

北京邮电大学 计算机学院

《计算机网络》实验报告

姓名 王睿嘉

学号 2015211906

班级 2015211307

实验 协议数据的捕获和解析

一、实验内容和步骤描述

1. 实验内容

- 1) 使用 Wireshark 软件捕获在使用 ping 命令时产生的 ICMP 消息；
- 2) 分析网络层 IP 包头格式，理解各字段作用，对分段及校验和进行验证；
- 3) 使用 Wireshark 软件捕获 ARP 消息，分析其消息格式，理解其工作原理；
- 4) 使用 Wireshark 捕获 DHCP 消息，分析其消息序列，理解 DHCP 功能和操作原理；
- 5) 使用 Wireshark 捕获 TCP 消息，分析其报文段头格式，理解连接建立及释放、差错控制、序号及窗口管理的原理。

2. 实验步骤

2.1 准备工作

- 1) 下载 Wireshark 并了解其功能和使用方法；
- 2) 确保计算机已连接到网络；
- 3) 启动 Wireshark，设置捕获接口为本机网卡，并选中混杂模式捕获选项，选择合适的捕获过滤器：
对于 ping 命令，设置过滤器为 icmp；
对于 DHCP 消息，设置过滤器为 udp port 67；
对于 ARP 消息，设置过滤器为 arp；
通过网页浏览应用来捕获 TCP 消息，设置过滤器为 tcp port 80；
- 4) 开始捕获。

2.2 数据捕获

2.2.1 捕获 ICMP 协议数据

- 1) 运行 ping 命令（例如：ping 192.168.0.1），远程主机地址可以是本机地址、网关路由器地址或域名；
- 2) 使用 Windows 中 ping 命令的 -l 选项（例如：ping -l 8000 192.168.0.1），生成大于 8000 字节的 IP 包并发送，捕获后分析其分段传输的包结构。

2.2.2 捕获 DHCP 协议数据

- 1) 使用 ipconfig 命令释放计算机 IP 地址（ipconfig -release）；
- 2) 使用 ipconfig 命令重新申请 IP 地址（ipconfig -renew），此时 Wireshark 窗口中可捕获到完整的 DHCP 地址分配流程。

2.2.3 捕获 ARP 协议数据

采用与 2.2.2 相同的方法释放 IP 地址并重新申请，在 Wireshark 窗口中可捕获到 ARP 请求和响应消息。

2.2.4 捕获 TCP 协议数据

打开浏览器，输入一个页面内容较简单的网页的 URL（例如：www.baidu.com），网页全部显示后关闭浏览器。

2.3 协议分析

- 1) IP 包头分析：对于采用 ping 命令-l 选项捕获的 ICMP 消息，就承载消息的 IP 包进行分析，记录包头各字段的值，对照讲义和教材分析各字段功能，并对分段进行验证；
- 2) ICMP 消息分析：记录并分析 ICMP 消息中各字段功能；
- 3) DHCP 消息分析：针对一次地址分配过程（Transaction ID 相同的 4 个消息），分析其通信过程，画出地址分配的消息序列图，并记录采用 DHCP 协议配置的各个参数；
- 4) ARP 消息分析：对照讲义理解 ARP 的操作过程，记录并分析消息中各字段的功能；
- 5) TCP 报头及消息分析：针对 TCP 连接建立、释放、数据和应答报文段，对照讲义和教材分析各字段功能。针对一次完整的 TCP 通信过程，画出消息序列图，包含连接建立、数据传送和连接释放阶段。

2.4 撰写实验报告

对于捕获到的数据进行认真分析，归纳各协议的工作原理和实现要点。

二、 协议数据解析

1. IP 协议分析

1) IP 包头校验和校验原理

IP 包头的校验和字段是根据 IP 包头计算的校验和码，它不对包头后面的数据进行计算。

为了计算某数据包的 IP 校验和，首先把校验和字段置为 0。

然后，对包头中每个 16bit 进行二进制反码求和，并将结果存放在校验和字段中。

当收到一份 IP 数据包后，同样对包头中每个 16bit 进行二进制反码的求和。由于接收方在计算过程中包含了发送方存在包头中的校验和，因此，若包头在传输过程中没有发生任何差错，接收方计算的结果应该为全 1。若结果不全为 1，即出现校验和错误，那么 IP 就丢弃收到的数据包，但不生成差错报文，由上层发现丢失的数据包并进行重传。

2) IP 包分段原理

链路层具有最大传输单元 MTU，它限制了数据帧的最大长度，不同的网络类型都有一个上限值。若网络层有数据报要传，且数据报的长度超过了 MTU，那么 IP 就要对数据报进行分段操作，使每一片的长度都小于或等于 MTU。

```
Microsoft Windows [版本 10.0.15063]
(c) 2017 Microsoft Corporation. 保留所有权利。

C:\Users\dell>ping -l 8000 10.122.192.1

正在 Ping 10.122.192.1 具有 8000 字节的数据:
来自 10.122.192.1 的回复: 字节=8000 时间=6ms TTL=255
来自 10.122.192.1 的回复: 字节=8000 时间=6ms TTL=255
来自 10.122.192.1 的回复: 字节=8000 时间=6ms TTL=255
来自 10.122.192.1 的回复: 字节=8000 时间=6ms TTL=255

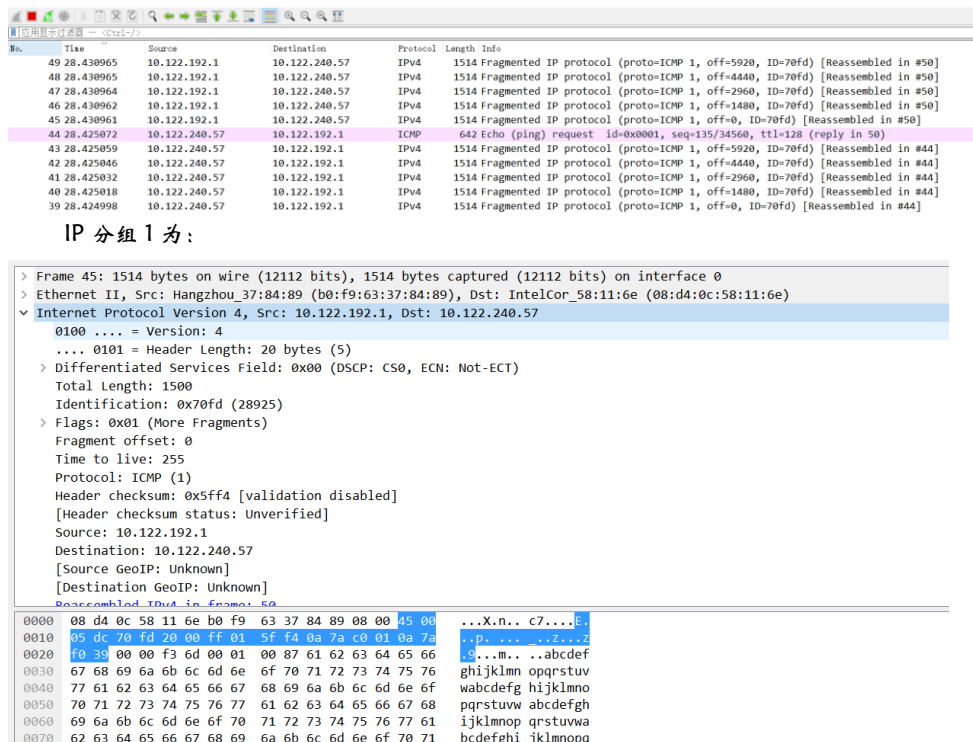
10.122.192.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 6ms, 最长 = 6ms, 平均 = 6ms
```

由上图可知 8000 字节的 IP 包被分成 6 个分组发送。

IP 包头包含了分片和重组所需的信息：

- ① 16 位的标识：用于目标主机确定一个新到达的分段属于哪一个数据报。同一个数据报的所有段包含同样的标识值。
 - ② 3 位的标志字段：
 - R：保留未用；
 - DF：“不分段”标志位，若将其置 1，将不对数据报进行分段；
 - MF：“更多的段”标志位，除了最后一个段以外，其他所有的段都必须设置这一位；
 - ③ 分段偏移量：指明该段在当前数据报中的位置，偏移的字节数是该值乘 8。
- 此外，当数据报被分段后，每个段的总长度值要改为该片段的长度值。

下面通过对这六 6 个 IP 分组包头的分析，验证分段原理。



IP 分组 1 为：

```
> Frame 45: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
> Internet Protocol Version 4, Src: 10.122.192.1, Dst: 10.122.240.57
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x70fd (28925)
  > Flags: 0x01 (More Fragments)
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x5ff4 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.122.192.1
    Destination: 10.122.240.57
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame #50
  0000  08 d4 0c 58 11 6e b0 f9 63 37 84 89 08 00 45 00  ...X.n... c7...E.
  0010  05 dc 70 fd 20 00 ff 01 5f f4 0a 7a c0 01 0a 7a  ...p... ..Z...Z
  0020  f0 30 00 00 f3 6d 00 01 00 87 61 62 63 64 65 66  ...m... ..abcde
  0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
  0040  77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f  wabcdefg hijklmno
  0050  70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68  pqrstuvwxyz abcdefgh
  0060  69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61  ijklmnop qrstuvw
  0070  62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71  bcdefghi jklmnopq
```

由上图可知：

字段	报文 (16 进制)	备注
版本	4	IPV4
包头长度	5	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	分组长度 1500 字节
标识	70fd	序列号为 28925
标志	01	DF=0, MF=1，允许分段，且此片不是最后一片
偏移值	000	偏移量为 0
生存周期	ff	每跳生存周期为 255s
协议	01	携带的数据来自 ICMP 协议
头部校验和	5ff4	IP 包头校验和为 5ff4
源地址	0a7ac001	源地址为 10.122.192.1

目的地址 0a7af039 目的地址为 10.122.240.57

上述为第一片，由于数据包总长度为 1500 字节，而 IP 包头占 20 字节，因此实际的数据只有 1480 字节，那么分组 2 的偏移量应为 1480 字节。实际采集到的 IP 分组 2 为：

```
> Frame 46: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
< Internet Protocol Version 4, Src: 10.122.192.1, Dst: 10.122.240.57
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x70fd (28925)
  > Flags: 0x01 (More Fragments)
    Fragment offset: 1480
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x5f3b [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.122.192.1
    Destination: 10.122.240.57
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Decomposed IPv4 in frames: 50
0000 08 d4 0c 58 11 6e b0 f9 63 37 84 89 08 00 45 00 ...X.n.. c7....E.
0010 05 dc 70 fd 20 b9 ff 01 5f 3b 0a 7a c0 01 0a 7a ..p....j.z...Z
0020 f0 39 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e .9abcdef ghijklmn
0030 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 opqrstuv wabcdefg
0040 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 hijklmno pqrstuvwxyz
0050 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefgh ijklmnop
0060 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvw bcdefghi
0070 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 jklmnopq rstuvwab
0080 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 cdefghij klmnopqr
0090 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b stuvwabc defghijk
```

由上图可知：

字段	报文 (16 进制)	备注
版本	4	IPV4
包头长度	5	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	分组长度 1500 字节
标识	70fd	序列号为 28925
标志	01	DF=0, MF=1, 允许分段, 且此片不是最后一片
偏移值	0b9	偏移量为 1480
生存周期	ff	每跳生存周期为 255s
协议	01	携带的数据来自 ICMP 协议
头部校验和	5f3b	IP 包头校验和为 5f3b
源地址	0a7ac001	源地址为 10.122.192.1
目的地址	0a7af039	目的地址为 10.122.240.57

上述为第二片，由于数据包总长度为 1500 字节，而 IP 包头占 20 字节，因此实际的数据只有 1480 字节，那么分组 3 的偏移量应为 1480*2=2960 字节。实际采集到的 IP 分组 3 为：

```
> Frame 47: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
< Internet Protocol Version 4, Src: 10.122.192.1, Dst: 10.122.240.57
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x70fd (28925)
  > Flags: 0x01 (More Fragments)
    Fragment offset: 2960
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x5e82 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.122.192.1
    Destination: 10.122.240.57
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Decomposed IPv4 in frames: 50
0000 08 d4 0c 58 11 6e b0 f9 63 37 84 89 08 00 45 00 ...X.n.. c7....E.
0010 05 dc 70 fd 21 72 ff 01 5e 82 0a 7a c0 01 0a 7a ..p.l.f..^..z...Z
0020 f0 39 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 .9ijklmn opqrstuv
0030 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f wabcdefg hijklmno
0040 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 pqrstuvwxyz abcdefgh
0050 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 ijklmnop qrstuvw
0060 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 bcdefghi jklmnopq
0070 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a rstuvwab cdefghij
0080 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 klmnopqr stuvwabc
```

由上图可知：

字段	报文 (16 进制)	备注
版本	4	IPV4
包头长度	5	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	分组长度 1500 字节
标识	70fd	序列号为 28925
标志	01	DF=0, MF=1, 允许分段, 且此片不是最后一片
偏移值	172	偏移量为 2960
生存周期	ff	每跳生存周期为 255s
协议	01	携带的数据来自 ICMP 协议
头部校验和	5e82	IP 包头校验和为 5e82
源地址	0a7ac001	源地址为 10.122.192.1
目的地址	0a7af039	目的地址为 10.122.240.57

上述为第三片, 由于数据包总长度为 1500 字节, 而 IP 包头占 20 字节, 因此实际的数据只有 1480 字节, 那么分组 4 的偏移量应为 $1480 \times 3 = 4440$ 字节。实际采集到的 IP 分组 4 为:

```
> Frame 48: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
> Internet Protocol Version 4, Src: 10.122.192.1, Dst: 10.122.240.57
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x70fd (28925)
  > Flags: 0x01 (More Fragments)
    Fragment offset: 4440
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x5dc9 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.122.192.1
    Destination: 10.122.240.57
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  Reassembled IPv4 in frame: 50
0000  08 d4 0c 58 11 6e b0 f9 63 37 84 89 08 00 45 00  ...X.n.. c7....E.
0010  05 dc 70 fd 22 2b ff 01 5d c9 0a 7a c0 01 0a 7a  ..p."+.. ]..Z...Z
0020  f0 39 71 72 73 74 75 76 77 61 62 63 64 65 66 67  .9qrstuv wabcdefg
0030  68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77  hijklmno pqrstuvw
0040  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70  abcdefgh ijklmnop
0050  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvw a bcdefghi
0060  6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62  jklmnopq rstuvwab
0070  63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72  cdefghij klmnopqr
0080  73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b  stuvwabc defghijk
0090  6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64  lmnopqrs tuvabcd
```

由上图可知：

字段	报文 (16 进制)	备注
版本	4	IPV4
包头长度	5	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	分组长度 1500 字节
标识	70fd	序列号为 28925
标志	01	DF=0, MF=1, 允许分段, 且此片不是最后一片
偏移值	22b	偏移量为 4440

生存周期	ff	每跳生存周期为 255s
协议	01	携带的数据来自 ICMP 协议
头部校验和	5dc9	IP 包头校验和为 5dc9
源地址	0a7ac001	源地址为 10.122.192.1
目的地址	0a7af039	目的地址为 10.122.240.57

上述为第四片，由于数据包总长度为 1500 字节，而 IP 包头占 20 字节，因此实际的数据只有 1480 字节，那么分组 5 的偏移量应为 $1480 \times 4 = 5920$ 字节。实际采集到的 IP 分组 5 为：

```
> Frame 49: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
✓ Internet Protocol Version 4, Src: 10.122.192.1, Dst: 10.122.240.57
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x70fd (28925)
> Flags: 0x01 (More Fragments)
    Fragment offset: 5920
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x5d10 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.122.192.1
    Destination: 10.122.240.57
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 50
0000 08 d4 0c 58 11 6e b0 f9 63 37 84 89 08 00 45 00 ...X.n.. c7....E.
0010 05 dc 70 fd 22 e4 ff 01 5d 10 0a 7a c0 01 0a 7a ...p."... ]..z...z
0020 f0 39 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f .9bcdefg hijklmno
0030 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 pqrstuvwxyz abcdefgh
0040 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 ijklmnop qrstuvw
0050 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 bcdefghi jklmnopq
0060 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a rstuvwab cdefghij
0070 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 klmnopqr stuvwabc
0080 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 defghijk lmnopqrs
```

由上图可知：

字段	报文 (16 进制)	备注
版本	4	IPV4
包头长度	5	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	分组长度 1500 字节
标识	70fd	序列号为 28925
标志	01	DF=0, MF=1, 允许分段，且此片不是最后一片
偏移值	2e4	偏移量为 5920
生存周期	ff	每跳生存周期为 255s
协议	01	携带的数据来自 ICMP 协议
头部校验和	5d10	IP 包头校验和为 5d10
源地址	0a7ac001	源地址为 10.122.192.1
目的地址	0a7af039	目的地址为 10.122.240.57

上述为第五片，由于数据包总长度为 1500 字节，而 IP 包头占 20 字节，因此实际的数据只有 1480 字节，那么分组 6 的偏移量应为 $1480 \times 5 = 7400$ 字节。实际采集到的 IP 分组 6（最后 1 包）为：

```

> Ethernet II, Src: IntelCor_58:11:6e (08:d4:0c:58:11:6e), Dst: Hangzhou_37:84:89 (b0:f9:63:37:84:89)
v Internet Protocol Version 4, Src: 10.122.240.57, Dst: 10.122.192.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 628
    Identification: 0x70fd (28925)
  > Flags: 0x00
    Fragment offset: 7400
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0xfebf [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.122.240.57
    Destination: 10.122.192.1
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  > [6 IPv4 Fragments (8000 bytes): #20(1480) #40(1480) #41(1480) #42(1480) #43(1480) #44(600)]
0000 b0 f9 63 37 84 89 08 d4 0c 58 11 6e 08 00 45 00 ..c7.... .X.n..E.
0010 02 74 70 fd 03 9d 80 01 fe bf 0a 7a f0 39 0a 7a .tp..... .z.9.z
0020 c0 01 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 .jklmno pqrstuvwxyz
0030 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefgh ijklmnop
0040 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvw abcdefghi
0050 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 jklmnopq rstuvwab
0060 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 cdefghij klmnopqr
0070 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b stuvwabc defghijk
0080 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 lmnopqrs tuvabcd
0090 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 efghijkl mnopqrst

```

由上图可知：

字段	报文 (16 进制)	备注
版本	4	IPv4
包头长度	5	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	分组长度 628 字节
标识	70fd	序列号为 28925
标志	00	DF=0, MF=0, 允许分段, 且此片是最后一片
偏移值	39d	偏移量为 7400
生存周期	80	每跳生存周期为 128s
协议	01	携带的数据来自 ICMP 协议
头部校验和	febf	IP 包头校验和为 febf
源地址	0a7af039	源地址为 10.122.240.57
目的地址	0a7ac001	目的地址为 10.122.192.1

此数据包总长度为 628 字节, 由于为 ICMP 包, ICMP 包头占用了 8 个字节, IP 包头占用了 20 字节, 因此实际的数据只有 600 字节。则数据报总长度为 $1480 \times 5 + 600 = 8000$ 字节, 分段原理得到验证。

2. ICMP 协议分析

1) ICMP 功能

ICMP 是 Internet 控制消息协议, 为 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。控制消息指网络通不通、目的主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据, 但对于数据的传递起着重要的作用。

2) ICMP 包格式

在网络中经常会使用 ICMP 协议，例如用于检查网络通不通的 ping 命令，这个“ping”的过程实际上就是 ICMP 协议工作的过程，检测如下：

```
Microsoft Windows [版本 10.0.15063]
(c) 2017 Microsoft Corporation。保留所有权利。

C:\Users\dell>ping 10.122.192.1

正在 Ping 10.122.192.1 具有 32 字节的数据:
来自 10.122.192.1 的回复: 字节=32 时间=3ms TTL=255
来自 10.122.192.1 的回复: 字节=32 时间=4ms TTL=255
来自 10.122.192.1 的回复: 字节=32 时间=2ms TTL=255
来自 10.122.192.1 的回复: 字节=32 时间=3ms TTL=255

10.122.192.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 2ms, 最长 = 4ms, 平均 = 3ms
```

ping 10.122.192.1 对应的 ICMP 包如下：

Figure 1: Wireshark packet capture showing ICMP Echo (ping) request and reply. The packet list shows a request from 10.122.240.57 to 10.122.192.1 and a reply from 10.122.192.1 to 10.122.240.57. The packet details show the ICMP Echo (ping) request with sequence number 140. The packet bytes show the raw ICMP data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.122.240.57	10.122.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=140/35840, ttl=128 (no response found!)
2	0.003050	10.122.192.1	10.122.240.57	ICMP	74	Echo (ping) reply id=0x0001, seq=140/35840, ttl=255 (request in 1)
3	1.004890	10.122.240.57	10.122.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=141/36096, ttl=128 (reply in 4)
4	1.009109	10.122.192.1	10.122.240.57	ICMP	74	Echo (ping) reply id=0x0001, seq=141/36096, ttl=255 (request in 3)
5	2.014807	10.122.240.57	10.122.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=142/36352, ttl=128 (no response found!)
6	2.017654	10.122.192.1	10.122.240.57	ICMP	74	Echo (ping) reply id=0x0001, seq=142/36352, ttl=255 (request in 5)
7	3.025577	10.122.240.57	10.122.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=143/36608, ttl=128 (reply in 8)
8	3.029042	10.122.192.1	10.122.240.57	ICMP	74	Echo (ping) reply id=0x0001, seq=143/36608, ttl=255 (request in 7)

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
 Internet Protocol Version 4, Src: 10.122.192.1, Dst: 10.122.240.57
 Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0x54cf [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence number (BE): 140 (0x008c)
 Sequence number (LE): 35840 (0x8c00)
 [Request frame: 1]
 [Response time: 3.050 ms]
 Data (32 bytes)

Offset	Hex	ASCII
0000	08 d4 0c 58 11 6e b0 f9 63 37 84 89 08 00 45 00	...X.n.. c7....E.
0010	00 3c 73 51 00 00 ff 01 83 40 0a 7a c0 01 0a 7a	.<sQ.... .@.Z...Z
0020	f0 39 00 00 54 cf 00 01 00 8c 61 62 63 64 65 66	.9..T... ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

上图即为捕获到的 ICMP 包的信息。

ICMP 包将自身封装一层 IP 头，然后在网络中进行传输，其格式如下：

类型 (8 位)	代码 (8 位)	校验和 (8 位)
类型或代码		

各字段功能如下：

类型：表示 ICMP 报文类型；

代码：进一步区分某类型的几种不同情况；

校验和：用来检验整个 ICMP 报文；

紧接着的 4 个字节的内容与 ICMP 类型有关，再后面为数据字段，其长度取决于 ICMP 类型。

3. DHCP 协议分析

1) DHCP 功能

DHCP，全称是动态主机配置协议，它的前身是 BOOTP，工作在 OSI 模型的应用层，是一种帮助计算机从指定的 DHCP 服务器获取它们配置信息的自举协议。

DHCP 使用客户端/服务器模式，请求配置信息的计算机称为 DHCP 客户端，而提供信息的称为 DHCP 服务器。DHCP 为客户端分配地址的方法有三种：手工配置、自动配置和动态配置。

其中，最重要的功能就是动态分配。除了 IP 地址，DHCP 分组还为客户端提供其他的配置信息，例如子网掩码，这使得客户端无需用户动手就能自动配置连接网络。

设置过滤器为 udp port 67 来过滤 DHCP 协议。

使用 ipconfig 命令释放计算机 IP 地址 (ipconfig -release) 后，再使用 ipconfig 命令重新申请 IP 地址 (ipconfig -renew)：

```
C:\Users\dell>ipconfig -release

Windows IP 配置

不能在 以太网 上执行任何操作，它已断开媒体连接。
不能在 本地连接* 1 上执行任何操作，它已断开媒体连接。

以太网适配器 以太网:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 本地连接* 1:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . :
    IPv6 地址 . . . . . : 2001:da8:215:8f01:a594:e434:2fd8:440
    临时 IPv6 地址 . . . . . : 2001:da8:215:8f01:acac:f9e0:1af6:b4
    本地链接 IPv6 地址 . . . . . : fe80::a594:e434:2fd8:440%8
    默认网关 . . . . . : fe80::b2f9:63ff:fe37:8489%8

隧道适配器 本地连接* 12:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

C:\Users\dell>ipconfig -renew

Windows IP 配置

不能在 以太网 上执行任何操作，它已断开媒体连接。
不能在 本地连接* 1 上执行任何操作，它已断开媒体连接。

以太网适配器 以太网:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 本地连接* 1:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . : bupt.edu.cn
    IPv6 地址 . . . . . : 2001:da8:215:8f01:a594:e434:2fd8:440
    临时 IPv6 地址 . . . . . : 2001:da8:215:8f01:acac:f9e0:1af6:b4
    本地链接 IPv6 地址 . . . . . : fe80::a594:e434:2fd8:440%8
    IPv4 地址 . . . . . : 10.122.240.57
    子网掩码 . . . . . : 255.255.192.0
    默认网关 . . . . . : fe80::b2f9:63ff:fe37:8489%8
                        10.122.192.1

隧道适配器 本地连接* 12:

    连接特定的 DNS 后缀 . . . . . :
    IPv6 地址 . . . . . : 2001:0:9d38:6ab8:38bb:2bc3:f585:fc6
    本地链接 IPv6 地址 . . . . . : fe80::38bb:2bc3:f585:fc6%13
    默认网关 . . . . . :
```

2) DHCP 包格式

如下表所示：

OP (1)	Htype (1)	Hlen (1)	Hops (1)
Transaction ID (4)			
Seconds (2)		Flags (2)	
Ciaddr (4)			
Yiaddr (4)			

Siaddr (4)
Giaddr (4)
Chaddr (16)
Sname (64)
File (128)
Options (variable)

OP: 若是客户端送给服务器的数据包, 置为 1, 反向为 2;

Htype: 硬件类别, Ethernet 为 1;

Hlen: 硬件长度, Ethernet 为 6;

Hops: 若数据包需经过 router 传送, 每站加 1, 若在同一网内, 则不改变;

Transaction ID: 事务 ID, 是个随机数, 用于客户端和服务端之间匹配请求和消息;

Seconds: 是由用户指定的时间, 指开始地址获取和更新进行后的时间;

Flags: 从 0-15bits, 最左一位为 1 时表示服务器将以广播方式传送数据包给客户端, 其余尚未使用;

Ciaddr: 用户 IP 地址;

Yiaddr: 服务器分配给客户的 IP 地址;

Siaddr: 服务器的 IP 地址;

Giaddr: 网关 IP 地址;

Chaddr: 用户的硬件地址;

Sname: 可选服务器名称, 以 0X00 结尾;

File: 启动文件名;

Options: 厂商标识, 可选的参数字段。

3) DHCP 抓包及分析

5 35.097085	10.122.240.57	10.3.9.2	DHCP	342 DHCP Release	- Transaction ID 0x1f41e6f3
6 43.902057	0.0.0.0	255.255.255.255	DHCP	343 DHCP Discover	- Transaction ID 0x24075796
7 43.906613	10.122.192.1	10.122.240.57	DHCP	342 DHCP Offer	- Transaction ID 0x24075796
8 43.906971	0.0.0.0	255.255.255.255	DHCP	369 DHCP Request	- Transaction ID 0x24075796
9 43.921500	10.122.192.1	10.122.240.57	DHCP	342 DHCP ACK	- Transaction ID 0x24075796

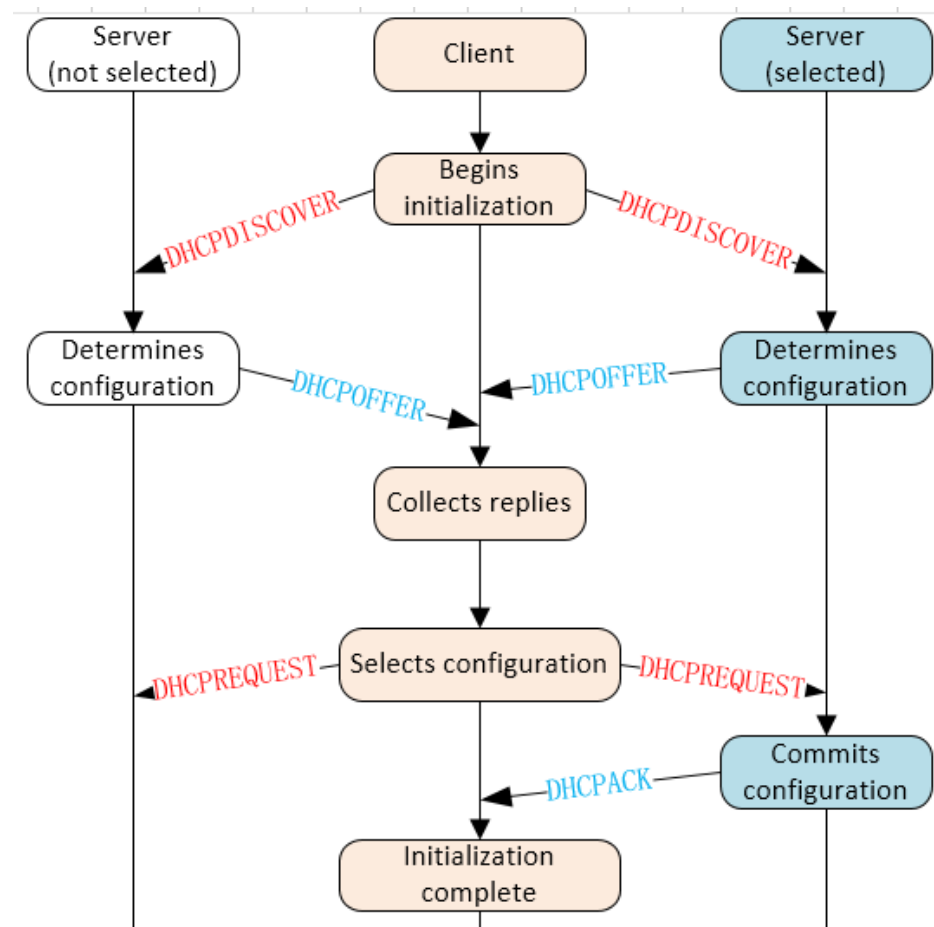
```
> Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: IntelCor_58:11:6e (08:d4:0c:58:11:6e), Dst: Hangzhou_37:84:89 (b0:f9:63:37:84:89)
v Internet Protocol Version 4, Src: 10.122.240.57, Dst: 10.3.9.2
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x5209 (21001)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xd9e3 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.122.240.57
    Destination: 10.3.9.2
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

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

```
0000  b0 f9 63 37 84 89 08 d4 0c 58 11 6e 00 00 45 00  ..c7.... .X.n..E.
0010  01 48 52 09 00 00 00 11 d9 e3 0a 7a f0 39 0a 03  .HR..... .z.9..
0020  09 02 00 44 00 43 01 34 79 b9 01 01 06 00 1f 41  ..D.C.4 y.....A
0030  e6 f3 1e 00 00 00 0a 7a f0 39 00 00 00 00 00 00  .....z .9.....
0040  00 00 00 00 00 00 08 d4 0c 58 11 6e 00 00 00 00  ..... .X.n....
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  .....
```

由上图可知，源端口号为 68，目的端口号为 67，且 DHCP 服务器不是由路由器充当：DHCP 服务器 IP 地址为 10.3.9.2，而路由器 IP 地址为 10.122.240.57。有 DHCP Relay，Relay agent IP address 为 10.122.192.1

工作流程如下：



① 寻找服务器

根据客户端是否是第一次登录网络，DHCP 工作形式会有所不同。

当 DHCP 客户端第一次登录网络时，它会向网络发送一个 DHCP DISCOVER 数据包。因为客户端还不知道自己属于哪一个网络，所以数据包的来源地址会为 0.0.0.0，而目的地址会为 255.255.255.255，然后附上 DHCP discover 信息，向网络进行广播。

DHCP discover 相应报文信息有：

```

> Frame 6: 343 bytes on wire (2744 bits), 343 bytes captured (2744 bits) on interface 0
> Ethernet II, Src: IntelCor_58:11:6e (08:d4:0c:58:11:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
✓ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total length: 329
  Identification: 0x2c55 (11349)
  > Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
  Header checksum: 0x0d50 [validation disabled]
  [Header checksum status: Unverified]
  Source: 0.0.0.0
  Destination: 255.255.255.255
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
  User Datagram Protocol, Src Port: 68, Dst Port: 67
  0000 ff ff ff ff ff ff 08 d4 0c 58 11 6e 00 00 45 00 .....X.n..E..
  0010 01 49 2c 55 00 00 00 11 0d 50 00 00 00 00 ff ff ..1.U....P....
  0020 ff ff 00 44 00 43 01 35 eb 47 01 01 06 00 24 07 ..D.C.5 .G...$.
  0030 57 96 00 00 00 00 00 00 00 00 00 00 00 00 00 00 W.....
  0040 00 00 00 00 00 00 08 d4 0c 58 11 6e 00 00 00 00 .....X.n....
  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 .....
  
```

此时还没有分配地址，所以源地址为零，也不知道 DHCP 服务器地址，所以目的地址为零。

```
> Frame 6: 343 bytes on wire (2744 bits), 343 bytes captured (2744 bits) on interface 0
> Ethernet II, Src: IntelCor_58:11:6e (08:d4:0c:58:11:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x24075796
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  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: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End

0000  ff ff ff ff ff ff 08 d4 0c 58 11 6e 08 00 45 00  ....X.n..E.
0010  01 49 2c 55 00 00 80 11 0d 50 00 00 00 00 ff ff  .I,U....P.....
0020  ff ff 00 44 00 43 01 35 eb 47 01 01 06 00 24 07  ...D.C.5 .G...$.
0030  57 96 00 00 00 00 00 00 00 00 00 00 00 00 00 00  W.....
0040  00 00 00 00 00 00 00 08 d4 0c 58 11 6e 00 00 00 00  ....X.n....
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  ....
```

字段	值	含义
OP	01	该数据包为客户端送往 DHCP 服务器
Htype	01	硬件类型为以太网
Hlen	06	硬件的物理地址长度为 6 个字节，即以太网
Hops	00	客户端被设置为 0，表示如果要用中继代理可以随意选择
Transaction ID	24075796	传输标识，一个由客户端选择的随机数，并在客户端和服务端通信中使用
Seconds	0000	客户端填写
Ciaddr	00000000	客户端 IP 地址，由于正在等待分配地址，所以该段用全 0 填写
Yiaddr	00000000	指定客户端的地址，在 Boot request 中为全 0
Siaddr	00000000	DHCP 服务器的 IP 地址
Giaddr	00000000	中继代理的 IP 地址，通过一个中继开机使用
Chaddr	08:d4:0c:58:11:6e	MAC 地址
Sname		未给出
File		未给出

② 提供 IP 租用地址

当 DHCP 服务器监听到客户端发出的 DHCP discover 广播后，会从那些还没有租出的地址范围内选择最前面的空置 IP，连同其它 TCP/IP 设定，响应给客户端一个 DHCP offer 数据包。

由于客户端在开始的时候还没有 IP 地址，所以在 DHCP discover 数据包内会带有其 MAC 地址信息，并且有一个 Transaction ID 来辨别该数据包。DHCP offer 数据包则会根据这些资料，传递相应信息给要求租约的客户。根据服务器端的设定，DHCP offer 数据包会包含一个租约期限的信息。DHCP offer 相应报文信息有：

```

> Frame 7: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
< Internet Protocol Version 4, Src: 10.122.192.1, Dst: 10.122.240.57
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xe0 (DSCP: CS7, ECN: Not-ECT)
    Total Length: 328
    Identification: 0xe34c (58188)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0x1149 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.122.192.1
    Destination: 10.122.240.57
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  < User Datagram Protocol, Src Port: 67, Dst Port: 68

```

0000	08 d4 0c 58 11 6e b0 f9 63 37 84 89 08 00 45 e0	...X.n... c7....E.
0010	01 48 e3 4c 00 00 ff 11 11 49 0a 7a c0 01 0a 7a	.H.L.... .I.Z...Z
0020	f0 39 00 43 00 44 01 34 e2 16 02 01 06 00 24 07	.9.C.D.4\$.
0030	57 96 00 00 00 00 00 00 00 00 0a 7a f0 39 00 00	W..... .z.9..
0040	00 00 0a 7a c0 01 08 d4 0c 58 11 6e 00 00 00 00	...Z.... .X.n....
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

此时，源端口号和目的端口号与 DHCP discover 的刚好相反，即 DHCP 服务器用端口号 67，客户端用端口号 68。

```

< User Datagram Protocol, Src Port: 67, Dst Port: 68
  Source Port: 67
  Destination Port: 68
  Length: 308
  Checksum: 0xe216 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 2]
< Bootstrap Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x24075796
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.122.240.57
  Next server IP address: 0.0.0.0
  Relay agent IP address: 10.122.192.1
  Client MAC address: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier
  > Option: (51) IP Address Lease Time
  > Option: (1) Subnet Mask
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  > Option: (255) End
  Padding: 0000000000

```

0000	08 d4 0c 58 11 6e b0 f9 63 37 84 89 08 00 45 e0	...X.n... c7....E.
0010	01 48 e3 4c 00 00 ff 11 11 49 0a 7a c0 01 0a 7a	.H.L.... .I.Z...Z
0020	f0 39 00 43 00 44 01 34 e2 16 02 01 06 00 24 07	.9.C.D.4\$.
0030	57 96 00 00 00 00 00 00 00 00 0a 7a f0 39 00 00	W..... .z.9..
0040	00 00 0a 7a c0 01 08 d4 0c 58 11 6e 00 00 00 00	...Z.... .X.n....
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 00 00 63 82 53 63 35 01 02 36 04 0ac. Sc5..6..
0120	03 09 02 33 04 00 00 0e 10 01 04 ff ff c0 00 03	...3.....
0130	04 0a 7a c0 01 06 0c 0a 03 09 04 0a 03 09 05 0a	...Z.....
0140	03 09 06 0f 0b 62 75 70 74 2e 65 64 75 2e 63 6ebup t.edu.cn
0150	ff 00 00 00 00 00

字段	值	含义
OP	02	该数据包为 DHCP 服务器送往客户端
Htype	01	硬件类型为以太网
Hlen	06	硬件的物理地址长度为 6 个字节，即以太网
Hops	00	客户端被设置为 0，表示如果要用中继代理可以随意选择
Transaction ID	24075796	传输标识，一个由客户端选择的随机数，并在客户端和服务端通信中使用
Seconds	0000	客户端填写
Ciaddr	00000000	客户端 IP 地址，由于正在等待分配地址，所以该段用全 0 填写
Yiaddr	0a7af039	用来指定客户端的地址，DHCP 分配的地址为 10.122.240.57
Siaddr	00000000	DHCP 服务器的 IP 地址
Giaddr	0a7ac001	中继代理的 IP 地址，通过一个中继开机使用
Chaddr	08:d4:0c:58:11:6e	MAC 地址
Sname		未给出
File		未给出

Magic cookie: DHCP			
✓	Option: (53) DHCP Message Type (Offer)		
	Length: 1		
	DHCP: Offer (2)		
✓	Option: (54) DHCP Server Identifier		
	Length: 4		
	DHCP Server Identifier: 10.3.9.2		
✓	Option: (51) IP Address Lease Time		
	Length: 4		
	IP Address Lease Time: (3600s) 1 hour		
✓	Option: (1) Subnet Mask		
	Length: 4		
	Subnet Mask: 255.255.192.0		
✓	Option: (3) Router		
	Length: 4		
	Router: 10.122.192.1		
✓	Option: (6) Domain Name Server		
	Length: 12		
	Domain Name Server: 10.3.9.4		
	Domain Name Server: 10.3.9.5		
	Domain Name Server: 10.3.9.6		
✓	Option: (15) Domain Name		
	Length: 11		
	Domain Name: bupt.edu.cn		
✓	Option: (255) End		
	Option End: 255		
	Padding: 0000000000		
0000	08 d4 0c 58 11 6e b0 f9	63 37 84 89 08 00 45 e0	...X.n.. c7...E.
0010	01 48 e3 4c 00 00 ff 11	11 49 0a 7a c0 01 0a 7a	.H.L.... .I.Z...Z
0020	f0 39 00 43 00 44 01 34	e2 16 02 01 06 00 24 07	.9.C.D.4\$.
0030	57 96 00 00 00 00 00 00	00 00 0a 7a f0 39 00 00	W..... ..Z.9..
0040	00 00 0a 7a c0 01 08 d4	0c 58 11 6e 00 00 00 00	...Z.... .X.n....
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

由上图可得：

DHCP 服务器地址为 10.3.9.2；

IP 地址租期为 1 小时；
子网掩码为 255.255.192.0；
域名是 bupt.edu.cn；
路由是 10.122.192.1；
DNS 服务器地址有 10.3.9.4/10.3.9.5/10.3.9.6；
DHCP 中继代理为 router，其地址为 10.122.192.1

③ 接受 IP 租约

若客户端收到网络上多台 DHCP 服务器的响应，只会挑选其中一个 DHCP offer，并向网络发送一个 DHCP request 广播数据包，告诉所有 DHCP 服务器它将指定接受哪一台服务器提供的 IP 地址。同时，客户端还会向网络发送一个 ARP 数据包，查询网络上有没有其他机器使用该 IP 地址，若发现该 IP 已被占用，客户端会送出一个 DHCP declient 数据包给 DHCP 服务器，拒绝接受 DHCP offer，并重新发送 DHCP discover 信息。

实际上，并不是所有 DHCP 客户端都会无条件接受 DHCP 服务器的 offer，尤其是这些主机安装有其它 TCP/IP 相关的客户软件。

DHCP request 相应报文信息有：

> Frame 8: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits) on interface 0	
▼ Ethernet II, Src: IntelCor_58:11:6e (08:d4:0c:58:11:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	
> Destination: Broadcast (ff:ff:ff:ff:ff:ff) > Source: IntelCor_58:11:6e (08:d4:0c:58:11:6e) Type: IPv4 (0x0800)	
▼ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255	
0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 355 Identification: 0x2c56 (11350) > Flags: 0x00 Fragment offset: 0 Time to live: 128 Protocol: UDP (17) Header checksum: 0x0d35 [validation disabled] [Header checksum status: Unverified] Source: 0.0.0.0 Destination: 255.255.255.255 [Source GeoIP: Unknown] [Destination GeoIP: Unknown]	
▼ User Datagram Protocol, Src Port: 68, Dst Port: 67	
Source Port: 68 Destination Port: 67 Length: 335 Checksum: 0x230e [unverified] [Checksum Status: Unverified] [Stream index: 1]	
> Bootstrap Protocol (Request)	
0000	ff ff ff ff ff 08 d4 0c 58 11 6e 08 00 45 00X.n..E.
0010	01 63 2c 56 00 00 80 11 0d 35 00 00 00 00 ff ff .c,V.... .5.....
0020	ff ff 00 44 00 43 01 4f 23 0e 01 01 06 00 24 07 ...D.C.O #.....\$.
0030	57 96 00 00 00 00 00 00 00 00 00 00 00 00 00 00 W.....
0040	00 00 00 00 00 00 08 d4 0c 58 11 6e 00 00 00 00X.n....
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 01c. Sc5...=..
0120	08 d4 0c 58 11 6e 32 04 0a 7a f0 39 36 04 0a 03 ...X.n2. .z.96...
0130	09 02 0c 0f 44 45 53 4b 54 4f 50 2d 4f 31 45 39DESK TOP-01E9
0140	4c 33 4e 51 12 00 00 00 44 45 53 4b 54 4f 50 2d L3NQ.... DESKTOP-
0150	4f 31 45 39 4c 33 4e 3c 08 4d 53 46 54 20 35 2e 01E9L3N< .MSFT 5.
0160	30 37 0d 01 03 06 0f 1f 21 2b 2c 2e 2f 79 f9 fc 07..... !+./y..

由上图可知，目的地址为广播地址，告诉所有 DHCP 服务器它将要指定接受哪一台服务器提供的 IP 地址。

```
> User Datagram Protocol, Src Port: 68, Dst Port: 67
▼ Bootstrap Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x24075796
  Seconds elapsed: 0
  ▼ Bootp flags: 0x0000 (Unicast)
    0... .. = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 0.0.0.0
  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: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  ▼ Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
  ▼ Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
  ▼ Option: (50) Requested IP Address
    Length: 4
    Requested IP Address: 10.122.240.57
  ▼ Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 10.3.9.2
  ▼ Option: (12) Host Name
    Length: 15
    Host Name: DESKTOP-01E9L3N
  ▼ Option: (81) Client Fully Qualified Domain Name
    Length: 18
    > Flags: 0x00
    A-RR result: 0
    Length: 18
    > Flags: 0x00
    A-RR result: 0
    PTR-RR result: 0
    Client name: DESKTOP-01E9L3N
    Length: 18
    > Flags: 0x00
    A-RR result: 0
    PTR-RR result: 0
    Client name: DESKTOP-01E9L3N
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End

0010 01 63 2c 56 00 00 80 11 0d 35 00 00 00 ff ff .C.V... .5.....
0020 ff ff 00 44 00 43 01 4f 23 0e 01 01 06 00 24 07 ...D.C.O #.....$
0030 57 96 00 00 00 00 00 00 00 00 00 00 00 00 00 W.....
0040 00 00 00 00 00 00 08 d4 0c 58 11 6e 00 00 00 .....X.n....
0050 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 .....
0070 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 .....
0090 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 .....
00b0 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 .....
00d0 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 .....
00f0 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 .....
0110 00 00 00 00 00 00 63 82 53 63 35 01 03 3d 07 01 .....C. Sc5...=..
0120 08 d4 0c 58 11 6e 32 04 0a 7a f0 39 36 04 0a 03 ...X.n2. .z.96...
0130 09 02 0c 0f 44 45 53 4b 54 4f 50 2d 4f 31 45 39 ...DESK TOP-01E9
0140 4c 33 4e 51 12 00 00 00 44 45 53 4b 54 4f 50 2d L3NQ.... DESKTOP-
0150 4f 31 45 39 4c 33 4e 3c 08 4d 53 46 54 20 35 2e 01E9L3N< .MSFT 5.
0160 30 37 0d 01 03 06 0f 1f 21 2b 2c 2e 2f 79 f9 fc 07..... !+./y..
0170 ff
```

此时，客户端 id 为 MAC 地址，request IP address 为 10.122.240.57。

④ 租约确认

DHCP 客户端发送的 DHCP request 广播消息会达到所有的 DHCP 服务器。DHCP request 消息中的 Server identifier 指明了客户端所使用的 DHCP 服务器，未被指明的服务器收到该消息后就认为客户端拒绝了自己的 offer 报文，不再向客户端发送回应报文了，而被选中的 DHCP 服务器则储存客户端的标识和分配的 IP 地址及其他信息于数据库中，并回应客户端一个 DHCP ack 消息。在 DHCP ack 消息中收到的任何参数都不能和之前收到的 DHCP offer 消息中的有冲突和不同，其中 Yiaddr 字段就是客户端即将分配的地址。

DHCP ack 相应报文信息有：

> Frame 9: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0		
▼ Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: IntelCor_58:11:6e (08:d4:0c:58:11:6e)		
> Destination: IntelCor_58:11:6e (08:d4:0c:58:11:6e)		
> Source: Hangzhou_37:84:89 (b0:f9:63:37:84:89)		
Type: IPv4 (0x0800)		
▼ Internet Protocol Version 4, Src: 10.122.192.1, Dst: 10.122.240.57		
0100 = Version: 4		
.... 0101 = Header Length: 20 bytes (5)		
> Differentiated Services Field: 0xe0 (DSCP: CS7, ECN: Not-ECT)		
Total length: 328		
Identification: 0xe34f (58191)		
> Flags: 0x00		
Fragment offset: 0		
Time to live: 255		
Protocol: UDP (17)		
Header checksum: 0x1146 [validation disabled]		
[Header checksum status: Unverified]		
Source: 10.122.192.1		
Destination: 10.122.240.57		
[Source GeoIP: Unknown]		
[Destination GeoIP: Unknown]		
▼ User Datagram Protocol, Src Port: 67, Dst Port: 68		
Source Port: 67		
Destination Port: 68		
Length: 308		
Checksum: 0xdf16 [unverified]		
[Checksum Status: Unverified]		
[Stream index: 2]		
> Bootstrap Protocol (ACK)		
0000	08 d4 0c 58 11 6e b0 f9 63 37 84 89 08 00 45 e0	...X.n.. c7....E.
0010	01 48 e3 4f 00 00 ff 11 11 46 0a 7a c0 01 0a 7a	.H.O.... .F.Z...Z
0020	f0 39 00 43 00 44 01 34 df 16 02 01 06 00 24 07	.9.C.D.4\$.
0030	57 96 00 00 00 00 00 00 00 00 0a 7a f0 39 00 00	W..... .z.9..
0040	00 00 0a 7a c0 01 08 d4 0c 58 11 6e 00 00 00 00	...Z.... .X.n....
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 0aC. Sc5..6..
0120	03 09 02 33 04 00 0e 10 01 04 ff ff c0 00 03	...3.....
0130	04 0a 7a c0 01 06 0c 0a 03 09 04 0a 03 09 05 0a	..Z.....
0140	03 09 06 0f 0b 62 75 70 74 2e 65 64 75 2e 63 6ebup t.edu.cn
0150	ff 00 00 00 00 00
> User Datagram Protocol, Src Port: 67, Dst Port: 68		
▼ Bootstrap Protocol (ACK)		
Message type: Boot Reply (2)		
Hardware type: Ethernet (0x01)		
Hardware address length: 6		
Hops: 0		
Transaction ID: 0x24075796		
Seconds elapsed: 0		
> Bootp flags: 0x0000 (Unicast)		
Client IP address: 0.0.0.0		
Your (client) IP address: 10.122.240.57		
Next server IP address: 0.0.0.0		
Relay agent IP address: 10.122.192.1		
Client MAC address: IntelCor_58:11:6e (08:d4:0c:58:11:6e)		
Client hardware address padding: 00000000000000000000		
Server host name not given		
Boot file name not given		
Magic cookie: DHCP		
▼ Option: (53) DHCP Message Type (ACK)		
Length: 1		
DHCP: ACK (5)		
▼ Option: (54) DHCP Server Identifier		
Length: 4		
DHCP Server Identifier: 10.3.9.2		
▼ Option: (51) IP Address Lease Time		
Length: 4		
IP Address Lease Time: (3600s) 1 hour		
▼ Option: (1) Subnet Mask		
Length: 4		
Subnet Mask: 255.255.192.0		
▼ Option: (3) Router		
Length: 4		
Router: 10.122.192.1		
▼ Option: (6) Domain Name Server		
Length: 12		
Domain Name Server: 10.3.9.4		
Domain Name Server: 10.3.9.5		
Domain Name Server: 10.3.9.6		
▼ Option: (15) Domain Name		
Length: 11		
Domain Name: bup.t.edu.cn		
▼ Option: (255) End		
Option End: 255		
Padding: 0000000000		
0000	08 d4 0c 58 11 6e b0 f9 63 37 84 89 08 00 45 e0	...X.n.. c7....E.
0010	01 48 e3 4f 00 00 ff 11 11 46 0a 7a c0 01 0a 7a	.H.O.... .F.Z...Z
0020	f0 39 00 43 00 44 01 34 df 16 02 01 06 00 24 07	.9.C.D.4\$.
0030	57 96 00 00 00 00 00 00 00 00 0a 7a f0 39 00 00	W..... .z.9..
0040	00 00 0a 7a c0 01 08 d4 0c 58 11 6e 00 00 00 00	...Z.... .X.n....
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 0aC. Sc5..6..
0120	03 09 02 33 04 00 0e 10 01 04 ff ff c0 00 03	...3.....
0130	04 0a 7a c0 01 06 0c 0a 03 09 04 0a 03 09 05 0a	..Z.....
0140	03 09 06 0f 0b 62 75 70 74 2e 65 64 75 2e 63 6ebup t.edu.cn
0150	ff 00 00 00 00 00

实际使用中,在 DHCP 客户端启动或 IP 地址租约期限达到一半时,DHCP 客户端会自动向 DHCP 服务器发送 DHCP request 报文,以完成 IP 租约的更新。如果此 IP 地址有效,则 DHCP 服务器回应 DHCP ack 报文,通知 DHCP 客户端已经获得新 IP 租约。

4. ARP 协议分析

1) ARP 功能及操作原理

ARP 即地址解析协议,实现通过 IP 地址得知其物理地址。

在 TCP/IP 网络环境下,每个主机都分配了一个 32 位 IP 地址,这种互联网地址是在网际范围标识主机的一种逻辑地址。而为了让报文在物理网络上传送,必须知道目的主机的物理地址。这样就存在把 IP 地址变换成物理地址的地址转换问题,而 ARP 协议就用来解决该问题。

其工作原理为:

以主机 A (192.32.65.5) 向主机 B (192.32.65.9) 发送数据为例。

当发送数据时,主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址,若找到了,也就知道了目标 MAC 地址,直接把目标 MAC 地址写入帧中发送即可;若未找到,则在网络上发送一个广播,向同一网段内所有主机发出这样的询问:“我是 192.32.65.5,我的硬件地址是(主机 A 的 MAC 地址),请问 IP 地址为 192.32.65.9 的 MAC 地址是什么?”网络上其他主机并不响应 ARP 询问,只有主机 B 接收到这个帧时,才会向主机 A 做出这样的回应:“192.32.65.9 的 MAC 地址是(主机 B 的 MAC 地址)”。这样主机 A 就知道了主机 B 的 MAC 地址,就可以向主机 B 发送信息了。

同时 A 和 B 更新自己的 ARP 缓存表,下次主机 A 再向主机 B 或主机 B 向主机 A 发送信息时,直接从各自的 ARP 缓存表里查找就可以了。

ARP 缓存表采用了老化机制(即设置了生存时间 TTL),在一段时间内若表中的某一行没有使用,就会被删除,这样大大减少 ARP 缓存表的长度,加快查询速度。

2) ARP 包格式

硬件类型		协议类型
物理地址长度	协议地址长度	操作
源物理地址		
源物理地址		源 IP 地址
源 IP 地址		目的物理地址
目的物理地址		
目的 IP 地址		

硬件类型:指定硬件接口类型,例如,1 表示 Ethernet;

协议类型:指定发送方支持的上层协议类型;

物理地址长度:指定物理地址长度;

协议地址长度:网络层协议的地址长度,例如,4 表示 IP 协议;

操作:指定 ARP 操作类型,例如,1 表示 ARP 请求,2 表示 ARP 应答;

源物理地址:发送方的物理地址;

源 IP 地址:发送方的 IP 地址;

目的物理地址:目的主机物理地址;

目的 IP 地址:目的主机 IP 地址。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	IntelCor_58:11:6e	Broadcast	ARP	42	Who has 169.254.4.64? Tell 0.0.0.0
2	0.994205	IntelCor_58:11:6e	Broadcast	ARP	42	Who has 169.254.4.64? Tell 0.0.0.0
3	1.994025	IntelCor_58:11:6e	Broadcast	ARP	42	Who has 169.254.4.64? Tell 0.0.0.0
4	2.996783	IntelCor_58:11:6e	Broadcast	ARP	42	Gratuitous ARP for 169.254.4.64 (Request)
5	4.097820	IntelCor_58:11:6e	Broadcast	ARP	42	Who has 10.122.192.1? Tell 10.122.240.57
6	4.102963	Hangzhou_37:84:89	IntelCor_58:11:6e	ARP	56	10.122.192.1 is at b0:f9:63:37:84:89
7	4.146525	IntelCor_58:11:6e	Broadcast	ARP	42	Who has 10.122.192.1? Tell 10.122.240.57
8	4.148388	Hangzhou_37:84:89	IntelCor_58:11:6e	ARP	56	10.122.192.1 is at b0:f9:63:37:84:89
9	4.497963	IntelCor_58:11:6e	Broadcast	ARP	42	Who has 10.122.240.57? Tell 0.0.0.0
10	5.497568	IntelCor_58:11:6e	Broadcast	ARP	42	Who has 10.122.240.57? Tell 0.0.0.0
11	6.493743	IntelCor_58:11:6e	Broadcast	ARP	42	Who has 10.122.240.57? Tell 0.0.0.0
12	7.494056	IntelCor_58:11:6e	Broadcast	ARP	42	Gratuitous ARP for 10.122.240.57 (Request)

```

> Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v Ethernet II, Src: IntelCor_58:11:6e (08:d4:0c:58:11:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
  Type: ARP (0x0806)
v Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
  Sender IP address: 10.122.240.57
  Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  Target IP address: 10.122.192.1

```

```

0000 ff ff ff ff ff ff 08 d4 0c 58 11 6e 08 06 00 01 .....X.n...
0010 08 00 06 04 00 01 08 d4 0c 58 11 6e 0a 7a f0 39 .....X.n.z.9
0020 00 00 00 00 00 00 0a 7a c0 01 .....Z ..

```

源 MAC 地址为本主机的 MAC 地址，目的 MAC 为广播地址。

ARP 消息部分显示其为 ARP 请求，硬件类型为以太网，硬件地址有 6 字节，在此之上是 IPv4 协议。

发送 IP 地址是本地 IP 地址，目的 IP 即为想要通信的主机 IP，目的 MAC 等待网关或想要通信主机回复给源主机，故为全 0。

```

v Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
  v Destination: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
    Address: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
    ....00. .... = LG bit: Globally unique address (factory default)
    ....00. .... = IG bit: Individual address (unicast)
  v Source: Hangzhou_37:84:89 (b0:f9:63:37:84:89)
    Address: Hangzhou_37:84:89 (b0:f9:63:37:84:89)
    ....00. .... = LG bit: Globally unique address (factory default)
    ....00. .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Trailer: 00000000000000000000000000000000
v Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Hangzhou_37:84:89 (b0:f9:63:37:84:89)
  Sender IP address: 10.122.192.1
  Target MAC address: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
  Target IP address: 10.122.240.57

```

```

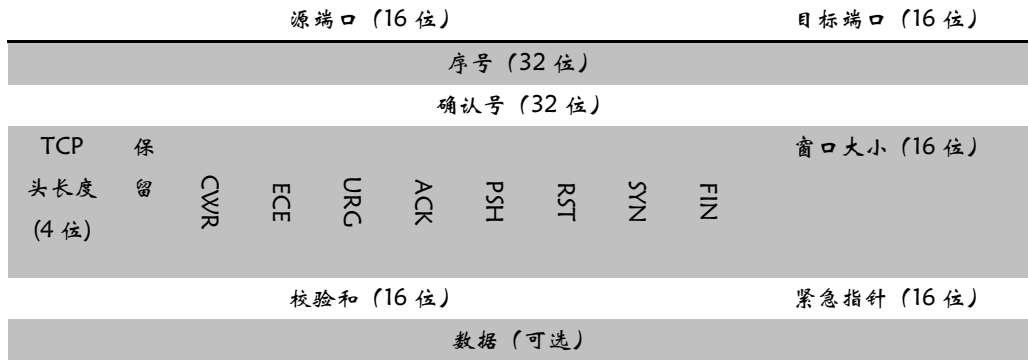
0000 08 d4 0c 58 11 6e b0 f9 63 37 84 89 08 06 00 01 ...X.n.. c7.....
0010 08 00 06 04 00 02 b0 f9 63 37 84 89 0a 7a c0 01 .....c7...z..
0020 08 d4 0c 58 11 6e 0a 7a f0 39 00 00 00 00 00 00 ...X.n.z .9.....
0030 00 00 00 00 00 00 00 00 .....

```

上图中源 MAC 是收到 ARP 请求广播的 IP 地址相符的主机的 MAC，目的 MAC 则是发送 ARP 请求的主机的地址。

5. TCP 协议分析

1) TCP 包格式



确认号：指定下一个期待的字节；

TCP 头长度：指明 TCP 头包含多少个 32 位的字；

CWR 和 ECE：当采用 RFC 3168 说明的显式拥塞通知时，CWR 和 ECE 用作拥塞控制的信号。当 TCP 接收端收到了来自网络的拥塞指示后，就设置 ECE 以便给 TCP 发送端发 ECN-Echo 信号，告诉发送端放慢发送速率。TCP 发送端设置 CWR，给 TCP 接收端发 CWR 信号，这样接收端就知道发送端已经放慢速率，不必再给发送端发 ECN-Echo 信号；

URG：若使用了紧急指针，则置为 1；

ACK：被设置为 1 表示确认号字段有效，否则该段不包含确认信息；

PSH：指明这是被推送数据，即一旦收到数据后立即将数据递交给应用程序，而不是将它缓冲起来直到整个缓冲区满为止；

RST：用于重置一个已经变得混乱的连接，也用于拒收一个无效的段，或拒绝一个连接请求；

SYN：用于建立连接过程；

FIN：用于释放一个连接；

窗口大小：指定了从被确认的字节算起可以发送多少个字节；

校验和：提供了额外的可靠性，校验的范围包括头、数据和与 UDP 一样的概念性伪头；

紧急指针：从当前序号开始找到紧急数据的字节偏移量。

2) TCP 工作流程

3 次握手建立连接：

2 0.129796	10.122.240.57	123.206.186.140	TCP	66 60749→443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3 0.159267	123.206.186.140	10.122.240.57	TCP	66 443→60749 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1386 SACK_PERM=1 WS=128
4 0.159575	10.122.240.57	123.206.186.140	TCP	54 60749→443 [ACK] Seq=1 Ack=1 Win=66304 Len=0

> Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0	
> Ethernet II, Src: IntelCor_58:11:6e (08:d4:0c:58:11:6e), Dst: Hangzhou_37:84:89 (b0:f9:63:37:84:89)	
> Internet Protocol Version 4, Src: 10.122.240.57, Dst: 123.206.186.140	
✖ Transmission Control Protocol, Src Port: 60749, Dst Port: 443, Seq: 0, Len: 0	
Source Port: 60749	
Destination Port: 443	
[Stream index: 1]	
[TCP Segment Len: 0]	
Sequence number: 0 (relative sequence number)	
Acknowledgment number: 0	
Header Length: 32 bytes	
> Flags: 0x002 (SYN)	
Window size value: 64240	
[Calculated window size: 64240]	
Checksum: 0x0001 (unverified)	

0000	b0 f9 63 37 84 89 08 d4 0c 58 11 6e 08 00 45 00	..c7....X.n..E.
0010	00 34 2d c2 40 00 00 06 9b f3 0a 7a f0 39 7b ce	.4-@... ..Z.9{.
0020	ba 8c ed 4d 01 bb 73 01 34 05 00 00 00 00 00 02	...M..s. 4.....
0030	fa f0 ad 01 00 00 02 04 05 b4 01 03 03 08 01 01
0040	04 02	..

第一帧，发送 SYN X：

SACK 使得接收端可以告诉发送端已经接收到的段的序号范围，是对确认号的补充，可用在一个

数据包已丢失但后续数据到达的特定情形。

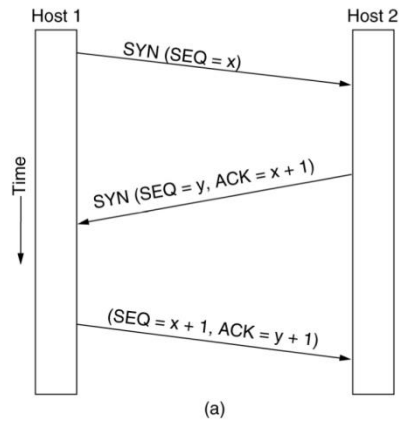
第二帧，发送 SYN Y, ACK X+1:

B->A, WIN=29200, WS=128, 窗口非常大, WS 也很多, 网络性能优良。

第三帧，发送 ACK Y+1:

A->B, 这是建立 TCP 连接的第 3 次握手, 因为在前两帧已经交互了各种 TCP 选项, 所以这次的确认不再带有 TCP 选项。

消息序列图如下:



TCP 数据传输:

16 0.629258	211.68.71.215	10.122.240.57	TCP	1440 [TCP segment of a reassembled PDU]
17 0.629821	10.122.240.57	211.68.71.215	TCP	54 63675->80 [ACK] Seq=649 Ack=11422 Win=259 Len=0
18 0.630725	211.68.71.215	10.122.240.57	TCP	1440 [TCP segment of a reassembled PDU]

```

> Frame 16: 1440 bytes on wire (11520 bits), 1440 bytes captured (11520 bits) on interface 0
> Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
> Internet Protocol Version 4, Src: 211.68.71.215, Dst: 10.122.240.57
< Transmission Control Protocol, Src Port: 80, Dst Port: 63675, Seq: 10036, Ack: 649, Len: 1386
  Source Port: 80
  Destination Port: 63675
  [Stream index: 2]
  [TCP Segment Len: 1386]
  Sequence number: 10036 (relative sequence number)
  [Next sequence number: 11422 (relative sequence number)]
  Acknowledgment number: 649 (relative ack number)
  Header Length: 20 bytes
  > Flags: 0x010 (ACK)
  Window size value: 192
  [calculated window size: 192]
0020 f0 39 00 50 f8 bb cc a1 a4 9c d5 8c c1 df 50 10 .9.P....P.
0030 00 c0 9c 29 00 00 ac 5d 07 bd 9e 67 11 5b 76 92 ...)]...g.[v.
0040 2c c6 09 69 8a 01 a5 56 22 da 6d 3a 16 43 d8 46 ,...i...V ".m:.C.F
  
```

```

> Frame 18: 1440 bytes on wire (11520 bits), 1440 bytes captured (11520 bits) on interface 0
> Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: IntelCor_58:11:6e (08:d4:0c:58:11:6e)
> Internet Protocol Version 4, Src: 211.68.71.215, Dst: 10.122.240.57
< Transmission Control Protocol, Src Port: 80, Dst Port: 63675, Seq: 11422, Ack: 649, Len: 1386
  Source Port: 80
  Destination Port: 63675
  [Stream index: 2]
  [TCP Segment Len: 1386]
  Sequence number: 11422 (relative sequence number)
  [Next sequence number: 12808 (relative sequence number)]
  Acknowledgment number: 649 (relative ack number)
  Header Length: 20 bytes
  > Flags: 0x010 (ACK)
  Window size value: 192
  [calculated window size: 192]
0020 f0 39 00 50 f8 bb cc a1 aa 06 d5 8c c1 df 50 10 .9.P....P.
0030 00 c0 6b e6 00 00 41 c7 b6 79 b5 e0 58 d2 49 55 ..k...A. .y..X.IU
0040 e4 1c 80 de e8 61 9f 7a 85 d4 99 9b fa 92 18 81 .....a.z .....
  
```

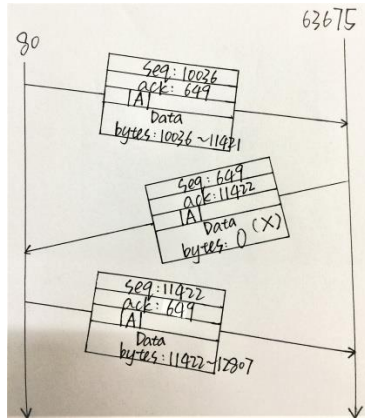
包头的发送序号 (Seq) 为数据部分第一字节的编号;

确认号 (Ack) 在 ACK 标志位有效时, 指明下一个期待的字节;

窗口大小 (Win) 指明接收窗口大小, 即最多还可接收的数据长度;

数据长度 (Len) 指明数据包的数据部分长度;

消息序列图如下:



还可能由于数据错误或超时出现重传情形:

36 0.884901	211.68.71.215	10.122.240.57	TCP	1110 [TCP Retransmission] 80→63674 [PSH, ACK] Seq=1 Ack=733 Win=180 Len=1056
37 0.884962	10.122.240.57	211.68.71.215	TCP	66 63674→80 [ACK] Seq=733 Ack=1057 Win=254 Len=0 SLE=1 SRE=1057

重传数据包设置了 PSH 标志位, 指明是被推送数据, 一旦收到立即递交给应用程序。

4 次握手释放链接:

677 6.381358	123.206.186.140	10.122.240.57	TCP	60 443→60749 [FIN, ACK] Seq=4025 Ack=697 Win=31360 Len=0
678 6.381516	10.122.240.57	123.206.186.140	TCP	54 60749→443 [ACK] Seq=697 Ack=4026 Win=65536 Len=0
679 6.381771	10.122.240.57	123.206.186.140	TCP	54 60749→443 [FIN, ACK] Seq=697 Ack=4026 Win=65536 Len=0
680 6.410939	123.206.186.140	10.122.240.57	TCP	60 443→60749 [ACK] Seq=4026 Ack=698 Win=31360 Len=0

第一帧, 发送 FIN X, ACK Y:

A->B, 客户端主动关闭连接, 变为 TIME_WAIT 状态;

第二帧, 发送 ACK X+1:

B->A, 关闭客户端至服务器的单向数据通道, 出现该情况的原因是服务器仍可能有数据待传输给客户端;

第三帧, 发送 FIN Y, ACK X+1:

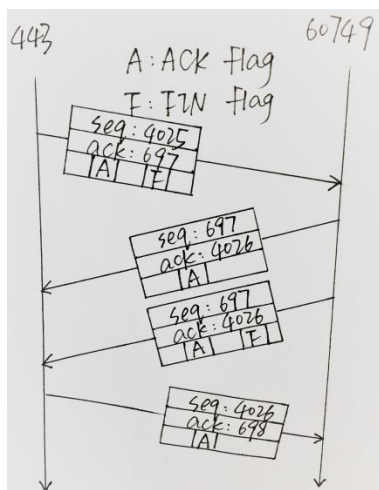
B->A, 服务器主动关闭连接, 变为 TIME_WAIT 状态;

第四帧, 发送 ACK Y+1:

A->B, 关闭客户端至服务器的单向数据通道。

通过 4 次握手分别释放双工信道两个方向的连接。

消息序列图如下:



三、实验结论和心得

1. 实验结论

通过此次实验，进一步了解了网络中常用的各协议格式和工作原理，重点解析了 IP、ICMP、DHCP、ARP、TCP 等协议，并对其中一些关键字段和主要原理有了更深入的理解和更理性的认识。

2. 实验心得

在本次实验中，遇到的主要问题有以下五点：

- ① 根据实验指导书，先进行 IP 协议的抓包与分析。但在使用远程地址为 www.baidu.com 的 ping 命令时，所产生的 IP 数据包均传输在 IPV6 协议下。然而对 IPV6 协议仅为了解，无需细致掌握，便困惑如何才能捕获到 IPV4 数据包。带着疑问，先进行了 DHCP 协议的分析，在此过程中发现将数据发送至 DHCP 中继代理路由器，所产生的 IP 数据包为 IPV4 数据包，该问题得到解决；
- ② IP 协议抓包结束后，擅自将结果以协议为关键字进行了排序，导致始终找不到最后一个分段数据包。随后，又按照正常的时间顺序查看结果，发现最后一个数据包为 ICMP 包，该问题得到解决；
- ③ 验证 IP 分段原理时，对于最后一个 ICMP 包，遗忘了其封装在 IP 包中，还存在 20 字节的 IP 包头，导致各段数据相加非 8000 字节，与同学讨论后发现该问题，得到解决；
- ④ TCP 协议的抓包过程耗费较长时间。起初所选网址不当，导致未出现清晰的两端口数据传输，后更换网址，该问题得到解决；
- ⑤ TCP 实际的连接释放过程与课本上所讲解的有出入。书本上的释放过程大致同连接建立过程，经 3 次握手完成释放，然而，抓包结果通常是经 4 次握手，两个传输方向分别释放。

实践出真知，本次协议数据的捕获和解析实验是对课堂和书本所学知识的补充。网络中的实际情形与已了解到的原理大体一致，但又复杂许多。通过自己动手、亲力亲为捕获数据包，并对 16 进制数据进行分析，加深了对包头各字段功能的理解和记忆，收获颇丰。