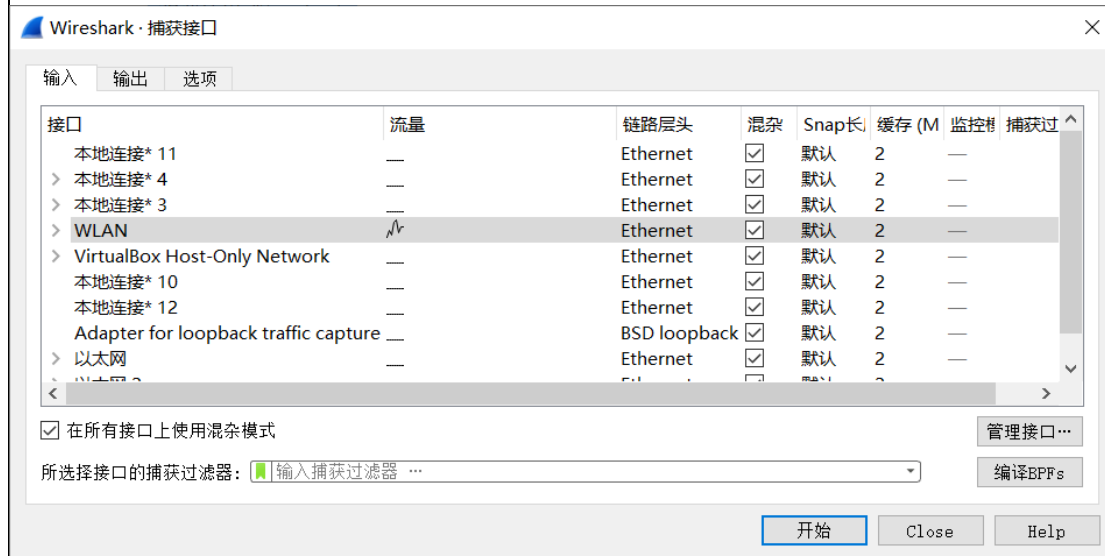


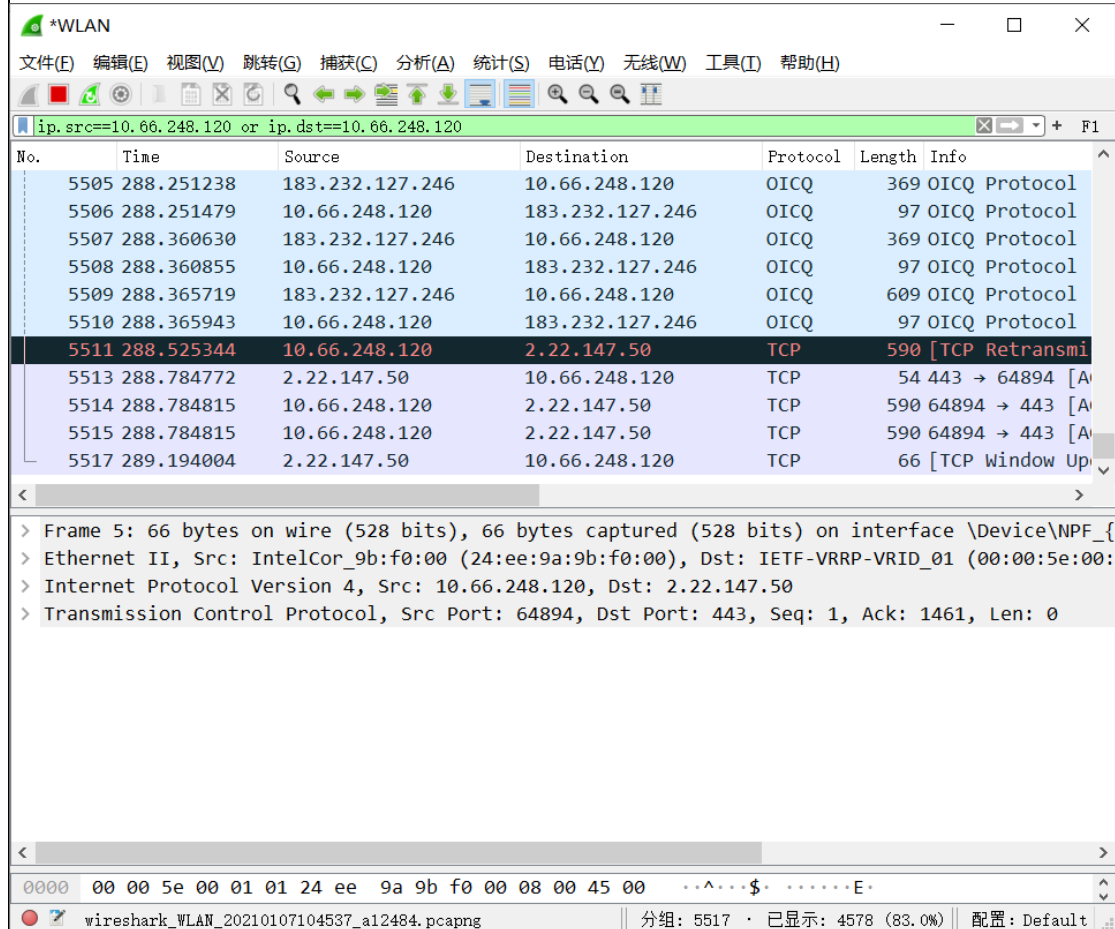
《计算机网络》实验报告

| | |
|--|---------|
| 实验项目序号及名称 | 基本报文分析 |
| 实验成员及分工：张楷 组长： 张楷 组员： 张楷 | |
| 报告执笔人（签名）：张楷 | 实验完成时间： |
| 实验目的： 1.理解 IP 层的作用以及 IP 地址的分类方法； 2.理解子网的划分和子网掩码的作用； 3.掌握 IP 数据包的组成和网络层基本功能； | |
| 实验设备和环境：校园网；装有 Wireshark 的 PC | |
| 实验过程及步骤：（给出相应的实验环境拓扑图和实验说明，可另附页） 一、 开始抓包； | |

1. 使用 Wireshark 开始捕获数据包;



2. 过滤。通过 ip.src== 10.66.248.120 or ip.dst== 10.66.248.120 指令，查看源地址或目标地址为 10.66.248.120 的数据包;



二、 TCP 三次握手;

1. 访问一个网址, 并用 http 指令过滤;
2. 寻找到 Info 为 GET/connecttext.txt HTTP/1.1,并追随 TCP 流;

The image shows a Wireshark network traffic capture window titled '*WLAN'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Tools, Help), a toolbar, and a packet list pane. The packet list pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet is 4709, which is an HTTP GET request for /connecttext.txt. The packet details pane shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the packet.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|---------------|---------------|----------|--------|----------------|
| 4808 | 118.990179 | 13.107.4.52 | 10.66.248.120 | TCP | 54 | 80 → 54002 [FI |
| 4809 | 118.990277 | 10.66.248.120 | 13.107.4.52 | TCP | 54 | 54002 → 80 [AC |
| 4810 | 118.990334 | 10.66.248.120 | 13.107.4.52 | TCP | 54 | 54002 → 80 [FI |
| 4815 | 119.219855 | 13.107.4.52 | 10.66.248.120 | HTTP | 568 | [TCP Spurious |
| 4817 | 119.534735 | 13.107.4.52 | 10.66.248.120 | HTTP | 568 | [TCP Spurious |
| 4829 | 120.133267 | 13.107.4.52 | 10.66.248.120 | HTTP | 568 | [TCP Spurious |
| 4845 | 121.338324 | 13.107.4.52 | 10.66.248.120 | HTTP | 568 | [TCP Spurious |
| 4846 | 121.338361 | 10.66.248.120 | 13.107.4.52 | TCP | 66 | [TCP Dup ACK 4 |
| 4987 | 125.293729 | 10.66.248.120 | 13.107.4.52 | TCP | 54 | [TCP Retransmi |
| 8344 | 162.854676 | 10.66.248.120 | 13.107.4.52 | TCP | 54 | [TCP Retransmi |
| 8577 | 166.224339 | 13.107.4.52 | 10.66.248.120 | TCP | 54 | 80 → 54002 [AC |

> Frame 4709: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device
> Ethernet II, Src: IntelCor_9b:f0:00 (24:ee:9a:9b:f0:00), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:
> Internet Protocol Version 4, Src: 10.66.248.120, Dst: 13.107.4.52
> Transmission Control Protocol, Src Port: 54002, Dst Port: 80, Seq: 1, Ack: 1, Len: 154
> Hypertext Transfer Protocol

0000 00 00 5e 00 01 01 24 ee 9a 9b f0 00 08 00 45 00 ..^...\$.E.

wireshark_WLAN_20210107105846_a05468.pcapng || 分组: 10458 · 已显示: 22 (0.2%) || 配置: Default

3. 第一次握手。标志位为 SYN，序列号为 0，代表客户端请求建立链接

*WLAN

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

tcp.stream eq 92

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|---------------|---------------|----------|--------|----------------------|
| 4599 | 115.701196 | 10.66.248.120 | 13.107.4.52 | TCP | 66 | 54002 → 80 [SYN] |
| 4684 | 116.704339 | 10.66.248.120 | 13.107.4.52 | TCP | 66 | [TCP Retransmission] |
| 4707 | 116.853016 | 13.107.4.52 | 10.66.248.120 | TCP | 66 | 80 → 54002 [SYN] |
| 4708 | 116.853080 | 10.66.248.120 | 13.107.4.52 | TCP | 54 | 54002 → 80 [ACK] |
| 4709 | 116.853242 | 10.66.248.120 | 13.107.4.52 | HTTP | 208 | GET /connectte |
| 4736 | 117.248846 | 13.107.4.52 | 10.66.248.120 | TCP | 66 | [TCP Retransmission] |
| 4737 | 117.248883 | 10.66.248.120 | 13.107.4.52 | TCP | 66 | [TCP Dup ACK 4] |
| 4773 | 118.059677 | 13.107.4.52 | 10.66.248.120 | TCP | 62 | [TCP Retransmission] |
| 4774 | 118.059713 | 10.66.248.120 | 13.107.4.52 | TCP | 66 | [TCP Dup ACK 4] |
| 4806 | 118.990179 | 13.107.4.52 | 10.66.248.120 | TCP | 54 | 80 → 54002 [ACK] |
| 4807 | 118.990179 | 13.107.4.52 | 10.66.248.120 | HTTP | 568 | HTTP/1.1 200 OK |

Sequence number (raw): 2813440752
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
> **Flags: 0x002 (SYN)**
Window size value: 64240
[Calculated window size: 64240]
Checksum: 0x1480 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> Options: (12 bytes). Maximum segment size. No-Operation (NOP). Window scale. No-Operation

0020 04 34 d2 f2 00 50 a7 b1 b2 f0 00 00 00 00 80 02 -4...P...

Flags (12 bits) (tcp.flags), 2 byte(s) | 分组: 20210 · 已显示: 22 (0.1%) | 配置: Default

4. 第二次握手。标志位为 SYN,ACK,将 Acknowledgment number 置为 1, 即用户发送的 ISN+1 (0+1);

*WLAN

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

tcp.stream eq 92

| Protocol | Length | Info |
|----------|--------|---|
| TCP | 66 | 54002 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| TCP | 66 | [TCP Retransmission] 54002 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA |
| TCP | 66 | 80 → 54002 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1 |
| TCP | 54 | 54002 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0 |
| HTTP | 208 | GET /connecttest.txt HTTP/1.1 |
| TCP | 66 | [TCP Retransmission] 80 → 54002 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 |
| TCP | 66 | [TCP Dup ACK 4708#1] 54002 → 80 [ACK] Seq=155 Ack=1 Win=66048 Len=0 SLE=0 SRE=1 |
| TCP | 62 | [TCP Retransmission] 80 → 54002 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 |
| TCP | 66 | [TCP Dup ACK 4708#2] 54002 → 80 [ACK] Seq=155 Ack=1 Win=66048 Len=0 SLE=0 SRE=1 |
| TCP | 54 | 80 → 54002 [ACK] Seq=1 Ack=155 Win=16737536 Len=0 |
| HTTP | 568 | HTTP/1.1 200 OK (text/plain) |

Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 2813440753
1000 = Header Length: 32 bytes (8)

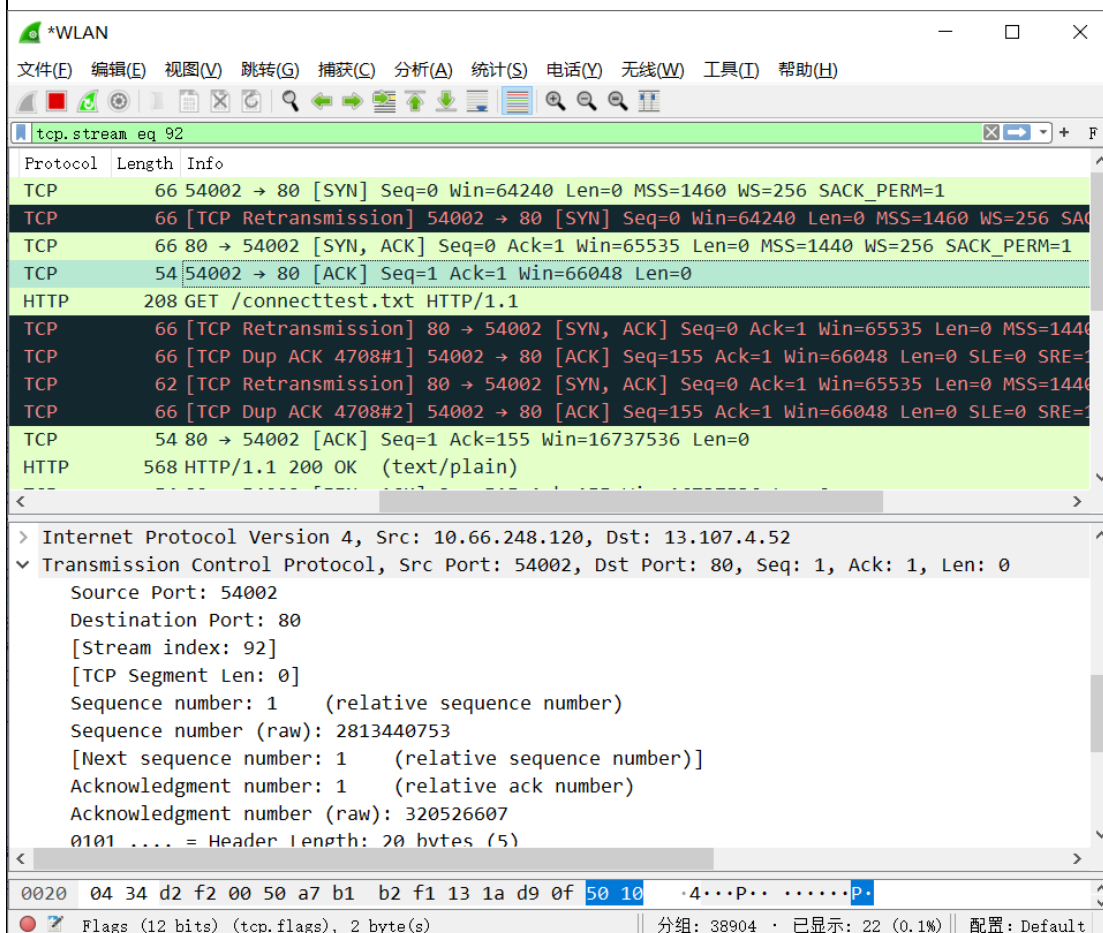
> Flags: 0x012 (SYN, ACK)
Window size value: 65535
[Calculated window size: 65535]
Checksum: 0x40ac [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

> Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation
> [SEQ/ACK analysis]
> [Timestamps]

0020 f8 78 00 50 d2 f2 13 1a d9 0e a7 b1 b2 f1 80 12 ..x.P.....

Flags (12 bits) (tcp.flags), 2 byte(s) || 分组: 31240 · 已显示: 22 (0.1%) || 配置: Default

5. 第三次握手。可见客户端再次发送确认包 号字段+1,放在确定字段中
发送给对方 就这样通过了 TCP 三次握手 客户端再次发送确认包
(ACK) SYN 标志位为 0,ACK 标志位为 1.并且把服务器发来 放在确定
字段中发送给对方.并且在数据段放写 ISN 的+1。



三、 IP 报文解析

捕获到的 IP 报文如下:

Internet Protocol Version 4, Src: 10.66.248.120, Dst: 13.107.4.52

0100 = Version: 4 //版本号为 4

.... 0101 = Header Length: 20 bytes (5) //首部长度为 20B

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 52 //总长度为 52B

Identification: 0xbf6a (49002) //标识符

Flags: 0x4000, Don't fragment //标志

0... = Reserved bit: Not set

.1. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0 //片偏移
Time to live: 64 //存活时间
Protocol: TCP (6) //协议
Header checksum: 0x0000 [validation disabled] 首部校验和
[Header checksum status: Unverified]
Source: 10.66.248.120 源地址
Destination: 13.107.4.52 目标地址

实验总结：（遇到问题、解决办法、收获和体会，可另附页）

大概明白了 IP 协议的报头