

计算机网络-实验2：Oucer勇闯链路层

姓名：翟一航 学号：23020011046

一、实验目的

To explore the details of Ethernet frames. Ethernet is a popular link layer protocol. Modern computers connect to Ethernet switches rather than use classic Ethernet.

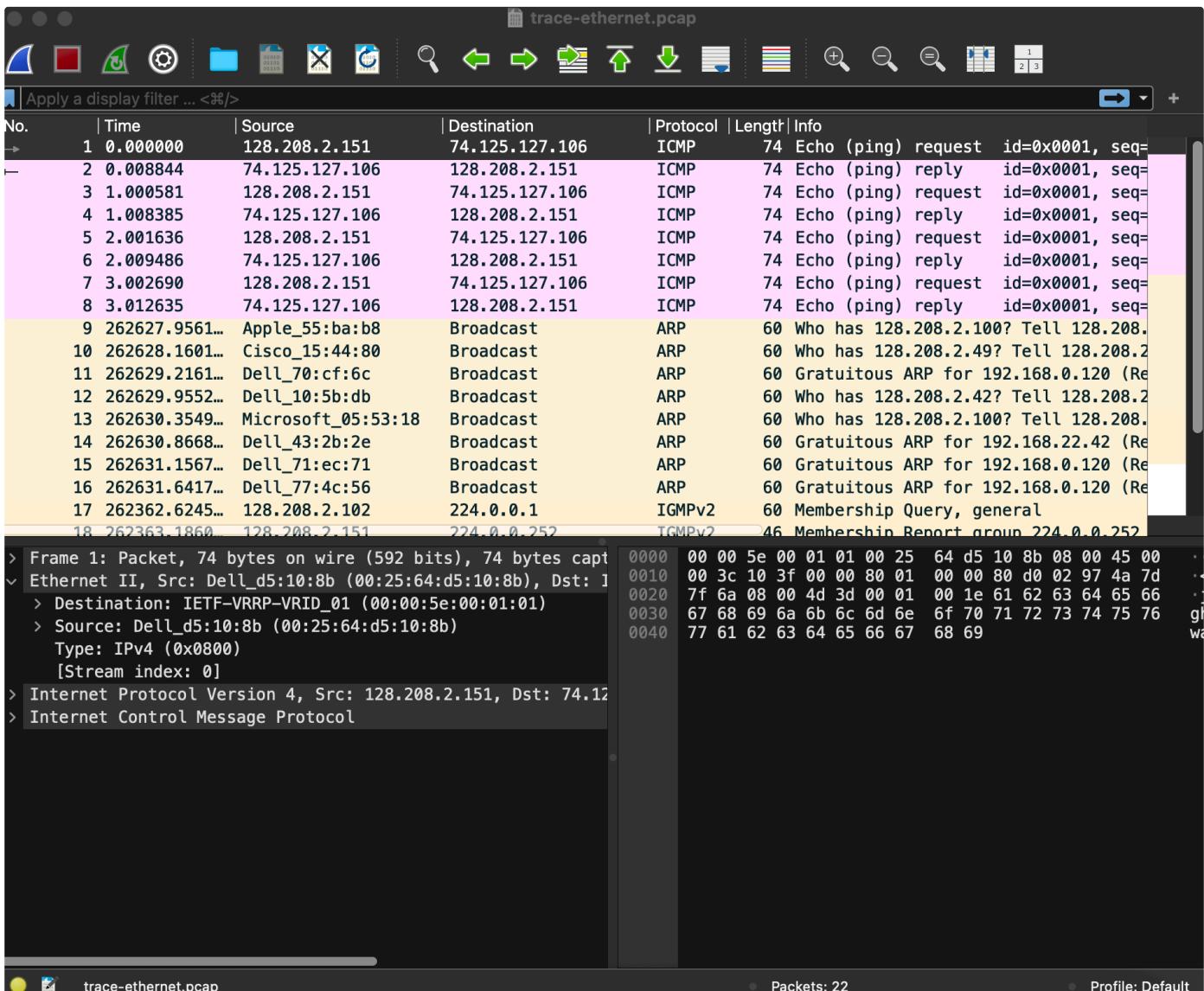
二、实验环境

环境	说明
操作系统	MacOS
抓包工具	Wireshark
网络接口	Wi-Fi:en0
数据包过滤器	ether multicast

三、实验内容

Step 1: Load the Lab Trace

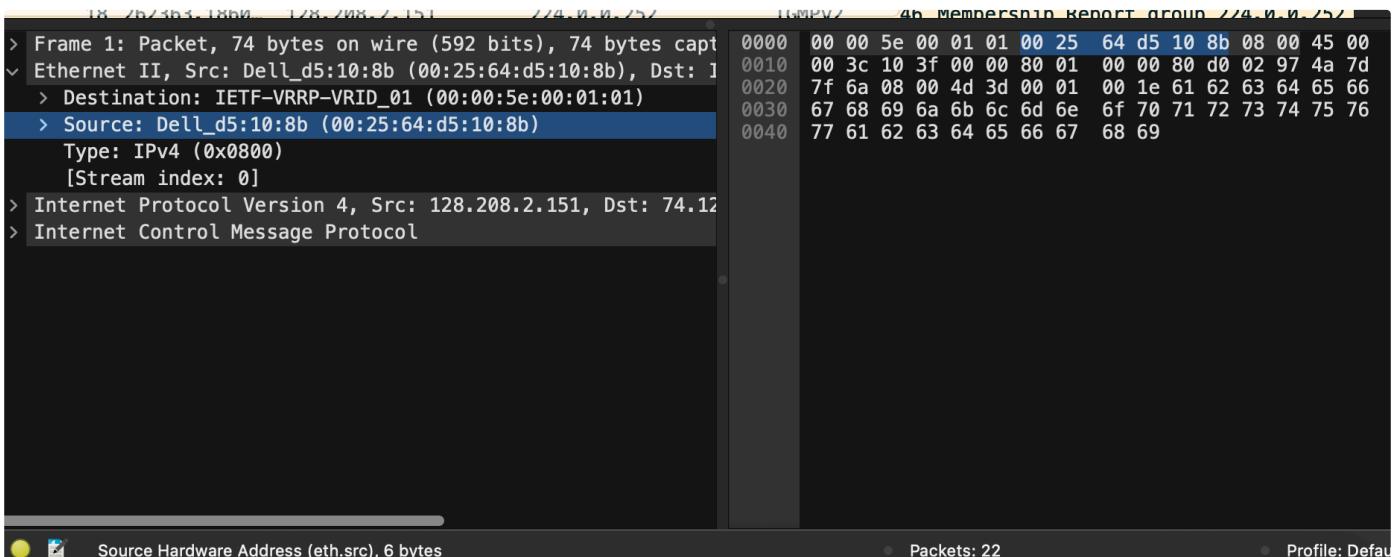
下载实验室的跟踪文件，并打开，得到如下界面：



Step 2: Inspect the Trace

Q1. What is the MAC address of the source of # 1 from IP address 128.208.2.151?

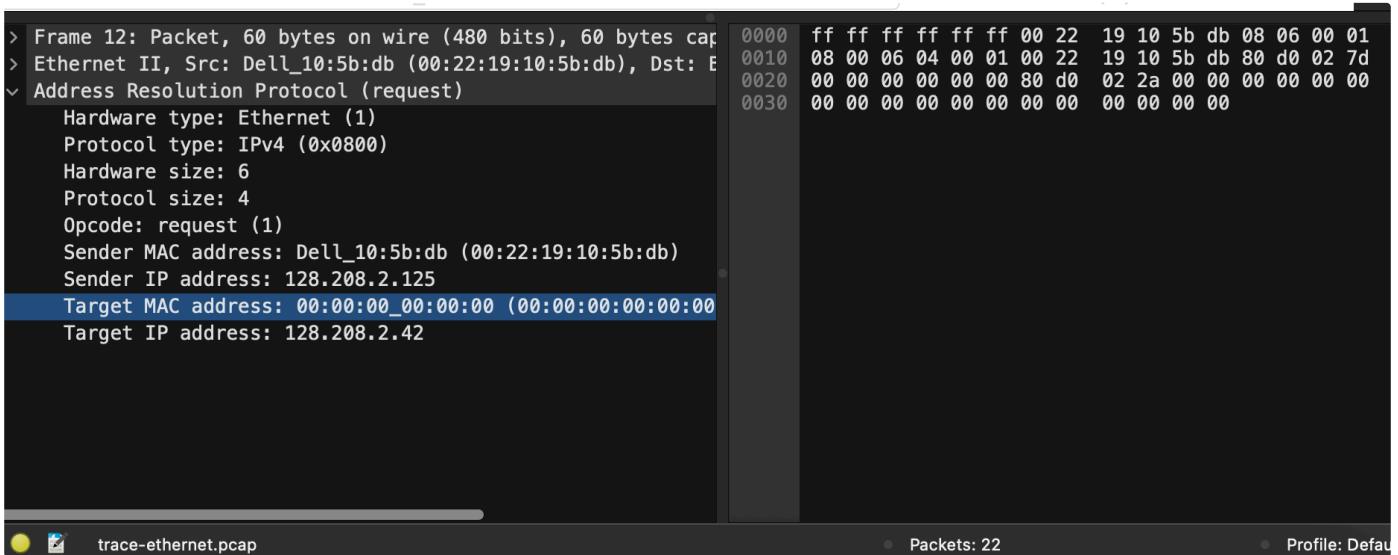
点击1号数据包，在下边的详细信息窗口查看数据包的具体内容。在以太网链路层可以看见源MAC地址（Source），长度为6字节，为 00:25:64:d5:10:8b。



Q2. Click on # 12 and expand the Address Resolution Protocol section in middle pane.
What does Target MAC address: 00:00:00:00:00 mean?

点击12号数据包并展开“Address Resolution Protocol”部分后，可以看到“Target MAC address: 00:00:00:00:00”，这说明发送这个ARP请求的设备还不知道目标 IP 地址对应的 MAC 地址是什么，它正在询问和等待这个信息，所以发送者使用一串全0作为占位符，来填充目标 MAC 地址字段。

之后，当拥有目标 IP 地址对应的 MAC 地址的设备收取到这个广播请求之后，它才会单独回复一个ARP应答，这个包中包含发送者缺少的那部分 MAC 地址。



Q3. Click again on # 12 and expand the Address Resolution Protocol section in middle pane.Why is the protocol type listed as IP when it is not an IP packet?

如上图所示，“Protocol type: IPv4 (0x0800)”。这是因为 ARP 协议的工作就是为 IP 协议服务的，它询问的内容是关于一个 IP 地址的信息，它定义了 ARP 请求和应答中携带的网络层地址类型。

Step 3:Ethern Frame Structure

Q1. Click on # 12 and expand the Address Resolution Protocol section in middle panel through the down arrow [v]. What does opcode (1) signify? What does opcode (2) signify?

仍然如上图所示，12号数据包的操作码为“request (1)”，这说明在此次抓包中，12号数据包是一个 ARP 请求，它的操作码是1。它是一台设备在局域网内发出的广播，目的是询问目标 IP 地址的 MAC 地址。

如下图所示，14号数据包的操作码为“reply (2)”，这说明在此次抓包中，14号数据包是一个 ARP 回复，它的操作码是 2。它是对于 ARP 请求的回复，即拥有目标 IP 地址和对应 MAC 地址的设备对该请求进行回复，由于该设备也不知道具体是哪个设备发出的请求，所以也以广播的形式进行回复，Target MAC address 也为 00:00:00:00:00:00。

Q2. Click on # 12 and expand using the [v] arrow and give the hexadecimal value for the two-byte Ethernet Frame type field?

如上图所示，查看12号数据包的具体内容，点击展开“Ethernet II”层内容，可以看到“Type: ARP (0x0806)”，因而两字节以太网帧类型字段的16进制值为 0x0806，这是对于 ARP 协议的固定值。

Step 4: Scope of Ethernet Addresses

1号数据包的内容：

1	0.000000	128.208.2.151	74.125.127.106	ICMP	74 Echo (ping) request	id=0x0001, seq=30/7680, ttl=128 (reply in 2)
2	0.008844	74.125.127.106	128.208.2.151	ICMP	74 Echo (ping) reply	id=0x0001, seq=30/7680, ttl=50 (request in 1)
3	1.000581	128.208.2.151	74.125.127.106	ICMP	74 Echo (ping) request	id=0x0001, seq=31/7936, ttl=128 (reply in 4)
4	1.008385	74.125.127.106	128.208.2.151	ICMP	74 Echo (ping) reply	id=0x0001, seq=31/7936, ttl=52 (request in 3)
5	2.001636	128.208.2.151	74.125.127.106	ICMP	74 Echo (ping) request	id=0x0001, seq=32/8192, ttl=128 (reply in 6)
6	2.009486	74.125.127.106	128.208.2.151	ICMP	74 Echo (ping) reply	id=0x0001, seq=32/8192, ttl=50 (request in 5)
7	3.002690	128.208.2.151	74.125.127.106	ICMP	74 Echo (ping) request	id=0x0001, seq=33/8448, ttl=128 (reply in 8)
8	3.012635	74.125.127.106	128.208.2.151	ICMP	74 Echo (ping) reply	id=0x0001, seq=33/8448, ttl=52 (request in 7)
9	262627.9561...	Apple_55:ba:b8	Broadcast	ARP	60 Who has 128.208.2.100? Tell 128.208.2.28	
10	262628.1601...	Cisco_15:44:80	Broadcast	ARP	60 Who has 128.208.2.49? Tell 128.208.2.102	
11	262629.2161...	Dell_70:cf:6c	Broadcast	ARP	60 Gratuitous ARP for 192.168.0.120 (Reply)	
12	262629.9552...	Dell_10:5b:db	Broadcast	ARP	60 Who has 128.208.2.42? Tell 128.208.2.125	
13	262630.3549...	Microsoft_05:53:18	Broadcast	ARP	60 Who has 128.208.2.100? Tell 128.208.2.89	
14	262630.8668...	Dell_43:2b:2e	Broadcast	ARP	60 Gratuitous ARP for 192.168.22.42 (Reply)	
15	262631.1567...	Dell_71:ec:71	Broadcast	ARP	60 Gratuitous ARP for 192.168.0.120 (Reply) (duplicate use of 192.168.0.12)	
16	262631.6417...	Dell_77:4c:56	Broadcast	ARP	60 Gratuitous ARP for 192.168.0.120 (Reply) (duplicate use of 192.168.0.12)	
17	262362.6245...	128.208.2.102	224.0.0.1	IGMPv2	60 Membership Query, general	
18	262363.1860...	128.208.2.151	224.0.0.252	IGMPv2	46 Membership Report group 224.0.0.252	
19	262363.6861...	128.208.2.151	239.255.255.250	IGMPv2	46 Membership Report group 239.255.255.250	
20	-42344255.1...	SMCNetworks_11:5e:...	Nearest-Customer-B...	STP	60 Conf. Root = 0/0/0:13:f7:1e:df:f0 Cost = 10000 Port = 0x801b	
21	-42344253.1...	SMCNetworks_11:5e:...	Nearest-Customer-B...	STP	60 Conf. Root = 0/0/0:13:f7:1e:df:f0 Cost = 10000 Port = 0x801b	

> Frame 1: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 ✓ Ethernet II, Src: Dell_d5:10:8b (00:25:64:d5:10:8b), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
 > Destination: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
 > Source: Dell_d5:10:8b (00:25:64:d5:10:8b)
 Type: IPv4 (0x0800)
 [Stream index: 0]
 > Internet Protocol Version 4, Src: 128.208.2.151, Dst: 74.125.127.106
 > Internet Control Message Protocol

2号数据包的内容：

1	0.000000	128.208.2.151	74.125.127.106	ICMP	74 Echo (ping) request	id=0x0001, seq=30/7680, ttl=128 (reply in 2)
2	0.008844	74.125.127.106	128.208.2.151	ICMP	74 Echo (ping) reply	id=0x0001, seq=30/7680, ttl=50 (request in 1)
3	1.000581	128.208.2.151	74.125.127.106	ICMP	74 Echo (ping) request	id=0x0001, seq=31/7936, ttl=128 (reply in 4)
4	1.008385	74.125.127.106	128.208.2.151	ICMP	74 Echo (ping) reply	id=0x0001, seq=31/7936, ttl=52 (request in 3)
5	2.001636	128.208.2.151	74.125.127.106	ICMP	74 Echo (ping) request	id=0x0001, seq=32/8192, ttl=128 (reply in 6)
6	2.009486	74.125.127.106	128.208.2.151	ICMP	74 Echo (ping) reply	id=0x0001, seq=32/8192, ttl=50 (request in 5)
7	3.002690	128.208.2.151	74.125.127.106	ICMP	74 Echo (ping) request	id=0x0001, seq=33/8448, ttl=128 (reply in 8)
8	3.012635	74.125.127.106	128.208.2.151	ICMP	74 Echo (ping) reply	id=0x0001, seq=33/8448, ttl=52 (request in 7)
9	262627.9561...	Apple_55:ba:b8	Broadcast	ARP	60 Who has 128.208.2.100? Tell 128.208.2.28	
10	262628.1601...	Cisco_15:44:80	Broadcast	ARP	60 Who has 128.208.2.49? Tell 128.208.2.102	
11	262629.2161...	Dell_70:cf:6c	Broadcast	ARP	60 Gratuitous ARP for 192.168.0.120 (Reply)	
12	262629.9552...	Dell_10:5b:db	Broadcast	ARP	60 Who has 128.208.2.42? Tell 128.208.2.125	
13	262630.3549...	Microsoft_05:53:18	Broadcast	ARP	60 Who has 128.208.2.100? Tell 128.208.2.89	
14	262630.8668...	Dell_43:2b:2e	Broadcast	ARP	60 Gratuitous ARP for 192.168.22.42 (Reply)	
15	262631.1567...	Dell_71:ec:71	Broadcast	ARP	60 Gratuitous ARP for 192.168.0.120 (Reply) (duplicate use of 192.168.0.12)	
16	262631.6417...	Dell_77:4c:56	Broadcast	ARP	60 Gratuitous ARP for 192.168.0.120 (Reply) (duplicate use of 192.168.0.12)	
17	262362.6245...	128.208.2.102	224.0.0.1	IGMPv2	60 Membership Query, general	
18	262363.1860...	128.208.2.151	224.0.0.252	IGMPv2	46 Membership Report group 224.0.0.252	
19	262363.6861...	128.208.2.151	239.255.255.250	IGMPv2	46 Membership Report group 239.255.255.250	
20	-42344255.1...	SMCNetworks_11:5e:...	Nearest-Customer-B...	STP	60 Conf. Root = 0/0/0:13:f7:1e:df:f0 Cost = 10000 Port = 0x801b	
21	-42344253.1...	SMCNetworks_11:5e:...	Nearest-Customer-B...	STP	60 Conf. Root = 0/0/0:13:f7:1e:df:f0 Cost = 10000 Port = 0x801b	

> Frame 2: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 ✓ Ethernet II, Src: Cisco_15:44:80 (00:18:74:15:44:80), Dst: Dell_d5:10:8b (00:25:64:d5:10:8b)
 > Destination: Dell_d5:10:8b (00:25:64:d5:10:8b)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 > Source: Cisco_15:44:80 (00:18:74:15:44:80)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)

网关 MAC 地址

现在本地设备要向远端服务器发送消息，但是不知道目标的 MAC 地址，因而将数据包发送给网关，正如1号数据包中的内容，本地设备的 MAC 地址为 `00:25:64:d5:10:8b`，网关的 MAC 地址为 `00:00:5e:00:01:01`。网关将信息转发给目标远端服务器，信息中还包含本地设备的 MAC 地址，因而远端服务器（MAC 地址为 `00:18:74:15:44:80`）可以直接回复本地设备，无需经过网关进行通信。（正如1号数据包中的注释“`reply in 2`”，和2号数据包中与之对应的“`request in 1`”）

Step 5:Broadcast Frames

在终端中输入命令 `wireshark &` 打开一个新的 Wireshark 窗口，并选择要监听的以太网端口。可以发现有 `en0 - en4` 共5个端口，但是我们选择监听 `en0` 端口。

Wireshark · Capture Options

Input	Output	Options				
Interface	Traffic	Link-layer Header	Promisc	Snaplen (t)	Buffer (ME)	Mc
ap1		Ethernet	<input checked="" type="checkbox"/>	default	2	—
> Wi-Fi: en0		Ethernet	<input checked="" type="checkbox"/>	default	2	<input checked="" type="checkbox"/>
> awdl0		Ethernet	<input checked="" type="checkbox"/>	default	2	—
> llw0		Ethernet	<input checked="" type="checkbox"/>	default	2	—
> utun0		BSD loopback	<input checked="" type="checkbox"/>	default	2	—
> utun1		BSD loopback	<input checked="" type="checkbox"/>	default	2	—
> utun2		BSD loopback	<input checked="" type="checkbox"/>	default	2	—
> utun3		BSD loopback	<input checked="" type="checkbox"/>	default	2	—
> Loopback: lo0		BSD loopback	<input checked="" type="checkbox"/>	default	2	—
anpi1		Ethernet	<input checked="" type="checkbox"/>	default	2	—
anpi0		Ethernet	<input checked="" type="checkbox"/>	default	2	—
Ethernet Adapter (en3): en3		Ethernet	<input checked="" type="checkbox"/>	default	2	—
Ethernet Adapter (en4): en4		Ethernet	<input checked="" type="checkbox"/>	default	2	—
Thunderbolt 1: en1		Ethernet	<input checked="" type="checkbox"/>	default	2	—
Thunderbolt 2: en2		Ethernet	<input checked="" type="checkbox"/>	default	2	—
Thunderbolt Bridge: bridge0		Ethernet	<input checked="" type="checkbox"/>	default	2	—
—		BSD loopback	<input checked="" type="checkbox"/>	default	2	—

这是因为我的电脑使用校园网进行上网，使用的是 `en0` 端口，观察图形化界面也可以看到只有该端口后有流量曲线，在终端中输入命令 `ifconfig` 查看也可以进行验证，如下图所示：

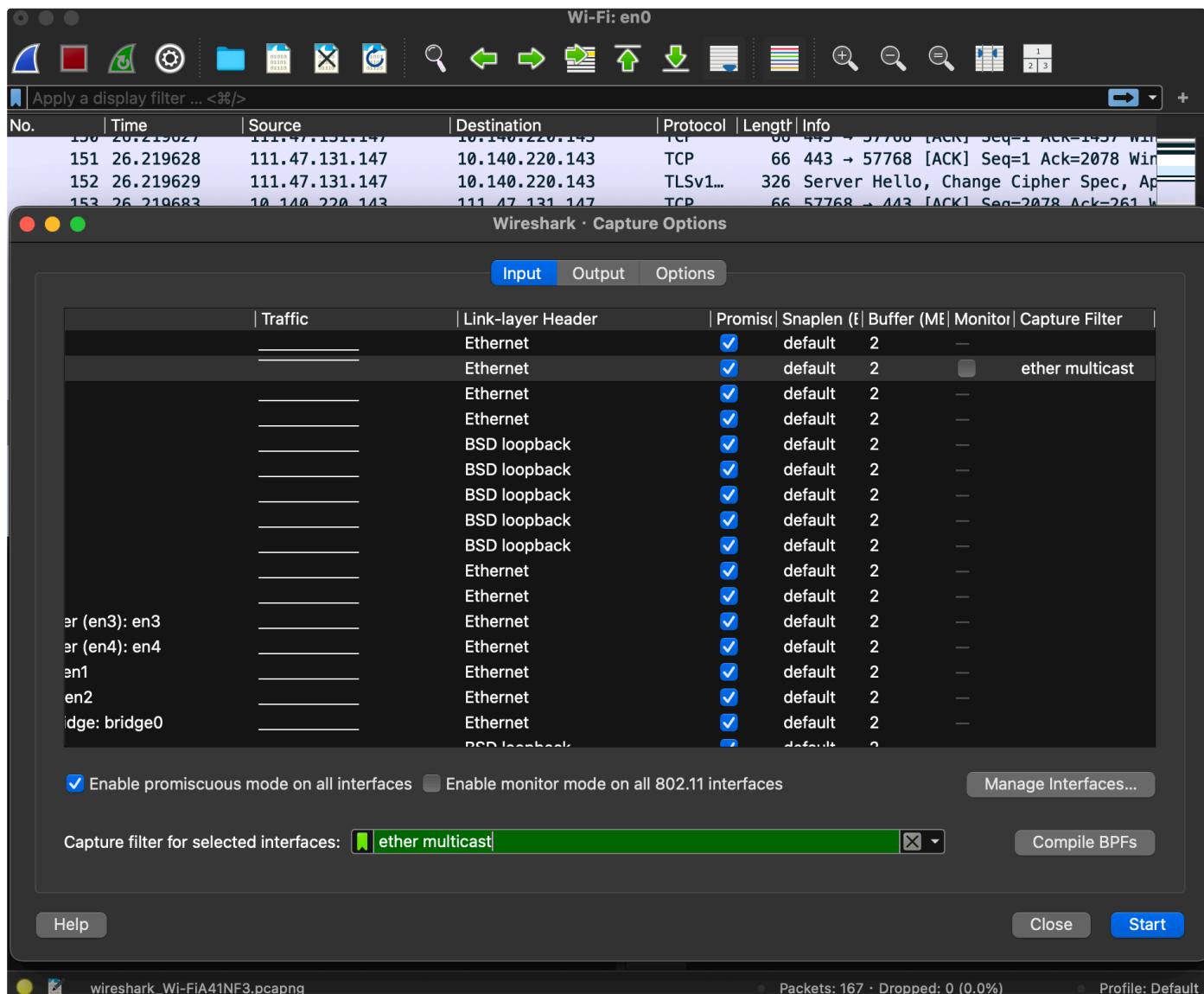
```

en3: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      options=400<CHANNEL_IO>
      ether 1a:48:ad:74:84:82
      nd6 options=201<PERFORMNUD,DAD>
      media: none
      status: inactive
en4: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      options=400<CHANNEL_IO>
      ether 1a:48:ad:74:84:83
      nd6 options=201<PERFORMNUD,DAD>
      media: none
      status: inactive
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
      options=460<TS04,TS06,CHANNEL_IO>
      ether 36:65:e5:b2:fa:80
      media: autoselect <full-duplex>
      status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
      options=460<TS04,TS06,CHANNEL_IO>
      ether 36:65:e5:b2:fa:84
      media: autoselect <full-duplex>
      status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      options=6460<TS04,TS06,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
      ether 66:43:46:09:d4:bc
      inet6 fe80::185b:c74d:9b63:63df%en0 prefixlen 64 secured scopeid 0xb
      inet 10.140.220.143 netmask 0xffffffff broadcast 10.140.223.255
      inet6 240c:ca02:2140:dbc:4:2047:726b:cc47 prefixlen 64 autoconf secured
      inet6 240c:ca02:2140:dbc:e87c:81b4:31d:db37 prefixlen 64 autoconf temporary
      nd6 options=201<PERFORMNUD,DAD>
      media: autoselect
      status: active

```

可以发现只有 `en0` 端口的 `status` 为 `active`，其余都为 `inactive`。

接下来需要选择 filter，要注意的是只有先停止捕获数据包才能够更改，如下图所示：



Examining Live Ethernet Multicast Traffic

过滤器 `ether multicast` 的作用是只捕获和显示目标 MAC 地址为广播或者多播类型的以太网帧

a. What is the broadcast Ethernet address, written in standard form as Wireshark displays it?

广播以太网地址的标准形式为 `ff:ff:ff:ff:ff:ff`，这个目标地址会使得该数据包能够被所有设备进行捕获。

可以点击一个广播以太网数据包进行查看，如图：

```

> Frame 1: Packet, 56 bytes on wire (448 bits), 56 bytes captured
  Ethernet II, Src: HuaweiTechno_ae:c9:ed (d4:4f:67:ae:c9:ed)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: HuaweiTechno_ae:c9:ed (d4:4f:67:ae:c9:ed)
    Type: Unknown (0x8300)
      [Stream index: 0]
> Data (42 bytes)

0000 ff ff ff ff ff d4 4f 67 ae c9 ed 83 00 00 00
0010 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Destination Hardware Address (eth.dst), 6 bytes
Packets: 57 · Dropped: 0 (0.0%) · Profile: Default

```

b. Which bit of the Ethernet address is used to determine whether it is unicast or multicast/broadcast?

数据包的第一个字节的最低有效位

如果这一位为1，则说明这是一个广播或者多播的地址，指向一组接收者；

如果这一位为0，则说明这是一个单播地址，指向网络中的某一个具体的设备。

补充：

广播和多播的数据包的第一个字节的最低有效位尽管都为1，但是他们的 Destination 还是有着显著的差别，以下为一个多播数据包的具体内容：

```

> Frame 19: Packet, 100 bytes on wire (800 bits), 100 bytes captured
  Ethernet II, Src: 8e:e9:49:84:45:98 (8e:e9:49:84:45:98), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
    > Destination: IPv4mcast_fb (01:00:5e:00:00:fb)
    > Source: 8e:e9:49:84:45:98 (8e:e9:49:84:45:98)
    Type: IPv4 (0x0800)
      [Stream index: 2]
> Internet Protocol Version 4, Src: 10.140.220.21, Dst: 224.0.0.1
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)

0000 01 00 5e 00 00 fb 8e e9 49 84 45 98 08 00 45 00
0010 00 56 c2 d7 00 00 ff 11 31 22 0a 8c dc 15 e0 00
0020 00 fb 14 e9 14 e9 00 42 e0 71 00 00 00 00 00 00 02
0030 00 00 00 00 00 00 0f 5f 63 6f 6d 70 61 6e 69 6f
0040 6e 2d 6c 69 6e 6b 04 5f 74 63 70 05 6c 6f 63 61
0050 6c 00 00 0c 00 01 07 5f 72 64 6c 69 6e 6b c0 1c
0060 00 0c 00 01

iTerm
wireshark_Wi-FiK1J6E3.pcapng
Packets: 25 · Dropped: 0 (0.0%) · Profile: Default

```

可以发现 Destination 并非全为 ff，只是仍然保证了第一个字节的最低有效位为1。

四、总结建议

通过此次实验，我对于计算机网络的链路层、以太网帧的结构和工作原理都有了更深刻的理解。

通过分析捕获的数据包，我更直观地认识了以太网帧的各个字段，包括源/目的 MAC地址、类型字段等，更直观地认识到了他们在网络通信中的作用。

通过观察ARP请求和应答数据包，我理解了 ARP 协议如何完成从 IP 地址到 MAC 地址的解析过程。特别是理解了操作码1和2分别代表请求和应答，以及目标MAC地址全零的含义。

除此之外，我还学会了通过 MAC 地址的第一个字节的最低位来区分单播、多播/广播地址，这是识别网络流量类型的重要技能，还认识了广播和多播在局域网中的作用，它们是链路层局域网正常通信的基础。