《网络与通信》课程实验报告

实验三：数据包结构分析

姓名	邱姜铭	院系	计算机学院	学号	22122861
任课教师	刘通		指导教师	刘通	
实验地点	计 706		实验时间	15:00	
实验课表现	出勤、表现得分(10)		实验报告得分(40)		实验总分	
	操作结果得分(50)					

实验目的：

1. 了解 Sniffer 的工作原理，掌握 Sniffer 抓包、记录和分析数据包的方法；
2. 在这个实验中，你将使用抓包软件捕获数据包，并通过数据包分析每一层协议。

实验内容：

使用抓包软件捕获数据包，并通过数据包分析每一层协议。

实验要求：（学生对预习要求的回答）（10 分）　　得分：

- 常用的抓包工具

Wireshark、Charles、Fiddler、Microsoft Network Monitor、NetXray、Sniffer Pro

实验过程中遇到的问题如何解决的？（10 分）　　得分：

问题 1：选择 Sniffer 软件

由于我平时使用的是 Mac 电脑，实验提供的 SnifferPro 软件为 Windows 版本，不能直接使用。于是经过网络搜集信息，我选用了 Wireshark 作为替代的抓包软件。

问题 2：选择捕获的接口

抓包需要选择监听的接口，根据流量的活跃情况，只有 Wi-Fi: en0 和 Loopback: lo0 有较多流量，其中 Loopback: lo0 根据名字可以得出是本地回环使用，所以选择监听 Wi-Fi: en0，之后的实验过程也能辅助证明这一点。

问题 3：数据包过多，分析困难

Wireshark 提供了强大的过滤功能，我根据实验目标设置了 IP 地址过滤条件（例如 ip.addr == 182.61.200.6），将显示范围缩小到与目标主机相关的通信数据包。这大大减少了无关数据包的干扰，使得分析更加高效。

本次实验的体会（结论）（10 分）　　得分：

通过本次实验，我深入理解了每一层网络协议的工作机制，特别是以太网、IP、ICMP 协议的交互过程。在对 ICMP 的 Echo 请求/响应分析过程中，我观察到了报文的详细结构、时延、TTL 等关键信息，使我更切实的体会到网络协议的工作过程。

思考题：（10 分）

思考题 1：（4 分）　　得分：

写出捕获的数据包格式。

Frame 15: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
Section number: 1
Interface id: 0 (en0)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 14, 2024 10:26:05.385776000 CST
UTC Arrival Time: Oct 14, 2024 02:26:05.385776000 UTC
Epoch Arrival Time: 1728872765.385776000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.090227000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.395573000 seconds]
Frame Number: 15
Frame Length: 98 bytes (784 bits)
Capture Length: 98 bytes (784 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]

Ethernet II, Src: 4e:b4:6a:81:51:9d (4e:b4:6a:81:51:9d), Dst: RuijieNetwor_3f:e1:1e (80:05:88:3f:e1:1e)
Destination: RuijieNetwor_3f:e1:1e (80:05:88:3f:e1:1e)
Source: 4e:b4:6a:81:51:9d (4e:b4:6a:81:51:9d)
Type: IPv4 (0x0800)
[Stream index: 1]

Internet Protocol Version 4, Src: 10.89.94.71, Dst: 182.61.200.6
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0xfefe (65278)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x94c6 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.89.94.71
Destination Address: 182.61.200.6

[Stream index: 0]

Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xe029 [correct]
[Checksum Status: Good]
Identifier (BE): 25176 (0x6258)
Identifier (LE): 22626 (0x5862)
Sequence Number (BE): 12 (0x000c)
Sequence Number (LE): 3072 (0x0c00)
[Response frame: 18]
Timestamp from icmp data: Oct 14, 2024 10:26:05.385567000 CST
[Timestamp from icmp data (relative): 0.000209000 seconds]
Data (48 bytes)

思考题2：（6分）　　得分：

写出实验过程并分析实验结果。

首先打开终端，使用ping命令

```
➜  ~ ping www.baidu.com
PING www.a.shifen.com (182.61.200.6): 56 data bytes
64 bytes from 182.61.200.6: icmp_seq=0 ttl=43 time=34.359 ms
64 bytes from 182.61.200.6: icmp_seq=1 ttl=43 time=33.961 ms
64 bytes from 182.61.200.6: icmp_seq=2 ttl=43 time=77.243 ms
64 bytes from 182.61.200.6: icmp_seq=3 ttl=43 time=33.087 ms
64 bytes from 182.61.200.6: icmp_seq=4 ttl=43 time=48.383 ms
64 bytes from 182.61.200.6: icmp_seq=5 ttl=43 time=33.518 ms
64 bytes from 182.61.200.6: icmp_seq=6 ttl=43 time=34.783 ms
64 bytes from 182.61.200.6: icmp_seq=7 ttl=43 time=36.732 ms
64 bytes from 182.61.200.6: icmp_seq=8 ttl=43 time=45.008 ms
64 bytes from 182.61.200.6: icmp_seq=9 ttl=43 time=41.076 ms
64 bytes from 182.61.200.6: icmp_seq=10 ttl=43 time=34.036 ms
64 bytes from 182.61.200.6: icmp_seq=11 ttl=43 time=33.341 ms
64 bytes from 182.61.200.6: icmp_seq=12 ttl=43 time=34.169 ms
64 bytes from 182.61.200.6: icmp_seq=13 ttl=43 time=40.277 ms
64 bytes from 182.61.200.6: icmp_seq=14 ttl=43 time=177.322 ms
64 bytes from 182.61.200.6: icmp_seq=15 ttl=43 time=34.040 ms
^C
--- www.a.shifen.com ping statistics ---
16 packets transmitted, 16 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 33.087/48.208/177.322/35.007 ms
```

从ping命令输出的信息可以得出实际访问的地址是182.61.200.6
所以设置过滤条件为：ip.addr == 182.61.200.6
最后任意选择一条内容作为实验内容

数据包分析：

1. 物理层和数据链路层：以太网帧结构（Ethernet II Frame）

以太网帧 (Ethernet II) 包含的字段：

- **目的MAC地址 (Destination MAC)**: 80:05:88:3f:e1:1e
  这是目标主机的 MAC 地址。在局域网中，数据首先通过 MAC 地址进行寻址。
- **源MAC地址 (Source MAC)**: 4e:b4:6a:81:51:9d
  这是发送方的 MAC 地址，表明数据包是由该地址对应的设备发送的。
- **以太网类型 (EtherType)**: 0x0800
  此字段表示上层使用的协议，这里 0x0800 表示数据包中封装的是 IPv4 协议。

2. 网络层：IPv4协议头 (Internet Protocol Version 4)

- **版本号 (Version)**: 4
  该字段表明使用的是 IPv4 协议。
- **头部长度 (Header Length)**: 20 bytes
  该字段表示 IP 头部的长度，单位是 32 位字（4 字节），本次报文的头部长度是 5 * 4 = 20 字节。
- **区分服务 (Differentiated Services Field)**: 0x00
  表示默认的服务类型，未使用特定的 QoS 优先级。
- **总长度 (Total Length)**: 84
  数据包的总长度，包括头部和数据部分，总共为 84 字节。
- **标识符 (Identification)**: 0xfefe (65278)
  用于唯一标识该报文，并在需要分片时对报文进行标识。
- **生存时间 (TTL - Time to Live)**: 64
  表示数据包在网络中允许通过的最大路由跳数。在每经过一个路由器时，TTL 减 1，当 TTL 为 0 时，数据包将被丢弃。
- **协议 (Protocol)**: 1 (ICMP)
  表示使用的上层协议为 ICMP 协议。
- **源IP地址 (Source IP)**: 10.89.94.71
  数据包的发送方 IP 地址。
- **目的IP地址 (Destination IP)**: 182.61.200.6
  数据包的接收方 IP 地址（目标地址）。

3. 传输层：ICMP 协议 (Internet Control Message Protocol)

ICMP 报文字段：

- **类型 (Type)**: 8 (Echo Request)
  该字段表示 ICMP 报文的类型，类型 8 表示 Echo 请求，即 ping 请求。

- **代码 (Code)**: 0

  对于 Echo 请求，Code 始终为 0。
- **校验和 (Checksum)**: 0xe029

  用于校验报文内容的完整性。在 Wireshark 中，该校验和已验证通过。
- **标识符 (Identifier)**: 0x6258 (25176)

  用于标识 Echo 请求的唯一性，服务器收到此请求后可以根据该标识符进行匹配。
- **序列号 (Sequence Number)**: 12

  用于对多个 Echo 请求进行排序和区分，确保请求和响应能够一一对应。
- **数据 (Data)**: 48 字节

  Echo 请求中的数据部分通常包含时间戳等信息，便于检测网络延迟。在本次报文中，数据部分为 48 字节。

指导教师评语：

日期：