# 北京邮电大学《计算机网络》课程实验报告

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **实验**  **名称** | **IP 和 TCP 数据分组的捕获和解析** | | **学 院** | 计算机 | **指导教师** |  |
| **班 级** | **班内序号** | **学 号** | | **学生姓名** | **成绩** | |
|  |  |  | |  |  | |
| **实**  **验**  **内**  **容** | 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。  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。  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。  分析 TCP 建立连接，拆除连接和数据通信的流程。 | | | | | |
| **学生实验报告** | （详见“实验报告”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。

目录

[北京邮电大学《计算机网络》课程实验报告 1](#_Toc137067948)

[一、 实验目的 2](#_Toc137067949)

[二、 实验环境 2](#_Toc137067950)

[三、 实验步骤及结果分析 3](#_Toc137067951)

[1. 捕获 DHCP 报文并分析 3](#_Toc137067952)

[1.1 DHCP概述 3](#_Toc137067953)

[1.2 DHCP报文的捕获 5](#_Toc137067954)

[1.3 DHCP报文的分析 8](#_Toc137067955)

[2. 获取ARP分组并分析 12](#_Toc137067956)

[2.1 ARP概述 12](#_Toc137067957)

[2.2 ARP报文的捕获 13](#_Toc137067958)

[2.3 ARP报文的分析 14](#_Toc137067959)

[3. 获取IP/ICMP分组并分析 14](#_Toc137067960)

[3.1 IP/ICMP概述 14](#_Toc137067961)

[3.2 IP报文的捕获 15](#_Toc137067962)

[3.3 IP报文的分析 17](#_Toc137067963)

[4. 获取TCP分组并分析 18](#_Toc137067964)

[4.1 TCP概述 18](#_Toc137067965)

[4.2 TCP报文的捕获 19](#_Toc137067966)

[4.3 TCP报文的分析 20](#_Toc137067967)

[五、 实验总结 26](#_Toc137067968)

## 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。

4. 分析 TCP 建立连接，拆除连接和数据通信的流程。

## 实验环境

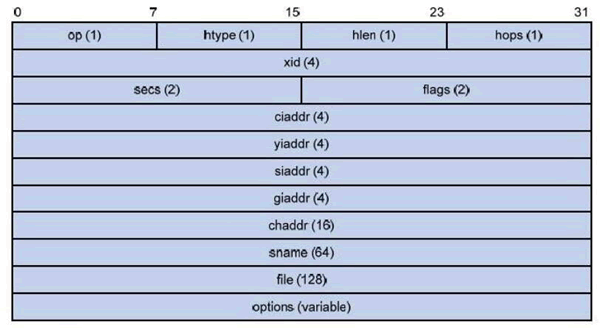
1. Windows 操作系统的 PC 机，要求能够连接到 Internet.
2. WireShark 软件。

## 实验步骤及结果分析

## 捕获 DHCP 报文并分析

## DHCP概述

1. DHCP（Dynamic Host Configuration Protocol，动态主机配置协议），用于局域网环境，主要作用是集中管理、分配IP地址，使客户端动态获得IP地址、Gateway地址、DNS服务器地址，提升地址的利用率。
2. DHCP报文格式：



（1）op：报文的操作类型。分为请求报文和响应报文。客户端发送给服务器的包为请求报文，值为 1；服务器发送给客户端的包为响应报文，值为 2。

（2）htype：DHCP 客户端的 MAC 地址类型。MAC 地址类型其实是指明网络类型，htype 值为 1 时表示为最常见的以太网 MAC 地址类型。

（3）hlen：硬件地址长度。以太网 MAC 地址长度为 6 个字节，即 hlen 值为 6。

（4）hops：跳数，DHCP 报文经过的中继数量。每经过一个路由器，该字段就会增加 1。如果没有经过路由器，则值为 0（同一网内）。

（5）xid：事务 ID。客户端发起一次请求时选择的随机数，用来标识一次地址请求过程。在一次请求中所有报文的 xid 都是一样的。

（6）secs：DHCP 客户端从获取到 IP 地址或者续约过程开始到现在所过去的时间，以秒为单位。在没有获得 IP 地址前，该字段始终为 0。

（7）flags：BOOTP 标志位。只使用第 0 比特位，是广播应答标识位，用来标识 DHCP 服务器应答报文是采用单播还是广播发送。其中，0 表示采用单播发送方式，1 表示采用广播发送方式。其余位尚未使用。

（8）ciaddr：DHCP 客户端的 IP 地址。仅在 DHCP 服务器发送的 ACK 报文中显示，在其他报文中均显示为 0。这是因为在得到 DHCP 服务器确认前，DHCP 客户端还没有分配到 IP 地址。

（9）yiaddr：DHCP 服务器分配给客户端的 IP 地址。仅在 DHCP 服务器发送的 Offer 和 ACK 报文中显示，其他报文中显示为 0。

（10）siaddr：为 DHCP 客户端分配 IP 地址等信息的其他 DHCP 服务器 IP 地址。仅在 DHCP Offer、DHCP ACK 报文中显示，其他报文中显示为 0。

（11）giaddr：转发代理（网关）IP 地址，DHCP 客户端发出请求报文后经过的第一个 DHCP 中继的 IP 地址。如果没有经过 DHCP 中继，则显示为 0。

（12）chaddr：DHCP 客户端的 MAC 地址。在每个报文中都会显示对应 DHCP 客户端的 MAC 地址。

（13）sname：为客户端分配 IP 地址的服务器名称（DNS 域名格式）。只在 DHCP Offer 和 DHCP ACK 报文中显示发送报文的 DHCP 服务器名称，其他报文显示为 0。

（14）file：DHCP 服务器为 DHCP 客户端指定的启动配置文件名称及路径信息。仅在 DHCP Offer 报文中显示，其他报文中显示为空。

（15）options：可选选项，格式为“代码+长度+数据”。

3. DHCP报文一共有八种：

(1) Discover(0x01)

DHCP客户端在请求IP地址时并不知道DHCP服务器的位置，因此DHCP客户端会在本地网络内以广播方式发送Discover请求报文，以发现网络中的DHCP服务器。所有收到Discover报文的DHCP服务器都会发送应答报文，DHCP客户端据此可以知道网络中存在的DHCP服务器的位置。

(2) Offer(0x02)

DHCP服务器收到Discover报文后，就会在所配置的地址池中查找一个合适的IP地址，加上相应的租约期限和其他配置信息（如网关、DNS服务器等），构造一个Offer报文，发送给DHCP客户端，告知用户本服务器可以为其提供IP地址。但这个报文只是告诉DHCP客户端可以提供IP地址，最终还需要客户端通过ARP来检测该IP地址是否重复。

(3) Request(0x03)

DHCP客户端可能会收到很多Offer请求报文，所以必须在这些应答中选择一个。通常是选择第一个Offer应答报文的服务器作为自己的目标服务器，并向该服务器发送一个广播的Request请求报文，通告选择的服务器，希望获得所分配的IP地址。另外，DHCP客户端在成功获取IP地址后，在地址使用租期达到50%时，会向DHCP服务器发送单播Request请求报文请求续延租约，如果没有收到ACK报文，在租期达到87.5%时，会再次发送广播的Request请求报文以请求续延租约。

(4) Decline(0x04)

DHCP客户端收到DHCP服务器ACK应答报文后，通过地址冲突检测发现服务器分配的地址冲突或者由于其他原因导致不能使用，则会向DHCP服务器发送Decline请求报文，通知服务器所分配的IP地址不可用，以期获得新的IP地址。

(5) ACK(0x05)

DHCP服务器收到Request请求报文后，根据Request报文中携带的用户MAC来查找有没有相应的租约记录，如果有则发送ACK应答报文，通知用户可以使用分配的IP地址。

(6) NAK(0x06)

如果DHCP服务器收到Request请求报文后，没有发现有相应的租约记录或者由于某些原因无法正常分配IP地址，则向DHCP客户端发送NAK应答报文，通知用户无法分配合适的IP地址。

(7) Release(0x07)

当DHCP客户端不再需要使用分配IP地址时（一般出现在客户端关机、下线等状况）就会主动向DHCP服务器发送RELEASE请求报文，告知服务器用户不再需要分配IP地址，请求DHCP服务器释放对应的IP地址。

(8) Inform(0x08)

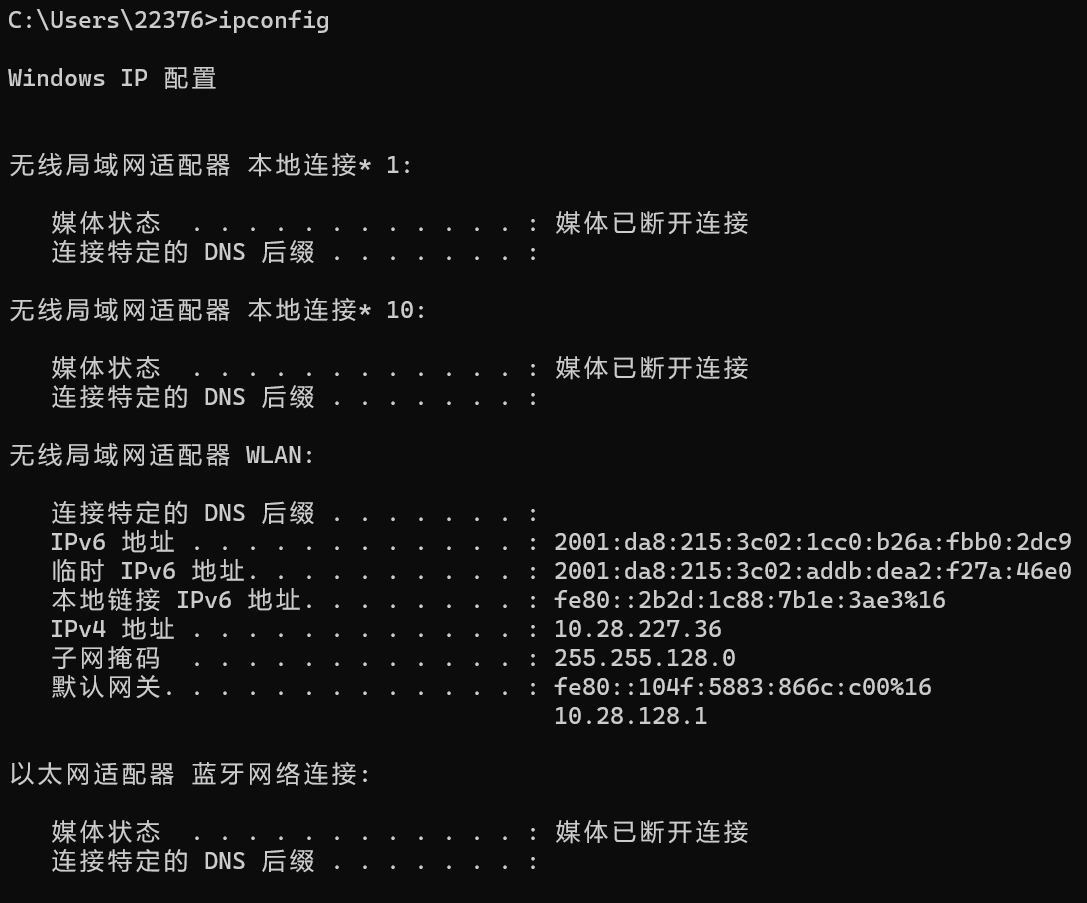
DHCP客户端如果需要从DHCP服务器端获取更为详细的配置信息，则向DHCP服务器发送Inform请求报文；DHCP服务器在收到该报文后，将根据租约进行查找到相应的配置信息后，向DHCP客户端发送ACK应答报文。目前基本上不用了。

## DHCP报文的捕获

第一步：运行Wireshark软件，在首页选择进行连接的网络，这里选择WLAN

第二步：设置 WirkShark 显示过滤器，在工作画面 Filter 设置 udp.port==68,这样在捕获的报文中，仅显示 UDP 端口号 68 的报文（DHCP 报文）

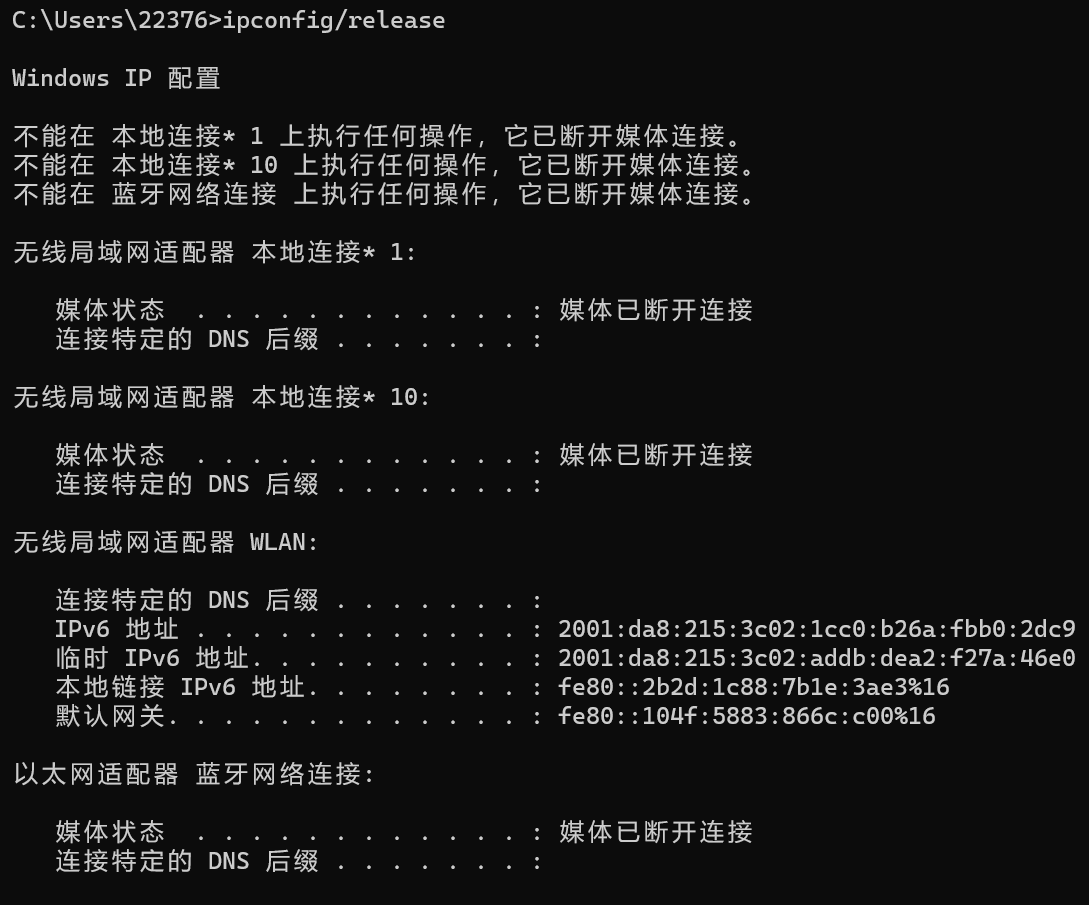
第三步： 打开命令提示符窗口，执行ipconfig，查看未释放IP地址前本机IP地址。



图一：执行ipconfig查看释放前的IP地址

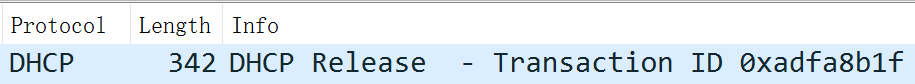
可以看到，释放前的IP地址为10.28.227.36

第四步：执行ipconfig/release释放已经申请的IP地址



图二：执行ipconfig/release释放已经申请的IP地址

可以看到，释放已经申请的IP地址对无线局域网起作用，显示已经断开连接。在Wireshark中抓到DHCP的Release报文：



第五步：执行ipconfig命令查看释放IP地址后的IP地址。



图三：释放完IP地址后执行ipconfig命令

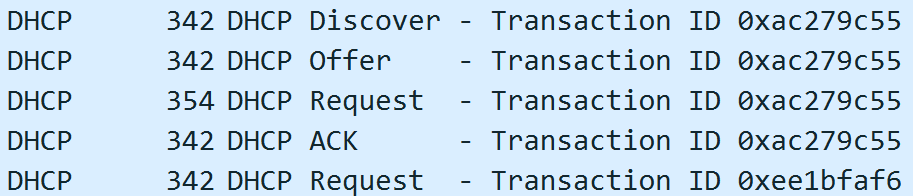
释放完IP地址后显示的IP地址是自动配置的IP地址：169.254.91.210

第六步：执行ipconfig/renew，获取新的IP地址

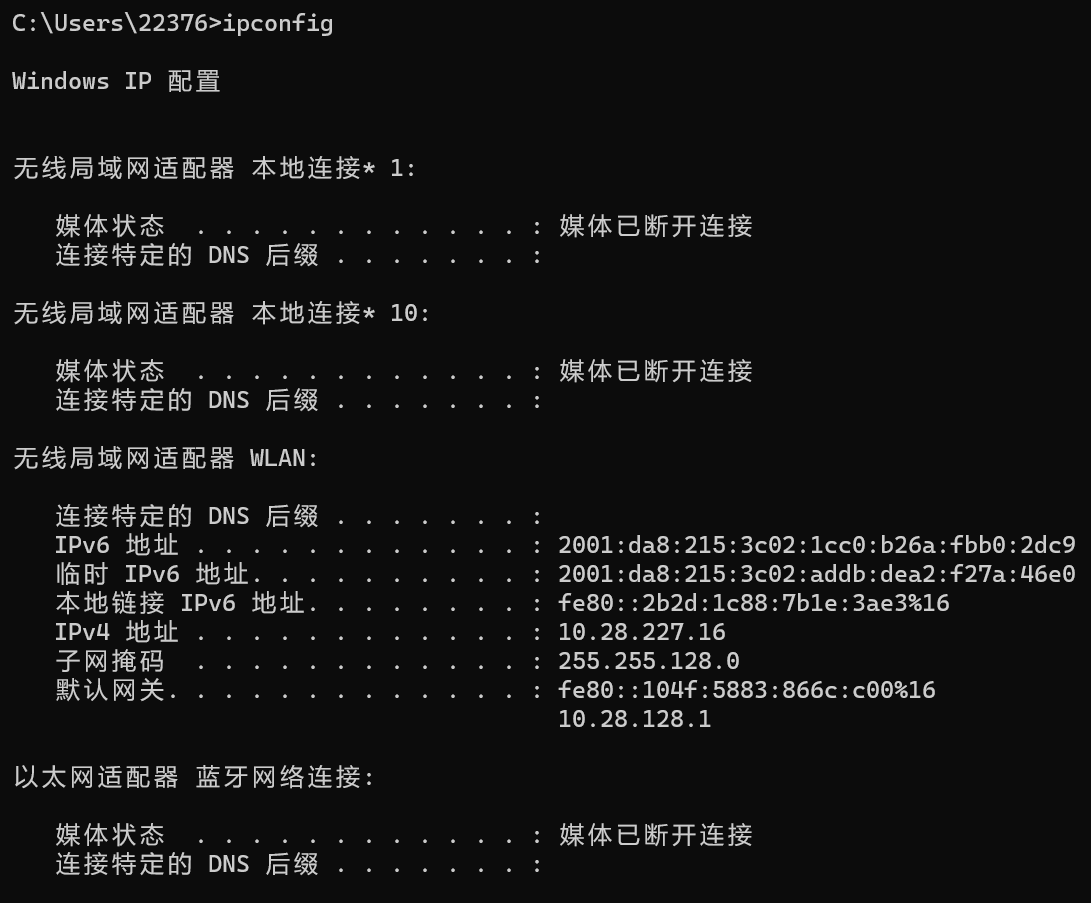


图四：执行ipconfig/renew，获取新的IP地址

可以看到，获取的新的IP地址为10.28.227.16，这与之前的IP地址10.28.227.36不同。在这个过程中，Wireshark抓到四个报文：



第七步：执行ipconfig查看新获取到的IP地址



图五：执行ipconfig，显示新的IP地址

## DHCP报文的分析

分析在执行ipconfig/renew后抓到的报文信息。下面四个报文实现了四次握手。

1. Discover报文：
2. 总体信息：

源地址：0.0.0.0，目的地址：255.255.255.255，协议：DHCP，长度：342字节。

DHCP客户端会在本地网络内以广播方式发送Discover请求报文，以发现网络中的DHCP服务器。

1. 详细分析：

0000 ff ff ff ff ff ff c4 23 60 0b 54 64 08 00 45 00 .......#`.Td..E.

0010 01 48 52 09 00 00 80 11 00 00 00 00 00 00 ff ff .HR.............

0020 ff ff 00 44 00 43 01 34 8a 7c 01 01 06 00 ac 27 ...D.C.4.|.....'

0030 9c 55 0d 00 80 00 00 00 00 00 00 00 00 00 00 00 .U..............

0040 00 00 00 00 00 00 c4 23 60 0b 54 64 00 00 00 00 .......#`.Td....

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0110 00 00 00 00 00 00 63 82 53 63 35 01 01 3d 07 01 ......c.Sc5..=..

0120 c4 23 60 0b 54 64 32 04 0a 1c e3 24 0c 07 48 50 .#`.Td2....$..HP

0130 5a 68 61 6e 58 3c 08 4d 53 46 54 20 35 2e 30 37 ZhanX<.MSFT 5.07

0140 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 fc ff ......!+,./wy...

0150 00 00 00 00 00 00 ......

从编号0开始第284字节为0x01，代表该报文是Discover报文。

0-5字节是0xff ff ff ff ff ff，代表目的MAC地址为ff:ff:ff:ff:ff:ff

6-11字节是0xc4 23 60 0b 54 64，代表源MAC地址为IntelCor\_0b:54:64

26-29字节是0x00 00 00 00，代表源IP地址为0.0.0.0

33-33字节是0xff ff ff ff，代表目的IP地址为255.255.255.255

34-35字节是0x00 44，代表UDP协议源端口号为68.

36-37字节是0x00 43，代表UDP协议目的端口号为67.

这些信息说明该报文被客户端以广播形式在本地网络发送。完成第一次握手，寻找DHCP服务器。

1. Offer报文：

（1） 总体信息：

源地址：10.3.9.2，目的地址：255.255.255.255，协议：DHCP，长度：342字节。

DHCP服务器收到Discover报文后，就会在所配置的地址池中查找一个合适的IP地址，加上相应的租约期限和其他配置信息（如网关、DNS服务器等），构造一个Offer报文，发送给DHCP客户端，告知用户本服务器可以为其提供IP地址。

（2） 详细分析：

0000 c4 23 60 0b 54 64 10 4f 58 6c 0c 00 08 00 45 00 .#`.Td.OXl....E.

0010 01 48 b1 92 40 00 3b 11 7a 0e 0a 03 09 02 ff ff .H..@.;.z.......

0020 ff ff 00 43 00 44 01 34 00 00 02 01 06 01 ac 27 ...C.D.4.......'

0030 9c 55 0d 00 80 00 00 00 00 00 0a 1c e3 10 00 00 .U..............

0040 00 00 0a 1c 80 01 c4 23 60 0b 54 64 00 00 00 00 .......#`.Td....

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0110 00 00 00 00 00 00 63 82 53 63 35 01 02 36 04 0a ......c.Sc5..6..

0120 03 09 02 33 04 00 00 1c 20 01 04 ff ff 80 00 03 ...3.... .......

0130 04 0a 1c 80 01 06 08 0a 03 09 2d 0a 03 09 2c ff ..........-...,.

0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0150 00 00 00 00 00 00 ......

从编号0开始第284字节为0x02，代表该报文是Offer报文。

0-5字节是0xc4 23 60 0b 54 64，代表目的MAC地址为IntelCor\_0b:54:64

6-11字节是0x10 4f 58 6c 0c 00，代表源MAC地址为ArubaaHe\_6c:0c:00

26-29字节是0x0a 03 09 02，代表源IP地址为10.3.9.2

33-33字节是0xff ff ff ff，代表目的IP地址为255.255.255.255

34-35字节是0x00 43，代表UDP协议源端口号为67.

36-37字节是0x00 44，代表UDP协议目的端口号为68.

58-61字节是0x0a 1c e3 10，代表DHCP服务器找的的合适的IP地址是10.28.277.16

287-290字节是0x0a 03 09 02，代表DHCP服务器的IP地址是10.3.9.2

293-296字节是0x00 00 1c 20，代表IP地址的租期是7200s（两小时）

299-302字节是0xff ff 80 00，代表子网掩码是255.255.128.0

305-308字节是0x0a 1c 80 01，代表DHCP中继代理路由器的地址为10.28.128.1

311-314字节是0x0a 03 09 2d，代表DNS服务器的地址是10.3.9.45

315-318字节是0x0a 03 09 2c，代表另一个DNS服务器地址是10.3.9.44

这些信息说明DHCP服务器向客户端提供IP地址，实现第二次握手。需要注意的是，DHCP服务器和DHCP客户端并没有在一个子网里，DHCP客户端通过访问同一个子网下的代理路由器来与DHCP服务器取得连接。

1. Request报文：

（1） 总体信息：

源地址：0.0.0.0，目的地址：255.255.255.255，协议：DHCP，长度：342字节。

DHCP客户端可能会收到很多Offer请求报文，所以必须在这些应答中选择一个。通常是选择第一个Offer应答报文的服务器作为自己的目标服务器，并向该服务器发送一个广播的Request请求报文，通告选择的服务器，希望获得所分配的IP地址。

（2） 逐段分析：

0000 ff ff ff ff ff ff c4 23 60 0b 54 64 08 00 45 00 .......#`.Td..E.

0010 01 54 52 0a 00 00 80 11 00 00 00 00 00 00 ff ff .TR.............

0020 ff ff 00 44 00 43 01 40 d8 f6 01 01 06 00 ac 27 ...D.C.@.......'

0030 9c 55 0d 00 80 00 00 00 00 00 00 00 00 00 00 00 .U..............

0040 00 00 00 00 00 00 c4 23 60 0b 54 64 00 00 00 00 .......#`.Td....

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0110 00 00 00 00 00 00 63 82 53 63 35 01 03 3d 07 01 ......c.Sc5..=..

0120 c4 23 60 0b 54 64 32 04 0a 1c e3 10 36 04 0a 03 .#`.Td2.....6...

0130 09 02 0c 07 48 50 5a 68 61 6e 58 51 0a 00 00 00 ....HPZhanXQ....

0140 48 50 5a 68 61 6e 58 3c 08 4d 53 46 54 20 35 2e HPZhanX<.MSFT 5.

0150 30 37 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 07......!+,./wy.

0160 fc ff ..

从编号0开始第284字节为0x03，代表该报文是Request报文。

0-5字节是0xff ff ff ff ff ff，代表目的MAC地址为ff:ff:ff:ff:ff:ff

6-11字节是0xc4 23 60 0b 54 64，代表源MAC地址为IntelCor\_0b:54:64

26-29字节是0x00 00 00 00，代表源IP地址为0.0.0.0

33-33字节是0xff ff ff ff，代表目的IP地址为255.255.255.255

34-35字节是0x00 44，代表UDP协议源端口号为68.

36-37字节是0x00 43，代表UDP协议目的端口号为67.

296-299字节是0x0a 1c e3 10，代表客户端请求的IP地址是10.28.227.16

以上信息表面客户端以广播形式发送Request报文，向DHCP服务器请求的IP地址是：10.28.227.16。完成第三次握手，客户端接受DHCP服务器的IP续约服务并发送请求。

4. ACK报文：

（1） 总体信息：

源地址：10.3.9.2，目的地址：10.28.227.16，协议：DHCP，长度：342字节。

DHCP服务器收到Request请求报文后，根据Request报文中携带的用户MAC来查找有没有相应的租约记录，如果有则发送ACK应答报文，以单播方式通知用户可以使用分配的IP地址。

1. 逐段分析：

0000 c4 23 60 0b 54 64 10 4f 58 6c 0c 00 08 00 45 00 .#`.Td.OXl....E.

0010 01 48 8e e8 40 00 3b 11 af 8b 0a 03 09 02 0a 1c .H..@.;.........

0020 e3 10 00 43 00 44 01 34 2f 14 02 01 06 00 ee 1b ...C.D.4/.......

0030 fa f6 00 00 00 00 0a 1c e3 10 0a 1c e3 10 00 00 ................

0040 00 00 00 00 00 00 c4 23 60 0b 54 64 00 00 00 00 .......#`.Td....

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0110 00 00 00 00 00 00 63 82 53 63 35 01 05 36 04 0a ......c.Sc5..6..

0120 03 09 02 33 04 00 00 1b fd 01 04 ff ff 80 00 03 ...3............

0130 04 0a 1c 80 01 06 08 0a 03 09 2c 0a 03 09 2d ff ..........,...-.

0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0150 00 00 00 00 00 00 ......

从编号0开始第284字节为0x05，代表该报文是ACK报文。

0-5字节是0xc4 23 60 0b 54 64，代表目的MAC地址为IntelCor\_0b:54:64

6-11字节是0x10 4f 58 6c 0c 00，代表源MAC地址为ArubaaHe\_6c:0c:00

26-29字节是0x0a 03 09 02，代表源IP地址为10.3.9.2

33-33字节是0x0a 1c e3 10，代表目的IP地址为10.28.227.16

34-35字节是0x00 43，代表UDP协议源端口号为67.

36-37字节是0x00 44，代表UDP协议目的端口号为68.

58-61字节是0x0a 1c e3 10，代表客户端IP地址是10.28.277.16

287-290字节是0x0a 03 09 02，代表DHCP服务器的IP地址是10.3.9.2

293-296字节是0x00 00 1b fd，代表IP地址的租期还有7165s

299-302字节是0xff ff 80 00，代表子网掩码是255.255.128.0

305-308字节是0x0a 1c 80 01，代表DHCP中继代理路由器的地址为10.28.128.1

311-314字节是0x0a 03 09 2d，代表DNS服务器的地址是10.3.9.45

315-318字节是0x0a 03 09 2c，代表另一个DNS服务器地址是10.3.9.44

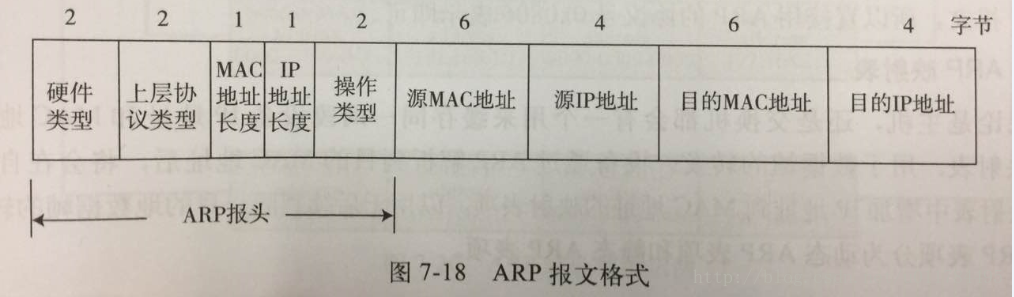
以上信息表明，DHCP服务器以单播的形式回复给客户端ACK，将客户端的续约请求确认。需要主义的是，续约的租期减少了35秒，这是因为续约时间在DHCP服务器发出Offer报文时就启动计时并减少。这完成了第四次握手，至此，DHCP服务完成。

## 2. 获取ARP分组并分析

## 2.1 ARP概述

1. ARP（Address Resolution Protocol），是根据IP地址获取物理地址的一个TCP/IP协议。每一个主机都设有一个 ARP 高速缓存(ARP cache)，里面有所在的局域网上的各主机和路由器的 IP 地址到硬件地址的映射表。

2. ARP报文格式：



（1）硬件类型：占两字节，表示ARP报文可以在哪种类型的网络上传输，值为1时表示为以太网地址。

（2）上层协议类型：占两字节，表示硬件地址要映射的协议地址类型，映射IP地址时的值为0x0800。

（3）MAC地址长度：占一字节，标识MAC地址长度，以字节为单位，此处为6。

（4）IP协议地址长度：占一字节，标识IP得知长度，以字节为单位，此处为4。

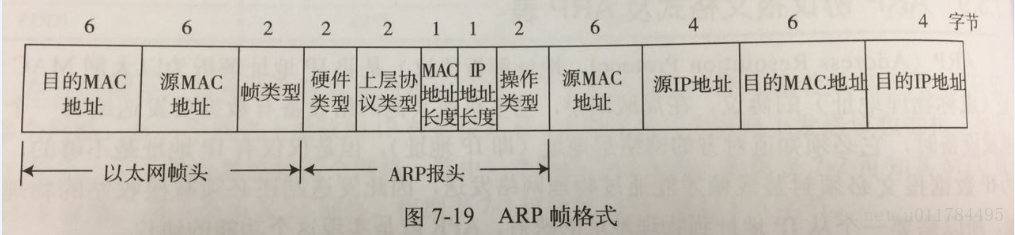
（5）操作类型：占2字节，指定本次ARP报文类型。1标识ARP请求报文，2标识ARP应答报文。

（6）源MAC地址：占6字节，标识发送设备的硬件地址。

（7）源IP地址：占4字节，标识发送方设备的IP地址。

（8）目的MAC地址：占6字节，表示接收方设备的硬件地址，在请求报文中该字段值全为0，即00-00-00-00-00-00，表示任意地址，因为现在不知道这个MAC地址。

（9）目的IP地址：占4字节，表示接受方的IP地址。



（1）目的MAC地址：占6字节，如果是ARP请求帧，因为它是一个广播帧，所以要填上广播MAC地址（FF-FF-FF-FF-FF-FF），其目标主机是网络上的所有主机。

（2）源MAC地址：占6字节，这是发送ARP帧的节点MAC地址。

（3）帧类型：占两字节，这里用来标识帧封装的上层协议，因为本帧的数据部分是ARP报文，所以直接用ARP的协议号0x0806表示就可以了。

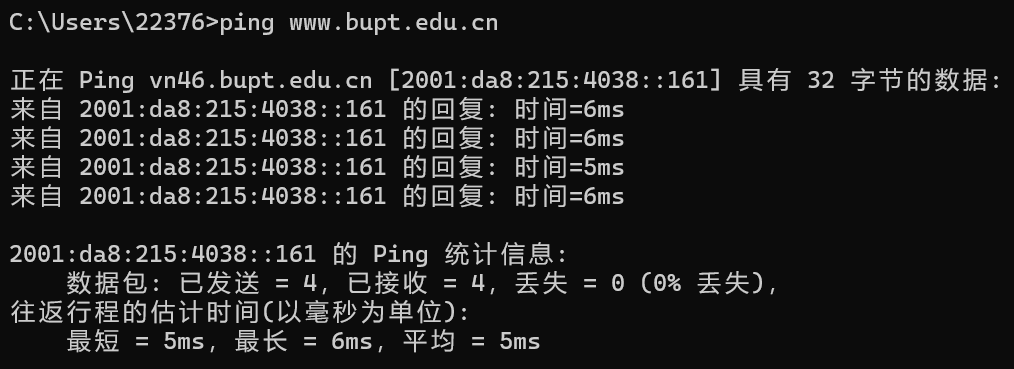
1. ARP报文种类：
2. ARP请求报文
3. ARP应答报文

## ARP报文的捕获

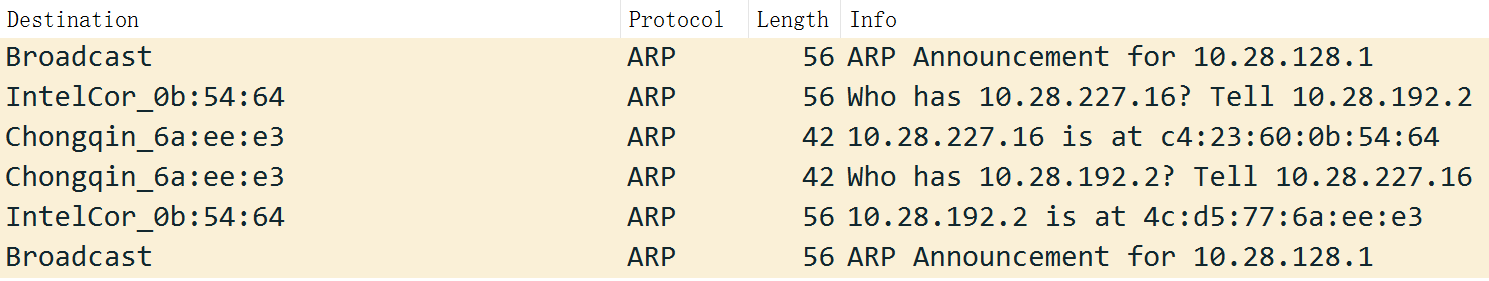
第一步：运行Wireshark软件，在首页选择进行连接的网络，选择WLAN

第二步：在应用显示过滤器中输入arp，过滤出ARP报文

第三步：打开命令提示符窗口，输入ping www.bupt.edu.cn，回车执行



第四步：观察Wireshark中抓到的报文。



## ARP报文的分析

1. ARP请求报文
2. 总体信息：

源：ArubaaHe\_6c:0c:00，目的：Broadcast，协议类型：ARP，长度：56字节，信息：ARP Announcement for 10.28.128.1

1. 详细分析：

0000 ff ff ff ff ff ff 10 4f 58 6c 0c 00 08 06 00 01 .......OXl......

0010 08 00 06 04 00 01 10 4f 58 6c 0c 00 0a 1c 80 01 .......OXl......

0020 00 00 00 00 00 00 0a 1c 80 01 a9 84 58 00 00 00 ............X...

0030 00 01 ff 03 d5 20 00 00 ..... ..

从编号0开始，第20-21字节为0x00 01，代表该报文种类为请求报文。

0-5字节为0xff ff ff ff ff ff，代表目的MAC地址为ff:ff:ff:ff:ff:ff

6-11字节为0x10 4f 58 6c 0c 00，代表源MAC地址为ArubaaHe\_6c:0c:00

28-31字节为0x0a 1c 80 01，代表源IP地址为10.28.128.1

38-41字节为0x0a 1c 80 01，代表目的IP地址为10.28.128.1

以上信息表明，ARP请求10.28.128.1的MAC地址。

1. ARP应答报文
2. 总体信息：

源：IntelCor\_0b:54:64，目的：Chongqin\_6a:ee:e3，协议类型：ARP，长度：42字节，信息：10.28.227.16 is at c4:23:60:0b:54:64

1. 详细分析：

0000 4c d5 77 6a ee e3 c4 23 60 0b 54 64 08 06 00 01 L.wj...#`.Td....

0010 08 00 06 04 00 02 c4 23 60 0b 54 64 0a 1c e3 10 .......#`.Td....

0020 4c d5 77 6a ee e3 0a 1c c0 02 L.wj......

从编号0开始，第20-21字节为0x00 02，代表该报文种类为应答报文。

0-5字节为0x4c d5 77 6a ee e3，代表目的MAC地址为Chongqin\_6a:ee:e3

6-11字节为0x c4 23 60 0b 54 64，代表源MAC地址为IntelCor\_0b:54:64

22-27字节为0x c4 23 60 0b 54 64，代表源MAC地址为IntelCor\_0b:54:64

28-31字节为0x0a 1c e3 10，代表源IP地址为10.28.227.16

32-37字节为0x4c d5 77 6a ee e3，代表目的MAC地址为Chongqin\_6a:ee:e3

38-41字节为0x0a 1c c0 02，代表目的IP地址为10.28.192.2

以上信息表面ARP请求10.28.227.16的MAC地址是IntelCor\_0b:54:64

## 3. 获取IP/ICMP分组并分析

## 3.1 IP/ICMP概述

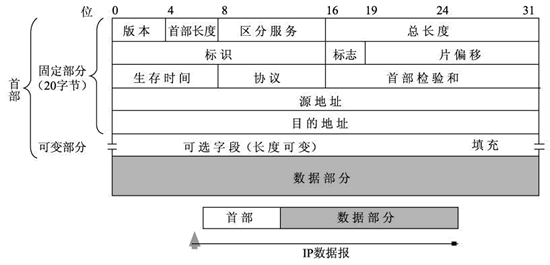
1. IP 协议（Internet Protocol，互联网协议）是 TCP/IP 协议栈中最核心的协议之一。它通过 IP 地址，保证了联网设备的唯一性，实现了网络通信的面向无连接和不可靠的传输功能。IP 协议负责将网络层的 IP 数据报（IP 分组）传输到链路层，由链路层将数据封装成帧。帧最多只能封装 1500 字节（默认）的数据，当超过上限时，就需要分割数据，放到多个数据帧中传输，到达目标主机后，再将数据重组起来。

ICMP（Internet Control Message Protocol，因特网控制报文协议）是 TCP/IP 协议族中的一个重要子协议，通常被 IP 层或更高层协议（TCP 或 UDP）使用，属于网络层协议。它主要用于在 IP 主机和路由器之间传递控制消息，用于报告主机是否可达、路由是否可用等。

ICMP 报文被封装在 IP 数据包内部，作为 IP 数据包的数据部分通过互联网传递。当数据包处理过程出现差错时，ICMP 向数据包的源端设备报告这个差错，它既不会纠正这个差错，也不会通知中间的网络设备。

IP 数据报是 Internet Protocol 的缩写，它是 TCP/IP 协议族中的一个重要子协议。IP 数据报是指在 IP 网络上传输的数据包。IP 数据报由首部和数据两个部分组成。首部的前部分属于固定部分，占 20 个字节；后面部分属于可变部分，长度是可变的。

2. IP数据报格式：



IP 数据报就是 IP 协议传输的数据，它有固定的格式。IP 数据报的格式是固定的，由首部（称为报头）和数据两部分组成。首部的前一部分是固定长度，共 20 字节，是所有 IP 数据报必须具有的。在首部的固定部分的后面是一些可选字段，其长度是可变的。每个 IP 数据报都以一个 IP 报头开始。源计算机构造这个 IP 报头，而目的计算机利用 IP 报头中封装的信息处理数据。IP 报头中包含大量的信息，如源 IP 地址、目的 IP 地址、数据报长度、IP 版本号等。每个信息都被称为一个字段。

1. IP数据报种类：

如果数据过大，则对IP数据报进行分片，每一片称为Ipv4分组。

1. 允许分片的IP数据报
2. 不允许分片的IP数据报

## IP报文的捕获

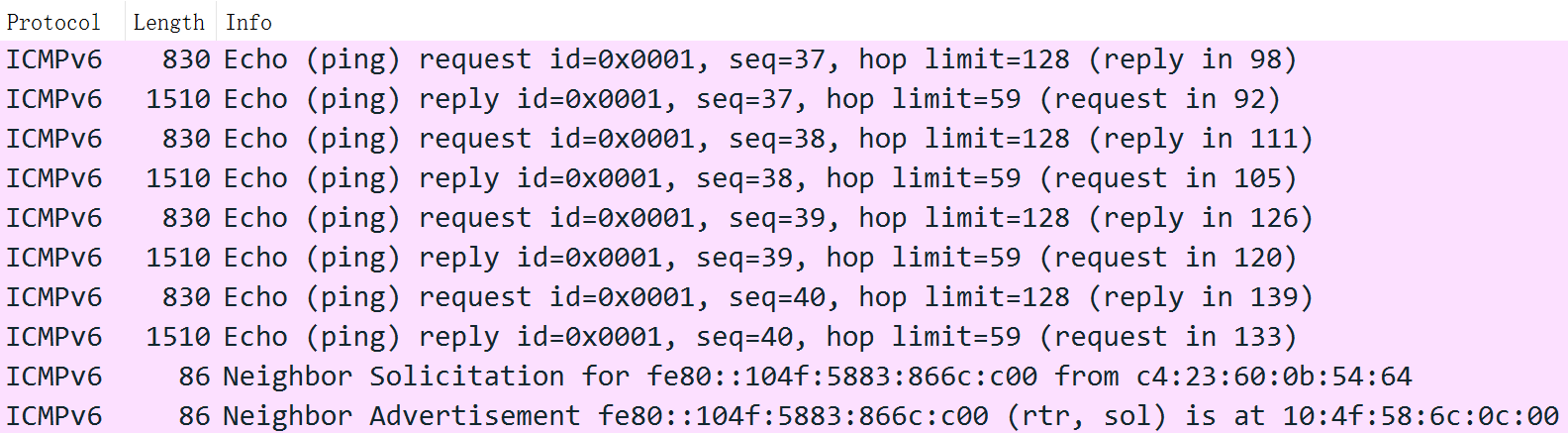
1. 第一步：运行Wireshark软件，在首页选择进行连接的网络，选择WLAN

2. 第二步：在应用显示过滤器中输入icmpv6，过滤出ICMP报文（ICMP 分组是一种特殊的 IP 分组，它的数据部分包含了 ICMP 报文），在北邮校园网内使用的是IPv6地址，因此过滤选项为icmpv6而不是icmp

3． 第三步：打开命令提示符窗口，输入ping -l 8000 www.bupt.edu.cn，回车执行。这个命令会向 www.bupt.edu.cn 发送一个大小为 8000 字节的 ICMP 回显请求数据包。-l 参数用于指定发送缓冲区大小。

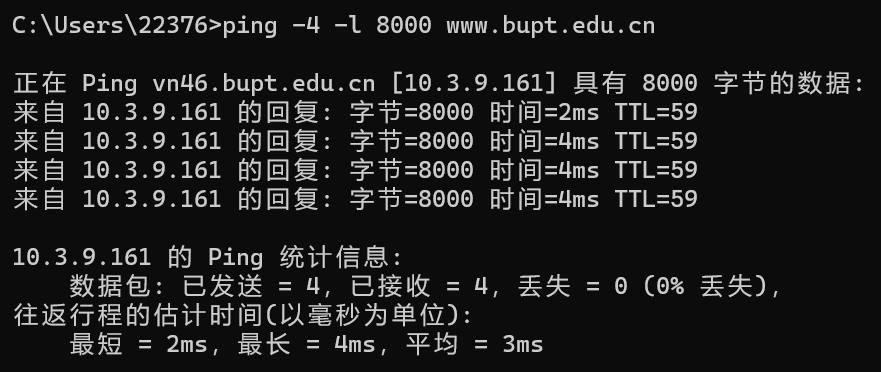


1. 第四步：观察Wireshark中抓到的包

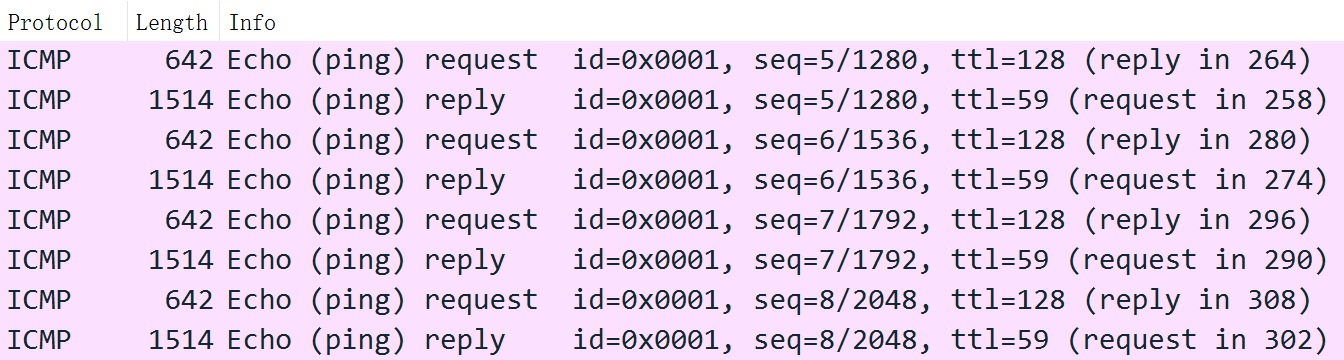


分析IPv6数据报格式，发现其中并没有片偏移段，IPv6的数据报格式要比IPv4简单，简化了路由器对数据报的处理过程，这与我们的实验目的不同，我们的实验目的是为了着重分析IP数据报的分段。因此，选择重新设置参数并抓包。

1. 运行Wireshark软件，在首页选择进行连接的网络，选择WLAN
2. 在应用显示过滤器中输入icmp，过滤出ICMP报文
3. 打开命令提示符窗口，输入ping -4 -l 8000 www.bupt.edu.cn，回车执行。该命令用于向 www.bupt.edu.cn 发送一个大小为 8000 字节的 ICMP 回显请求数据包，并强制使用 IPv4 协议。



1. 观察Wireshark中抓到的包



## IP报文的分析

1. 分析抓到的第一个IPv4数据报
2. 总体信息：

源IP地址：10.28.227.16，目的IP地址：10.3.9.161，协议类型：ICMP，长度：642字节，信息：Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 264)

1. 详细分析：

0000 10 4f 58 6c 0c 00 c4 23 60 0b 54 64 08 00 45 00 .OXl...#`.Td..E.

0010 02 74 06 c8 03 9d 80 01 00 00 0a 1c e3 10 0a 03 .t..............

0020 09 a1 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 ..jklmnopqrstuvw

0030 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefghijklmnop

0040 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi

0050 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 jklmnopqrstuvwab

0060 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 cdefghijklmnopqr

0070 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b stuvwabcdefghijk

0080 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 lmnopqrstuvwabcd

0090 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 efghijklmnopqrst

00a0 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d uvwabcdefghijklm

00b0 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 nopqrstuvwabcdef

00c0 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnopqrstuv

00d0 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f wabcdefghijklmno

00e0 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 pqrstuvwabcdefgh

00f0 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 ijklmnopqrstuvwa

0100 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 bcdefghijklmnopq

0110 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a rstuvwabcdefghij

0120 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 klmnopqrstuvwabc

0130 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 defghijklmnopqrs

0140 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c tuvwabcdefghijkl

0150 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 mnopqrstuvwabcde

0160 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 fghijklmnopqrstu

0170 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e vwabcdefghijklmn

0180 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 opqrstuvwabcdefg

0190 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 hijklmnopqrstuvw

01a0 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefghijklmnop

01b0 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi

01c0 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 jklmnopqrstuvwab

01d0 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 cdefghijklmnopqr

01e0 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b stuvwabcdefghijk

01f0 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 lmnopqrstuvwabcd

0200 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 efghijklmnopqrst

0210 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d uvwabcdefghijklm

0220 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 nopqrstuvwabcdef

0230 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnopqrstuv

0240 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f wabcdefghijklmno

0250 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 pqrstuvwabcdefgh

0260 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 ijklmnopqrstuvwa

0270 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 bcdefghijklmnopq

0280 72 73 rs

这是一个 IPv4 数据报的十六进制表示。数据报的前 20 个字节是 IPv4 基本首部。

从编号0开始，0-5字节（10 4f 58 6c 0c 00）是数据报的源 MAC 地址ArubaaHe\_6c:0c:00

6-11 字节（c4 23 60 0b 54 64）是数据报的目的 MAC 地址IntelCor\_0b:54:64

12-13 字节（08 00）表示协议类型为 IPv4。

14 字节（45）表示 IPv4 版本号为 4，首部长度为 5。

16-17 字节（02 74）表示数据报总长度为 628 字节。

18-19 字节（06 c8）是数据报的标识。数据报的标识为1736

20-21 字节（03 9d）表示标志和片偏移。片偏移量为7400字节。标志位DF=0，表示允许分片；MF=0，表示是分组的最后一片。

22 字节（80）表示生存时间为 128。

23 字节（01）表示协议类型为 ICMP。

接下来的 8 字节是源地址和目的地址。源地址为 `10.28.227.16`，目的地址为 `10.3.9.161`。

剩余的字节是 ICMP 数据报的内容。

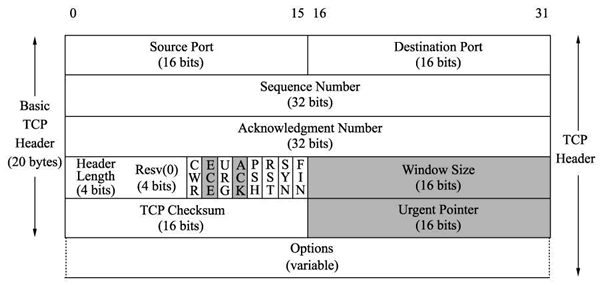
以上信息表面，该IP数据报是当前分组的最后一片，数据报总长度为628字节，去掉IP头部的20字节后为608字节。Offest为0x03 9d，表面偏移量为925\*8=7400字节。因此，原始数据报的总长度为7400+608=8008字节。

## 4. 获取TCP分组并分析

## 4.1 TCP概述

1. TCP（Transmission Control Protocol，传输控制协议）是一种面向连接的、可靠的、基于字节流的传输层通信协议。它是Internet协议套件的核心协议之一，与IP（Internet Protocol）协同工作，因此整个套件通常被称为TCP/IP。TCP提供了可靠、有序、经过错误检查的数据流传输，用于在通过IP网络通信的主机上运行的应用程序之间进行数据传输。主要的Internet应用程序，如万维网、电子邮件、远程管理和文件传输都依赖于TCP。TCP是面向连接的，客户端和服务器之间必须先建立连接才能发送数据。服务器必须处于监听状态（被动打开），才能与客户端建立连接。三次握手（主动打开）、重传和错误检测增加了可靠性，但延长了延迟。不需要可靠数据流服务的应用程序可以使用用户数据报协议（UDP），它提供了一种无连接的数据报服务，优先考虑时间而非可靠性。

2. TCP报文格式：



TCP报文格式包括固定首部和可变部分。固定首部长度为20字节，可变部分长度为0~40字节。固定首部包括以下字段：

- 源端口号（16位）：标识发送报文的计算机端口或进程。

- 目的端口号（16位）：标识接收报文的计算机端口或进程。

- 序列号（32位）：表示本报文段所发送数据的第一个字节的编号。

- 确认号（32位）：表示接收方期望收到发送方下一个报文段的第一个字节数据的编号。

- 数据偏移（4位）：单位为4字节，它指出报文数据距TCP报头的起始处有多远。

- 保留字段（6位）：保留今后使用，目前置0处理。

- 标志位字段（6位）：包括URG、ACK、PSH、RST、SYN和FIN标志位。

- 窗口大小（16位）：表示从Ack Number开始还可以接收多少字节的数据量，也表示当前接收端的接收窗口还有多少剩余空间。

- 校验和（16位）：用于确认传输的数据是否有损坏。

- 紧急指针字段（16位）：仅当URG控制位为1时才有意义。它指出本数据段中为紧急数据的字节数。

可选项字段长度可变，最多包含40字节。

3. TCP报文种类：

在TCP中，数据被分割成一些称为TCP报文段（TCP segment）的小块，每个TCP报文段携带了一部分数据，以及一些用于传输控制的信息。TCP报文段的结构包括源端口号、目标端口号、序列号、确认号、数据偏移、保留字段、标志位（URG、ACK、PSH、RST、SYN、FIN）、窗口大小、检验和、紧急指针字段和选项字段等。

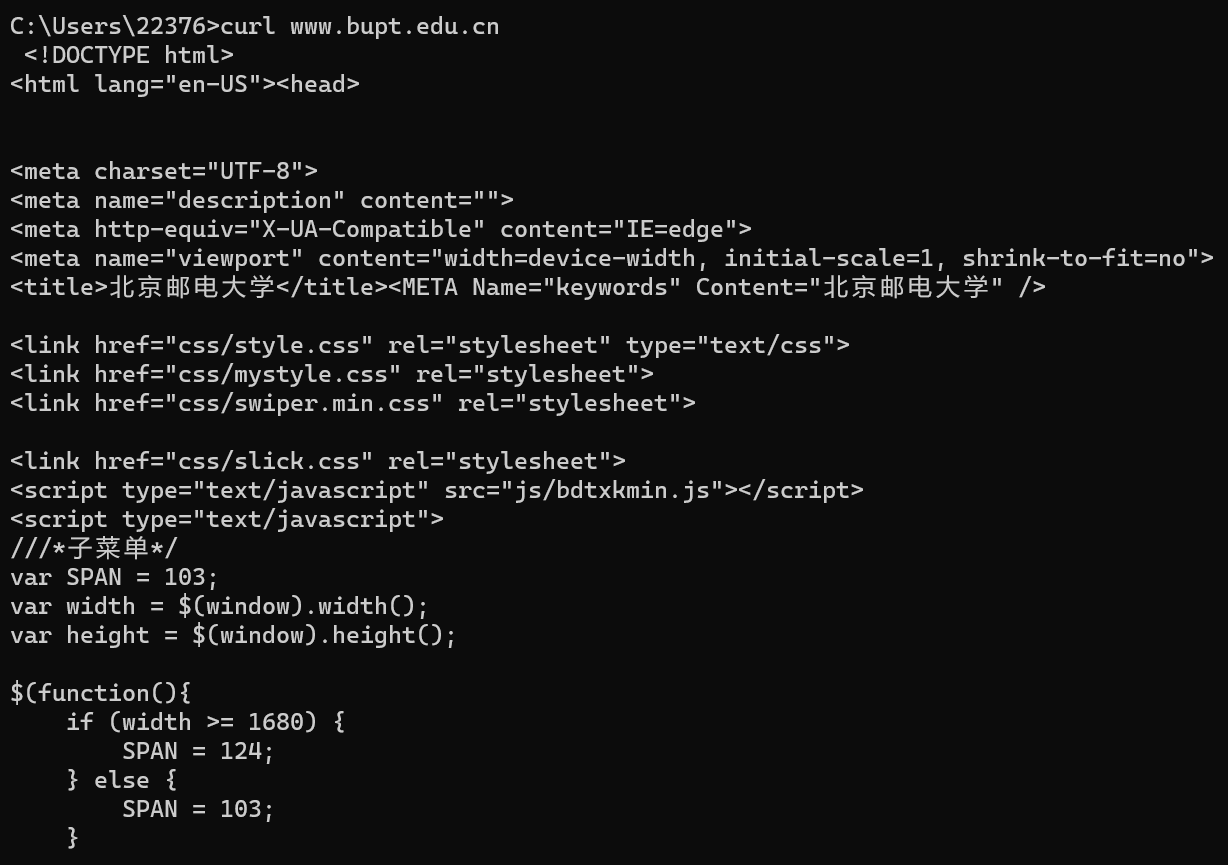
标志位中的URG表示紧急指针字段有效，ACK表示确认号字段有效，PSH表示接收方应尽快地交付给接收应用进程，RST表示TCP连接中出现严重差错，必须释放连接，然后再重新建立运输连接，SYN表示这是一个连接请求或连接接受报文，FIN表示发送端的数据已发送完毕，并要求释放运输连接。

## 4.2 TCP报文的捕获

1. 运行Wireshark软件，在首页选择进行连接的网络，选择WLAN

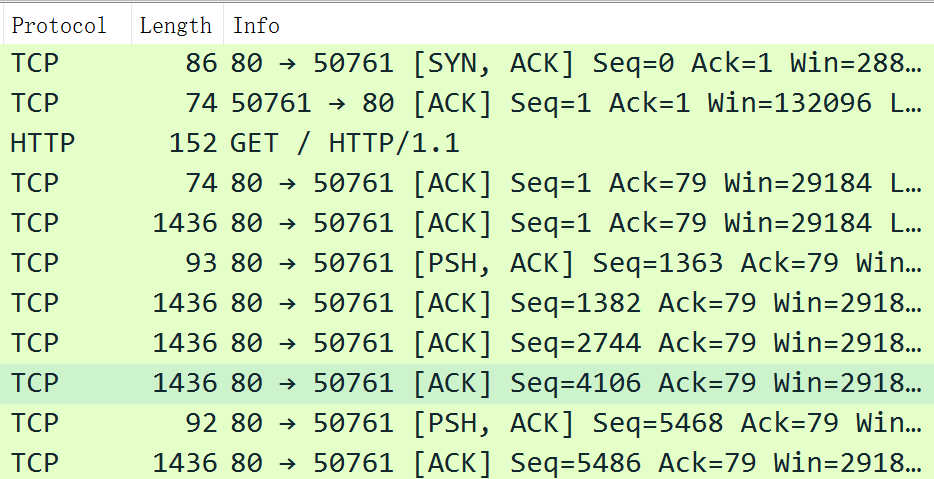
2. 在应用显示过滤器中输入tcp || http，将用于连接的TCP分组和用于数据传输的HTTP分组和用于拆除链接的TCP分组过滤出来。

3. 打开命令提示符窗口，输入curl [www.bupt.edu.cn](http://www.bupt.edu.cn)命令，curl 命令会向 www.bupt.edu.cn 发送一个 HTTP GET 请求，并将响应内容输出到命令行窗口中。响应内容是网页的 HTML 代码。



可以发现，HTML代码里除了ASCII码，还有中文字符，这是因为使用了UTF-8的字符编码格式。

1. 观察Wireshark中抓到的包



## TCP报文的分析

一、TCP建立连接时的三次握手的数据包

1. 第一次握手的SYN 包

（1）总体信息：

源IP地址：2001:da8:215:3c02:e880:4b0d:f171:acf3，目的IP地址：2001:da8:215:4038::161，协议：TCP，长度：86字节，信息：50761 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK\_PERM

（2）详细分析：

0000 10 4f 58 6c 0c 00 c4 23 60 0b 54 64 86 dd 60 07 .OXl...#`.Td..`.

0010 cc 8e 00 20 06 40 20 01 0d a8 02 15 3c 02 e8 80 ... .@ .....<...

0020 4b 0d f1 71 ac f3 20 01 0d a8 02 15 40 38 00 00 K..q.. .....@8..

0030 00 00 00 00 01 61 c6 49 00 50 ef f6 05 25 00 00 .....a.I.P...%..

0040 00 00 80 02 fd 20 af 31 00 00 02 04 05 a0 01 03 ..... .1........

0050 03 08 01 01 04 02 ......

源MAC地址是c4:23:60:0b:54:64（第6-11字节）

目的MAC地址是10:4f:58:6c:0c:00（第0-5字节）

使用IPv6协议，源IP地址是2001:0da8:0215:3c02:e880:4b0d:f171:acf3（第22-37字节）

目的IP地址是2001:0da8:0215:4038::0001（第38-53字节）

源端口号是50793（第54-55字节）

目的端口号是80（第56-57字节）

这个数据包的序列号是随机生成的4025877797（第58-61字节）

确认号为0（第62-65字节）

TCP标志位为SYN（第66字节）

这个数据包是一个 IPv6 数据包，它包含了一个 TCP SYN 包，用于建立 TCP 连接。该包由客户端向服务器发出，该过程实现建立TCP连接的第一次握手。

2. 第二次握手的SYN-ACK包

（1）总体信息：

源IP地址：2001:da8:215:4038::161，目的IP地址：2001:da8:215:3c02:e880:4b0d:f171:acf3，协议：TCP，长度：86字节，信息：80 → 50761 [SYN, ACK] Seq=0 Ack=1 Win=28800 Len=0 MSS=1362 SACK\_PERM WS=512

（2）详细分析：

0000 c4 23 60 0b 54 64 10 4f 58 6c 0c 00 86 dd 60 00 .#`.Td.OXl....`.

0010 00 00 00 20 06 3b 20 01 0d a8 02 15 40 38 00 00 ... .; .....@8..

0020 00 00 00 00 01 61 20 01 0d a8 02 15 3c 02 e8 80 .....a .....<...

0030 4b 0d f1 71 ac f3 00 50 c6 49 3b 9a 84 ec ef f6 K..q...P.I;.....

0040 05 26 80 12 70 80 d3 98 00 00 02 04 05 52 01 01 .&..p........R..

0050 04 02 01 03 03 09 ......

源MAC地址是c4:23:60:0b:54:64（第0-5字节）

目的MAC地址是10:4f:58:6c:0c:00（第6-11字节）

使用IPv6协议，源IP地址是2001:0da8:0215:4038::0001（第22-37字节）

目的IP地址是2001:0da8:0215:3c02:e880:4b0d:f171:acf3（第38-53字节）

源端口号是80（第54-55字节）

目的端口号是50793（第56-57字节）

数据包的序列号是随机生成的999982316（第58-61字节）

确认号为4025877798（第62-65字节）

TCP标志位为SYN+ACK（第66字节）

这个数据包是一个 IPv6 数据包，它包含了一个 TCP SYN-ACK 包，用于建立 TCP 连接。该包由服务器向客户端发出，该过程实现建立TCP连接的第二次握手。需要注意的是，确认号为4025877798，等于SYN包的序列号4025877797再加上1，这是因为SYN包不带数据，但是消耗1个序列号。

3. 第三次握手的ACK包

（1）总体信息：

378 9.616129 2001:da8:215:3c02:e880:4b0d:f171:acf3 2001:da8:215:4038::161 TCP 74 50761 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0

（2）详细分析：

0000 10 4f 58 6c 0c 00 c4 23 60 0b 54 64 86 dd 60 07 .OXl...#`.Td..`.

0010 cc 8e 00 14 06 40 20 01 0d a8 02 15 3c 02 e8 80 .....@ .....<...

0020 4b 0d f1 71 ac f3 20 01 0d a8 02 15 40 38 00 00 K..q.. .....@8..

0030 00 00 00 00 01 61 c6 49 00 50 ef f6 05 26 3b 9a .....a.I.P...&;.

0040 84 ed 50 10 02 04 af 25 00 00 ..P....%..

源MAC地址是c4:23:60:0b:54:64（第6-11字节）

目的MAC地址是10:4f:58:6c:0c:00（第0-5字节）

使用IPv6协议，源IP地址是2001:0da8:0215:3c02:e880:4b0d:f171:acf3（第22-37字节）

目的IP地址是2001:0da8:0215:4038::0001（第38-53字节）

源端口号是50793（第54-55字节）

目的端口号是80（第56-57字节）

数据包的序列号是4025877798（第58-61字节）

确认号为999982317（第62-65字节）

TCP标志位为ACK（第66字节）

这个数据包是一个 IPv6 数据包，它包含了一个 TCP ACK 包，用于建立 TCP 连接。该包由客户端向服务器发出，该过程完成建立TCP连接的第三次握手。注意到，确认号为999982317，等于SYN-ACK的序列号999982316再加上1，这是因为SYN-ACK包不带数据，但消耗1个序列号。

二、HTTP传输数据的数据包

1. HTTP GET请求数据包

（1）总体信息：

源IP地址：2001:da8:215:3c02:e880:4b0d:f171:acf3，目的IP地址：2001:da8:215:4038::161协议：HTTP长度：152字节，信息：GET / HTTP/1.1

（2）详细分析：

0000 10 4f 58 6c 0c 00 c4 23 60 0b 54 64 86 dd 60 07 .OXl...#`.Td..`.

0010 cc 8e 00 62 06 40 20 01 0d a8 02 15 3c 02 e8 80 ...b.@ .....<...

0020 4b 0d f1 71 ac f3 20 01 0d a8 02 15 40 38 00 00 K..q.. .....@8..

0030 00 00 00 00 01 61 c6 49 00 50 ef f6 05 26 3b 9a .....a.I.P...&;.

0040 84 ed 50 18 02 04 af 73 00 00 47 45 54 20 2f 20 ..P....s..GET /

0050 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1..Host:

0060 77 77 77 2e 62 75 70 74 2e 65 64 75 2e 63 6e 0d www.bupt.edu.cn.

0070 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 63 75 72 .User-Agent: cur

0080 6c 2f 38 2e 30 2e 31 0d 0a 41 63 63 65 70 74 3a l/8.0.1..Accept:

0090 20 2a 2f 2a 0d 0a 0d 0a \*/\*....

源MAC地址是c4:23:60:0b:54:64（第6-11字节）

目的MAC地址是10:4f:58:6c:0c:00（第0-5字节）

使用IPv6协议，源IP地址是2001:0da8:0215:3c02:e880:4b0d:f171:acf3（第22-37字节）

目的IP地址是2001:0da8:0215:4038::0001（第38-53字节）

源端口号是50793（第54-55字节），目的端口号是80（第56-57字节）

序列号是4025877798（第58-61字节）

确认号为999982317（第62-65字节）

TCP标志位为PSH+ACK（第66字节）。

这个数据包是一个 IPv6 数据包，由客户端向服务器发出，它包含了一个 HTTP GET 请求，目标地址是 `www.bupt.edu.cn`。从第74字节开始，可以看到HTTP请求行和请求头。请求行中显示这是一个GET请求，请求的URL为`/`，使用的HTTP版本为1.1。请求头中包含了`Host`和`User-Agent`字段。在这时，客户端向服务器请求发送数据。需要注意的是，上一个到达客户端的包的序列号为999982316，本数据包的确认号为999982317，代表当前客户端期待下一个到达的序列号为999982317

2. HTTP响应数据包

（1）总体信息：

源IP地址：2001:da8:215:4038::161，目的IP地址：2001:da8:215:3c02:e880:4b0d:f171:acf3协议：HTTP，长度：659字节，信息：HTTP/1.1 200 OK (text/html)

（2）详细分析：

0000 c4 23 60 0b 54 64 10 4f 58 6c 0c 00 86 dd 60 00 .#`.Td.OXl....`.

0010 00 00 02 5d 06 3b 20 01 0d a8 02 15 40 38 00 00 ...].; .....@8..

0020 00 00 00 00 01 61 20 01 0d a8 02 15 3c 02 e8 80 .....a .....<...

0030 4b 0d f1 71 ac f3 00 50 c6 49 3b 9b 84 72 ef f6 K..q...P.I;..r..

0040 05 74 50 18 00 39 51 d0 00 00 69 63 6f 6e 22 29 .tP..9Q...icon")

0050 2e 73 68 6f 77 28 29 3b 0d 0a 20 20 20 20 20 20 .show();..

0060 20 20 20 20 20 20 20 20 20 20 20 2f 2f e6 90 9c //...

0070 e7 b4 a2 e6 a1 86 e5 85 b3 e9 97 ad e9 80 bb e8 ................

0080 be 91 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 ....

0090 20 20 20 76 61 72 20 73 63 72 65 65 6e 57 69 64 var screenWid

00a0 74 68 20 3d 20 24 28 77 69 6e 64 6f 77 29 2e 77 th = $(window).w

00b0 69 64 74 68 28 29 3b 0d 0a 20 20 20 20 20 20 20 idth();..

00c0 20 20 20 20 20 20 20 20 69 66 28 73 63 72 65 65 if(scree

00d0 6e 57 69 64 74 68 20 3c 3d 20 31 36 30 30 29 7b nWidth <= 1600){

00e0 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ..

00f0 20 20 20 20 20 20 73 65 74 54 69 6d 65 6f 75 74 setTimeout

0100 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 (function(){..

0110 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0120 20 20 20 20 20 24 28 22 2e 72 69 67 68 74 2d 6c $(".right-l

0130 69 6e 6b 22 29 2e 72 65 6d 6f 76 65 43 6c 61 73 ink").removeClas

0140 73 28 22 73 65 72 2d 6f 6e 22 29 3b 20 20 20 20 s("ser-on");

0150 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0d .

0160 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .

0170 20 20 20 20 20 7d 2c 33 30 30 29 20 20 20 20 20 },300)

0180 20 20 20 20 20 20 20 20 20 0d 0a 20 20 20 20 20 ..

0190 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 24 $

01a0 28 22 23 6c 6f 67 6f 44 69 76 22 29 2e 72 65 6d ("#logoDiv").rem

01b0 6f 76 65 43 6c 61 73 73 28 22 6c 6f 67 6f 2d 73 oveClass("logo-s

01c0 73 22 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 s");..

01d0 20 20 20 20 20 20 20 20 20 20 24 28 22 23 6c 6f $("#lo

01e0 67 6f 44 69 76 22 29 2e 61 64 64 43 6c 61 73 73 goDiv").addClass

01f0 28 22 6c 6f 67 6f 2d 73 22 29 3b 0d 0a 20 20 20 ("logo-s");..

0200 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0210 20 24 28 22 23 6c 6f 67 6f 44 69 76 22 29 2e 63 $("#logoDiv").c

0220 73 73 28 22 77 69 64 74 68 22 2c 22 22 29 3b 0d ss("width","");.

0230 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .

0240 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 7d 0d }.. }.

0250 0a 20 20 20 20 20 20 20 20 7d 29 3b 0d 0a 0d 0a . });....

0260 0d 0a 20 20 20 20 7d 29 0d 0a 3c 2f 73 63 72 69 .. })..</scri

0270 70 74 3e 0d 0a 0d 0a 20 0d 0a 0d 0a 3c 2f 62 6f pt>.... ....</bo

0280 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 0d 0a 30 0d dy></html>....0.

0290 0a 0d 0a ...

源MAC地址是c4:23:60:0b:54:64（第6-11字节）

目的MAC地址是10:4f:58:6c:0c:00（第0-5字节）

使用IPv6协议，源IP地址是2001:0da8:0215:4038::0001（第22-37字节）

目的IP地址是2001:0da8:0215:3c02:e880:4b0d:f171:acf3（第38-53字节）

源端口号是80（第54-55字节）

目的端口号是50793（第56-57字节）

这个数据包的序列号是1000047730（第58-61字节）

确认号为4025877876（第62-65字节）

TCP标志位为PSH+ACK（第66字节）。

这个数据包是一个 IPv6 数据包，由服务器向客户端发出它包含了一个 HTTP 响应，包含一个PSH-ACK包。

从第74字节开始，可以看到HTTP响应头和响应体。响应体中包含了HTML、JavaScript和CSS代码。在这时，TCP服务已经完成，数据已经传输完毕。需要注意的是，本数据包的确认号为4025877876，而上一个到达服务器的包的序列号为4025877876，序列号没有变化，上一个到达的包是客户端向服务器发出的请求拆除连接的ACK包，则表明服务器传输完成后发出的HTTP响应并不对ACK包进行处理，而是在下一个向客户端发出的FIN-ACK包中进行处理。

1. TCP拆除连接的数据包

1. 第一步释放的FIN-ACK包

（1）总体信息：

源IP地址：2001:da8:215:3c02:e880:4b0d:f171:acf3，目的IP地址：2001:da8:215:4038::161协议：TCP，长度：74字节，信息：50761 → 80 [FIN, ACK] Seq=79 Ack=65999 Win=131328 Len=0

（2）详细分析：

0000 10 4f 58 6c 0c 00 c4 23 60 0b 54 64 86 dd 60 07 .OXl...#`.Td..`.

0010 cc 8e 00 14 06 40 20 01 0d a8 02 15 3c 02 e8 80 .....@ .....<...

0020 4b 0d f1 71 ac f3 20 01 0d a8 02 15 40 38 00 00 K..q.. .....@8..

0030 00 00 00 00 01 61 c6 49 00 50 ef f6 05 74 3b 9b .....a.I.P...t;.

0040 86 bb 50 11 02 01 af 25 00 00 ..P....%..

源MAC地址是c4:23:60:0b:54:64（第6-11字节）

目的MAC地址是10:4f:58:6c:0c:00（第0-5字节）

使用IPv6协议，源IP地址是2001:0da8:0215:3c02:e880:4b0d:f171:acf3（第22-37字节）

目的IP地址是2001:0da8:0215:4038::0001（第38-53字节）

源端口号是80（第54-55字节）

目的端口号是50793（第56-57字节）

数据包的序列号是4025877876（第58-61字节）

确认号为1000048315（第62-65字节）

TCP标志位为FIN+ACK（第66字节）

这个数据包是一个 IPv6 数据包，由客户端向服务器发出，它包含了一个 TCP FIN-ACK包。表示客户端已经收到所有数据，请求拆除TCP连接。

1. 第二步释放的FIN-ACK包
2. 总体信息：

源IP地址：2001:da8:215:4038::161，目的IP地址：2001:da8:215:3c02:e880:4b0d:f171:acf3协议：TCP，长度：74字节，信息：80 → 50761 [FIN, ACK] Seq=65999 Ack=80 Win=29184 Len=0

1. 详细分析：

0000 c4 23 60 0b 54 64 10 4f 58 6c 0c 00 86 dd 60 00 .#`.Td.OXl....`.

0010 00 00 00 14 06 3b 20 01 0d a8 02 15 40 38 00 00 .....; .....@8..

0020 00 00 00 00 01 61 20 01 0d a8 02 15 3c 02 e8 80 .....a .....<...

0030 4b 0d f1 71 ac f3 00 50 c6 49 3b 9b 86 bb ef f6 K..q...P.I;.....

0040 05 75 50 11 00 39 82 33 00 00 .uP..9.3..

源MAC地址是c4:23:60:0b:54:64（第6-11字节）

目的MAC地址是10:4f:58:6c:0c:00（第0-5字节）

使用IPv6协议，源IP地址是2001:0da8:0215:4038::0001（第22-37字节）

目的IP地址是2001:0da8:0215:3c02:e880:4b0d:f171:acf3（第38-53字节）

源端口号是80（第54-55字节）

目的端口号是50793（第56-57字节）

数据包的序列号是1000048315（第58-61字节）

确认号为4025877877（第62-65字节）

TCP标志位为FIN+ACK（第66字节）

这个数据包是一个 IPv6 数据包，由服务器发出，它包含了一个 TCP FIN-ACK包。代表服务器收到了客户端的关闭连接请求，服务器启动关闭连接计时器。需要注意的是，当前包的确认号为4025877877，上一个收到的包的序列号为4025877876，则表明在拆除TCP连接时，FIN-ACK包并不传输数据，但是会消耗一个序列号。

1. 第三步释放的ACK包
2. 总体信息：

源IP地址：2001:da8:215:3c02:e880:4b0d:f171:acf3，目的IP地址：2001:da8:215:4038::161，协议：TCP，长度：74字节，信息：50761 → 80 [ACK] Seq=80 Ack=66000 Win=131328 Len=0

1. 详细分析：

0000 10 4f 58 6c 0c 00 c4 23 60 0b 54 64 86 dd 60 07 .OXl...#`.Td..`.

0010 cc 8e 00 14 06 40 20 01 0d a8 02 15 3c 02 e8 80 .....@ .....<...

0020 4b 0d f1 71 ac f3 20 01 0d a8 02 15 40 38 00 00 K..q.. .....@8..

0030 00 00 00 00 01 61 c6 49 00 50 ef f6 05 75 3b 9b .....a.I.P...u;.

0040 86 bc 50 10 02 01 af 25 00 00 ..P....%..

源MAC地址是c4:23:60:0b:54:64（第6-11字节）

目的MAC地址是10:4f:58:6c:0c:00（第0-5字节）

使用IPv6协议，源IP地址是2001:0da8:0215:3c02:e880:4b0d:f171:acf3（第22-37字节）

目的IP地址是2001:0da8:0215:4038::0001（第38-53字节）

源端口号是80（第54-55字节）

目的端口号是50793（第56-57字节）

序列号是4025877877（第58-61字节）

确认号为1000048316（第62-65字节）

TCP标志位为ACK（第66字节）

这个数据包是一个 IPv6 数据包，由客户端向服务器发出，它包含了一个 TCP ACK包。代表客户端收到了来自服务器的关闭请求包，这个包是客户端发出的最后的确认关闭包，发送后启动计时器，在计时器超时后自动关闭连接。而服务器收到当前包时关闭TCP连接。需要注意的是，当前包的确认号为1000048316，而上一个到达的包的序列号为1000048315，这表明在拆除TCP连接时，FIN-ACK包并不传输数据，但是会消耗一个序列号。至此，一个完整的TCP服务结束。

## 实验总结

本次实验主要内容是抓取DHCP分组，了解该报文的结构和作用，知道动态获取IP地址的过程；抓取ARP分组，了解该报文的结构和作用，知道由IP地址找到MAC地址的过程；抓取IP数据分组，通过抓取特殊的IP分组ICMP分组来完成，了解IP分组的结构和作用，清楚IP分组的分片的实现；抓取TCP分组，了解该报文的结构和作用，了解一次完整的TCP连接的过程。

在做这次实验前，我并不喜欢使用Wireshark这一工具，因为其中的信息充满着0和1，我很难明白其中的内涵。但通过这次实验，我见识到了这一抓包工具的强大，并且能够初步使用这一工具，Wireshark不仅能将任何包抓到，还能将包的每个部分清晰的解释清楚，让我能快速学习包的结构而对协议进行了解。

本次实验让我对学过的课本上的知识有了实实在在的认识，网络是一门充满着实践的课程。而在抓包工具面前，这些第一眼看过去令人别扭的协议名称也有了具体且实际的展现。我了解了ICMP协议、DHCP协议、ARP协议、IP协议、UDP协议、TCP协议等等一系列重要且实际的协议。

本次实验遇到了一些困难。首先，我在之前并不了解ICMPv6协议，在抓取ICMPv6报文时，将筛选器参数设置为icmp，这样并没有抓到该报文，而只能抓到ICMPv4的报文，通过查阅资料，我认识到ICMPv6和ICMP是不同的协议，需要设置不同的参数来抓其所对应的报文。其次，我并不了解如何清晰地抓取一次TCP的完整过程产生的包。通过查阅资料，我找到了curl这一强大的命令行工具，它能有效快速建立一次TCP服务，因此我能有效的将该服务产生的包清晰的抓取出来并对其进行分析。