**实验说明：每份实验报告注明您的学号、姓名。（如果发现抄袭，本次实验成绩为零）**

实验二：网络协议分析

# 一、基本要求

通过网络抓包软件，捕获真实网络传输的实时数据，通过对数据报头的分析，更深刻的理解协议，巩固理论知识。

# 二、实验内容

1. 学习 Wireshark 基本操作： 重点掌握捕获过滤器和显示过滤器。

2. 观察 MAC 地址： 了解 MAC 地址的组成，辨识 MAC 地址类型。

3. 分析以太网帧结构： 观察以太网帧的首部和尾部，了解数据封装成帧的原理。

4. 分析 ARP 协议： 抓取 ARP 请求和应答报文，分析其工作过程。

5. 执行 ping 命令， 观察 IP 数据报和 ICMP 询问报文的结构： 通过 Wireshark监视器观察捕获流量中的 ICMP 询问报文和 IP 数据报的结构。注意比较 ICMP 请求帧与回应帧，及其 IP 头部数据字段的异同。

6. 改变 ping 命令的参数，观察 IP 数据报分片：更改 ping 命令参数 MTU，使其发出长报文以触发 IP 数据报分片，再观察 IP 数据报的结构变化。

7. 执行 Traceroute 命令，观察 ICMP 差错报文的结构， 并分析其工作原理： 使用 Linux 操作系统提供的 traceroute 命令（或者 Windows 系统提供的 tracert 命令）， 捕获和分析该命令所产生的 IP 数据报， 特别注意相关的 ICMP 差错报文。结合 捕获的具体数据， 画出命令执行过程中数据交互的示意图， 掌握 traceroute 的工作原理。

# 三、实验步骤

## **3.1** WireShark 基本使用

1. 通过 Wireshark 官网下载最新版软件，按默认选项安装。

2. 运行 Wireshark 软件，程序界面会显示当前的网络接口列表，单击要观察的网络

接口，开始捕捉数据包，Wireshark 软件选择网络接口的界面如图1.1-2所示。

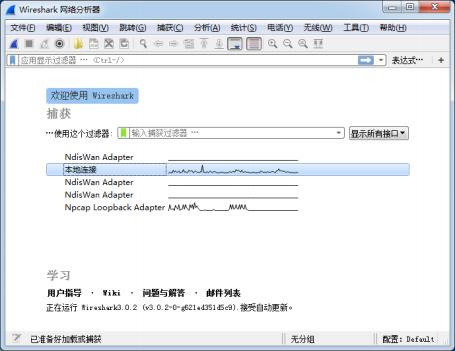


图 1.1-2 Wireshark 软件启动界面

3. 点击工具栏上的红色方块按钮停止捕捉。

4. 菜单、工具栏、状态栏和主窗口如图1.1-3所示，可以根据需要通过菜单“视图” 以及“编辑/首选项/外观”的相关选项对基本设置进行更改。例如图1.1-4 中的语言、字体缩放、颜色、布局等项目。

5. 使用“显示过滤器”可以方便地从捕获的数据包中筛选出要观察的数据包。显示 过滤器支持若干的过滤选项： 源 MAC、目的 MAC、源 IP、目的 IP、TCP/UDP传输协议、应用层协议（HTTP, DHCP）、源端口Port、目的端口Port 等。在显示过滤器栏中输入过滤表达式（更详细的显示过滤语法可以查看 WireShark 的官方文档），例如下面的命令：

arp //显示 arp 协议报文，例如图1.1--5

ip.src == a.b.c.d && icmp //显示源地址为 a.b.c.d 的 icmp报文

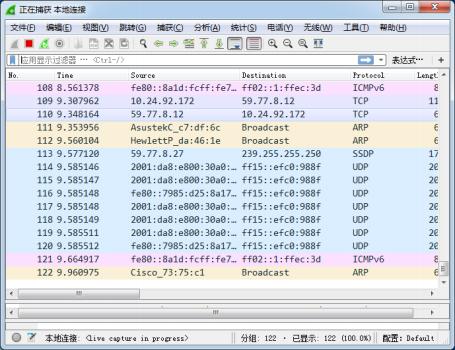


图 1.1-3 Wireshark 主窗口界面

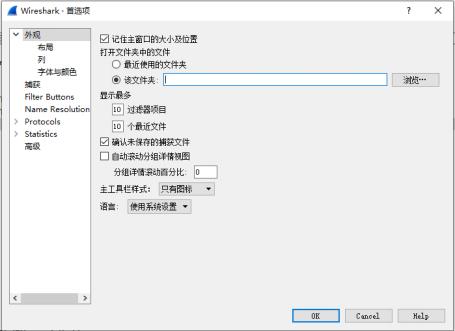


图 1.1-4 Wireshark 的设置界面

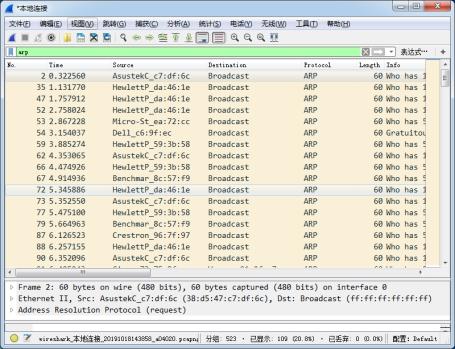


图 1.1-5 显示过滤规则的示例

6. 通过主菜单“文件”/ “导出特定分组”（如图 1.1–6 ），可以保存捕获的网络数据（也可以先选中某些包，只保存部分数据）。

7. 如果只想捕捉特定的数据包， 可以使用菜单“捕获”/ “捕获过滤器”选定想要 的类型（如图 1.1–7 ）。例如， 选择“IPv4 only”，Wireshark 只抓取 ipv4 类型的数据包。 Wireshark 过滤器官方文档提供了更加全面详细的语法和常用示例。

8. Wireshark 还提供了丰富的统计功能供用户选用，如图1.1–8。更多文档可以查询Wireshark 使用帮助。

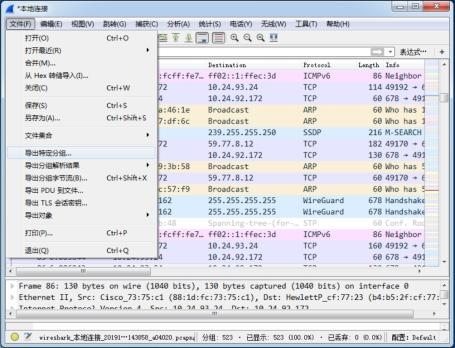


图 1.1-6 操作主菜单保存数据文件

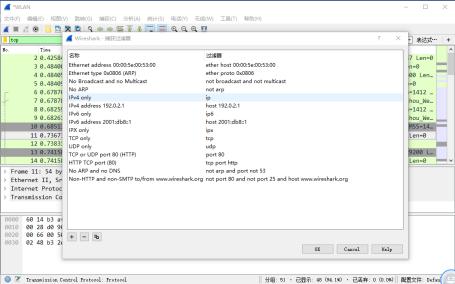


图 1.1-7 选中特定的捕获类型

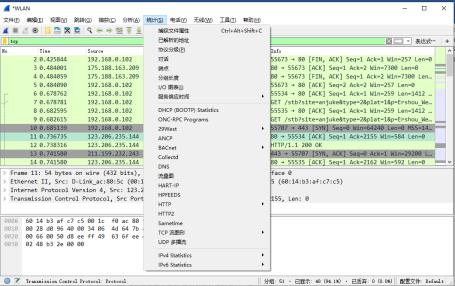


图 1.1-8 统计功能

## 3.2 观察 MAC 地址

启动 Wireshark 捕捉数据包， 在命令行窗口分别 ping 网关和 ping 同网段的一台主 机， 分析本机发出的数据包。重点观察以太网帧的 Destination 和 Source 的 MAC 地址，

辨识MAC地址类型，解读 OUI 信息、I/G 和 G/L 位。

## 3.3 分析以太网的帧结构

选择其中一个数据包，点击 Ethernet II 展开（图1.1-9 ），查看 MAC 帧的各个字段。

## 3.4 ARP 协议分析

1. 使用arp -d 命令（其语法见图1.1-10)，清空本机的 ARP 缓存，开启 Wireshark，ping 本机的同网段地址， 在显示过滤器条框中输入“arp”， 观察捕获的 ARP 报文的各个字段，分析请求/响应的过程。

2. 使用 arp -d 命令， 清空本机的 ARP 缓存。开启 Wireshark，ping 与本机网段不同的 IP 地址或域名，观察捕获的 ARP 报文的各个字段，分析请求/响应的过程。

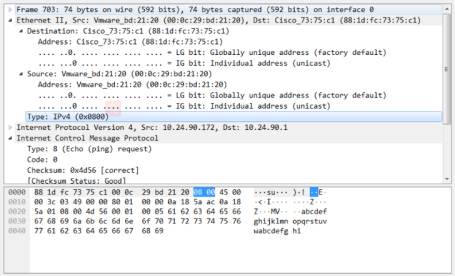


图 1.1-9 以太网帧结构展开界面

arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]

-a 显示所有接口/特定接口的当前 ARP 缓存表

-g 同 -a

-d 删除所有/指定的 IP 地址项

-s 在 ARP 缓存中添加对应 InetAddr 地址的 EtherAddr 地址静态项

图 1.1-10 arp 命令语法及参数

## 3.5 ping 命令

本机（示例 IP 为 <192.168.1.251> ）启动 Wireshark 软件， 选择要监听的网络接口（如

eth0 、wlan0 ）；然后在终端发起网络命令： ping IP 地址/域名。

1. 在 Wireshark 监视器中设置过滤条件。例如图1.2–3设置过滤条件为 icmp，则显

示出所捕获的 ICMP 数据包。

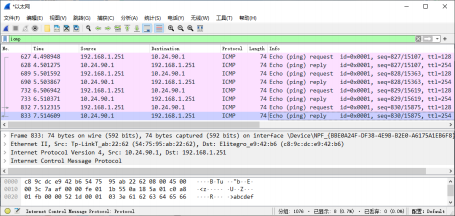


图 1.2–3 Wireshark 监视器界面

2. 点击 Internet Protocol Version 4 展开（如图 1.2–4 ），查看 IP 数据报，特别观察 IP

数据报的首部字段及其内容。

3. 点击 Internet Control Message Protocol 展开（如图1.2–5 ），查看 ICMP 报文，并解

释回显（Echo Request 和 Echo Reply）报文的首部字段。

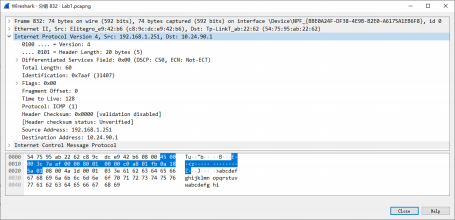


图 1.2-4 查看 IP 数据报

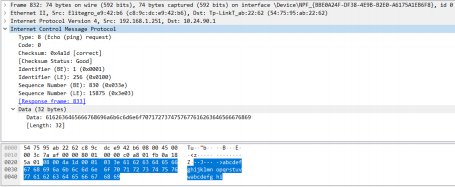


图 1.2-5 Echo request 示例

4. 清空 Wireshark 监控器， 重新发起网络命令（如图1.2–6 ）： ping IP 地址/域名 -l #length，并解释对比前后两次执行 ping 命令的结果。其中，-l #length确定echo数据报的长度为#length，其默认值为 32 字节，且小于 65,527 字节。

5. 可以多次改变 #length 的大小（例如 1000 字节、 2000 字节和 4000 字节）， 观察 IP 数据报何时会分片？请解释 IP 数据报分片的原因和具体情况。提示： 请先确认该网络的 MTU ，可在 Wireshark 记录中查找“IPv4 fragments”项目。

## 3.6 traceroute 命令

本机（示例 IP 为 <192.168.1.251> ）启动 Wireshark 软件， 选择要监听的网络接口（如

eth0 、wlan0 ）；然后在终端发起网络命令： traceroute IP 地址/域名。

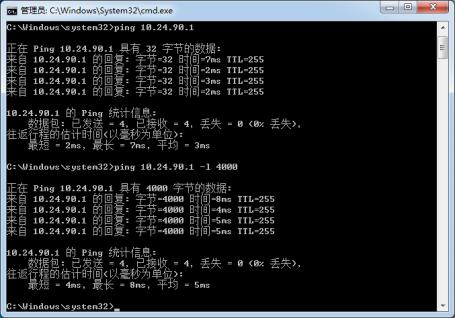


图 1.2-6 ping 命令执行示例

1. 启动 Wireshark 软件， 选择要监听的网络接口，设置过滤条件 icmp（如图1.2-7 ）。

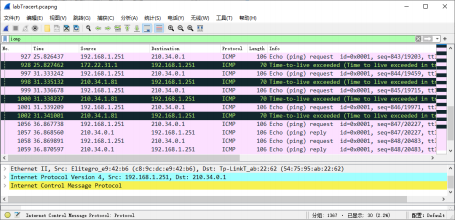


图 1.2–7 在 Wireshark 中设置过滤条件

2. 在终端中使用 traceroute 命令， 目的主机是外网的一台设备（如图 1.2-8，示例 IP为 <210.34.0.1> ）。

3. 点击 Internet Control Message Protocol 展开，查看 ICMP 差错报文，观察并解释ICMP 报文结构和字段内容。

4. 结合 ICMP 报文记录画出数据交互示意图，并描述 tracert 工作原理。

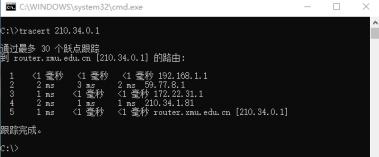


图 1.2–8 在终端中执行 traceroute 命令示例

# 4 思考题

1. 使用了显示过滤器后，Wireshark 的抓包工作量会减少吗？

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。

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？

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？

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？

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。

7. 在有线局域网中， PC1 的 IP 地址为 <192.168.1.5>/24 ，默认路由器的 IP 地址为 <192.168.1.1>；PC2 的 IP 地址为 <192.168.2.6>/24，默认路由器的 IP 地址为 <192.168.2.1>。 在 PC1 向 PC2 发送数据的传输过程中， 以太网数据帧的首部字段和 IP 数据 报的首部字段是怎样变化的？如果有条件，请搭建实验平台进行实验，并使用Wireshark 软件验证你的答案。

8. 拒绝服务（ Denial of Service，DoS ）攻击， DoS 通过消耗目标主机设备的某种资

源，导致其网络服务不能被正常用户使用。

(a) IP 数据报分片机制可能被攻击者利用来构建拒绝服务攻击。试设计一种利用 IP 数据报分片机制发动 DoS 攻击的方法，并提出防御的思路。

(b) 请思考利用 ICMP 报文构建 DoS 攻击的可能性以及防御方法。

9. 在实际操作中， Traceroute 命令返回的某些条目以“ \* ”号表示。请思考有哪些原

因可能导致这样的情况。

10. 发送方要怎样决定 IP 数据报分组大小，才能避免因为不同网络 MTU 不一致而

引起分片呢？

11. 从 PC1 给 PC2 （其地址为#IP）发送三个 ping 命令，请比较命令的结果，并用Wireshark 软件进行观察分析。

(a) ping #IP -l 1472 -f -n 1

(b) ping #IP -l 1473 -f -n 1

(c) ping #IP -l 1473 -n 1

# 5考核方法

报告内容应包含以下内容，相关的分析解释都需要截图证明，并与提交的 Wireshark 抓包数据文件相吻合。

1. Wireshark 的基本使用。
2. 以太网帧格式分析： MAC 地址类型、头部信息、长度及封装。
3. 结合捕捉的网络数据，分析 ARP 数据包，描述 ARP 协议工作过程。
4. 实施 ping 命令，记录引发的 IP 数据报和 ICMP 报文， 保存为 pcapng 文件 解释任一个 IP 数据报的首部，并对比 ICMP Echo 请求帧和回应帧；改变ping 的长度参数，解释 IP 数据报分片情况。
5. 实施 tracert 命令， 记录引发的 ICMP 报文， 保存为 pcapng 文件； 解释 任一个 ICMP 差错报文的结构； 描述 tracert 工作原理， 结合 ICMP 报文记录画出数据交互示意图。
6. 回答思考题。
7. 记录自己在本次实验中所遇到的问题，以及心得感悟。如果遇到异常情况，或者无法完成任务时，也请分析错误产生的原因。