

中山大學

SUN YAT-SEN UNIVERSITY



课程名称：计算机网络

实验名称：网络抓包与协议分析

姓 名：周德峰

学 号：21312210

专 业：智能科学与技术

WireShark使用

1 概念介绍

ICMP: Internet Control Message Protocol（因特网控制消息协议），它是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息

Ping: (Packet Internet Groper):因特网包探索器，用于测试网络连接量的程序。Ping发送一个ICMP；回声请求消息给目的地并报告是否收到所希望的ICMP echo（ICMP回声应答）。它是用来检查网络是否通畅或者网络连接速度的命令

RTT: 往返时间。

TTL: 表示IP数据报在网络中的寿命，其单位为秒。在目前的实际应用中，常以“跳”为单位。该字段指定IP包被路由器丢弃之前允许通过的最大网段数量

2 界面

打开WireShark界面，在命令行进行ping抓包，并在过滤区进行筛选，即可得到对应的数据包

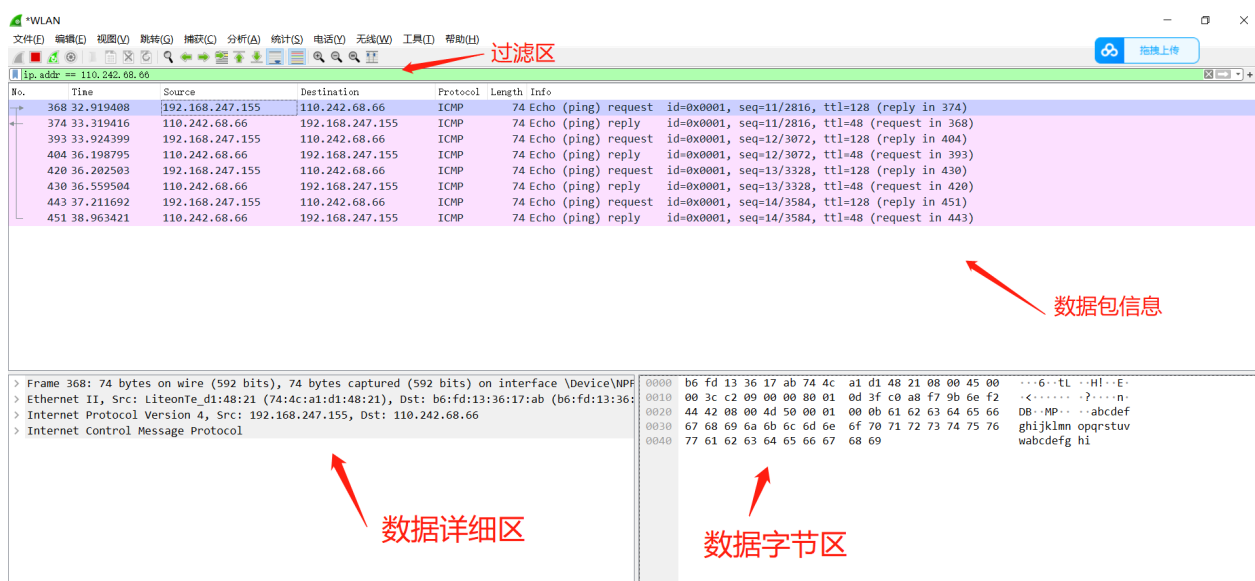


图 1 抓包界面介绍

3 数据包信息

数据详细区由以下部分组成

1. **Frame:** 物理层的以太网帧概况
2. **Ethernet II:** 数据链路层以太网帧头部信息
3. **Internet Protocol Version 4:** 互联网层IP包头部信息

4. Internet Control Message Protocol: 传输层T的数据段头部信息，此处是TCP

4 过滤器设置

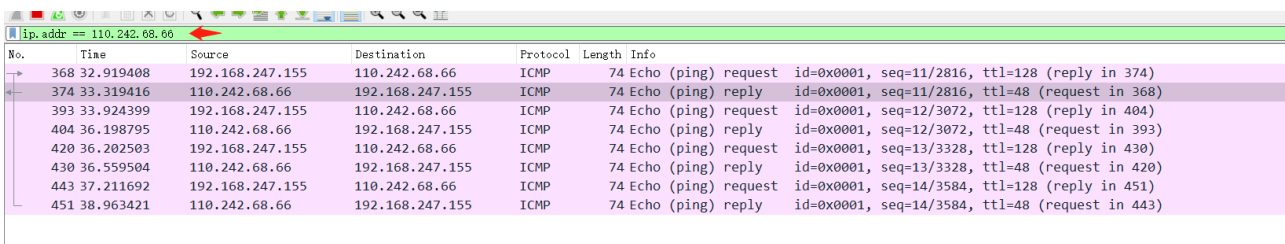
抓包过滤器包括 过滤类型Type (host、net、port)、方向Dir (src、dst)、协议Proto (ether、ip、tcp、udp、http、icmp、ftp等)、逻辑运算符 (&& 与、|| 或、! 非)

1. 协议过滤

在抓包过滤框中直接输入协议名即可只显示某协议的数据包列表

2. ip过滤

- 1 | `ip.src == 192.168.1.104` 显示源地址为192.168.1.104的数据包列表
- 2 | `ip.dst == 192.168.1.104`, 显示目标地址为192.168.1.104的数据包列表
- 3 | `ip.addr == 192.168.1.104` 显示源IP地址或目标IP地址为192.168.1.104的数据包列表



No.	Time	Source	Destination	Protocol	Length	Info
368	32.919408	192.168.247.155	110.242.68.66	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 374)
374	33.319416	110.242.68.66	192.168.247.155	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=48 (request in 368)
393	33.924399	192.168.247.155	110.242.68.66	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 404)
404	36.198795	110.242.68.66	192.168.247.155	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=48 (request in 393)
420	36.202503	192.168.247.155	110.242.68.66	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 430)
430	36.559504	110.242.68.66	192.168.247.155	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=48 (request in 420)
443	37.211692	192.168.247.155	110.242.68.66	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 451)
451	38.963421	110.242.68.66	192.168.247.155	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=48 (request in 443)

3. 端口过滤

- 1 | `port 80`
- 2 | `src port 80`
- 3 | `dst port 80`

4. 逻辑运算符&& 与、|| 或、! 非

- 1 | `src host 192.168.1.104 && dst port 80` 抓取主机地址为192.168.1.80、目的端口为80的数据包
- 2 | `host 192.168.1.104 || host 192.168.1.102` 抓取主机为192.168.1.104或者192.168.1.102的数据包
- 3 | `! broadcast` 不抓取广播数据包

以太网帧格式分析

1 概念

MAC地址 (Media Access Control Address)：局域网地址，以太网地址或者物理地址，与ip地址不同，MAC地址只与硬件设备有关，全球唯一

MAC地址用于在网络中唯一标示一个网卡，一台设备若有一或多个网卡，则每个网卡都需要并会有一个唯一的MAC地址。MAC地址共48位 (6个字节)，通常表示为 12 个 16 进制数，如：00-16-EA-AE-3C-40。



前24位（3个字节）代表网络硬件制造商的编号，即**组织唯一标志符 (OUI)**，由IEEE（电气和电子工程师协会）决定如何分配，后24位由实际生产该网络设备的厂商自行制定，代表该制造商所生产的某个网络产品（如网卡）的**系列号**，例广播地址：FF:FF:FF:FF:FF:FF

I/G (Individual/Group) 位，如果I/G=0，则是某台设备的MAC地址，即单播地址；如果I/G=1，则是多播地址（组播+广播=多播）。

G/L (Global/Local, 也称为U/L位, 其中U表示Universal) 位，如果G/L=0，则是全局管理地址，由IEEE分配；如果G/L=1，则是本地管理地址，是网络管理员为了加强自己对网络管理而指定的地址。

在cmd中输出 `ipconfig/all` 即可看到

1.1 本地/以太网连接

本地连接和以太网所代表的含义相同，仅为表述不同

“本地连接”只出现于Windows7或XP系统中，在Windows8和10系统，被更名为“以太网”

```
以太网适配器 以太网:

媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :
描述. . . . . : Realtek PCIe GbE Family Controller
物理地址. . . . . : 38-F3-AB-E7-44-14
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
```

可以看出，媒体断开连接，即没有配置对应的网卡

网卡：作为TCP/IP层的接口，可以在物理层传输信号，在网络层传输数据包。无论位于哪个层，它都充当计算机或服务器和数据网络之间的中间媒介。当用户发送一个web页面请求时，网卡从用户设备中获取数据，并将其发送到网络服务器，然后接收所需的数据展示给用户。

1.2 WLAN连接

Ping默认网关

网关：网关（Gateway）是一个网络中连接两个不同网络的设备或程序，它能够实现两个不同的网络之间的通信。网关一般位于网络边缘，是网络中的重要组成部分，用于连接两个或多个网络并进行数据传输。网关的作用是将来自本地网络的数据包转发到其他网络，并将来自其他网络的数据包转发到本地网络。

在计算机网络中，网关一般指路由器。当计算机需要访问 Internet 或其他网络时，它首先需要将数据包发送给本地网关，由网关将数据包转发到 Internet 或其他网络中的目标主机。网关不仅仅是一个传输数据的设备，它还可以对数据进行一些处理，例如对数据进行过滤、转换、加密等操作，以实现更高级的网络功能，如安全性控制、负载均衡、流量控制等。

除了路由器之外，网关还可以是一些其他设备或程序，例如代理服务器、防火墙等，它们也可以实现连接两个或多个网络的功能。在企业网络中，网关通常是一个专门的设备或服务，由网络管理员进行管理和配置，以保证网络的安全性和稳定性。

IP：网络地址+主机地址

子网掩码：用于区分网络地址与主机地址的标准

	10进制	2进制	
IP地址	192 . 168 . 1 . 1	11000000 . 10101000.00000001	00000001
子网掩码	255 . 255 . 255 . 0	11111111 . 11111111.11111111	00000000
		网络地址	主机地址

网络地址：IP 地址中被 连续的1 遮住的部分，即 11000000.10101000.00000001.00000000, 对应的网络地址：192.168.1.0

主机地址：IP 地址中被 连续的0 遮住的部分，即 00000000.00000000.00000000.00000001, 对应的网络地址：0.0.0.1

可以看到，由于是WLAN连接，所以对应以太网帧显示的mac地址为WLAN的mac地址

```
C:\Windows\system32\cmd.exe
自动配置已启用. . . . . : 是

无线局域网适配器 WLAN:

连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
物理地址. . . . . : 74-4C-A1-D1-48-21
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
本地链接 IPv6 地址. . . . . : fe80::ec88:f0df:e77c:c9cf%13(首选)
IPv4 地址 . . . . . : 192.168.124.6(首选)
子网掩码 . . . . . : 255.255.255.0
获得租约的时间 . . . . . : 2023年5月13日 14:23:09
租约过期的时间 . . . . . : 2023年5月14日 14:23:08
默认网关 . . . . . : 192.168.124.1
DHCP 服务器 . . . . . : 192.168.124.1
DHCPv6 IAID . . . . . : 208948385
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-28-6C-58-33-38-F3-AB-E7-44-14
DNS 服务器 . . . . . : 192.168.124.1
TCP/IP 上的 NetBIOS . . . . . : 已启用

以太网适配器 蓝牙网络连接:

媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Bluetooth Device (Personal Area Network)
物理地址. . . . . : 74-4C-A1-D1-48-22
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
```

1.3 ICMP

是互联网协议族的核心协议之一。它用于网际协议（IP）中发送控制消息，提供可能发生在通信环境中的各种问题反馈。通过这些信息，使管理者可以对所发生的问题作出诊断，然后采取适当的措施解决。ICMP 依靠 IP 来完成它的任务，它是 IP 的主要部分。它与传输协议（如 TCP 和 UDP）显著不同：它一般不用于在两点间传输数据。它通常不由网络程序直接使用，除了 ping 和 traceroute 这两个特别的例子。IPv4 中的 ICMP 被称作 ICMPv4，IPv6 中的 ICMP 则被称作 ICMPv6。

1.4 Ping

ping 是 ICMP 最著名的一个应用，通过 ping 可以测试网络的可达性，即网络上的报文能否成功到达目的地。使用 ping 命令时，源设备向目的设备发送 Echo request 消息，目的地址是目的设备的 IP 地址。目的设备收到 Echo request 消息后，向源设备回应一个 Echo reply 消息，可知目的设备是可达的。

✓ Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x4579 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 2018 (0x07e2)
 Sequence Number (LE): 57863 (0xe207)
[\[Response frame: 14\]](#)

图 14 request

✓ Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0x4d79 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 2018 (0x07e2)
 Sequence Number (LE): 57863 (0xe207)
[\[Request frame: 13\]](#)
 [Response time: 16.379 ms]

图 15 reply

2 Ping网关及以太帧分析

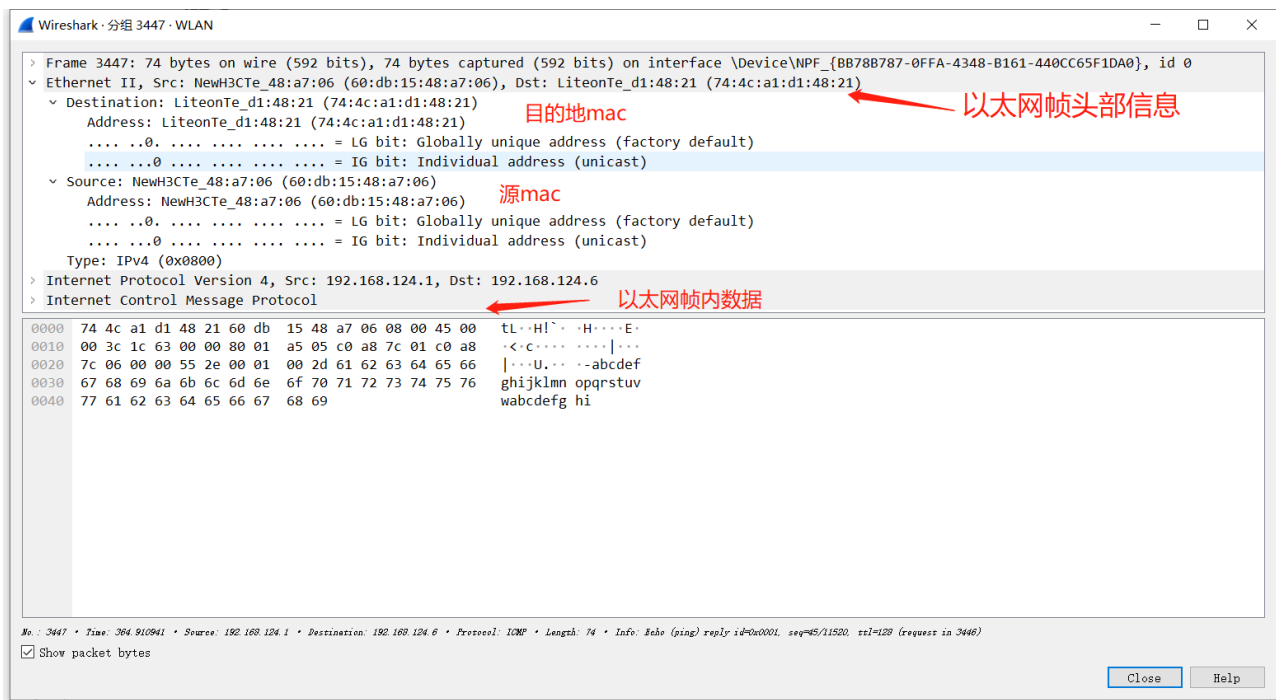
ping网关.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(H)

icmp 00ip.addr == 192.168.124.1

每包数据的信息

No.	Time	Source	Destination	Protocol	Length	Info
3446	364.908343	192.168.124.6	192.168.124.1	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 3447)
3447	364.910941	192.168.124.1	192.168.124.6	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=128 (request in 3446)
3454	365.911265	192.168.124.6	192.168.124.1	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 3455)
3455	365.924016	192.168.124.1	192.168.124.6	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=128 (request in 3454)
3458	366.914254	192.168.124.6	192.168.124.1	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (reply in 3459)
3459	366.915489	192.168.124.1	192.168.124.6	ICMP	74	Echo (ping) reply id=0x0001, seq=47/12032, ttl=128 (request in 3458)
3468	367.917267	192.168.124.6	192.168.124.1	ICMP	74	Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (reply in 3470)
3470	367.918525	192.168.124.1	192.168.124.6	ICMP	74	Echo (ping) reply id=0x0001, seq=48/12288, ttl=128 (request in 3468)



Type: IPV4 (0x0800) , 说明数据包为IPV4类型

可以看到, I/G位 (图中为IG bit) 和L/G位 (图中为LG bit) 均为0

通过MAC地址查询可以获取路由器的具体信息

MAC地址 74-4C-A1-D1-48-21

查询MAC地址

MAC地址 74-4C-A1-D1-48-21

组织唯一标识符 74-4C-A1

登记类型 MA-L

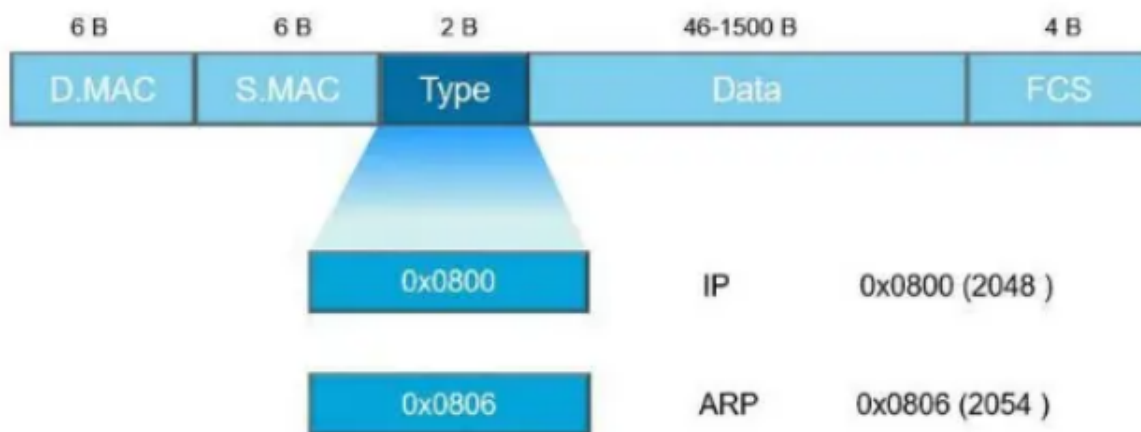
地区 台湾 (中国) TW

制造商 Liteon Technology Corporation

地址 4F,90,Chien 1 Road,ChungHo,Taipei Hsien,Taiwan,
TaiPei TaiWan 23585

I/G位 单播 组播

U/L位 全局唯一 本地管理



前导字符	目的MAC地址	源MAC地址
8字节	6字节	6字节
类型	IP数据报	帧检验
2字节	46-1500字节	4字节

接下来对 Ethernet II 进行分析，在以太网链路 上的数据包称作以太帧。以太帧起始部分由前导 码和帧开始符组成。后面紧跟着一个以太网报头， 以 MAC 地址说明目的地址和源地址。帧的中部是 该帧负载的包含其他协议报头的数据包 (例如 IP 协议)。以太帧由一个 32 位冗余校验码结尾。它用于检验数 据传输是否出现损坏。

除了前面提到的 mac 地址外，一个 0x0800 的 以太类型说明这个帧包含的是 IPv4 数据报。同样 的，一个 0x0806 的以太类型说明这个帧是一个 ARP 帧，0x8100 说明这是一个 IEEE 802.1Q 帧，而 0x86DD 说明这是一个 IPv6 帧。

由表1可知，以太网数据帧的长度在 64-1518 字节之间。数据部分在 46-1500 字节之间。数据包 在 以太网物理介质上传播之前必须封装头部和尾 部信息。封装后的数据包称为数据帧，数据帧的封 装的信息决定了数据如何传输。

3 Ping其他主机

对应主机信息：

无线局域网适配器 WLAN:

连接特定的 DNS 后缀 :
描述 : Intel(R) Wi-Fi 6 AX201 160MHz
物理地址. : A4-42-3B-04-18-48
DHCP 已启用 : 是
自动配置已启用 : 是
本地链接 IPv6 地址 : fe80::645f:8f70:9f54:7b83%3(首选)
IPv4 地址 : 192.168.124.28(首选)
子网掩码 : 255.255.255.0
获得租约的时间 : 2023年5月13日 18:11:49
租约过期的时间 : 2023年5月14日 18:11:48
默认网关 : 192.168.124.1
DHCP 服务器 : 192.168.124.1
DHCPv6 IAID : 61096507
DHCPv6 客户端 DUID : 00-01-00-01-2A-B4-D3-3F-A4-42-3B-04-18-48
DNS 服务器 : 192.168.124.1
TCP/IP 上的 NetBIOS : 已启用

命令行中ping得到的报文

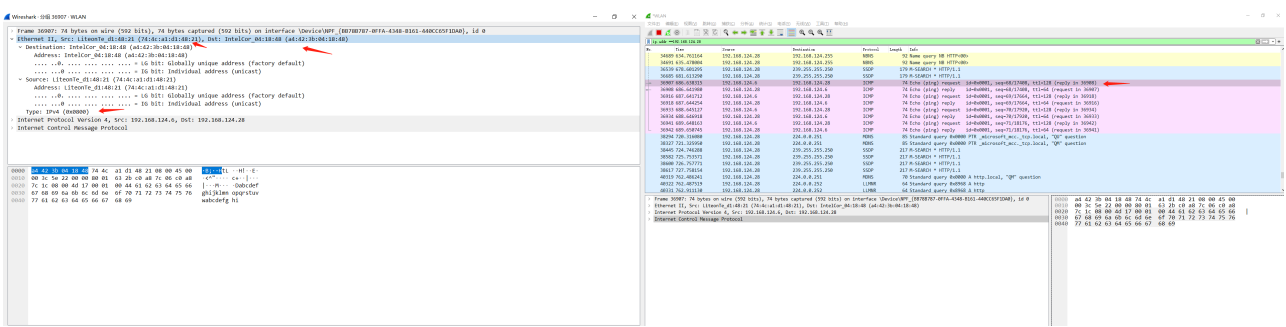
```
C:\Users\lenovo>ping 192.168.124.28

正在 Ping 192.168.124.28 具有 32 字节的数据:
来自 192.168.124.28 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.124.28 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.124.28 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.124.28 的回复: 字节=32 时间=2ms TTL=64

192.168.124.28 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 = 1ms, 最长 = 3ms, 平均 = 2ms

C:\Users\lenovo>
```

对应Wireshark中的数据分析，可以看到对应的Dst MAC和Sur



ARP数据包分析

1 概念

ARP (Address Resolution Protocol)，即地址解析协议，是根据IP地址获取物理地址的一个TCP/IP协议。主机发送信息时将包含目标IP地址的ARP请求广播（broadcast）到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址；收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间，下次请求时直接查询ARP缓存以节约资源。地址解析协议是建立在网络中各个主机互相信任

的基础上的，局域网络上的主机可以自主发送ARP应答消息，其他主机收到应答报文时不会检测该报文的真实性就会将其记入本机ARP缓存；

2 ARP缓存表

ARP缓存（ARP Cache），用来存放IP地址和MAC地址的关联信息。如果缓存表中存在对方设备的MAC地址，则直接采用该MAC地址来封装帧，然后将帧发送出去。如果缓存表中不存在相应的信息，则通过发送ARP request报文来获得它。学习到的IP地址和MAC地址的映射关系会被放入ARP缓存表中存放一段时间。在有效期内，设备可以直接从这个表中查找目的MAC地址来进行数据封装，而无需进行ARP查询。过了这段有效期，ARP表项会被自动删除。如果目标设备位于其他网络则源设备会在ARP缓存表中查找网关的MAC地址，然后将数据发送给网关，网关再把数据转发给目的设备。

ARP表项又分为动态ARP表项和静态ARP表项。

2.1 动态ARP表项

动态ARP表项由ARP协议通过ARP报文自动生成和维护，可以被老化，可以被新的ARP报文更新，可以被静态ARP表项覆盖。每个动态ARP缓存项的潜在生命周期是10分钟。新加到缓存中的项目带有时间戳，如果某个项目添加后2分钟内没有再使用，则此项目过期并从ARP缓存中删除；如果某个项目已在使用，则又收到2分钟的生命周期；如果某个项目始终在使用，则会另外收到2分钟的生命周期，一直到10分钟的最长生命周期。

2.2 静态ARP表项

静态ARP表项通过手工配置和维护，不会被老化，不会被动态ARP表项覆盖。直到重新启动计算机为止。

配置静态ARP表项可以增加通信的安全性。静态ARP表项可以限制和指定IP地址的设备通信时只使用指定的MAC地址，此时攻击报文无法修改此表项的IP地址和MAC地址的映射关系，从而保护了本设备和指定设备间的正常通信。

静态ARP表项分为短静态ARP表项和长静态ARP表项。

- 在配置长静态ARP表项时，除了配置IP地址和MAC地址项外，还必须配置该ARP表项所在VLAN和出接口。长静态ARP表项可以直接用于报文转发。
- 在配置短静态ARP表项时，只需要配置IP地址和MAC地址项。如果出接口是三层以太网接口，短静态ARP表项可以直接用于报文转发；如果出接口是VLAN虚接口，短静态ARP表项不能直接用于报文转发，当要发送IP数据包时，先发送ARP请求报文，如果收到的响应报文中的源IP地址和源MAC地址与所配置的IP地址和MAC地址相同，则将接收ARP响应报文的接口加入该静态ARP表项中，之后就可以用于IP数据包的转发。

一般情况下，ARP动态执行并自动寻求IP地址到以太网MAC地址的解析，无需管理员的介入。

当希望设备和指定用户只能使用某个固定的IP地址和MAC地址通信时，可以配置短静态ARP表项，当进一步希望限定这个用户只在某VLAN内的某个特定接口上连接时就可以配置长静态ARP表项。

3 工作过程

假设主机A和B在**同一个网段（子网）**，主机A要向主机B发送信息，具体的地址解析过程如下：

1. 主机A首先查看自己的**ARP缓存表**，确定其中是否包含有主机B对应的**ARP表项**。如果找到了对应的MAC地址，则主机A直接利用ARP表中的MAC地址，对IP数据包进行帧封装，并将数据包发送给主机B。
2. 如果主机A在ARP表中找不到对应的MAC地址，则将缓存该数据报文，然后以广播方式**发送一个ARP请求报文**。ARP请求报文中的发送端IP地址和发送端MAC地址为主机A的IP地址和MAC地址，目标IP地址和目标MAC地址为主机B的IP地址和**全0的MAC地址**。由于ARP请求报文以广播方式发送，**该网段上的所有主机**都可以接收到该请求，但只有被请求的主机（即主机B）会对该请求进行处理。
3. 主机B比较自己的IP地址和ARP请求报文中的目标IP地址，当两者相同时进行如下处理：将ARP请求报文中的发送端（即主机A）的IP地址和MAC地址**存入自己的ARP表中**。之后以**单播方式**发送ARP响应报文给主机A，其中包含了自己的**MAC地址**。
4. 主机A收到ARP响应报文后，将主机B的MAC地址加入到自己的ARP表中以用于后续报文的转发，同时将IP数据包进行封装后发送出去。

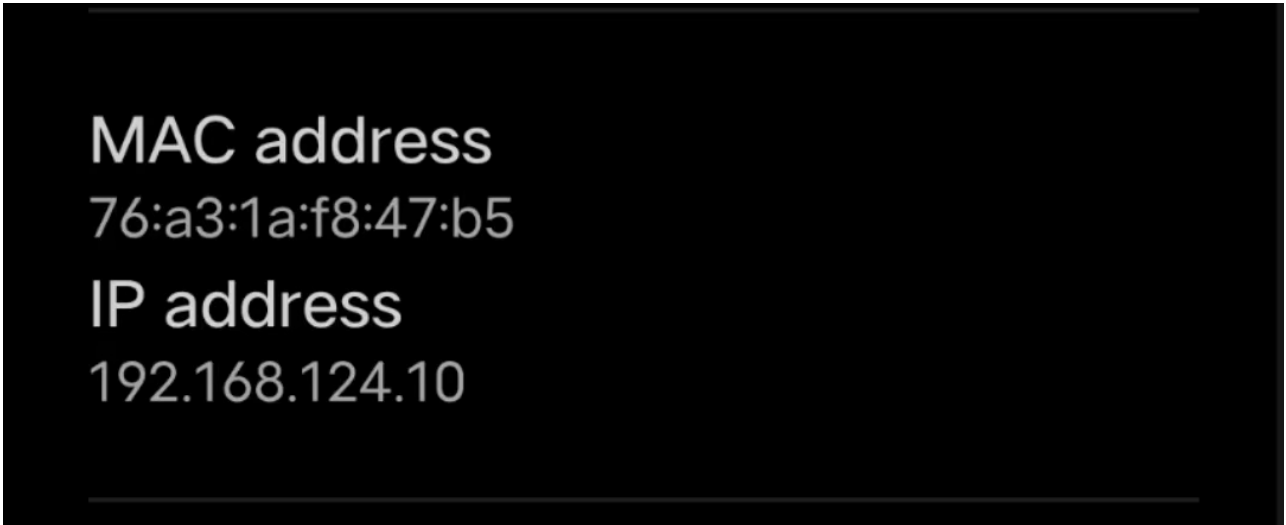
当主机A和主机B**不在同一网段**时，主机A就会先向**网关**发出ARP请求，ARP请求报文中的目标IP地址为**网关的IP地址**。当主机A从收到的响应报文中获得网关的MAC地址后，将报文封装并发给网关。如果网关没有主机B的ARP表项，**网关会广播ARP请求**，目标IP地址为主机B的IP地址，当网关从收到的响应报文中获得主机B的MAC地址后，就可以将报文发给主机B；如果网关已经有主机B的ARP表项，**网关直接把报文发给主机B**。

4 实验

先以管理员身份进入命令行窗口，`arp-d`清除arp缓存，然后打开wireshark，进行Ping命令

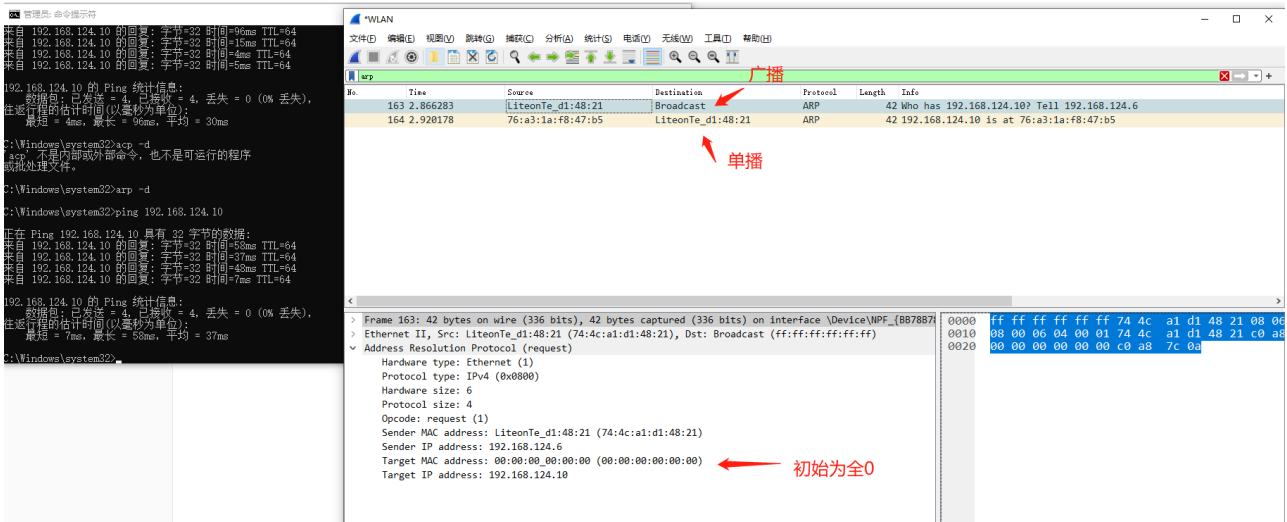
4.1 ping 同一网段

这里ping一下自己的手机，打开手机里的WiFi，然后打开advance settings，里面有对应的 `ip address` 和 `MAC address`



```
MAC address
76:a3:1a:f8:47:b5
IP address
192.168.124.10
```

在清除缓存后进行报文抓取工作

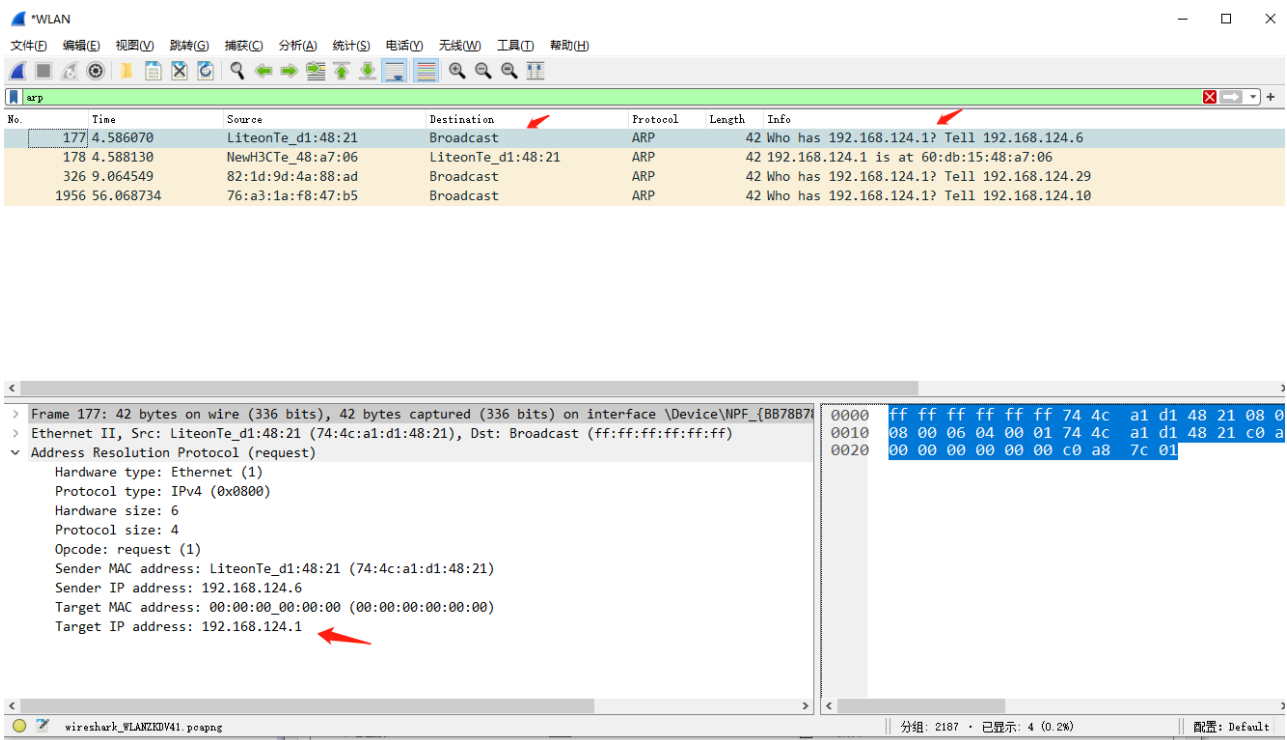


可以发现，如上理论一样，**Target MAC address**为0，最开始先广播，在广播找到后，由目标地址对主机单播，并告知其MAS

我们观察第二个报文，可以看到其地址为**76:a3:1a:f8:47:b5**，与手机上MAS一致

4.2 ping不同网段

按照上述理论，在清除本机的arp cache后，进行ping请求，本机的arp请求的目的ip是网关的ip，对报文分析，结果一致



按照理论，如果网关中的**ARP Cache**中存储着对应网段的MAC，则数据将由网关直接发出到对应目的的主机，而本机则无法捕捉对应目的主机的MAS

从报文结果也可以看出，在本机与网关进行arp请求和回应后，并没有相关更多的请求了，验证了这一点

```
C:\Windows\system32>ping 185.199.108.153

正在 Ping 185.199.108.153 具有 32 字节的数据:
来自 185.199.108.153 的回复: 字节=32 时间=209ms TTL=39
来自 185.199.108.153 的回复: 字节=32 时间=208ms TTL=39
来自 185.199.108.153 的回复: 字节=32 时间=215ms TTL=39
来自 185.199.108.153 的回复: 字节=32 时间=218ms TTL=39

185.199.108.153 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 = 208ms, 最长 = 218ms, 平均 = 212ms

C:\Windows\system32>arp -a

接口: 192.168.124.6 --- 0xd
Internet 地址          物理地址              类型
192.168.124.1          60-db-15-48-a7-06     动态
224.0.0.22             01-00-5e-00-00-16     静态
224.0.0.251            01-00-5e-00-00-fb     静态
224.0.0.252            01-00-5e-00-00-fc     静态
239.255.255.250        01-00-5e-7f-ff-fa     静态

C:\Windows\system32>
```

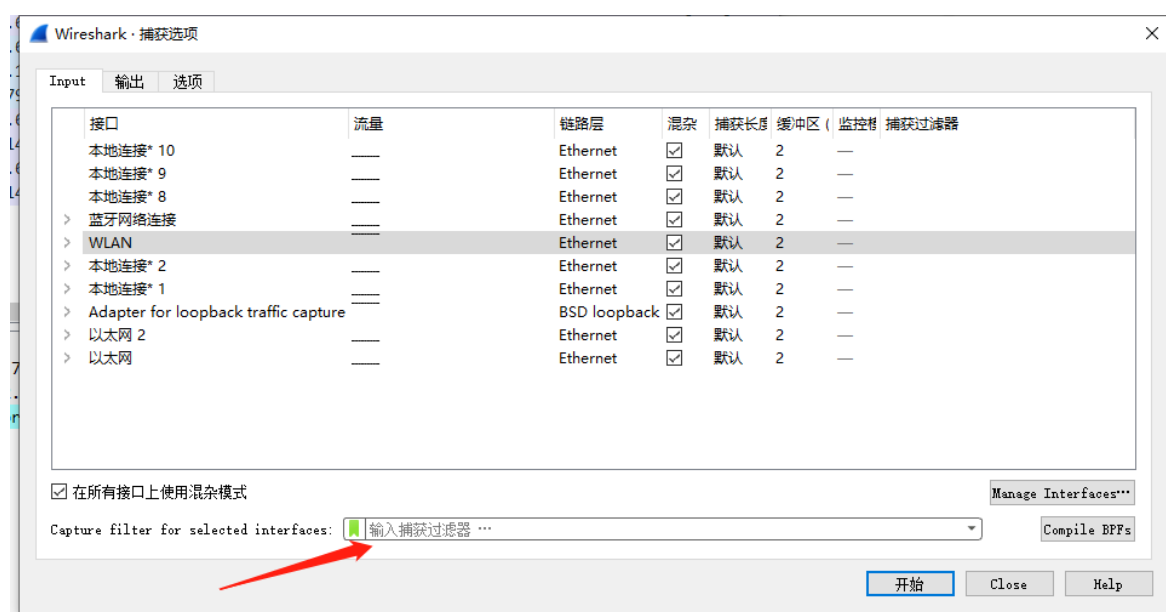
可以利用 `arp -a` 来查看当前本机的ARP Cache，可以看出，也没有保存对应网段的MAS

思考题

1. 使用了了显示过滤器后，Wireshark 的抓包工作量会减少吗？

不会减少，过滤只是查找只显示的信息，不会减少任何抓包工作量。

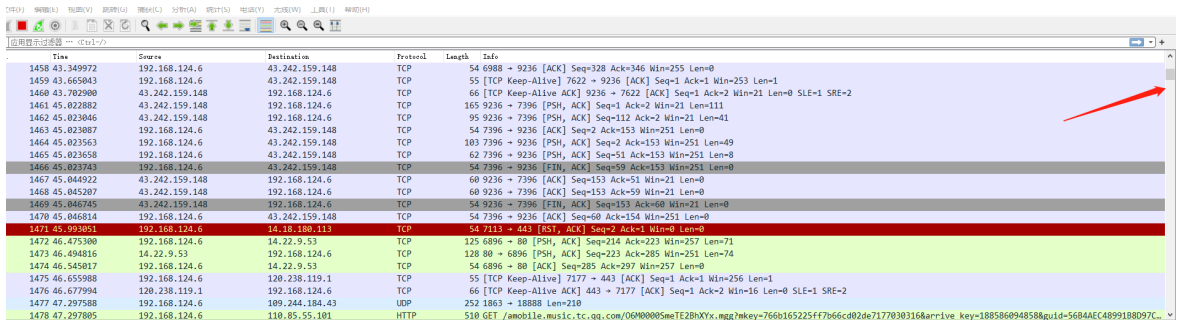
但捕抓过滤会减少，对确定的捕抓类型抓包。



捕获过滤器的语法格式为：

1 <Protocol> <Direction> <Host> <Value> <Logical Operation> <other expression>

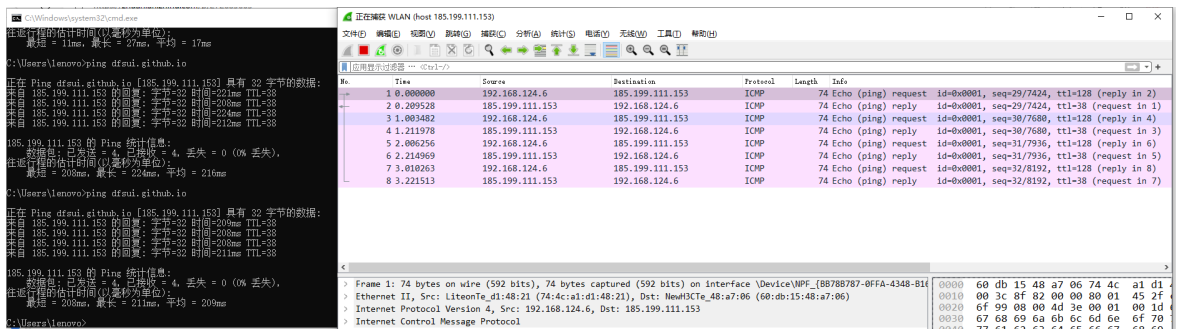
以下为显示过滤器，可以看出只是筛选出对应条件的分组，但其余抓包还在进行



No.	Time	Source	Destination	Protocol	Length	Info
1458	43.349972	192.168.124.6	43.242.159.148	TCP	54	6988 → 9236 [ACK] Seq=328 Ack=346 Win=255 Len=0
1459	43.665043	192.168.124.6	43.242.159.148	TCP	55	[TCP Keep-Alive] 7622 → 9236 [ACK] Seq=1 Ack=1 Win=253 Len=1
1460	43.702980	43.242.159.148	192.168.124.6	TCP	66	[TCP Keep-Alive ACK] 9236 → 7622 [ACK] Seq=1 Ack=2 Win=21 Len=0 SLE=1 SRE=2
1461	45.022882	43.242.159.148	192.168.124.6	TCP	165	9236 → 7396 [PSH, ACK] Seq=1 Ack=2 Win=21 Len=111
1462	45.023046	43.242.159.148	192.168.124.6	TCP	95	9236 → 7396 [PSH, ACK] Seq=112 Ack=2 Win=21 Len=41
1463	45.023087	192.168.124.6	43.242.159.148	TCP	54	7396 → 9236 [ACK] Seq=2 Ack=153 Win=251 Len=0
1464	45.023563	192.168.124.6	43.242.159.148	TCP	183	7396 → 9236 [PSH, ACK] Seq=2 Ack=153 Win=251 Len=49
1465	45.023658	192.168.124.6	43.242.159.148	TCP	62	7396 → 9236 [PSH, ACK] Seq=51 Ack=153 Win=251 Len=0
1466	45.023743	192.168.124.6	43.242.159.148	TCP	54	7396 → 9236 [FIN, ACK] Seq=59 Ack=153 Win=251 Len=0
1467	45.044922	43.242.159.148	192.168.124.6	TCP	60	9236 → 7396 [ACK] Seq=153 Ack=51 Win=21 Len=0
1468	45.045207	43.242.159.148	192.168.124.6	TCP	60	9236 → 7396 [ACK] Seq=153 Ack=59 Win=21 Len=0
1469	45.066785	43.242.159.148	192.168.124.6	TCP	54	9236 → 7396 [FIN, ACK] Seq=153 Ack=60 Win=21 Len=0
1470	45.066814	192.168.124.6	43.242.159.148	TCP	54	7396 → 9236 [ACK] Seq=60 Ack=154 Win=251 Len=0
1471	45.993091	192.168.124.6	14.18.180.113	TCP	54	7113 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
1472	46.475300	192.168.124.6	14.22.9.53	TCP	125	6896 → 80 [PSH, ACK] Seq=214 Ack=223 Win=257 Len=71
1473	46.490816	14.22.9.53	192.168.124.6	TCP	128	80 → 6896 [PSH, ACK] Seq=223 Ack=285 Win=251 Len=74
1474	46.545017	192.168.124.6	14.22.9.53	TCP	54	6896 → 80 [ACK] Seq=285 Ack=297 Win=257 Len=0
1475	46.655988	192.168.124.6	120.238.119.1	TCP	55	[TCP Keep-Alive] 7177 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1
1476	46.677994	120.238.119.1	192.168.124.6	TCP	66	[TCP Keep-Alive ACK] 443 → 7177 [ACK] Seq=1 Ack=2 Win=16 Len=0 SLE=1 SRE=2
1477	47.297588	192.168.124.6	109.244.184.43	UDP	252	1863 → 18888 Len=210
1478	47.297805	192.168.124.6	110.85.55.101	HTTP	510	GET /mobile.mssl.c.ta.qq.com/QM00005mTE2BhXYx.mgz?key=766b165225f77b66cd02de7172030316&arrive_key=188586094858&guid=56044EC4899188097C...

以下为添加捕获过滤器后的抓包工作，可以看出，对应抓包工作只会捕获满足条件的信息，从而减小抓包工作量

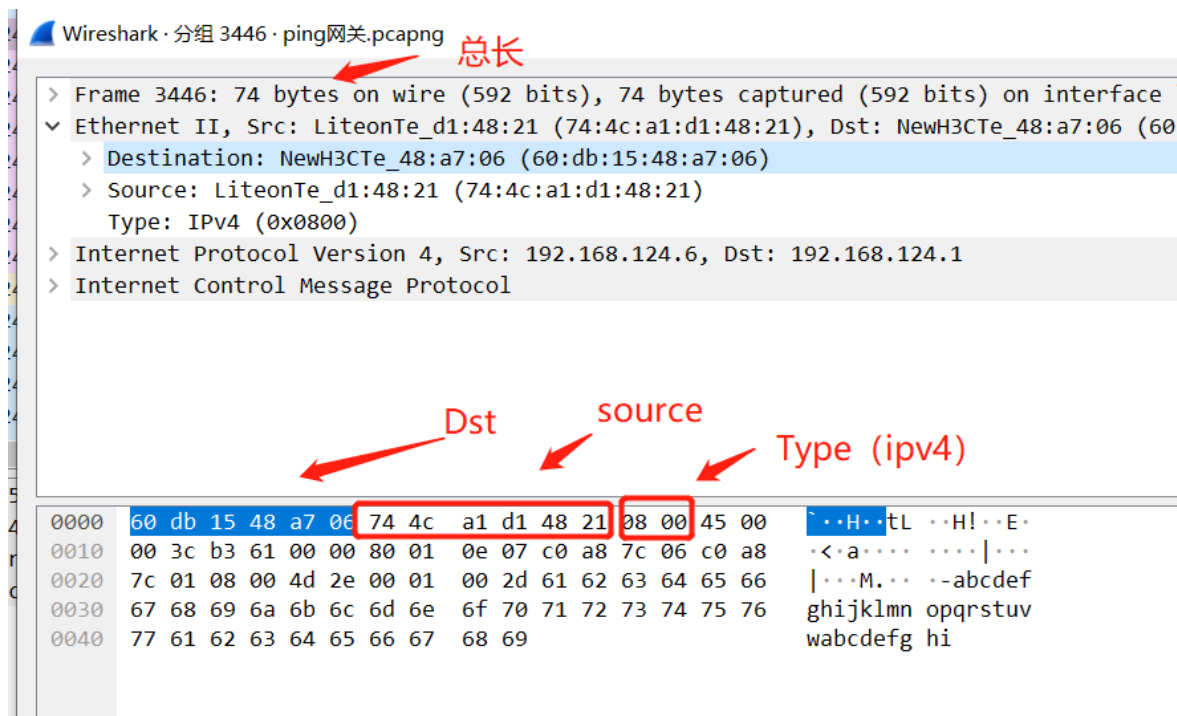
Ps: `dfsui.github.io` 为个人网站，而不是ping www.baidu.com，因为百度会有多个ip，所以无法确定具体ping时会ping到哪一个



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.124.6	185.199.111.153	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (reply in 2)
2	0.209528	185.199.111.153	192.168.124.6	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424, ttl=38 (request in 1)
3	1.003482	192.168.124.6	185.199.111.153	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (reply in 4)
4	1.211978	185.199.111.153	192.168.124.6	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=38 (request in 3)
5	2.006256	192.168.124.6	185.199.111.153	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (reply in 6)
6	2.214969	185.199.111.153	192.168.124.6	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=38 (request in 5)
7	3.010263	192.168.124.6	185.199.111.153	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (reply in 8)
8	3.221513	185.199.111.153	192.168.124.6	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=38 (request in 7)

2. MAC 帧的长度和 IP 数据报的长度有怎样的关系？请用你的数据记录进行验证。

MAC帧 = 6字节源mac地址 + 6字目标mac地址 + 2字节类型（ipv4或ipv6） + ip数据报（46~1500字节） + 4字节帧检验序列FCS
MAC帧长度是需要在64~1518字节之间的，太长或者太短都是无效的帧。

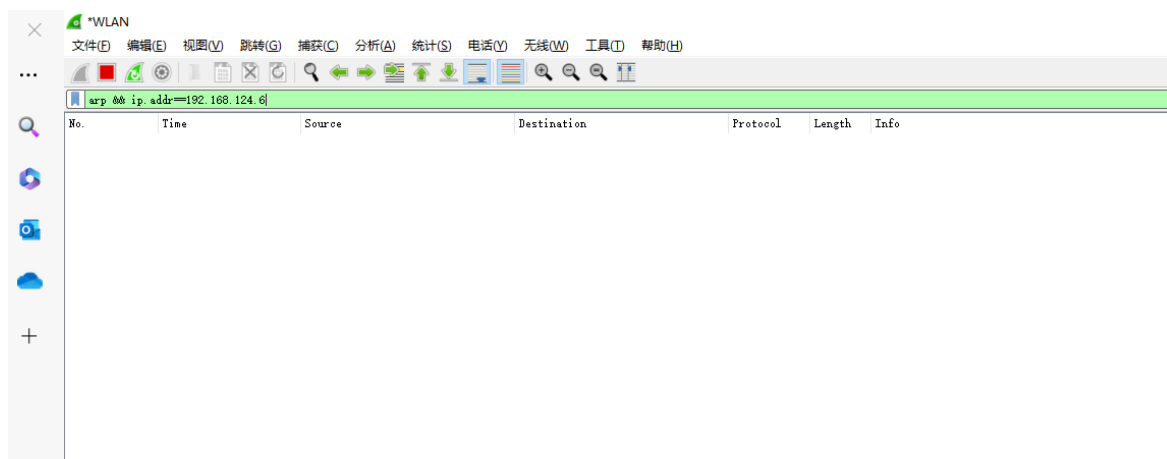


3. 假设本机 IP 地址是 192.168.0.38，在本机上运行 Wireshark 捕获报文，使用

“ip.addr==192.168.0.38”作为过滤条件，能否过滤出本机发出/收到的 ARP 报文？为什么？

不能，因为 ARP 协议是工作在 OSI 模型的第二层（数据链路层），而不是第三层（网络层）。

过滤条件 “ip.addr==192.168.0.38” 只能过滤出源或目的 IP 地址为 192.168.0.38 的报文，这些报文都是基于 IP 协议进行传输的，而 ARP 协议并不是基于 IP 协议进行传输的，因此无法通过该过滤条件来过滤 ARP 报文。实验如下图，可以看出，没有任何信息



如果要过滤本机发出/收到的 ARP 报文，可以使用以下过滤条件之一：

(a) arp: 过滤出所有 ARP 报文；

(b) arp and (ether src host 本机 MAC 地址 or ether dst host 本机 MAC 地址): 过滤出本机发出/收到的 ARP 报文。其中，ether src/dst host 本机 MAC 地址是以太网帧中源/目的 MAC 地址为本机 MAC 地址的过滤条件

以下为清除 ARP Cache 后重新开始接受报文

本机地址为 **192.168.124.6**，可以看出清除ARP缓存后，主机的第一件事是请求网卡位置

正在捕获 WLAN

文件(F) 编辑(E) 视图(V) 刷新(R) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(H)

arp 0% eth.addr=74:4c:a1:d1:48:21

No.	Time	Source	Destination	Protocol	Length	Info
71	8.307868	LiteonTe_d1:48:21	Broadcast	ARP	42	Who has 192.168.124.1? Tell 192.168.124.6
72	8.309406	NewH3CTe_48:a7:06	LiteonTe_d1:48:21	ARP	42	192.168.124.1 is at 60:db:15:48:a7:06

4. ping 同一局域网内的主机和局域网外的主机，都会产生 ARP 报文么？所产生的 ARP 报文有何不同，为什么？

先分析**同一局域网**的主机；

在同一局域网内的主机，若是A ping B，且A中ARP Cache中有储存B的MAS和ip，则无需发ARP报文，会根据查询到的信息，直接将ip数据报发送过去

若是缓存表中没有或者清除了ARP Cache，则会产生**广播ARP报文**，并将B的MAS和ip**单播**给A。

若是**局域网外**的主机

则是看主机A是否有网关的MAS地址，如果有，则直接将IP数据包发送个网关，**不会产生ARP报文**

而若没有，则A会进行**广播**，寻找网关的MAS，**产生ARP报文**

之后再由网关负责将数据包发送给B

5. ARP 请求数据包是支撑 TCP/IP 协议正常运作的广播包。如果滥发或错发 ARP 广播包会产生那些不良影响？如何发现和应对？

会发生ARP欺骗或攻击

ARP欺骗

地址解析协议是建立在网络中各个主机**互相信任**的基础上的，它的诞生使得网络能够更加高效的运行，但其本身也存在缺陷：

ARP地址转换表是依赖于计算机中高速缓冲存储器动态更新的，而高速缓冲存储器的更新是受到更新周期的限制的，只保存最近使用的地址的映射关系表项，这使得攻击者有了可乘之机，可以在高速缓冲存储器更新表项之前修改地址转换表，实现攻击。ARP请求为广播形式发送的，网络上的主机可以自主发送ARP应答消息，并且当其他主机收到应答报文时不会检测该**报文的真实性**就将其记录在本地的MAC地址转换表，这样攻击者就可以向目标主机发送**伪ARP应答报文**，从而**篡改本地的MAC地址表**。ARP欺骗可以导致**目标计算机与网关通信失败**，更会导致通信重定向，所有的数据都会通过攻击者的机器，因此存在极大的安全隐患

ARP攻击

ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的进行。基于ARP协议的这一工作特性，黑客向对方计算机不断发送有**欺诈性质的ARP数据包**，数据包内包含有与当前设备重复的Mac地址，使对方在回应报文时，由于简单的地址重复错误而导致不能进行正常的网络通信，或者如果不及时处理，便会造成**网络通道阻塞、网络设备的承载过重、网络的通讯质量不佳**等情况。

为了发现和应对滥发或错发 ARP 广播包的问题，可以采取以下措施：

- (a) 监控网络流量：使用网络流量监控工具，可以实时监控网络中的流量情况，发现是否有异常的 ARP 广播包，及时采取措施应对。
- (b) 使用网络防火墙：网络防火墙可以对网络流量进行过滤和管理，可以限制 ARP 广播包的发送和接收，从而避免网络拥堵和 ARP 欺骗攻击。
- (c) 加强网络安全措施：加强网络安全措施，如加密网络通信，限制网络访问，加强身份认证等，可以有效避免滥发或错发 ARP 广播包的问题，保障网络安全。
- (d) 及时更新网络设备：网络设备可能存在漏洞，容易受到攻击，及时更新设备固件和软件，可以修复漏洞，提高网络安全性。

6. 什么是免费 ARP（Gratuitous ARP）？它的作用是什么？请使用 Wireshark 进行捕捉和分析。

免费ARP

免费 ARP（Gratuitous ARP）包是一种特殊的ARP请求，它并非期待得到**IP对应的 MAC 地址**，而是当主机启动的时候，发送一个 Gratuitous ARP请求，即**请求自己的IP地址的MAC地址**。

免费ARP报文与普通ARP请求报文的区别在于报文中的目标IP地址。普通ARP报文中的目标IP地址是其他主机的IP地址；而免费ARP的请求报文中，**目标IP地址是自己的IP地址**。

免费 ARP 数据包有以下 3 个作用。

- 该类型报文起到一个**宣告作用**。它以广播的形式将数据包发送出去，**不需要得到回应**，只为了告诉其他计算机**自己的IP地址和MAC地址**。
- 可用于**检测IP地址冲突**。当一台主机发送了免费ARP请求报文后，如果收到了**ARP响应报文**，则说明网络内已经存在使用该IP地址的主机。
- 可用于**更新其他主机的ARP缓存表**。如果该主机更换了网卡，而其他主机的ARP缓存表仍然保留着原来的MAC地址。这时，可以发送免费的 ARP数据包。其他主机收到该数据包后，将更新ARP缓存表，将原来的 MAC地址替换为新的MAC地址。

ARP announcement协议

ARP announcement 是一种特殊的 ARP 请求，ARP 数据包的目的**协议地址和源协议地址相同**，并且目的**硬件地址为全 0**。所以，它又会是一个特殊的 ARP 响应。

ARP announcement 旨在**更新其它收到这个通告的主机的 ARP 缓存**。这种免费（不请自来）的 ARP 通常用于在**主机启动或更换网卡**时通知其它主机。又称 GARP（Gratuitous ARP，免费 ARP）。

作用：用作更新 ARP 缓存，网络中的其他主机收到该广播则更新缓存中的条目，收到该广播的主机无论是否存在与 IP 地址相关的条目都会强制更新，如果存在旧条目则会将 MAC 更新为广播包中的 MAC。

以下为一个设备在请求网关的信息

Seq.	Time	Source	Destination	Protocol	Length	Info
319	11.544559	86:a5:49:36:65:3e	Broadcast	ARP	42	Who has 192.168.124.1? Tell 192.168.124.24
348	13.848344	LiteonTe_d1:48:21	Broadcast	ARP	42	Who has 192.168.124.1? Tell 192.168.124.6
361	13.855707	NewH3CTe_48:a7:06	LiteonTe_d1:48:21	ARP	42	192.168.124.1 is at 60:db:15:48:a7:06
1297	45.608370	LiteonTe_d1:48:21	NewH3CTe_48:a7:06	ARP	42	Who has 192.168.124.1? Tell 192.168.124.6
1298	45.609816	NewH3CTe_48:a7:06	LiteonTe_d1:48:21	ARP	42	192.168.124.1 is at 60:db:15:48:a7:06
1463	47.284233	82:1d:9d:4a:88:ad	Broadcast	ARP	42	Who has 192.168.124.1? Tell 192.168.124.29
2088	72.680173	86:a5:49:36:65:3e	Broadcast	ARP	42	Who has 192.168.124.1? Tell 192.168.124.24
2245	79.951748	Apple_e6:d0:15	Broadcast	ARP	42	ARP Announcement for 192.168.124.17
2975	107.395010	82:1d:9d:4a:88:ad	Broadcast	ARP	42	Who has 192.168.124.1? Tell 192.168.124.29
3288	114.972941	BeijingX_b5:c9:f2	Broadcast	ARP	42	Who has 192.168.124.11? Tell 192.168.124.2
3301	118.249928	BeijingX_b5:c9:f2	Broadcast	ARP	42	Who has 192.168.124.17? Tell 192.168.124.2

数据包长度 源主机地址

Frame 319: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{BB78B787-0FFA-4348-B1-0000} Ethernet II, Src: 86:a5:49:36:65:3e (86:a5:49:36:65:3e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800) 类型
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: 86:a5:49:36:65:3e (86:a5:49:36:65:3e)
 Sender IP address: 192.168.124.24
 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00) 请求的MAC为全0
 Target IP address: 192.168.124.1 网关

数据报

问题与感悟

1 一些问题

1.1 关于baidu.com与www.baidu.com

1. 两者不是一个东西，baidu.com为一级域名，www.baidu.com为二级域名，两者都可以实现抓包
2. baidu.com有多个ip，可以保证不同地区和线路的用户都能获得最快速稳定的访问体验
3. ping www.baidu.com会自动变成www.a.shifen.com

```
C:\Users\lenovo>ping baidu.com

正在 Ping baidu.com [39.156.66.10] 具有 32 字节的数据:
来自 39.156.66.10 的回复: 字节=32 时间=2233ms TTL=47
来自 39.156.66.10 的回复: 字节=32 时间=3056ms TTL=47
来自 39.156.66.10 的回复: 字节=32 时间=2656ms TTL=47
来自 39.156.66.10 的回复: 字节=32 时间=1339ms TTL=47

39.156.66.10 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 = 1339ms, 最长 = 3056ms, 平均 = 2321ms

C:\Users\lenovo>ping baidu.com

正在 Ping baidu.com [110.242.68.66] 具有 32 字节的数据:
来自 110.242.68.66 的回复: 字节=32 时间=400ms TTL=48
来自 110.242.68.66 的回复: 字节=32 时间=2274ms TTL=48
来自 110.242.68.66 的回复: 字节=32 时间=357ms TTL=48
来自 110.242.68.66 的回复: 字节=32 时间=1752ms TTL=48

110.242.68.66 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 = 357ms, 最长 = 2274ms, 平均 = 1195ms
```

两个不同 ip

图 2 不同ip

1.2 Ping其他主机请求超时

ping出现time out的可能性原因:

- 1、经过的节点或目的ip设备的**防火墙**拦截的ping的request消息，导致高层无法收到，所以不回ping的reply消息。
- 2、跨网段环境中存在**ip冲突**，导致网关把ping的request消息发给**其他mac地址**。
- 3、也与目的主机的路由相关，没有回程路由，如同网段可能掩码错误，没有配置网关的话。
- 4、在目的侧抓包，有request和reply消息，但因回程路由指向其他ip地址，导致ping的reply消息的目的mac指向其他mac地址，没有回到request消息的源mac上去，导致源ip没有收到ping的reply消息。

在按照以下步骤排查后

1. 主机ping自己的地址，可排查**网卡问题**。若连接有问题，说明网卡有问题或者网络连接有问题。
2. 主机向外ping。可以判断是否网络连接有问题
3. 关闭其他主机的防火墙后，ping其他主机

在关闭目标主机后的防火墙后，成功ping通，**发现确实是防火墙的问题**

1.3 Ping手机时无法访问目标主机

确保ping手机时，手机不可熄屏，原因是手机熄屏后，手机会进入休眠状态以节省电力，此时手机的**网络接口也会进入休眠状态**，从而导致无法访问目标主机。这是因为在休眠状态下，手机会关闭 Wi-Fi 或移动数据连接，以节省电力。因此，当手机熄屏后，ping 手机时可能会出现无法访问目标主机的情况。

1.4 arp-d

使用 `arp-d` 要在管理员权限下进行

2 感悟与总结

本次实验借助 wireshark 工具，我深入了解了 IP 协议，arp 协议与 icmp 协议。这些协议都作用于网络层。网络层（Network Layer）是 OSI 模型中的第三层（TCP/IP 模型中的网际层），提供路由和寻址的功能，使两终端系统能够互连且决定最佳路径，并具有一定的拥塞控制和流量控制的能力。相当于发送邮件时需要地址一般重要。由于 TCP/IP 协议体系中的网络层功能由 IP 协议规定和实现，故又称 IP 层。当然网络层还有一些其他的协议，如 RARP、OSPF、IPX、RIP、IGRP 等，wireshark 的功能也远远不止在本次实验中体现的这些。因此在未来的学习生活中，我将继续研究计算机网络的“神奇”之处，以自顶向下的方法来探索网络领域。