华东师范大学软件工程学院实验报告

实验课程:	计算机网络	年 级:	2023 级
实验编号:	Lab 02	实验名称:	Ethernet
姓 名:	王海生	学 号:	10235101559

1 实验目的

- 1) 学会通过 Wireshark 获取以太网的帧
- 2) 掌握以太网帧的结构
- 3) 分析以太网地址范围
- 4) 分析以太网的广播帧

2 实验内容与实验步骤

2.1 实验内容

2.1.1 获取以太网的帧

在命令行中使用 ping 命令发起 ICMP 请求,然后使用 Wireshark 捕获以太网数据包。

2.1.2 分析以太网的帧

分析以太网的帧, 画出帧结构。

2.1.3 分析以太网的地址范围

分析以太网的地址范围, 画出图示关系图。

2.1.4 分析以太网的广播帧

启动 Wireshark, 在菜单栏的捕获 \rightarrow 选项中进行设置,选择已连接的以太网,设置捕获过滤器为 ether multicast,捕获以太网的广播帧。

分析以太网的广播帧,回答以下问题:

- 1. 以太网广播帧的地址是什么, 以标准的形式写在 Wireshark 上显示?
- 2. 哪几个比特位的以太网地址是用来确定是单播或多播/广播?

2.1.5 问题讨论

- 1. 与 DIX 以太网报头相比, IEEE 802.3 和 LLC 组合报头有多长?您可以使用 Wireshark 解决此问题。请注意, Trailer / Padding 和 Checksum 可能显示为标头的一部分,但它们位于帧的末尾。
- 2. 接收方计算机如何知道该帧是 DIX 以太网还是 IEEE 802.3? 提示: 您可能需要同时使用 Wireshark 查看数据包示例并查找相关文献。
- 3. 如果 IEEE 802.3 没有类型字段,那么如何确定下一层?使用 Wireshark 查找解复用键。

2.2 实验步骤

- 1) 打开命令行,使用 ping 命令发起 ICMP 请求
 - 1 PS> ping www.baidu.com
- 2) 启动 Wireshark,在菜单栏的捕获 \rightarrow 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 enable MAC name resolution. 然后开始捕获。
- 3) 回到命令行,再次使用 ping 命令发起 ICMP 请求
 - 1 PS> ping www.baidu.com
- 4) 回到 Wireshark, 停止捕获。
- 5) 分析捕获到的以太网的帧, 画出帧结构。
- 6) 分析以太网的地址范围,画出图示关系图。
- 7) 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 ether multicast,捕获以太网的广播帧。
- 8) 问题讨论

3 实验环境

- 操作系统: Windows 11 家庭中文版 23H2 22631.2715
- 网络适配器: Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter(201NGW)
- Wireshark: Version 4.2.0 (v4.2.0-0-g54eedfc63953)
- wget: GNU Wget 1.21.4 built on mingw32

4 实验过程与分析

4.1 获取以太网的帧

首先,我们在命令行中使用 ping 命令发起 ICMP 请求。

```
Lipen ping www.baidu.com

正在 Ping www.a.shifen.com [182.61.200.6] 具有 32 字节的数据:
来自 182.61.200.6 的回复: 字节=32 时间=36ms TTL=45
来自 182.61.200.6 的回复: 字节=32 时间=37ms TTL=45
来自 182.61.200.6 的回复: 字节=32 时间=40ms TTL=45
来自 182.61.200.6 的回复: 字节=32 时间=36ms TTL=45

182.61.200.6 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 = 36ms,最长 = 40ms,平均 = 37ms
```

图 1: 使用 ping 命令发起 ICMP 请求

打开 Wireshark, 在菜单栏的捕获 \rightarrow 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 enable MAC name resolution。然后开始捕获。

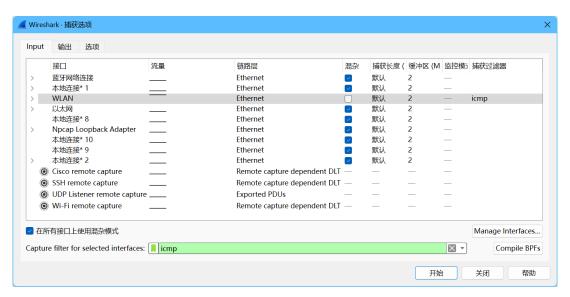


图 2: 设置 Wireshark 捕获过滤器

回到命令行,再次使用 ping 命令发起 ICMP 请求。

```
TER Ping www.a.shifen.com [182.61.200.6] 具有 32 字节的数据: 来自 182.61.200.6 的回复: 字节=32 时间=36ms TTL=45 来自 182.61.200.6 的回复: 字节=32 时间=37ms TTL=45 来自 182.61.200.6 的回复: 字节=32 时间=40ms TTL=45 来自 182.61.200.6 的回复: 字节=32 时间=40ms TTL=45 来自 182.61.200.6 的回复: 字节=32 时间=36ms TTL=45 化氢化 182.61.200.6 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 = 36ms,最长 = 40ms,平均 = 37ms
```

图 3: 再次使用 ping 命令发起 ICMP 请求

回到 Wireshark, 停止捕获。捕获结果如下图所示:

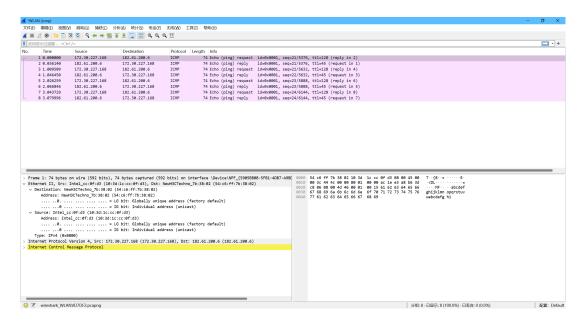


图 4: 捕获结果

4.2 分析以太网的单播帧

问题:基于对以太网帧格式的理解,绘制 ping 消息的图形,该图形以字节为单位显示以太网报头字段的位置和大小。图形可以简单地将框架显示为一个细长的矩形。先出现在包中的是最左边的字段,会先通过网络发送。在此图中,显示以太网报头和以太网负载的范围。最后添加一个虚线框来表示 4 字节校验和。

点击捕获到的数据包,选择 Ethernet II,可以看到以太网的帧结构如下图所示:

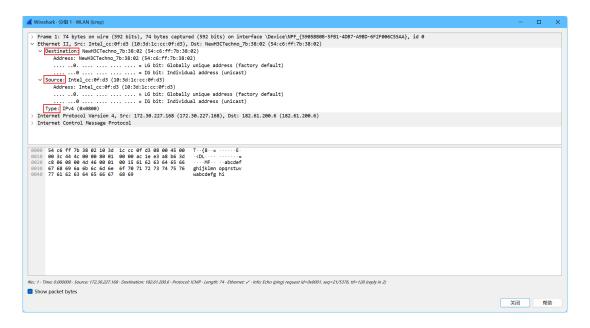
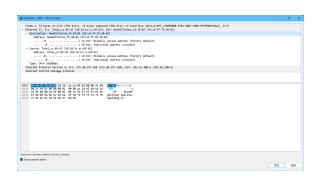


图 5: 以太网的帧结构

可以看到**以太网**头部包括了**目的地址** (Destination)、**源地址** (Source) 和**类型** (Type) 三部分。其中**目的地址**和**源地址**都是 6 个字节,**类型**是 2 个字节。



| Trees 1.1 | Price 1.2 | Pric

图 6: Destination

图 7: Source

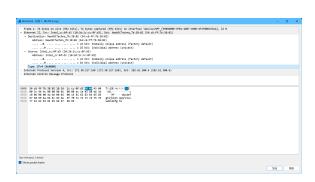


图 8: Type

画出的帧结构如下图所示:

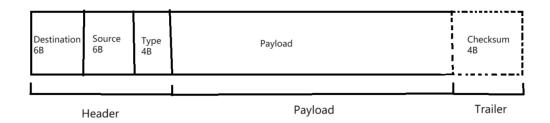


图 9: 以太网帧结构

4.3 分析以太网的地址范围

画一个图,显示你的电脑,路由器和远程服务器的相对位置。标记你的电脑和路由器的以太网地址。标记你的计算机和远程服务器的 IP 地址。

根据上面分析得到的**以太网**帧结构,我们可以得知本机 MAC 地址为 10:3d:1c:cc:0f:d3, IP 地址为 172.30.227.168, 路由器 MAC 地址为 54:c6:ff:7b:38:02,目标 IP 地址为 182.61.200.6。可以作出如下的关系图:

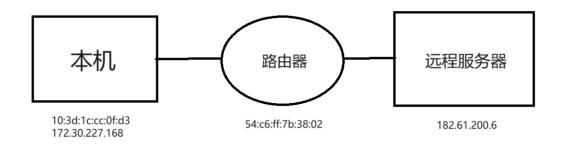


图 10: 以太网地址范围关系图

4.4 分析以太网的广播帧或多播帧

启动 Wireshark,在菜单栏的捕获 \rightarrow 选项中进行设置,选择已连接的以太网,设置捕获过滤器为 ether multicast,捕获以太网的广播帧。

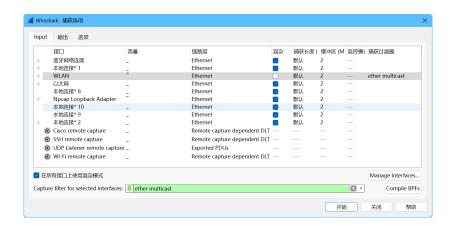


图 11: 设置 Wireshark 捕获过滤器

经过一段时间的捕获,捕获结果如下图所示:

Time	Source	Destination	Protocol	Length Info
1 0.000000	Cisco_e9:68:99	Broadcast	ARP	68 Gratuitous ARP for 0.0.0.0 (Reply)
2 5.026961	Cisco_e9:68:99	Broadcast	ARP	60 Gratuitous ARP for 172.30.128.1 (Reply)
3 5.329761	Cisco_e9:68:99	Broadcast	ARP	60 Gratuitous ARP for 172.30.128.1 (Reply)
4 5.631201	Cisco_e9:68:99	Broadcast	ARP	60 Gratuitous ARP for 172.30.128.1 (Reply)
5 5.735953	Cisco_e9:68:99	Broadcast	ARP	60 Gratuitous ARP for 172.30.128.1 (Reply)
6 6.255819	Cisco_e9:68:99	Broadcast	ARP	60 Gratuitous ARP for 172.30.128.1 (Reply)
7 6.665467	Cisco_e9:68:99	Broadcast	ARP	60 Gratuitous ARP for 172.30.128.1 (Reply)
8 20.070377	Cisco_e9:68:99	Broadcast	ARP	60 Gratuitous ARP for 172.30.128.1 (Reply)
9 20.889189	Cisco_e9:68:99	Broadcast	ARP	60 Gratuitous ARP for 172.30.128.1 (Reply)
10 36.551700	PC.local	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
11 37.561694	PC.local	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
12 38.561972	PC.local	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
13 39.563784	PC.local	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
14 48.844017	Cisco_e9:68:99	Broadcast	ARP	60 Gratuitous ARP for 172.30.128.1 (Reply)
15 49.980657	Cisco_e9:68:99	Broadcast	ARP	60 Gratuitous ARP for 0.0.0.0 (Request)
16 50.073119	Cisco_e9:68:99	Broadcast	ARP	60 Gratuitous ARP for 0.0.0.0 (Reply)
17 50.645886	PC.local	mdns.mcast.net	MDNS	90 Standard query 0x0000 PTR _microsoft_mcctcp.local, "QU" question
18 50.646705	PC.local	ff02::fb	MDNS	110 Standard query 0x0000 PTR _microsoft_mcctcp.local, "QU" question
19 51.638095	PC.local	mdns.mcast.net	MDNS	90 Standard query 0x0000 PTR _microsoft_mcctcp.local, "QM" question
28 51 638924	PC local	ffarfh	MONS	118 Standard quary AVARAR PTR microsoft mcc top local "OM" question

图 12: 捕获结果

选择其中的一个广播帧数据包,如下图所示:

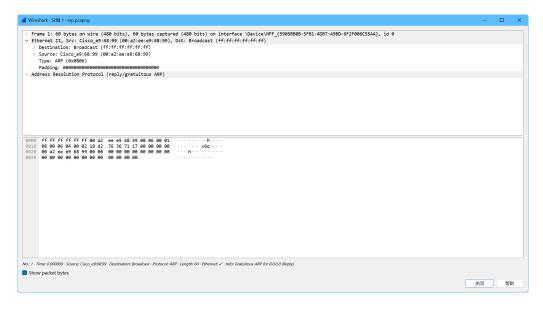


图 13: 广播帧数据包

问题:

1. 以太网广播帧的地址是什么,以标准的形式写在 Wireshark 上显示? 可以看出,广播帧的地址为 ff:ff:ff:ff:ff:

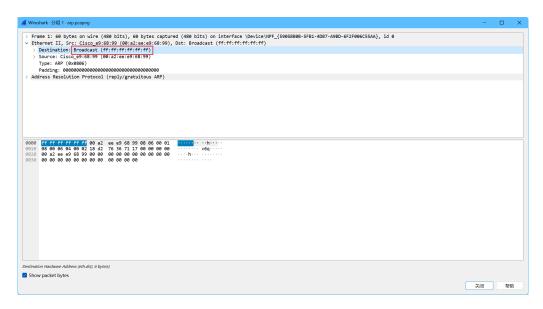
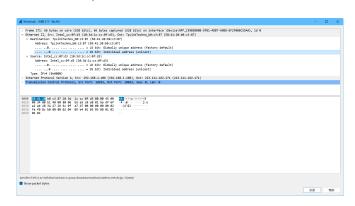


图 14: 广播帧地址

2. 哪几个比特位的以太网地址是用来确定是单播或多播/广播?

对比单播帧和广播帧,可以看出,**以太网**地址的第一个字节的最后一位(即第八位)为 **1**,所以可以确定是多播/广播。



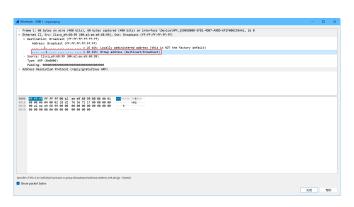


图 15: 单播帧

图 16: 广播帧

4.5 问题讨论

设置捕获过滤器为 11c,捕获以太网的帧,如下图所示:

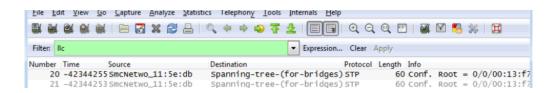


图 17: 捕获 IEEE 802.3 以太网的帧

1. 与 DIX 以太网报头相比, IEEE 802.3 和 LLC 组合报头有多长?您可以使用 Wireshark 解决此问题。请注意, Trailer / Padding 和 Checksum 可能显示为标头的一部分, 但它们位于帧的末尾。

答: DIX 以太网头部长度为 **14** 字节, IEEE 802.3 头部长度为 **14** 字节, LLC 头部长度为 **3** 字节。如下图所示:

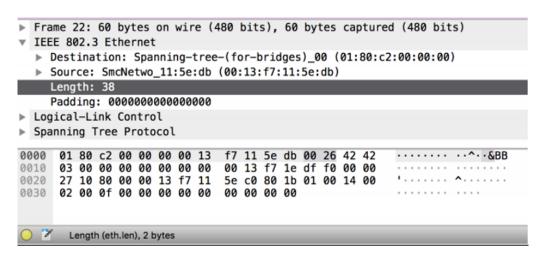


图 18: IEEE 802.3 以太网头部

2. 接收方计算机如何知道该帧是 DIX 以太网还是 IEEE 802.3? 提示: 您可能需要同时使用 Wireshark 查看数据包示例并查找相关文献。

答:根据 Type/Length 字段,如果该字段的值小于或等于 1500,则表示 Length,为 IEEE 802.3,否则表示 Type,为 DIX 以太网。

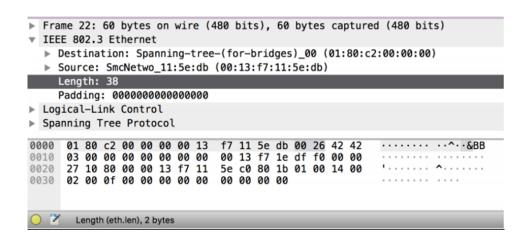


图 19: Length 字段

3. 如果 IEEE 802.3 没有类型字段,那么如何确定下一层?使用 Wireshark 查找解复用键。 答: LLC 头中的 DSAP 字段可以指示上层协议。例如,此处 DSAP 字段为 Øx42,则表示上层协议为 STP。

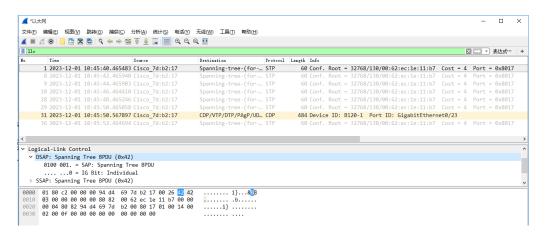


图 20: DSAP 字段

5 实验结果总结

通过本次实验,我学会了通过 Wireshark 获取以太网的帧,掌握了以太网帧的结构,分析了以太网地址范围,分析了以太网的广播帧。同时,我还了解到了 DIX 以太网和 IEEE 802.3 以太网的区别。

6 附录

无