**北京邮电大学《计算机网络》课程实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **实验**  **名称** | 网络层数据分组的捕获和解析 | | **学 院** | 计算机 | **指导教师** | 王晓茹 |
| **班 级** | **班内序号** | **学 号** | | **学生姓名** | **成绩** | |
| **2018211318** | **02** | **2018210074** | | **熊宇** |  | |
|  |  |  | |  |  | |
|  |  |  | |  |  | |
| **实**  **验**  **内**  **容** | 1）捕获在连接Internet过程中产生的网络层分组：DHCP分组，ARP分组，IP数据分组，ICMP分组。  2）分析各种分组的格式，说明各种分组在建立网络连接过程中的作用。  3）分析IP数据分组分片的结构。  通过本次实验了解计算机上网的工作过程，学习各种网络层分组的格式及其作用，理解长度大于1500字节IP数据组分片传输的结构。 | | | | | |
| **学生实验报告** | （详见“实验报告和源程序”册） | | | | | |
| **课**  **程**  **设**  **计**  **成**  **绩**  **评**  **定** | **评语**:  **成绩**:  指导教师签名：  年 月 日 | | | | | |

注：评语要体现每个学生的工作情况，可以加页。



**计算机网络实验报告**



**题目：网络层数据分组的捕获和解析**

**班 级： 2018211318班\_\_\_**

**学 号： 2018210074\_\_\_\_\_**

**姓 名： 熊宇\_\_\_\_\_\_\_\_\_\_\_**

**学 院： 计算机学院\_\_\_\_\_**

**2020年 6 月 5 日**

**实验报告**

**一 实验内容和实验目的**

（1）捕获在连接Internet过程中产生的网络层分组：DHCP分组，ARP分组，IP数据分组，ICMP分组。

（2）分析各种分组的格式，说明各种分组在建立网络连接过程中的作用。

（3）分析IP数据分组分片的结构。

通过本次实验了解计算机上网的工作过程，学习各种网络层分组的格式及其作用，理解长度大于1500字节IP数据组分片传输的结构。

**二 实验设备环境**

1台装有Windows操作系统的pc机，要求能够连接到Internet，并安装Wireshark等软件。

**三 实验步骤**

（1）准备工作

启动计算机，连接网络确保能够上网。断开连接，禁用网卡。

（2）捕获和分析网络层分组

开启监控，连接网络。一段时间后查看捕获的分组。分析各种分组的格式以及在上网过程中所起的作用。

（3）发送ICMP分组，捕获并分析格式

开启监控，使用ping命令，tracert命令, 捕获ICMP分组格式。

（4）分析数据分组的分片传输过程

制作8000字节的IP数据分组并发送，捕获后分析其分片传输的分组结构。

（5）撰写实验报告

按要求撰写实验报告，并接受实验指导教师面对面现场提问。

**四 实验内容**

（1）分析网络层分组结构

**A、捕获DHCP分组**

1、DHCP简介

DHCP，动态主机配置协议，前身是BOOTP协议，是一个局域网的网络协议，使用UDP协议工作，常用的2个端口：67(DHCP server),68(DHCP client)。DHCP通常被用于局域网环境，主要作用是集中的管理、分配IP地址，使client动态的获得IP地址、Gateway地址、DNS服务器地址等信息，并能够提升地址的使用率。简单来说，DHCP就是一个不需要账号密码登录的、自动给内网机器分配IP地址等信息的协议。

2、DHCP协议中的报文

DHCP DISCOVER ：客户端开始DHCP过程发送的包，是DHCP协议的开始

DHCP OFFER ：服务器接收到DHCP DISCOVER之后做出的响应，它包括了给予客户端的IP（yiaddr）、客户端的MAC地址、租约过期时间、服务器的识别符以及其他信息

DHCP REQUEST ：客户端对于服务器发出的DHCP OFFER所做出的响应。在续约租期的时候同样会使用。

DHCP ACK ：服务器在接收到客户端发来的DHCP REQUEST之后发出的成功确认的报文。在建立连接的时候，客户端在接收到这个报文之后才会确认分配给它的IP和其他信息可以被允许使用。

DHCP NAK ：DHCP ACK的相反的报文，表示服务器拒绝了客户端的请求。

DHCP RELEASE ：一般出现在客户端关机、下线等状况。这个报文将会使DHCP服务器释放发出此报文的客户端的IP地址

DHCP INFORM ：客户端发出的向服务器请求一些信息的报文

DHCP DECLINE :当客户端发现服务器分配的IP地址无法使用（如IP地址冲突时），将发出此报文，通知服务器禁止使用该IP地址。

3、DHCP的工作过程

Client端在局域网内发起一个DHCP Discover包，目的是想发现能够给它提供IP的DHCP Server。

可用的DHCP Server接收到Discover包之后，通过发送DHCP Offer包给予Client端应答，意在告诉Client端它可以提供IP地址。

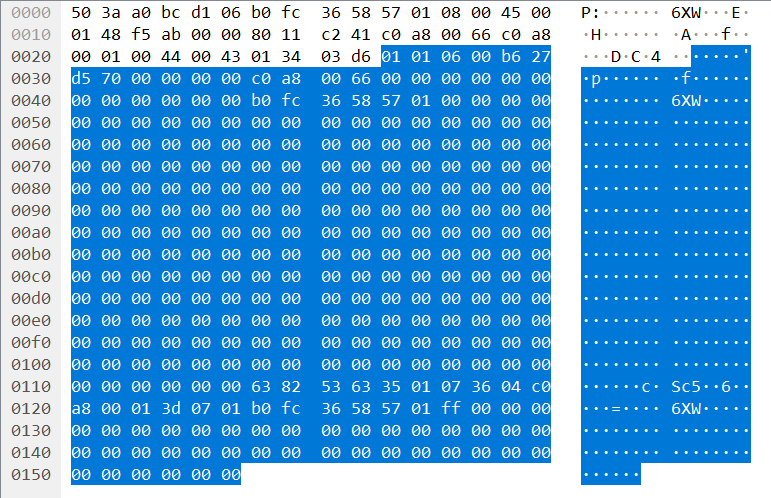
Client端接收到Offer包之后，发送DHCP Request包请求分配IP。

DHCP Server发送ACK数据包，确认信息。

4、实验步骤

打开Wireshark软件，在首页选择当前电脑所使用的接口（如WLAN），双击当前接口，弹出的页面中已经在不断的显示抓包的信息。在上方显示输入过滤器的条形窗口内输入bootp，使其只显示DHCP数据包。

打开命令提示符窗口，输入ipconfig /release 断开网络连接；此时计算机中所有网卡都已断开，Wireshark中显示截获到一个DHCP Release数据包。



Frame 106: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF\_{A1C9129E-1345-4E45-8F51-87974B691679}, id 0

Ethernet II, Src: CyberTAN\_58:57:01 (b0:fc:36:58:57:01), Dst: Shenzhen\_bc:d1:06 (50:3a:a0:bc:d1:06)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Release)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xb627d570

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 192.168.0.102

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: CyberTAN\_58:57:01 (b0:fc:36:58:57:01)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option: (53) DHCP Message Type (Release)

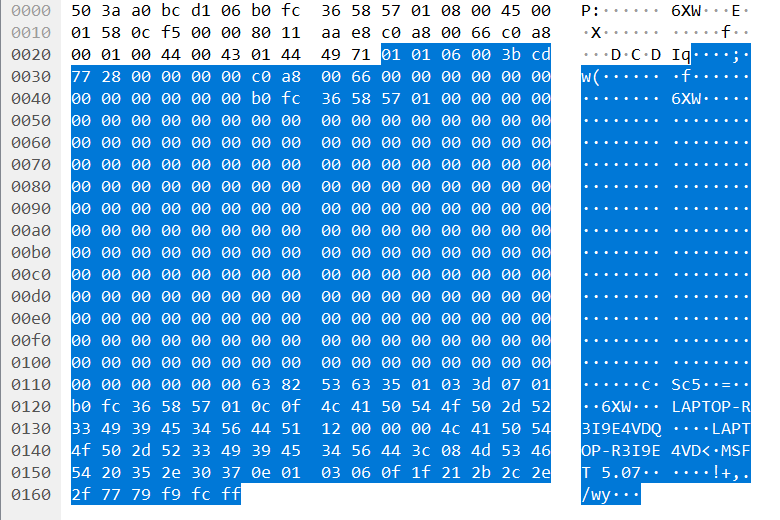
Option: (54) DHCP Server Identifier (192.168.0.1)

Option: (61) Client identifier

Option: (255) End

Padding: 000000000000000000000000000000000000000000000000…

继续在命令提示符窗口输入ipconfig /renew 请求网络连接；观察Wireshark中出现的新数据包，并依据DHCP工作过程进行数据包分析。



Encode分析如下：

Frame 40: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF\_{A1C9129E-1345-4E45-8F51-87974B691679}, id 0

Ethernet II, Src: CyberTAN\_58:57:01 (b0:fc:36:58:57:01), Dst: Shenzhen\_bc:d1:06 (50:3a:a0:bc:d1:06)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Request)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x3bcd7728

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 192.168.0.102

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: CyberTAN\_58:57:01 (b0:fc:36:58:57:01)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option: (53) DHCP Message Type (Request)

Option: (61) Client identifier

Option: (12) Host Name

Option: (81) Client Fully Qualified Domain Name

Option: (60) Vendor class identifier

Option: (55) Parameter Request List

Option: (255) End

计算机以广播方式发送一个DHCP request请求信息，该信息中包含向它所选定的DHCP服务器请求IP地址192.168.0.102.。

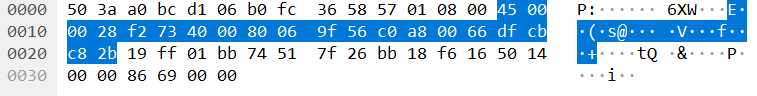
**B、捕获IP数据分组**

1、IP数据报报文格式

2、实验步骤

打开Wireshark，开启抓包，在过滤器一栏输入 ip.src eq 你要Ping的目标IP地址 or ip.dst eq 你要Ping的目标IP地址（如www.baidu.com,则输入 ip.src eq 61.135.169.121 or ip.dst eq 61.135.169.121），用来过滤IP。

命令提示符窗口输入 ping www.baidu.com,观察Wireshark中出现的新数据包，并分析数据包。



Encode分析如下：

Frame 3350: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{A1C9129E-1345-4E45-8F51-87974B691679}, id 0

Ethernet II, Src: CyberTAN\_58:57:01 (b0:fc:36:58:57:01), Dst: Shenzhen\_bc:d1:06 (50:3a:a0:bc:d1:06)

Destination: Shenzhen\_bc:d1:06 (50:3a:a0:bc:d1:06)

Address: Shenzhen\_bc:d1:06 (50:3a:a0:bc:d1:06)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Source: CyberTAN\_58:57:01 (b0:fc:36:58:57:01)

Address: CyberTAN\_58:57:01 (b0:fc:36:58:57:01)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 223.203.200.43

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

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

Total Length: 40

Identification: 0xf273 (62067)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x9f56 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.102

Destination: 223.203.200.43

Transmission Control Protocol, Src Port: 6655, Dst Port: 443, Seq: 989, Ack: 3736, Len: 0

Source Port: 6655

Destination Port: 443

[Stream index: 131]

[TCP Segment Len: 0]

Sequence number: 989 (relative sequence number)

Sequence number (raw): 1951498022

[Next sequence number: 989 (relative sequence number)]

Acknowledgment number: 3736 (relative ack number)

Acknowledgment number (raw): 3138975254

0101 .... = Header Length: 20 bytes (5)

Flags: 0x014 (RST, ACK)

000. .... .... = Reserved: Not set

...0 .... .... = Nonce: Not set

.... 0... .... = Congestion Window Reduced (CWR): Not set

.... .0.. .... = ECN-Echo: Not set

.... ..0. .... = Urgent: Not set

.... ...1 .... = Acknowledgment: Set

.... .... 0... = Push: Not set

.... .... .1.. = Reset: Set

.... .... ..0. = Syn: Not set

.... .... ...0 = Fin: Not set

[TCP Flags: ·······A·R··]

Window size value: 0

[Calculated window size: 0]

[Window size scaling factor: 256]

Checksum: 0x8669 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[Timestamps]

[Time since first frame in this TCP stream: 4.677887000 seconds]

[Time since previous frame in this TCP stream: 4.475056000 seconds]

IP分组格式为：



分析IP数据分组：

|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 | 包头长20字节 |
| 服务类型 | 00 | 正常时延正常吞吐量正常可靠性 |
| 总长度 | 0028 | 40 |
| 标识 | f273 | 标识为62607 |
| 标志 | 40 | DF=1 MF=0不允许分片 |
| 片偏移 | 00 | 偏移量为0 |
| 生存周期 | 80 | 每跳生存周期为128秒 |
| 协议 | 06 | 携带数据来自TCP协议 |
| 头部校验和 | 9f56 | 头部校验和为0x9f56 |
| 源地址 | c0a8 0066 | 源地址为192.168.0.102 |
| 目的地址 | dfcb c82b | 目的地址为223.203.200.43 |

**C、分析整个上网的工作过程，需要收发什么分组？每个分组的内容是什么？**

向默认网关发送一个DHCP REQUEST报文以申请获得IP地址。

网关收到报文后回送一个DHCP ACK

利用ARP数据报本机广播自己的地址映射关系，使其他主机知道当前主机的地址。

**D、捕获ICMP分组**

1、ICMP简介

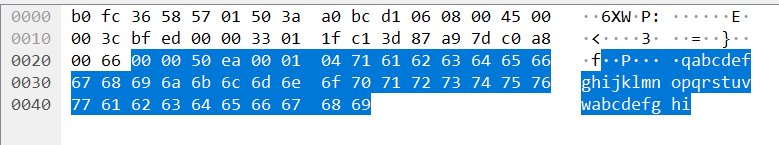
 ICMP是“Internet Control Message Protocol”（Internet控制消息协议）的缩写，它是TCP/IP协议族的一个子协议。用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息尽管并不传输用户数据。可是对于用户数据的传递起着关键的数据。ICMP报文作为IP层数据报的数据，加上数据报的首部，组成数据报发送出去。ICMP报文的种类有两种，即ICMP差错报告报文和ICMP询问报文。

2、ICMP分组格式

3、实验步骤

打开Wireshark，开启抓包，在过滤器一栏输入 icmp，使其只显示ICMP协议。

命令提示符窗口输入 ping www.baidu.com,观察Wireshark中出现的新数据包，并分析数据包。



Encode分析如下：

Frame 32390: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{A1C9129E-1345-4E45-8F51-87974B691679}, id 0

Ethernet II, Src: Shenzhen\_bc:d1:06 (50:3a:a0:bc:d1:06), Dst: CyberTAN\_58:57:01 (b0:fc:36:58:57:01)

Destination: CyberTAN\_58:57:01 (b0:fc:36:58:57:01)

Address: CyberTAN\_58:57:01 (b0:fc:36:58:57:01)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Source: Shenzhen\_bc:d1:06 (50:3a:a0:bc:d1:06)

Address: Shenzhen\_bc:d1:06 (50:3a:a0:bc:d1:06)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 61.135.169.125, Dst: 192.168.0.102

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

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

Total Length: 60

Identification: 0xbfed (49133)

Flags: 0x0000

Fragment offset: 0

Time to live: 51

Protocol: ICMP (1)

Header checksum: 0x1fc1 [validation disabled]

[Header checksum status: Unverified]

Source: 61.135.169.125

Destination: 192.168.0.102

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x50ea [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 1137 (0x0471)

Sequence number (LE): 28932 (0x7104)

[Request frame: 32389]

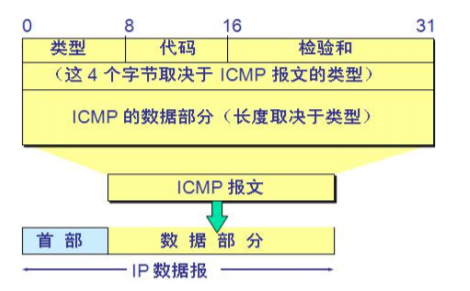
[Response time: 38.531 ms]

Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f707172737475767761…

[Length: 32]

ICMP分组格式：



分析ICMP分组：

|  |  |  |
| --- | --- | --- |
| 字段 | 报文（16进制） | 内容 |
| 类型 | 00 | Echo(ping) reply |
| 代码 | 00 |  |
| 校验和 | 5aea | 校验和为0x5aea |

**E、制作一个8000字节的IP数据分组，发送后捕获分析。由于分组长度大于1500字节，因此需要分片传输。按照2）中的方法分析所有分片的结构。**

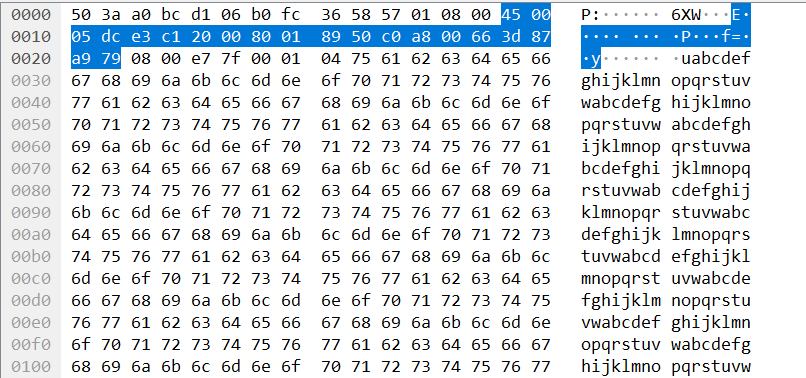
1、实验步骤

打开Wireshark，开启抓包，在过滤器一栏输入 ip.src eq 你要Ping的目标IP地址 or ip.dst eq 你要Ping的目标IP地址（如www.baidu.com,则输入 ip.src eq 61.135.169.121 or ip.dst eq 61.135.169.121），用来过滤IP。

命令提示符窗口输入 ping -l 8000 www.baidu.com（ping -l size ip 用来指定发送数据包的大小）,观察Wireshark中出现的新数据包，查看每个数据包的Fragment offset，分析所有分片的结构。

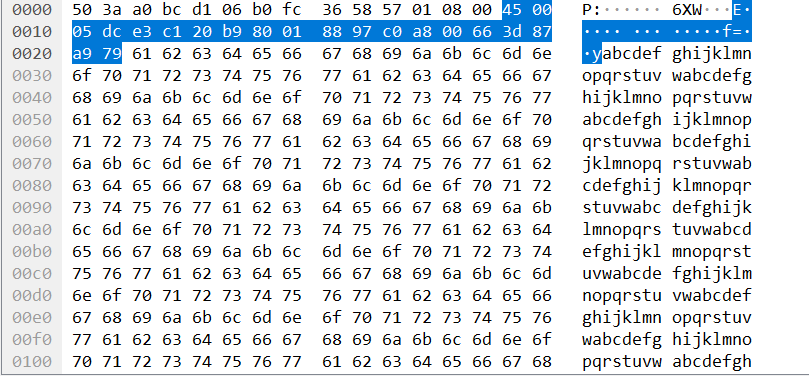
2.分片分析

第一个分片



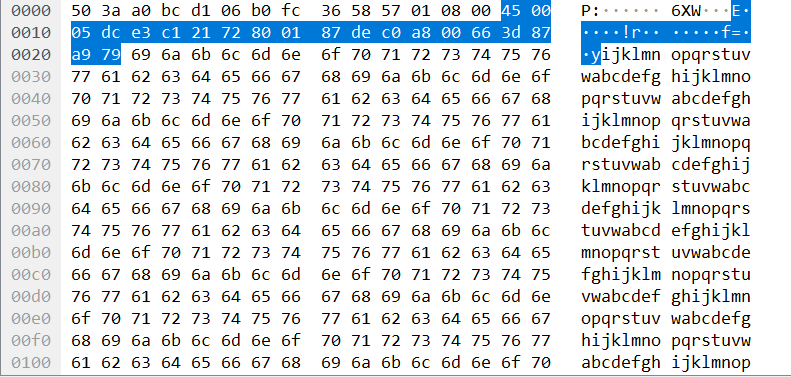
|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 | 包头长20字节 |
| 服务类型 | 00 | 正常时延正常吞吐量正常可靠性 |
| 总长度 | 05dc | 1500 |
| 标识 | e3c1 | 标识为58305 |
| 标志 | 20 | DF=0 MF=1允许分片且不是最后一片 |
| 片偏移 | 00 | 偏移量为0 |
| 生存周期 | 80 | 每跳生存周期为128秒 |
| 协议 | 01 | 携带数据来自ICMP(1)协议 |
| 头部校验和 | 8950 | 头部校验和为0x8950 |
| 源地址 | c0a8 0066 | 源地址为192.168.0.102 |
| 目的地址 | 3d87 a979 | 目的地址为61.135.169.121 |

第二个分片



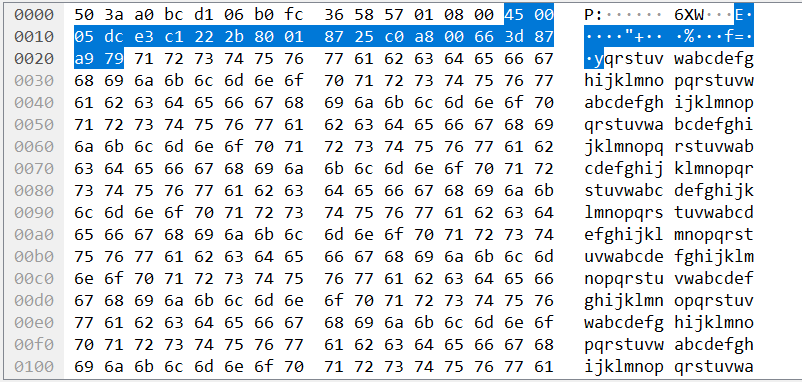
|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 | 包头长20字节 |
| 服务类型 | 00 | 正常时延正常吞吐量正常可靠性 |
| 总长度 | 05dc | 1500 |
| 标识 | e3c1 | 标识为58305 |
| 标志 | 20 | DF=0 MF=1允许分片且不是最后一片 |
| 片偏移 | b9 | 偏移量为1480 |
| 生存周期 | 80 | 每跳生存周期为128秒 |
| 协议 | 01 | 携带数据来自ICMP(1)协议 |
| 头部校验和 | 8897 | 头部校验和为0x8897 |
| 源地址 | c0a8 0066 | 源地址为192.168.0.102 |
| 目的地址 | 3d87 a979 | 目的地址为61.135.169.121 |

第三个分片



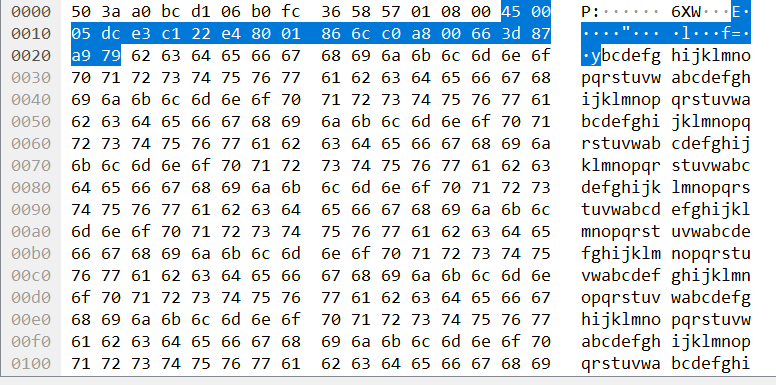
|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 | 包头长20字节 |
| 服务类型 | 00 | 正常时延正常吞吐量正常可靠性 |
| 总长度 | 05dc | 1500 |
| 标识 | e3c1 | 标识为58305 |
| 标志 | 21 | DF=0 MF=1允许分片且不是最后一片 |
| 片偏移 | 72 | 偏移量为2960 |
| 生存周期 | 80 | 每跳生存周期为128秒 |
| 协议 | 01 | 携带数据来自ICMP(1)协议 |
| 头部校验和 | 87de | 头部校验和为0x87de |
| 源地址 | c0a8 0066 | 源地址为192.168.0.102 |
| 目的地址 | 3d87 a979 | 目的地址为61.135.169.121 |

第四个分片



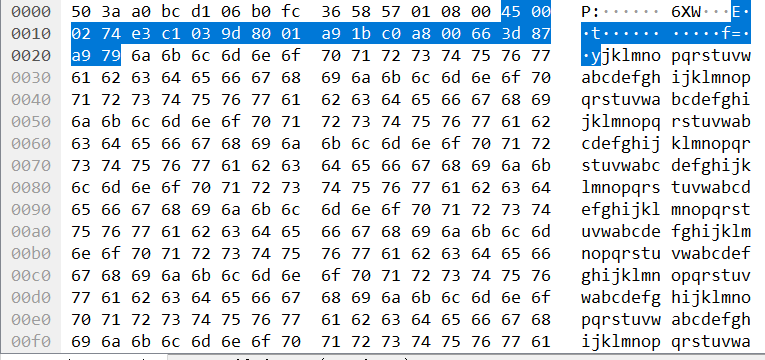
|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 | 包头长20字节 |
| 服务类型 | 00 | 正常时延正常吞吐量正常可靠性 |
| 总长度 | 05dc | 1500 |
| 标识 | e3c1 | 标识为58305 |
| 标志 | 22 | DF=0 MF=1允许分片且不是最后一片 |
| 片偏移 | 2b | 偏移量为4440 |
| 生存周期 | 80 | 每跳生存周期为128秒 |
| 协议 | 01 | 携带数据来自ICMP(1)协议 |
| 头部校验和 | 8725 | 头部校验和为0x8725 |
| 源地址 | c0a8 0066 | 源地址为192.168.0.102 |
| 目的地址 | 3d87 a979 | 目的地址为61.135.169.121 |

第五个分片



|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 | 包头长20字节 |
| 服务类型 | 00 | 正常时延正常吞吐量正常可靠性 |
| 总长度 | 05dc | 1500 |
| 标识 | e3c1 | 标识为58305 |
| 标志 | 22 | DF=0 MF=1允许分片且不是最后一片 |
| 片偏移 | e4 | 偏移量为5920 |
| 生存周期 | 80 | 每跳生存周期为128秒 |
| 协议 | 01 | 携带数据来自ICMP(1)协议 |
| 头部校验和 | 866c | 头部校验和为0x866c |
| 源地址 | c0a8 0066 | 源地址为192.168.0.102 |
| 目的地址 | 3d87 a979 | 目的地址为61.135.169.121 |

第六片分片



|  |  |  |
| --- | --- | --- |
| 字段 | 报文 | 内容 |
| 包头长度 | 45 | 包头长20字节 |
| 服务类型 | 00 | 正常时延正常吞吐量正常可靠性 |
| 总长度 | 0274 | 628 |
| 标识 | e3c1 | 标识为58305 |
| 标志 | 03 | DF=0 MF=0允许分片且是最后一片 |
| 片偏移 | 9d | 偏移量为7400 |
| 生存周期 | 80 | 每跳生存周期为128秒 |
| 协议 | 01 | 携带数据来自ICMP(1)协议 |
| 头部校验和 | a91b | 头部校验和为0xa91b |
| 源地址 | c0a8 0066 | 源地址为192.168.0.102 |
| 目的地址 | 3d87 a979 | 目的地址为61.135.169.121 |

上述前五个分组1500字节，净荷部分长度为1500 – 20 = 1480，五个共 1480 \* 5 = 7400；最后一个分组628字节，除了减去头部20字节以外，还要减去ICMP的8字节，净荷部分为628 – 20 – 8 = 600，7400 + 600 = 8000，总长度吻合，分片正确。

**六 实验总结**

（1）问题解决

完成本次实验花了大约2个小时左右，选择的时间是在周五晚上。

（2）心得体会

通过这次实验，我对课堂上介绍的各种分组的结构有了更加实际的认识，也理解得更加深刻。此外，在 wireshark 的智能性辅助下分析分组结构，让我感受到了 wireshark 的强大，却也增强了我今后独立分析分组结构的信心和决心。