实验报告：Ethernet

课程名称：计算机网络	年级：2023 级	实践成绩：
指导教师：章玥	姓名：张建夫	
实践名称：Ethernet	学号：10235101477	实践日期：2024/11/25
实践编号：	组号：	实践时间：8:00~9:30

一、目的

1、掌握网络抓包工具 Wireshark、网络诊断工具 ping 的用法；

2、使用网络诊断工具 ping 触发网络消息；

3、使用网络抓包工具 Wireshark 获取并分析以太网数据帧；

4、掌握以太网帧的结构；

5、分析以太网地址范围；

6、分析以太网的广播帧。

二、实验内容与实验步骤

1. 背景知识

以太网：

以太网（Ethernet）是一种计算机局域网技术。IEEE 组织的 IEEE 802.3 标准制定了以太网的技术标准，它规定了包括物理层的连线、电子信号和介质访问控制的内容。以太网是目前应用最普遍的局域网技术，取代了其他局域网标准如令牌环、FDDI 和 ARCNET。

以太网的标准拓扑结构为总线型拓扑，但目前的快速以太网（100BASE-T、1000BASE-T 标准）为了减少冲突，将能提高的网络速度和使用效率最大化，使用交换机（Switch hub）来进行网络连接和组织。如此一来，以太网的拓扑结构就成了星型；但在逻辑上，以太网仍然使用总线型拓扑和 CSMA/CD（Carrier Sense Multiple Access/Collision Detection，即载波多重访问/碰撞侦测）的总线技术。

Ping 命令：

ping：本实验使用“ ping”发送和接收消息。 ping 是用于检查另一台计算机是否响应的标准命令行实用程序。它广泛用于网络故障排除，并已预装在 Window，Linux 和 Mac 上。执行命令“ ping www.baidu.com”，计算机就会向远程计算机发送少量 ICMP ping 请求，每个请求都会引发一个 ICMP ping 响应。

假设您 ping 了一个远程 Internet 服务器，每个以太网帧携带一个源地址和目标地址。其中一个地址是你电脑的 MAC 地址,它是发送帧的源。但另一个地址通常不是远程服务器的以太网地址，因为以太网帧的地址只能在一个 LAN 中进行。它通常是路由器或默认网关的以太网地址，这是一个将你的局域网连接到互联网的设备。每个包的 IP 块中的 IP 地址指示了源端点和目的地端点，也就是您的的计算机和远程服务器的地址。

2.实验步骤

1）捕获单播：

1、启动 Wireshark，在菜单栏的捕获->选项中进行设置，选择已连接的以太网，设置捕获过滤器为“icmp”，将混杂模式设为关闭,勾选 Resolve MAC addresses 然后开始捕获。

2、打开命令行，输入 ping www.baidu.com.

3、打开 Wireshark， 停止捕获。

2）捕获多播：

将上面的捕获过滤器改为 ether multicast 即可，之后等待若干时间捕获流量（对于 802.3 的 stp 协议组播捕获需要开启混杂模式）

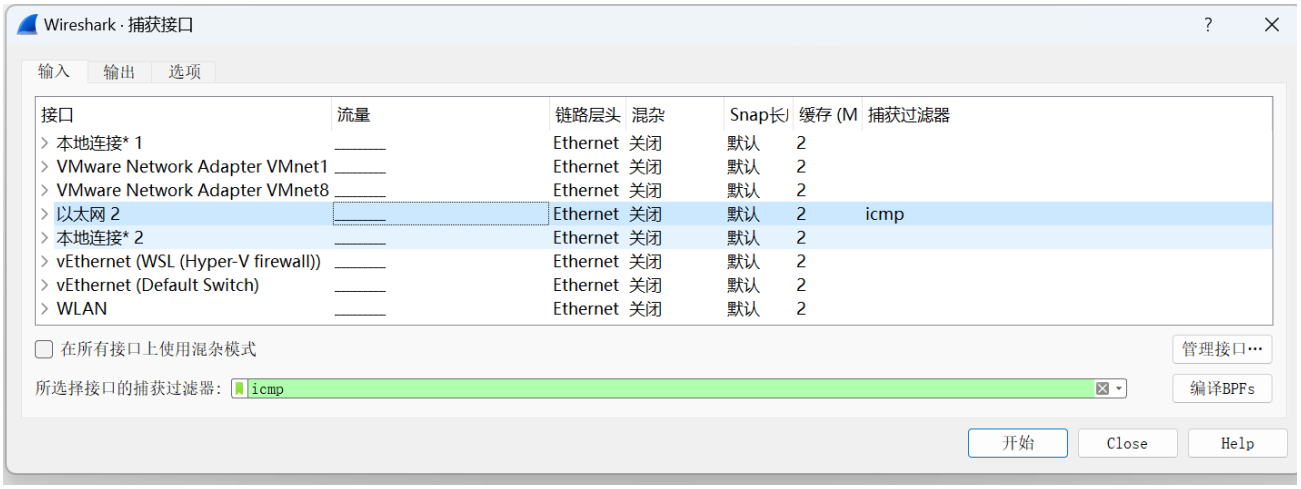
三、实验环境

调用 dxdiag 工具：

Operating System: Windows 11 家庭中文版 64-bit (10.0, Build 22621) (22621.ni_release.220506-1250)
Language: Chinese (Simplified) (Regional Setting: Chinese (Simplified))
System Manufacturer: HP
System Model: HP Pavilion Aero Laptop 13-be2xxx
BIOS: F.13 (type: UEFI)
Processor: AMD Ryzen 5 7535U with Radeon Graphics (12 CPUs), ~2.9GHz
Memory: 16384MB RAM
Available OS Memory: 15574MB RAM
Page File: 27604MB used, 5685MB available
Windows Dir: C:\WINDOWS
DirectX Version: DirectX 12
DX Setup Parameters: Not found
User DPI Setting: 144 DPI (150 percent)
System DPI Setting: 192 DPI (200 percent)
DWM DPI Scaling: UnKnown
Miracast: Available, with HDCP
Microsoft Graphics Hybrid: Not Supported

四、实验过程与分析

1.设置实验条件：



点击开始，并在命令行中 ping 百度的网址：

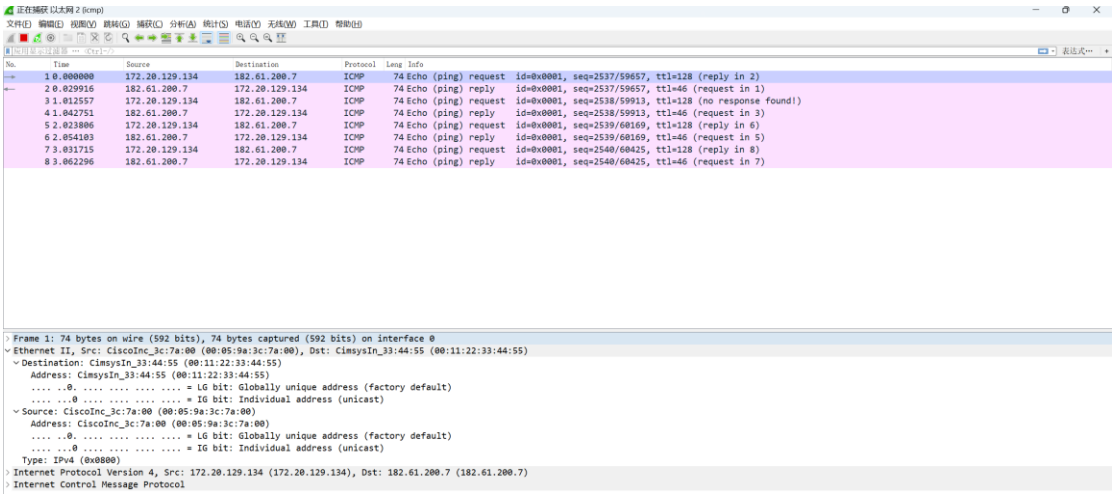
```
PS C:\Users\6666\Desktop> ping www.baidu.com

正在 Ping www.a.shifen.com [182.61.200.7] 具有 32 字节的数据：
来自 182.61.200.7 的回复：字节=32 时间=36ms TTL=46
来自 182.61.200.7 的回复：字节=32 时间=30ms TTL=46
来自 182.61.200.7 的回复：字节=32 时间=30ms TTL=46
来自 182.61.200.7 的回复：字节=32 时间=30ms TTL=46

182.61.200.7 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 = 30ms，最长 = 36ms，平均 = 31ms
```

2.单播：

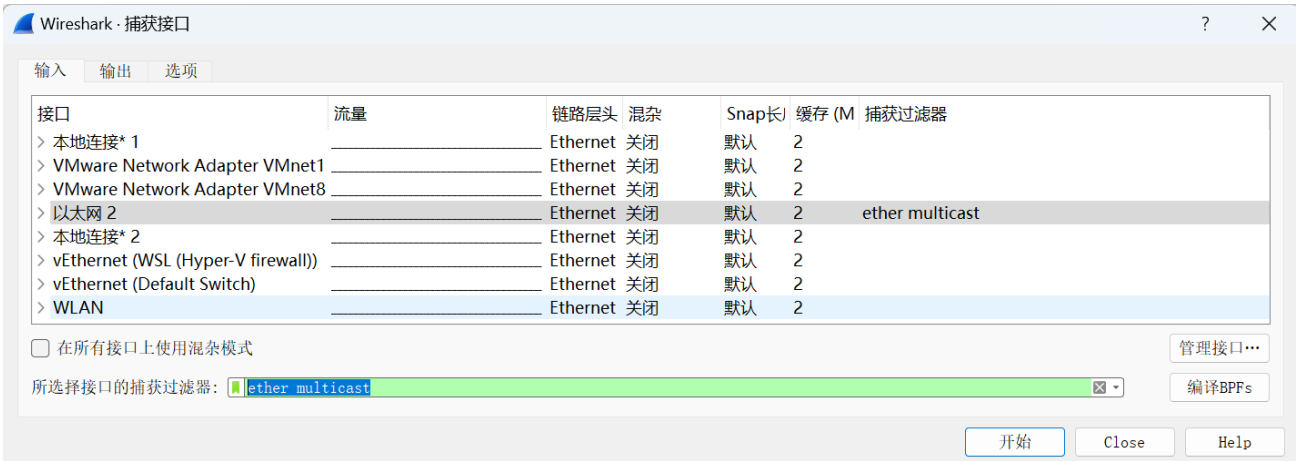
Ping 包发送完后抓到如下包：



在打开的以太网帧中可以看到源地址和目的地址（显然目的地址不是其 ip 地址）以及上层的协议 ipv4.

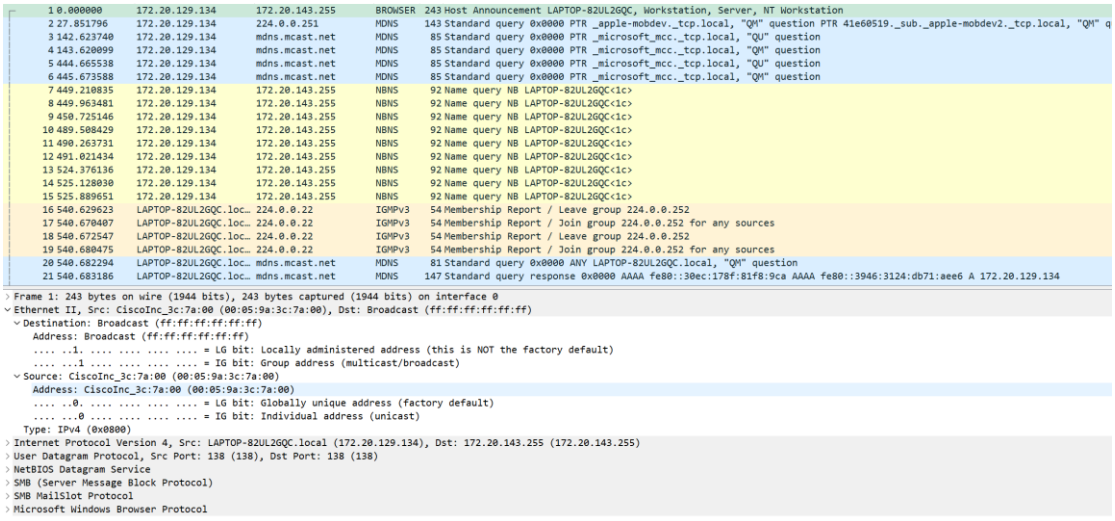
3.组播与广播：

先将过滤器改为如下：



开始捕获后，等待一定时间（学校台式机抓包特别快，笔记本需要等待一段时间）得到

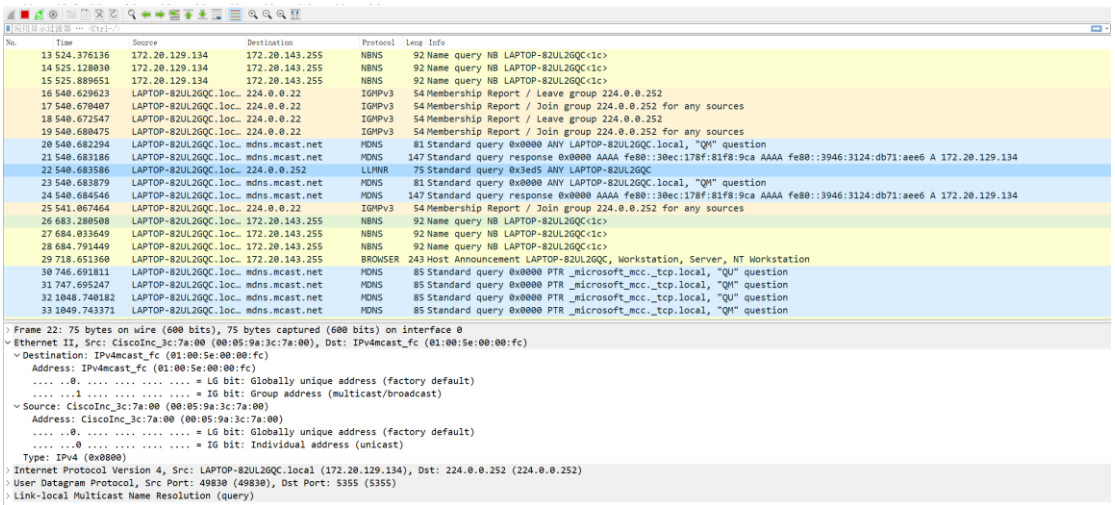
抓包结果如下：



No.	Time	Source	Destination	Protocol	Leng	Info
1	0.000000	172.20.129.134	172.20.143.255	BROWSER	243	Host Announcement LAPTOP-82UL2GQC, Workstation, Server, NT Workstation
2	27.851796	172.20.129.134	224.0.0.251	MDNS	143	Standard query 0x0000 PTR _apple-mobdev._tcp.local, "QM" question PTR 41e60519._sub._apple-mobdev2._tcp.local, "QM" q
3	142.623740	172.20.129.134	mdns.mcast.net	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
4	143.620099	172.20.129.134	mdns.mcast.net	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
5	444.665538	172.20.129.134	mdns.mcast.net	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
6	445.673588	172.20.129.134	mdns.mcast.net	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
7	449.210835	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
8	449.963481	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
9	450.725146	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
10	489.508429	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
11	490.263731	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
12	491.021434	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
13	524.376136	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
14	525.128030	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
15	525.889651	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
16	540.629623	LAPTOP-82UL2GQC.loc…	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
17	540.670407	LAPTOP-82UL2GQC.loc…	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
18	540.672547	LAPTOP-82UL2GQC.loc…	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
19	540.680475	LAPTOP-82UL2GQC.loc…	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
20	540.682294	LAPTOP-82UL2GQC.loc…	mdns.mcast.net	MDNS	81	Standard query 0x0000 ANY LAPTOP-82UL2GQC.local, "QM" question
21	540.683186	LAPTOP-82UL2GQC.loc…	mdns.mcast.net	MDNS	147	Standard query response 0x0000 AAAA fe80::30ec:178f:81f8:9ca AAAA fe80::3946:3124:db71:aee6 A 172.20.129.134

```
> Frame 1: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface 0
v Ethernet II, Src: CiscoInc_3c:7a:00 (00:05:9a:3c:7a:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: CiscoInc_3c:7a:00 (00:05:9a:3c:7a:00)
      Address: CiscoInc_3c:7a:00 (00:05:9a:3c:7a:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: LAPTOP-82UL2GQC.local (172.20.129.134), Dst: 172.20.143.255 (172.20.143.255)
> User Datagram Protocol, Src Port: 138 (138), Dst Port: 138 (138)
> NetBIOS Datagram Service
> SMB (Server Message Block Protocol)
> SMB MailSlot Protocol
> Microsoft Windows Browser Protocol
```

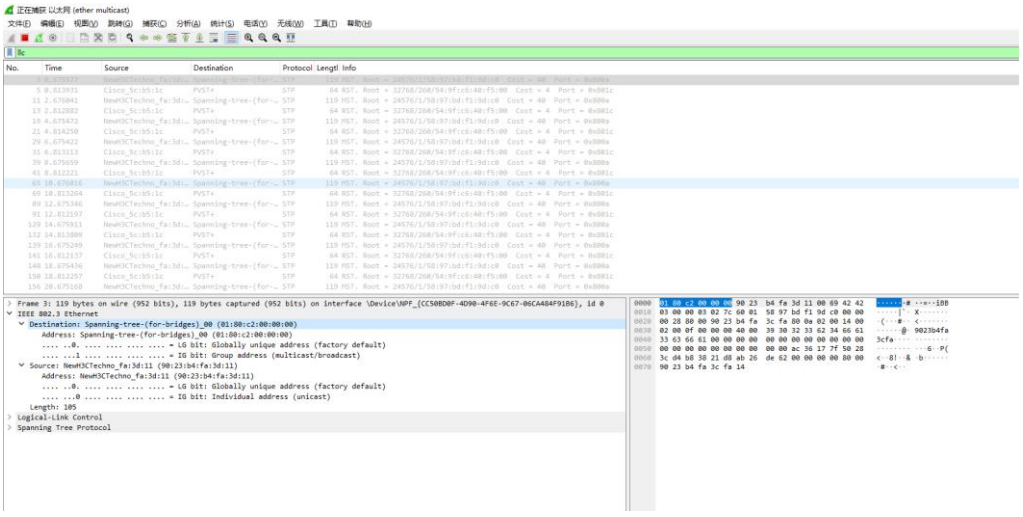
可以看到抓到的第一个帧是广播（Broadcast）,接下来再找个组播：



No.	Time	Source	Destination	Protocol	Leng	Info
13	524.376136	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
14	525.128030	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
15	525.889651	172.20.129.134	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
16	540.629623	LAPTOP-82UL2GQC.loc…	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
17	540.670407	LAPTOP-82UL2GQC.loc…	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
18	540.672547	LAPTOP-82UL2GQC.loc…	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
19	540.680475	LAPTOP-82UL2GQC.loc…	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
20	540.682294	LAPTOP-82UL2GQC.loc…	mdns.mcast.net	MDNS	81	Standard query 0x0000 ANY LAPTOP-82UL2GQC.local, "QM" question
21	540.683186	LAPTOP-82UL2GQC.loc…	mdns.mcast.net	MDNS	147	Standard query response 0x0000 AAAA fe80::30ec:178f:81f8:9ca AAAA fe80::3946:3124:db71:aee6 A 172.20.129.134
22	540.683586	LAPTOP-82UL2GQC.loc…	224.0.0.252	LLMNR	75	Standard query 0x3ed5 ANY LAPTOP-82UL2GQC
23	540.683879	LAPTOP-82UL2GQC.loc…	mdns.mcast.net	MDNS	81	Standard query 0x0000 ANY LAPTOP-82UL2GQC.local, "QM" question
24	540.684546	LAPTOP-82UL2GQC.loc…	mdns.mcast.net	MDNS	147	Standard query response 0x0000 AAAA fe80::30ec:178f:81f8:9ca AAAA fe80::3946:3124:db71:aee6 A 172.20.129.134
25	541.067464	LAPTOP-82UL2GQC.loc…	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
26	683.280508	LAPTOP-82UL2GQC.loc…	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
27	684.033649	LAPTOP-82UL2GQC.loc…	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
28	684.791449	LAPTOP-82UL2GQC.loc…	172.20.143.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
29	718.651360	LAPTOP-82UL2GQC.loc…	172.20.143.255	BROWSER	243	Host Announcement LAPTOP-82UL2GQC, Workstation, Server, NT Workstation
30	746.691811	LAPTOP-82UL2GQC.loc…	mdns.mcast.net	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
31	747.695247	LAPTOP-82UL2GQC.loc…	mdns.mcast.net	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
32	1048.740182	LAPTOP-82UL2GQC.loc…	mdns.mcast.net	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
33	1049.743371	LAPTOP-82UL2GQC.loc…	mdns.mcast.net	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question

```
> Frame 22: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
v Ethernet II, Src: CiscoInc_3c:7a:00 (00:05:9a:3c:7a:00), Dst: IPv4mcast_fc (01:00:5e:00:00:fc)
  v Destination: IPv4mcast_fc (01:00:5e:00:00:fc)
      Address: IPv4mcast_fc (01:00:5e:00:00:fc)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: CiscoInc_3c:7a:00 (00:05:9a:3c:7a:00)
      Address: CiscoInc_3c:7a:00 (00:05:9a:3c:7a:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: LAPTOP-82UL2GQC.local (172.20.129.134), Dst: 224.0.0.252 (224.0.0.252)
> User Datagram Protocol, Src Port: 49830 (49830), Dst Port: 5355 (5355)
> Link-local Multicast Name Resolution (query)
```

此处的 22 号帧就是组播，对于 ppt 里面的 802.3 的组播较为难以抓到，需要在学校的台式机上抓，并且要打开过滤器里的混杂模式并用 llc 过滤，以下是我在学校机子上的抓包截图：

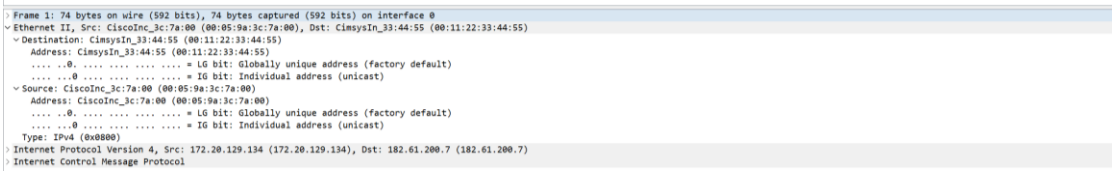


```
> Frame 3: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface \Device\NPF_{CC50BD8F-4D90-4F6E-9C67-06CA484F91B6}, id 0
v IEEE 802.3 Ethernet
  v Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
      Address: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: Newh3CTechno_fa:3d:11 (90:23:b4:fa:3d:11)
      Address: Newh3CTechno_fa:3d:11 (90:23:b4:fa:3d:11)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Length: 105
> Logical-Link Control
> Spanning Tree Protocol
```

可以看到的是 802.3 的组播采用的是 stp 协议，14 个字节里面的最后两个字节保存的不再是下一层使用的协议，而是一个长度，表示数据部分的字节数（这与 EthernetII 的格式并不一样）

五、实验结果总结

1.分析以太网单播帧：

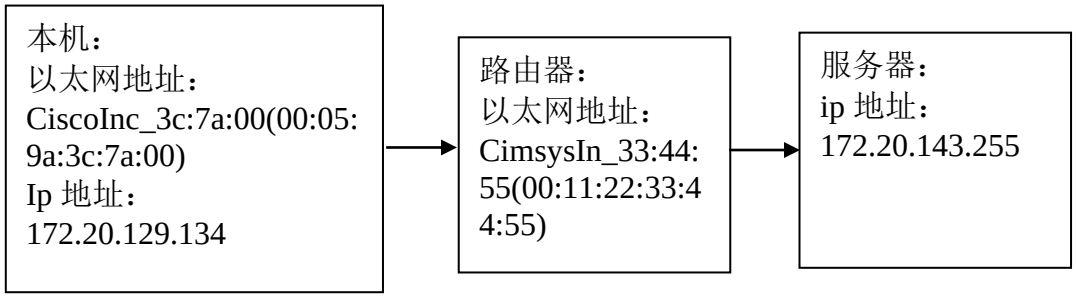


该图是上面抓单播帧包的下半部分，可以看出以太网头部是 6（目的地址）+6（源地址）+2（下一层协议类型）组成，由此可画出 ping 消息的图形：

对于目的地址，这边显示的是 CimsysIn_33:44:55(00:11:22:33:44:55),即本机连上的路由器的以太网地址（该帧是本机对服务器进行请求，而不是 reply）

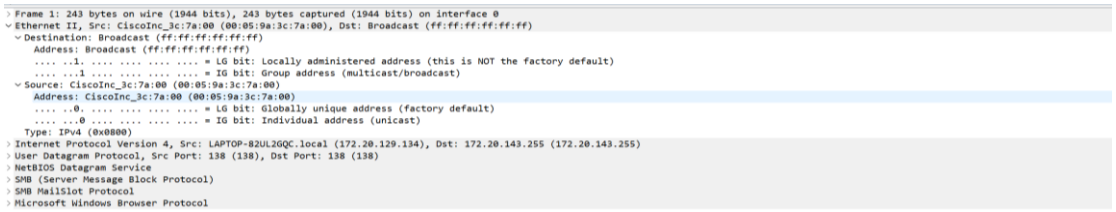
而源地址为 CiscoInc_3c:7a:00(00:05:9a:3c:7a:00),为本机以太网地址

在下面的 ip 协议中记录了源地址的 ip 和目的地址的 ip，可以画出本机，路由器和远程服务器的相对位置：



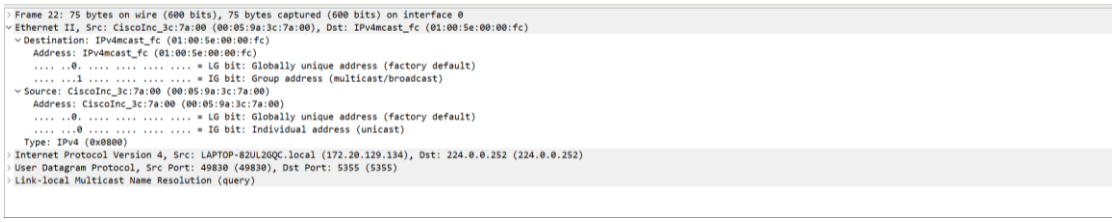
2.分析以太网多播帧：

对于广播帧：



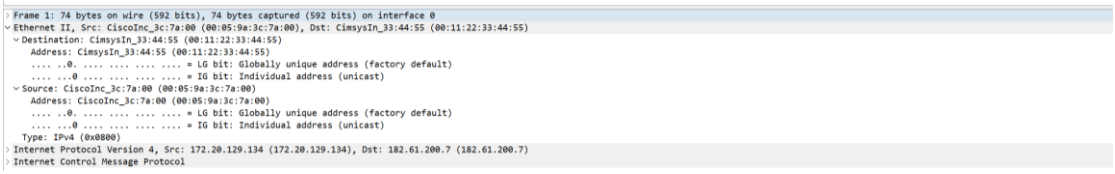
可以看出以太网广播帧的地址以 Wireshark 显示的标准形式写出为 0xff:ff:ff:ff:ff:ff

而对于组播：

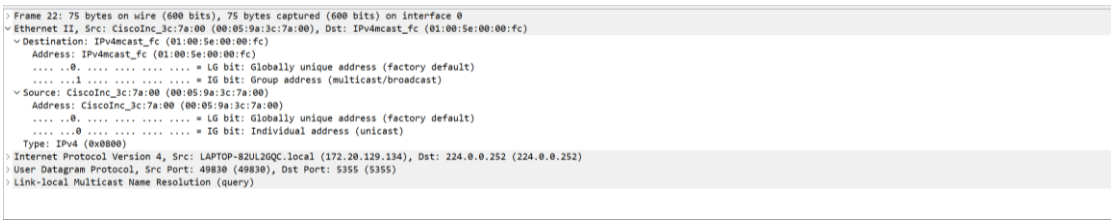


不再是 broadcast 开头，而是以其他形式开头（例如上图的 ipv4mcast），且图中最上面的 1 变成了 0.

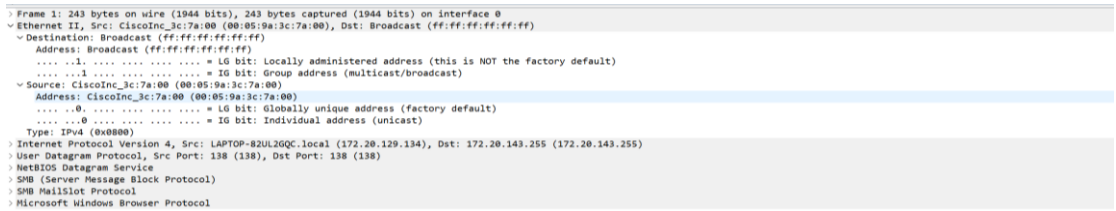
4. 接下来比较单播帧，组播帧和广播帧：



（单播）



（组播）

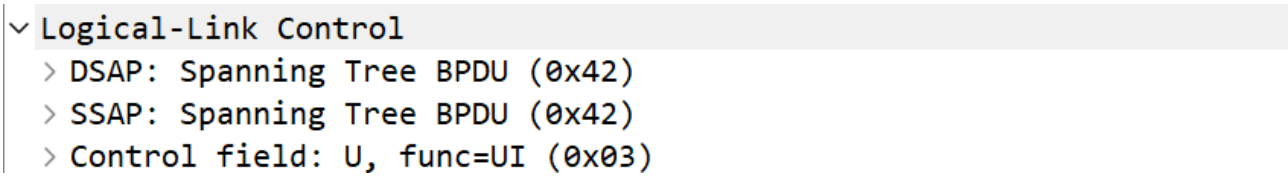


（广播）

可以观察到组播和广播的第一个字节的最后一位为 1，而单播的为 0（即 destination 里面的 IG 位），又由于以太网线路上是以大端法传送字节的，故第 48 位比特位是用来控制单播或者是多播的

5. 思考题部分：

在第四部分中已给出 802.3 的抓包截图：



第一个问题：

1.与 DIX 以太网报头相比，IEEE 802.3 和 LLC 组合报头有多长？

可以看到 IEEE802.3 的头部长度为 14 字节（同样 6+6+2，只不过 2 变为了有效负载的长度），而 llc 的头部为 3 字节（1(DSAP)+1(SSAP)+1(CTRL)）故组合报头为 17 字节

第二个问题：

2. 接收方计算机如何知道该帧是 DIX 以太网还是 IEEE 802.3？

由于二者的区别在于那 14 个字节中的最后两个字节，结合网上查找的资料可知，当 type 字段（IEEE802.3 是 length）值小于等于 1500（0x05DC）时，帧使用的是 IEEE 802.3 格式。当 type 字段值大于等于 1536（0x0600）时，帧使用的是 Ethernet II 格式

第三个问题：

3. 如果 IEEE 802.3 没有类型字段，那么如何确定下一层？

IEEE802.3 没有类型字段，但是多了个 llc 字段，llc 字段中的 DSAP 和 SSAP 标识了源地址和目标地址之间使用的协议，ipv4，stp……等，可以用这部分来确定下一层的协议

六、个人总结

本次实验让我很好地理解了以太网帧的结构（EthernetII 和 IEEE802.3），了解了网络数据的传输是在各个路由器之间接力传输的，只有在网络层的部分才显示了源 ip 地址和目的 ip 地址，而数据链路层的地址只是下一个路由器的地址。除此之外，对 wireshark 的使用也更加熟练。