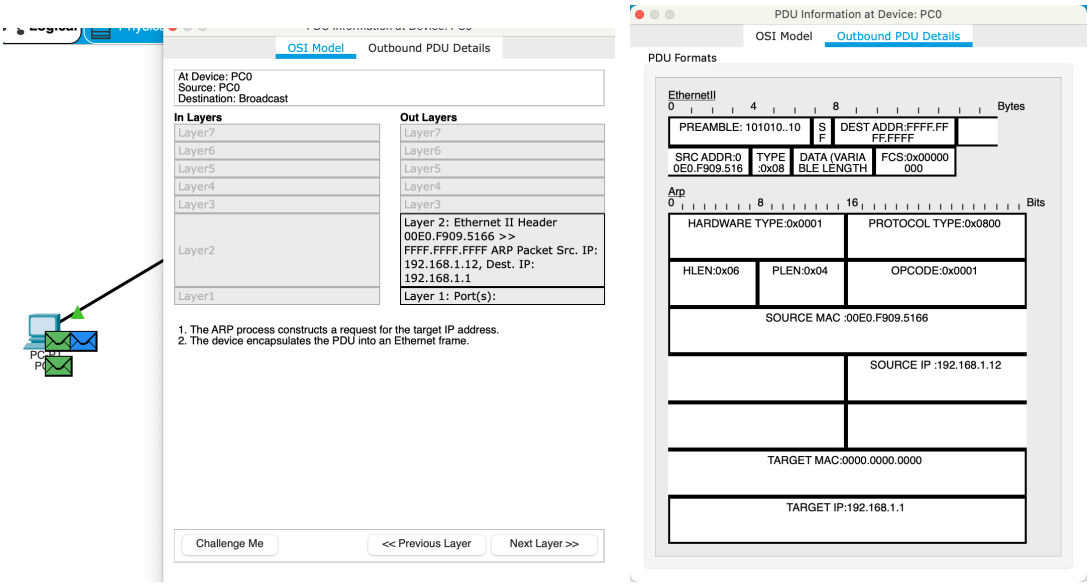
Command Prompt

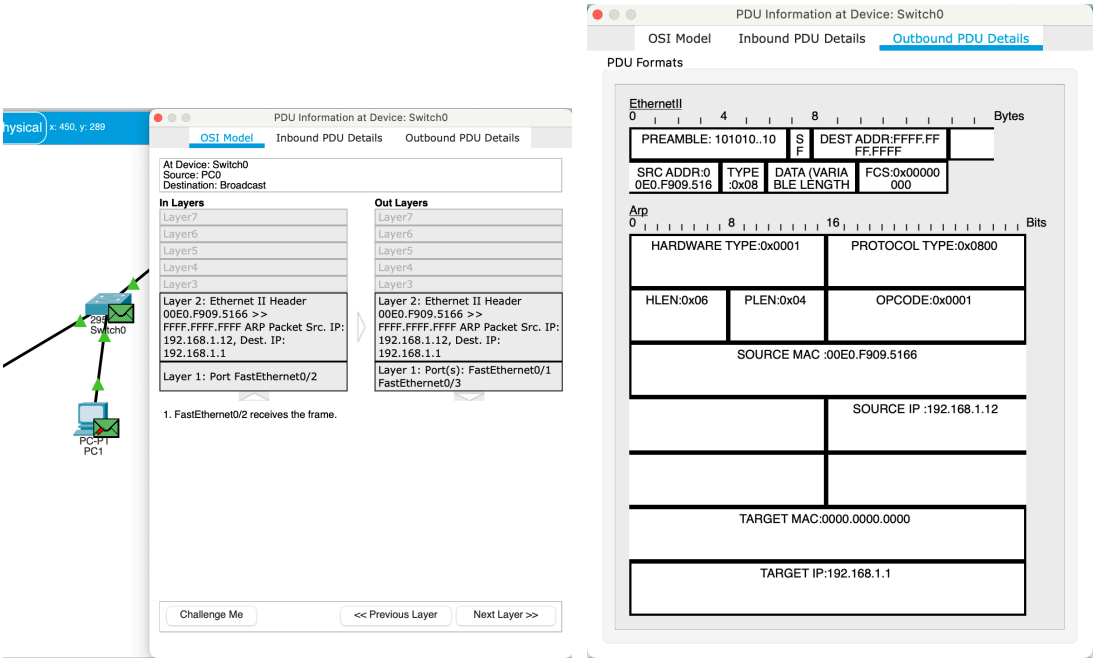
```
Packet Tracer PC Command Line 1.0
C:\>arp
C:\>arp
Packet Tracer PC ARP
Display ARP entries: arp -a
Clear ARP table: arp -d

C:\>arp -d
C:\>
C:\>
C:\> arp
C:\>arp -a
No ARP Entries Found
C:\>
```

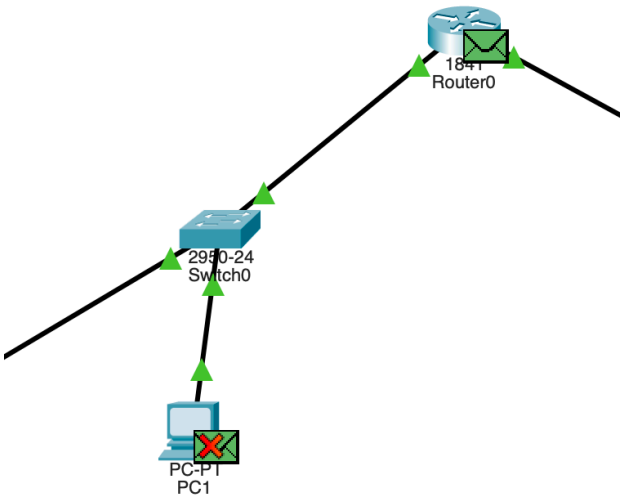
```
Router#clear?
clear
Router#clear ?
  aaa                 Clear AAA values
  access-list         Clear access list statistical information
  arp-cache           Clear the entire ARP cache
  cdp                 Reset cdp information
  frame-relay         Clear Frame Relay information
  ip                  IP
  ipv6                IPv6
  line                Reset a terminal line
  mac-address-table   MAC forwarding table
  vtp                 Clear VTP items
Router#clear arp
Router#clear arp-cache
Router#
```

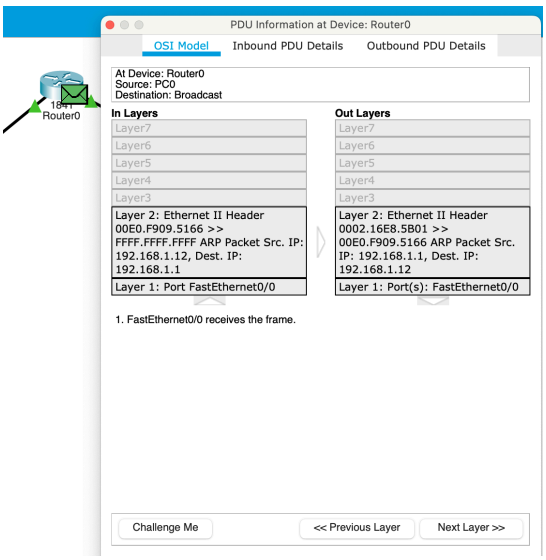
Command+F6 to exit CLI focus

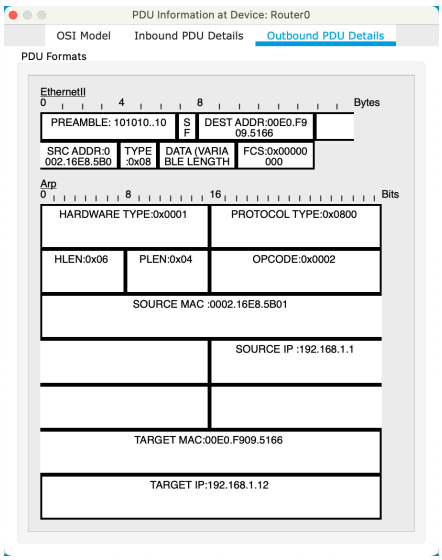
3.抓取分析过程。

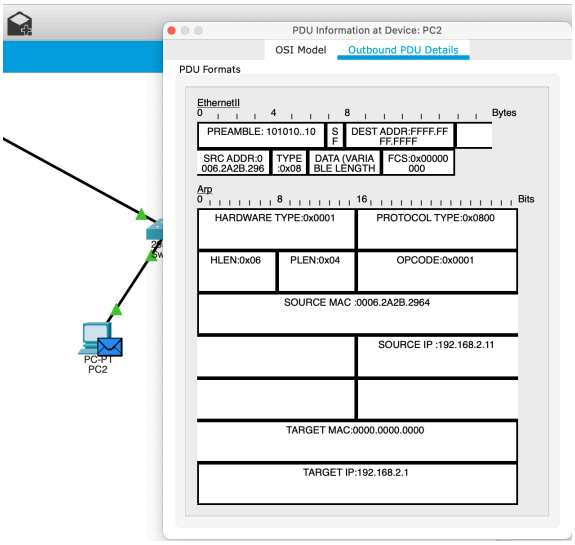

OSI Model
Outbound PDU Details
At Device: PC0
Source: PC0
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1
Layer 2: Ethernet II Header 00E0.F909.5166 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.12, Dest. IP: 192.168.1.1
Layer 1: Port(s):
1. The ARP process constructs a request for the target IP address.
2. The device encapsulates the PDU into an Ethernet frame.
Challenge Me
<< Previous Layer
Next Layer >>
PDU Information at Device: PC0
OSI Model
Outbound PDU Details
PDU Formats
EthernetII
Bytes
PREAMBLE: 101010..10
SF
DEST ADDR:FFFF.FFFF.FFFF
SRC ADDR:00E0.F909.516
TYPE :0x08
DATA (VARIABLE LENGTH
FCS:0x00000000
Arp
Bits
HARDWARE TYPE:0x0001
PROTOCOL TYPE:0x0800
HLEN:0x06
PLEN:0x04
OPCODE:0x0001
SOURCE MAC :00E0.F909.5166
SOURCE IP :192.168.1.12
TARGET MAC:0000.0000.0000
TARGET IP:192.168.1.1


PDU Information at Device: Switch0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Switch0
Source: PC0
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 00E0.F909.5166 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.12, Dest. IP: 192.168.1.1
Layer 1: Port FastEthernet0/2
Layer 1: Port(s): FastEthernet0/1 FastEthernet0/3
1. FastEthernet0/2 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>
Switch0
PC1
PDU Information at Device: Switch0
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
EthernetII
Bytes
PREAMBLE: 101010..10
SF
DEST ADDR:FFFF.FFFF.FFFF
SRC ADDR:00E0.F909.516
TYPE :0x08
DATA (VARIABLE LENGTH
FCS:0x00000000
Arp
Bits
HARDWARE TYPE:0x0001
PROTOCOL TYPE:0x0800
HLEN:0x06
PLEN:0x04
OPCODE:0x0001
SOURCE MAC :00E0.F909.5166
SOURCE IP :192.168.1.12
TARGET MAC:0000.0000.0000
TARGET IP:192.168.1.1


Router0
2950-24
Switch0
PC-PT
PC1


PDU Information at Device: Router0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Router0
Source: PC0
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 00E0.F909.5166 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.12, Dest. IP: 192.168.1.1
Layer 1: Port FastEthernet0/0
Layer 2: Ethernet II Header 0002.16E8.5B01 >> 00E0.F909.5166 ARP Packet Src. IP: 192.168.1.1, Dest. IP: 192.168.1.12
Layer 1: Port(s): FastEthernet0/0
1. FastEthernet0/0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>
Router0


PDU Information at Device: Router0
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
EthernetII
Bytes
PREAMBLE: 101010..10
SF
DEST ADDR:00E0.F909.5166
SRC ADDR:0002.16E8.5B0
TYPE :0x08
DATA (VARIABLE LENGTH
FCS:0x00000000
Arp
Bits
HARDWARE TYPE:0x0001
PROTOCOL TYPE:0x0800
HLEN:0x06
PLEN:0x04
OPCODE:0x0002
SOURCE MAC :0002.16E8.5B01
SOURCE IP :192.168.1.1
TARGET MAC:00E0.F909.5166
TARGET IP:192.168.1.12



4.查看机器 ARP。

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.1           0002.16e8.5b01        dynamic
```

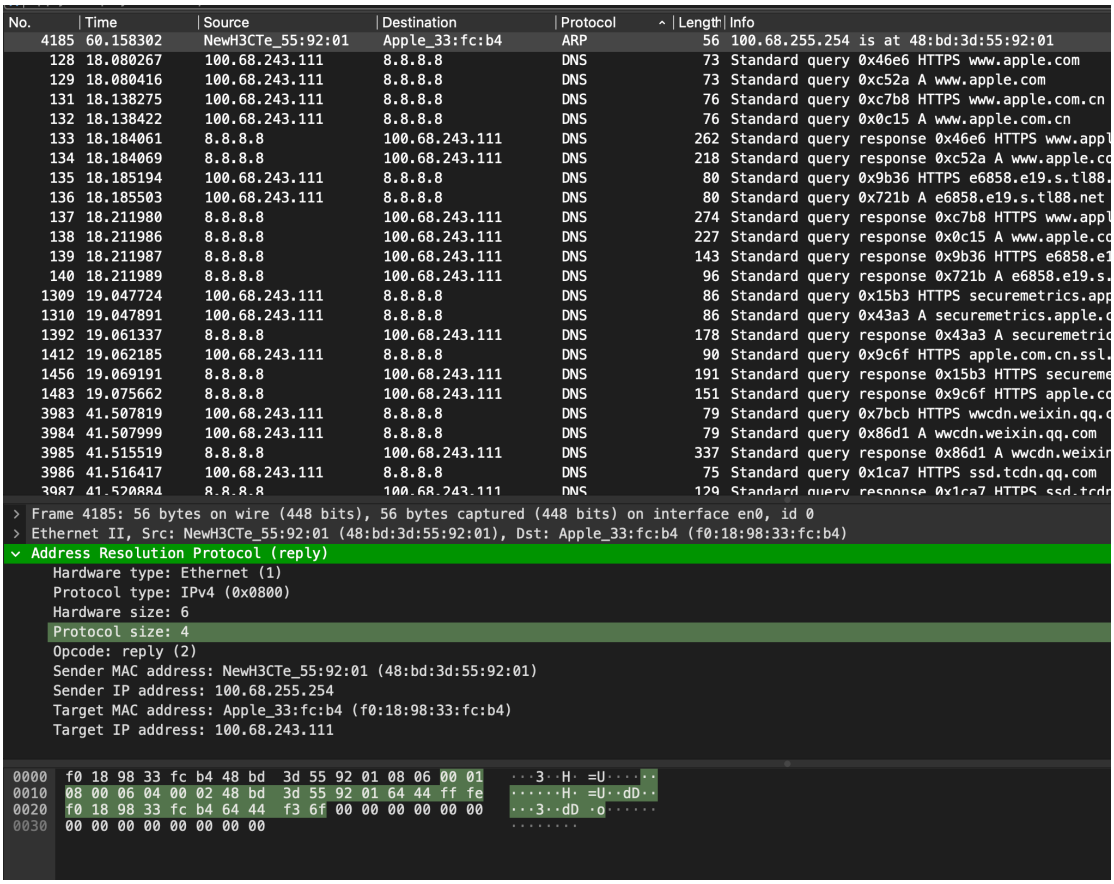
5.Wireshark ARP 抓取报文分析

Request 包：

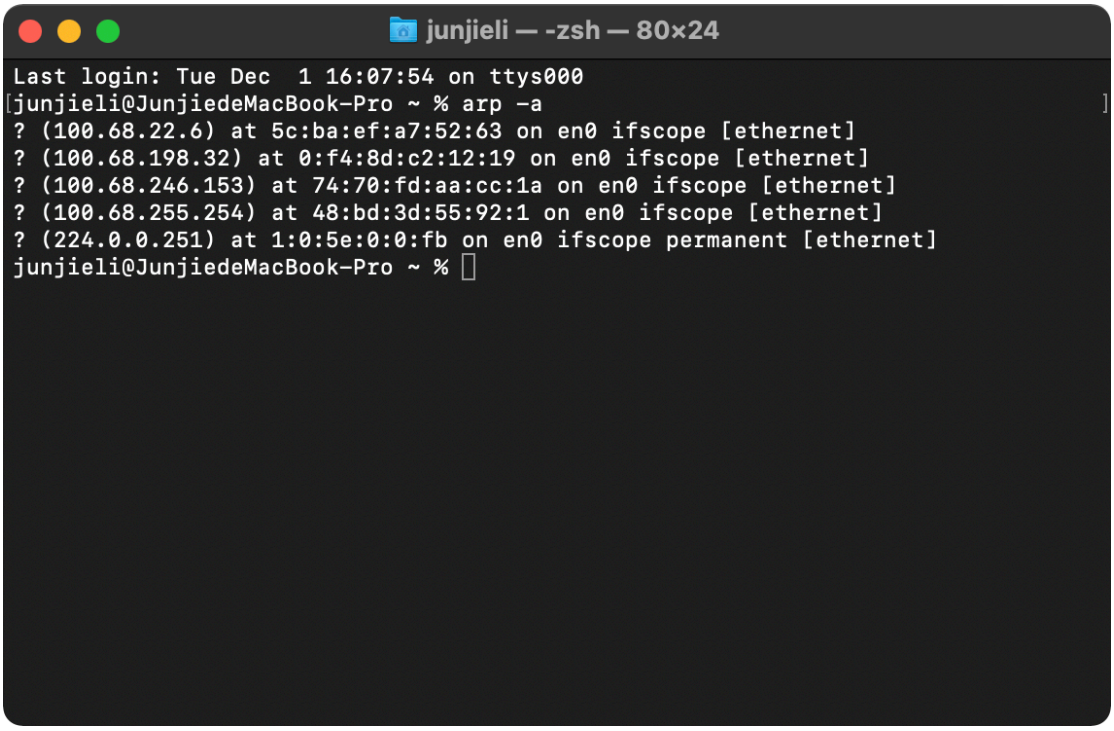
No.	Time	Source	Destination	Protocol	Length	Info
4185	60.158302	NewH3CTe_55:92:01	Apple_33:fc:b4	ARP	56	100.68.255.254 is at 48:bd:3d:55:92:01
8527	119.438807	IntelCor_aa:cc:1a	Apple_33:fc:b4	ARP	56	Who has 100.68.243.111? Tell 100.68.246.153
8528	119.438934	Apple_33:fc:b4	IntelCor_aa:cc:1a	ARP	42	100.68.243.111 is at f0:18:98:33:fc:b4
8723	150.449005	NewH3CTe_55:92:01	Apple_33:fc:b4	ARP	56	100.68.255.254 is at 48:bd:3d:55:92:01
8893	189.537652	NewH3CTe_55:92:01	Broadcast	ARP	60	Gratuitous ARP for 100.68.255.254 (Reply)
8894	189.640589	NewH3CTe_55:92:01	Broadcast	ARP	60	Gratuitous ARP for 100.68.255.254 (Reply)
8979	203.361489	NewH3CTe_55:92:01	Broadcast	ARP	60	Gratuitous ARP for 100.68.255.254 (Reply)
8980	204.078086	NewH3CTe_55:92:01	Broadcast	ARP	60	Gratuitous ARP for 100.68.255.254 (Reply)
111…	229.780326	NewH3CTe_55:92:01	Broadcast	ARP	60	Gratuitous ARP for 100.68.255.254 (Reply)
113…	240.803217	NewH3CTe_55:92:01	Apple_33:fc:b4	ARP	56	100.68.255.254 is at 48:bd:3d:55:92:01
116…	248.620217	NewH3CTe_55:92:01	Broadcast	ARP	60	Gratuitous ARP for 100.68.255.254 (Reply)
122…	249.439377	NewH3CTe_55:92:01	Broadcast	ARP	60	Gratuitous ARP for 100.68.255.254 (Reply)
125…	250.259704	NewH3CTe_55:92:01	Broadcast	ARP	60	Gratuitous ARP for 100.68.255.254 (Reply)
128	18.080267	100.68.243.111	8.8.8.8	DNS	73	Standard query 0x46e6 HTTPS www.apple.com
129	18.080416	100.68.243.111	8.8.8.8	DNS	73	Standard query 0xc52a A www.apple.com
131	18.138275	100.68.243.111	8.8.8.8	DNS	76	Standard query 0xc7b8 HTTPS www.apple.com.cn
132	18.138422	100.68.243.111	8.8.8.8	DNS	76	Standard query 0x0c15 A www.apple.com.cn
133	18.184061	8.8.8.8	100.68.243.111	DNS	262	Standard query response 0x46e6 HTTPS www.apple.c
134	18.184069	8.8.8.8	100.68.243.111	DNS	218	Standard query response 0xc52a A www.apple.com C
135	18.185194	100.68.243.111	8.8.8.8	DNS	80	Standard query 0x9b36 HTTPS e6858.e19.s.tl88.net
136	18.185503	100.68.243.111	8.8.8.8	DNS	80	Standard query 0x721b A e6858.e19.s.tl88.net
137	18.211980	8.8.8.8	100.68.243.111	DNS	274	Standard query response 0xc7b8 HTTPS www.apple.c
138	18.211986	8.8.8.8	100.68.243.111	DNS	227	Standard query response 0x0c15 A www.apple.com.c
139	18.211987	8.8.8.8	100.68.243.111	DNS	143	Standard query response 0x9b36 HTTPS e6858.e19.s

```
> Frame 8527: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface en0, id 0
> Ethernet II, Src: IntelCor_aa:cc:1a (74:70:fd:aa:cc:1a), Dst: Apple_33:fc:b4 (f0:18:98:33:fc:b4)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_aa:cc:1a (74:70:fd:aa:cc:1a)
    Sender IP address: 100.68.246.153
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 100.68.243.111

0000  f0 18 98 33 fc b4 74 70  fd aa cc 1a 08 06 00 01   ···3··tp ······ ··
0010  08 00 06 04 00 01 74 70  fd aa cc 1a 64 44 f6 99   ····tp ····dD··
0020  00 00 00 00 00 00 64 44  f3 6f 00 00 00 00 00 00   ····dD ·o····
0030  00 00 00 00 00 00 00 00                           ····
```

Reply 包：



6.查看本机 ARP 表。



【分析讨论】