华东师范大学软件工程学院实验报告

实验课程:	计算机网络	年　　级:	2022 级
实验编号:	Lab 03	实验名称:	IPV4
姓　　名:	李鹏达	学　　号:	10225101460

1 实验目的

1) 学会通过 Wireshark 分析 IP 协议
2) 了解 IP 数据报的组成
3) 了解 IP 各部分的含义

2 实验内容与实验步骤

2.1 实验内容

2.1.1 捕获数据

启动 Wireshark，在菜单栏的捕获 → 选项中进行设置，选择已连接的以太网，设置捕获过滤器为 `tcp port 80`，捕获 `IP` 数据报。

然后在命令行中使用 `wget` 命令向 `http://www.baidu.com` 发送 `HTTP` 请求。

打开 Wireshark 的捕获窗口，停止捕获。

2.1.2 分析 IPV4 包并绘制报文结构

根据你对 `IP` 报文的理解，画出 `IP` 报文的结构。需要显示出 `IP` 报头字段的位置和大小（字节为单位）。

2.1.3 数据分析

分析所捕获的 `IP` 数据报。在分析时，需要具体分析捕获所得包的以下内容的含义：

1. 版本号（Version）：长度 4 bit 。标识目前采用的 IP 协议的版本号。一般的值为 0100（IPv4），0110（IPv6）
2. 首部长度（Header Length）：长度 4 bit 。这个字段的作用是为了描述 IP 报头的长度，因为在 IP 报头中有变长的可选部分。
3. 区分服务（Differentiated Services ）：8bit，用于为不同的 IP 数据报定义不同的服务质量
4. 总长度（Total Length）：长度 16 bit 。以字节为单位计算的 IP 包的长度（包括头部和数据），所以 IP 包最大长度 65 535 字节。所以，数据包有效载荷的大小 = IP 包总长度（Total Length）- IP 报头长度（Header Length）

5. 标识（Identifier）：长度 16 bit 。该字段和 Flags 和 Fragment Offest 字段联合使用，对较大的数据报进行分段（fragment）操作。路由器将一个数据报拆分后，所有拆分开的分段被标记相同的值，以便目的端设备能够区分哪个包属于被拆分开的包的一部分。
6. 标志（Flags）：长度 3 bit ，该字段第一位不使用。第二位是 DF（Don’ t Fragment）位，DF = 1 时表明路由器不能对该数据报分段。如果一个上层数据报无法在不分段的情况下进行转发，则路由器会丢弃该上层数据包并返回一个错误信息。第三位是 MF（More Fragments）位，MF=1 表示后面还有分片的数据报，MF=0 表示这已经是若干数据报片中的最后一个。
7. 片偏移（Fragment Offset）：长度 13 bit，以 8 个字节为偏移单位。片偏移量用来告诉接收端这个分片在原数据报的相对位置，相对于原数据报的数据部分，该分片从何处开始，是开始还是中间，以便于进行重组还原 IP 包。
8. 生存时间（TTL）：长度 8 bit，以跳数为单位。用以表明数据报文在网络传输过程中能经过的跳数。根据操作系统不同，TTL 默认值不同，每经过一个三层设备如路由器的处理，TTL 值会减去 1，当 TTL=0 的时候，此数据报就会被丢弃。这个字段可以防止由于路由环路而导致 IP 包在网络中不停被转发。
9. 协议（Protocol）：长度 8 bit 。标识了上层所使用的协议。
10. 首部校验和（Header Checksum）：长度 16 bit 。用来做 IP 头部的正确性检测，但不包含数据部分

2.1.4 回答问题

By looking at the IP packets in your trace, answer these questions:

1. What are the IP addresses of your computer and the remote server?
2. Does the Total Length field include the IP header plus IP payload, or just the IP payload?
3. How does the value of the Identification field change or stay the same for different packets? For instance, does it hold the same value for all packets in a TCP connection or does it differ for each packet? Is it the same in both directions? Can you see any pattern if the value does change?
4. What is the initial value of the TTL field for packets sent from your computer? Is it the maximum possible value, or some lower value?
5. How can you tell from looking at a packet that it has not been fragmented? Most often IP packets in normal operation are not fragmented. But the receiver must have a way to be sure. Hint: you may need to read your text to confirm a guess.
6. What is the length of the IP Header and how is this encoded in the header length field? Hint: notice that only 4 bits are used for this field, as the version takes up the other 4 bits of the byte. You may guess and check your text.

2.1.5 Internet Path

在命令行下使用 tracert 命令，查看到达 `www.baidu.com` 的路由路径。根据输出画出网络路径。

2.1.6 计算 `checksum`

IP 报头的校验和可以用来验证一个数据包是否正确。

选择一个 IP 报文，计算它的 checksum。

计算对 IP 首部检验和的算法如下：

(1) 把 IP 数据包的校验和字段置为 0。
(2) 把首部看成以 16 位为单位的数字组成，依次进行二进制求和（注意：求和时应将最高位的进位保存，所以加法应采用 32 位加法）。
(3) 将上述加法过程中产生的进位（最高位的进位）加到低 16 位（采用 32 位加法时，即为将高 16 位与低 16 位相加，之后还要把该次加法最高位产生的进位加到低 16 位）。
(4) 将上述的和取反，即得到校验和。

2.1.7 问题讨论

We encourage you to explore IP on your own once you have completed this lab. Some ideas：

1. Read about and experiment with IPv6. Modern operating systems already include support for IPv6so you may be able to capture IPv6 traffic on your network. You can also "join the IPv6'backbone by tunneling to an IPv6 provider.
2. Learn about tunnels, which wrap an IP packet within another IP header.
3. Read about IP geolocation, It is the process of assigning a geographical location to an IP addressusing measurements or clues from its name administrative databases. Try a geolocation service.
4. Learn about IPsec or IP security. It provides confidentiality and authentication for IP packets, and isoften used as part of VPNs.

2.2 实验步骤

1) 启动 `Wireshark`，在菜单栏的捕获 → 选项中进行设置，选择已连接的以太网，设置捕获过滤器为 `tcp port 80`，将混杂模式设为关闭, 勾选 `enable network name resolution`. 然后开始捕获。
2) 回到命令行，使用 `wget` 命令发起 `HTTP` 请求

```
1 PS> wget http://www.baidu.com
```

3) 回到 `Wireshark`，停止捕获。
4) 分析捕获到的 `IP` 数据报，画出其结构。
5) 对捕获到的 `IP` 数据报进行数据分析，并回答相关问题。
6) 在命令行中使用 `tracert` 命令，查看到达 `www.baidu.com` 的路由路径。

```
1 PS> tracert www.baidu.com
```

7) 选择一个 `IP` 数据报，计算它的 checksum。
8) 问题讨论

3 实验环境

- 操作系统：Windows 11 家庭中文版 23H2 22631.2715
- 网络适配器：Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter(201NGW)
- Wireshark：Version 4.2.0 (v4.2.0-0-g54eedfc63953)
- wget：GNU Wget 1.21.4 built on mingw32

4 实验结果与分析

4.1 捕获数据

首先，我们启动 Wireshark，在菜单栏的捕获 → 选项中进行设置，选择已连接的以太网，设置捕获过滤器为 tcp port 80，捕获 IP 数据报。

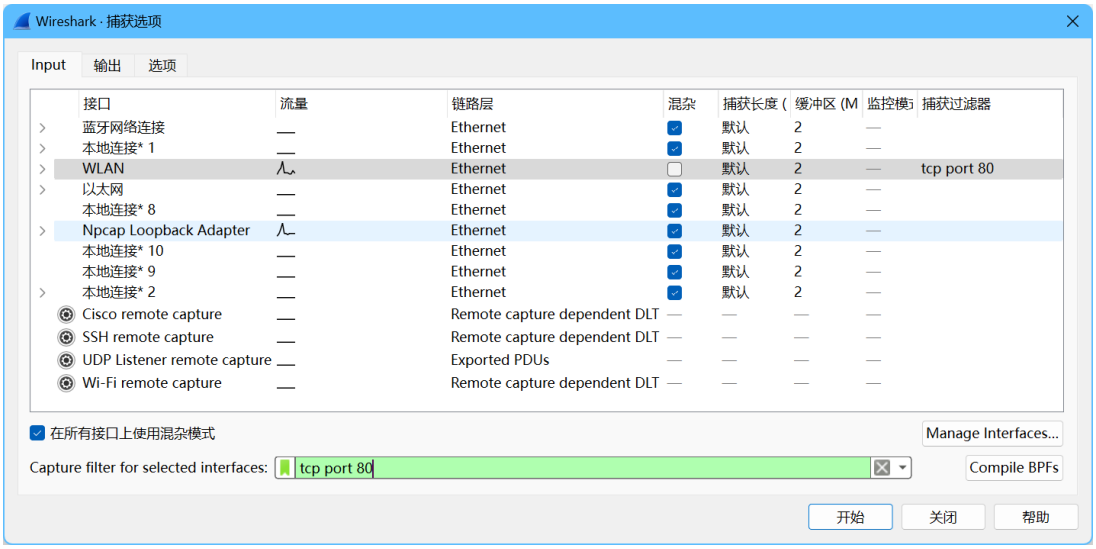

图 1: 设置捕获选项

然后，在命令行中使用 wget 命令向 http://www.baidu.com 发送 HTTP 请求。

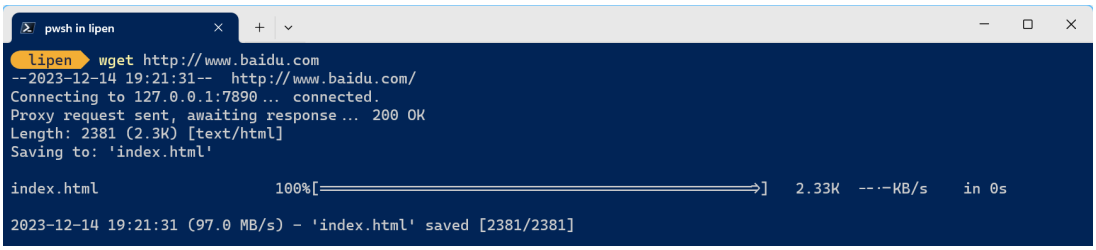

图 2: 使用 wget 发送 HTTP 请求

打开 Wireshark 的捕获窗口，停止捕获。捕获结果如下图所示：

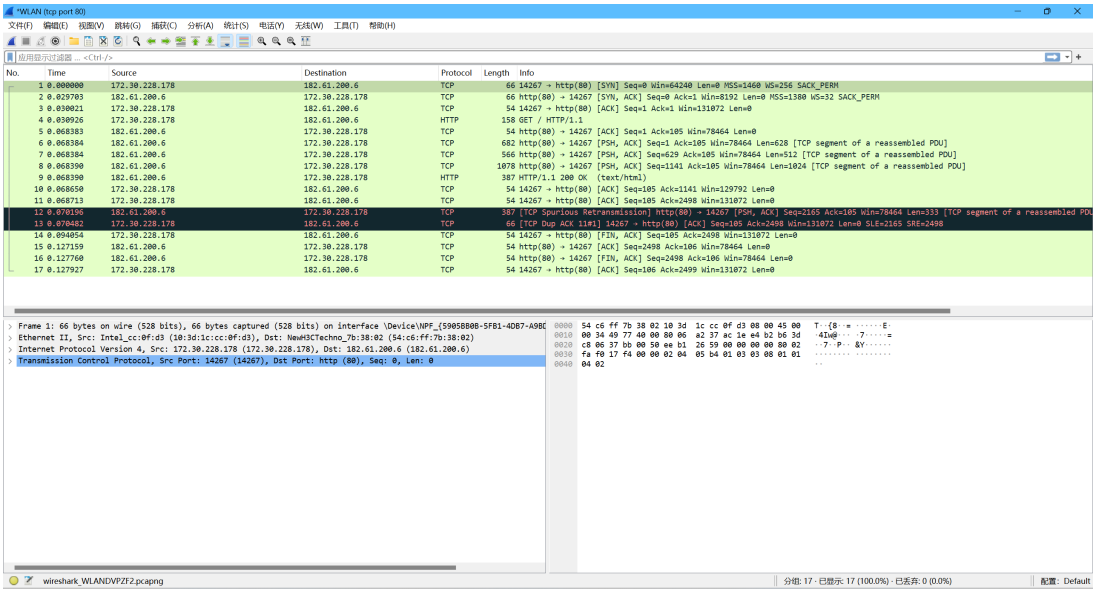

图 3: 捕获结果

4.2 分析 IPV4 包并绘制报文结构 & 数据分析

我们选择其中的一个 IP 数据报，分析其结构，如下图所示：

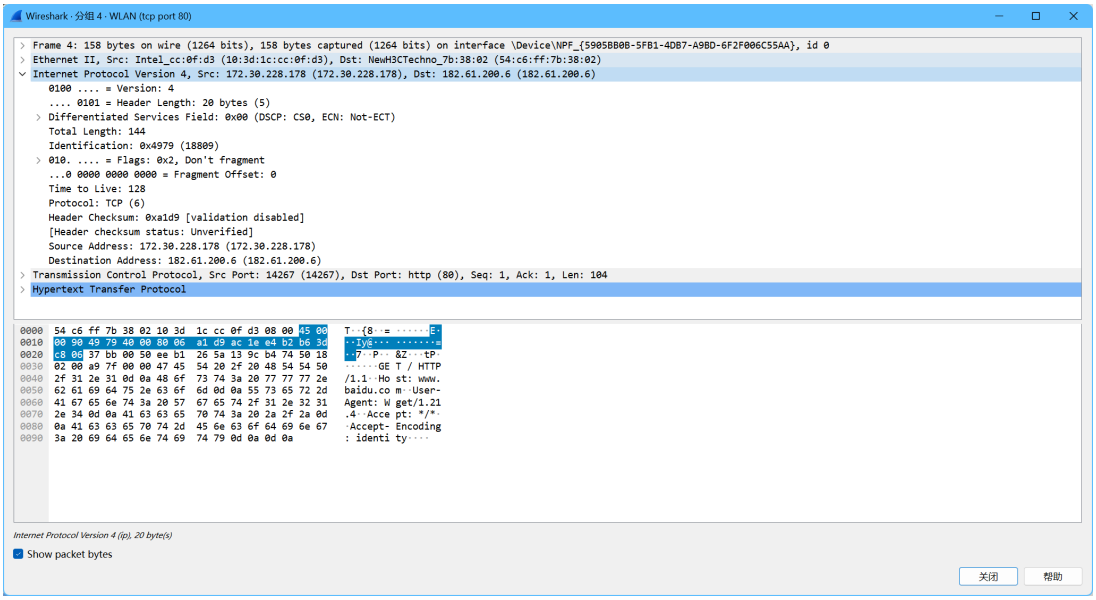

图 4: IP 数据报结构

可以看到，第一个字段表示版本号，长度为 4bit，表示目前采用的 IP 协议的版本号。一般为 0100(IPv4) 或 0110(IPv6)。

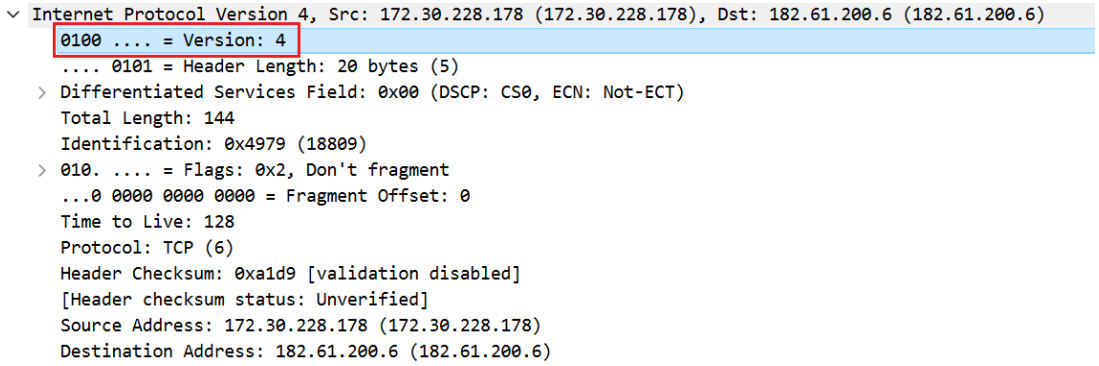

图 5: Version 字段

第二个字段表示首部长度，长度为 4bit，表示 IP 报头的长度。在这个数据报中，首部长度为 20 bytes。

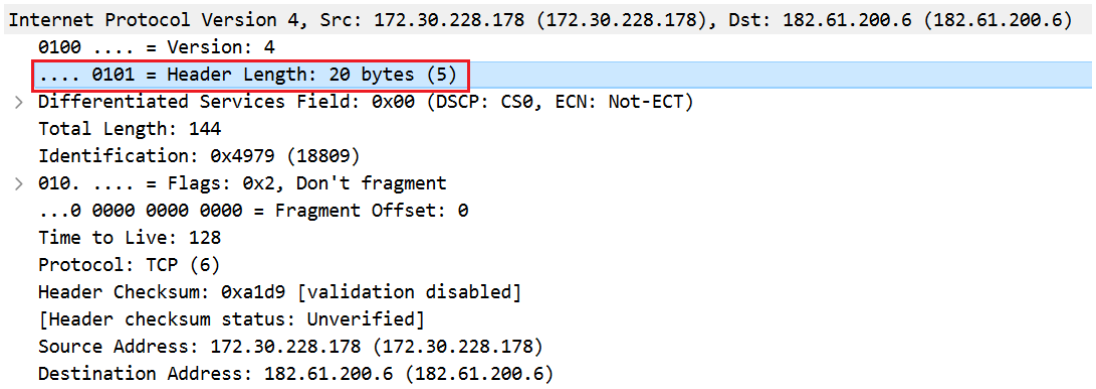

图 6: Header Length 字段

第三个字段表示区分服务，长度为 1 byte，用于为不同的 IP 数据报定义不同的服务质量。

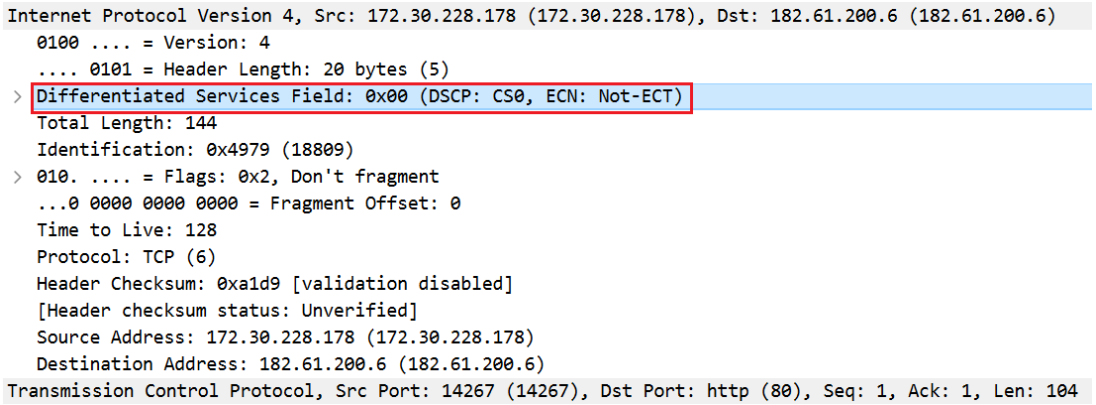

图 7: Differentiated Services 字段

在这个字段中，包括两个部分，第一个部分是 DSCP，长度为 6 bit，表示区分服务代码点，用于区分不同的

服务质量。第二个部分是 ECN，长度为 2 bit，表示显式拥塞通知，用于指示网络拥塞。在这个数据报中，DSCP 的值为 0x00，表示默认服务，ECN 的值为 0x00，表示没有拥塞。

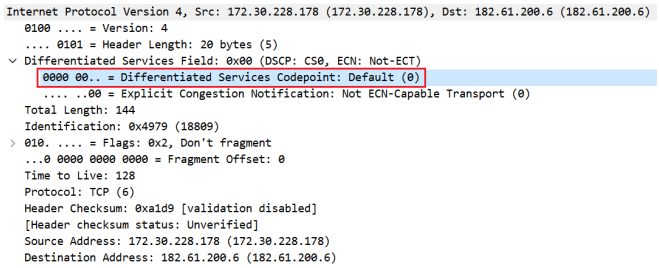

图 8: DSCP 字段

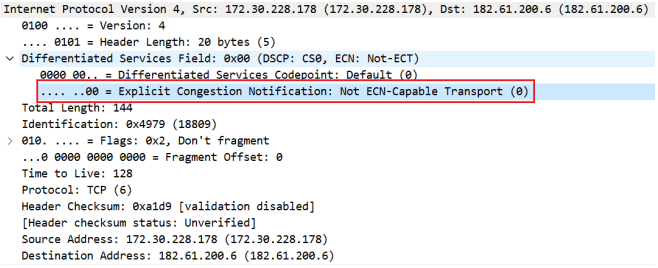

图 9: ECN 字段

第四个字段表示总长度，长度为 2 bytes，表示以字节为单位计算的 IP 包的长度（包括头部和数据），所以 IP 包最大长度 65 535 bytes。数据包有效载荷的大小 = IP 包总长度（Total Length）- IP 报头长度（Header Length）。在这个数据报中，总长度为 144 bytes。

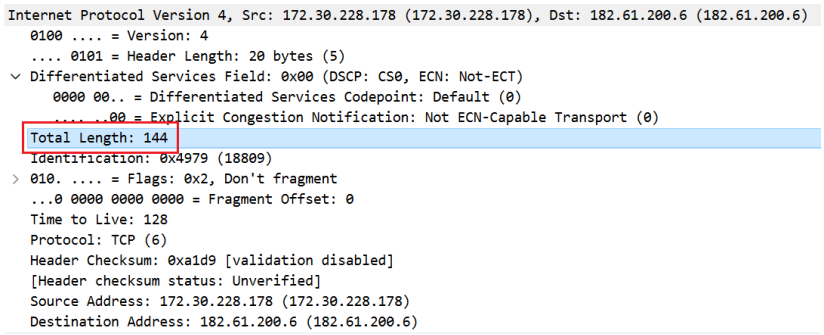

图 10: Total Length 字段

第五个字段为标识，长度为 2 bytes，该字段和 Flags 和 Fragment Offest 字段联合使用，对较大的数据报进行分段（fragment）操作。路由器将一个数据报拆分后，所有拆分开的分段被标记相同的值，以便目的端设备能够区分哪个包属于被拆分开的包的一部分。在这个数据报中，标识为 0x4979。

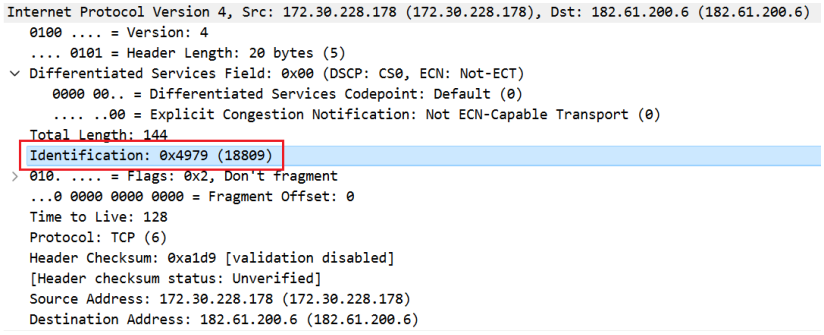

图 11: Identifier 字段

第六个字段为标志，长度为 3 bit，该字段第一位不使用。第二位是 DF（Don’t Fragment）位，DF = 1 时表明路由器不能对该数据报分段。如果一个上层数据报无法在不分段的情况下进行转发，则路由器会丢弃该上层数据包并返回一个错误信息。第三位是 MF（More Fragments）位，MF=1 表示后面还有分片的数据报，MF=0 表示这已经是若干数据报片中的最后一个。在这个数据报中，标志为 0x02，表示不分段，且后面没有分片的数据报。

```
Internet Protocol Version 4, Src: 172.30.228.178 (172.30.228.178), Dst: 182.61.200.6 (182.61.200.6)
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 ⌄ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
   Total Length: 144
   Identification: 0x4979 (18809)
 › 010. .... = Flags: 0x2, Don't fragment
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 128
   Protocol: TCP (6)
   Header Checksum: 0xa1d9 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 172.30.228.178 (172.30.228.178)
   Destination Address: 182.61.200.6 (182.61.200.6)
```

图 12: Flags 字段

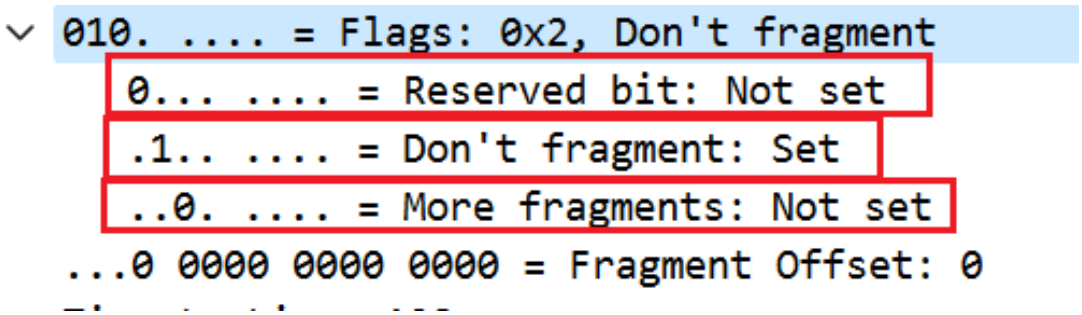

图 13: Flags 字段内容

第七个字段为片偏移，长度为 13 bit，以 8 个字节为偏移单位。片偏移量用来告诉接收端这个分片在原数据报的相对位置，相对于原数据报的数据部分，该分片从何处开始，是开始还是中间，以便于进行重组还原 IP 包。在这个数据报中，片偏移为 0。

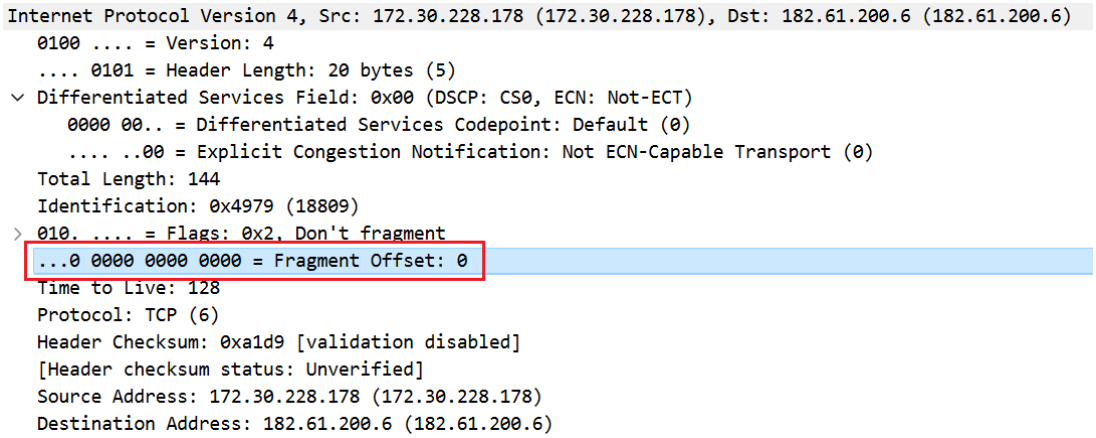

图 14: Fragment Offset 字段

第八个字段为生存时间，长度为 8 bit，以跳数为单位。用以表明数据报文在网络传输过程中能经过的跳数。根据操作系统不同，TTL 默认值不同，每经过一个三层设备如路由器的处理，TTL 值会减去 1，当 TTL=0 的时候，此数据报就会被丢弃。这个字段可以防止由于路由环路而导致 IP 包在网络中不停被转发。在这个数据报中，生存时间为 128。

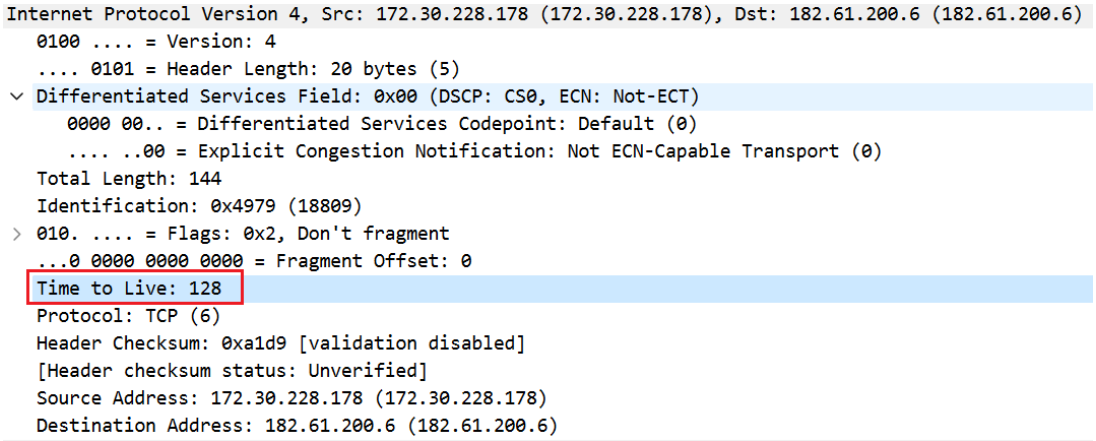

图 15: TTL 字段

第九个字段为协议，长度为 8 bit。标识了上层所使用的协议。在这个数据报中，协议为 TCP，值为 0x06。

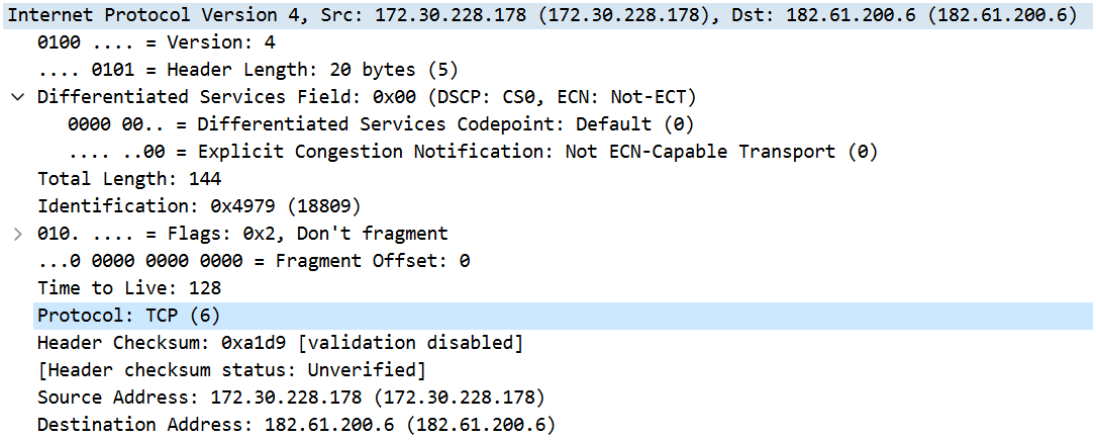

图 16: `Protocol` 字段

第十个字段为首部校验和，长度为 `16 bit`。用来做 IP 头部的正确性检测，但不包含数据部分。在这个数据报中，首部校验和为 `0xa1d9`。

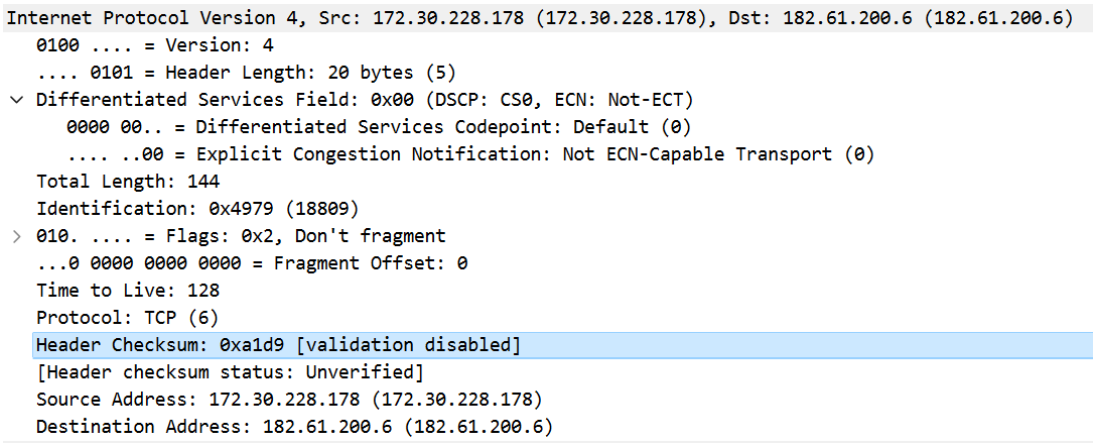

图 17: `Header Checksum` 字段

第十一个字段为源 IP 地址，长度为 `32 bit`，表示发送方的 IP 地址。在这个数据报中，源 IP 地址为 `172.30.228.178`

```
Internet Protocol Version 4, Src: 172.30.228.178 (172.30.228.178), Dst: 182.61.200.6 (182.61.200.6)
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 ⌄ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
   Total Length: 144
   Identification: 0x4979 (18809)
 › 010. .... = Flags: 0x2, Don't fragment
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 128
   Protocol: TCP (6)
   Header Checksum: 0xa1d9 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 172.30.228.178 (172.30.228.178)
   Destination Address: 182.61.200.6 (182.61.200.6)
```

图 18: Source Address 字段

第十二个字段为目的 IP 地址，长度为 32 bit，表示接收方的 IP 地址。在这个数据报中，目的 IP 地址为 182.61.200.6

```
Internet Protocol Version 4, Src: 172.30.228.178 (172.30.228.178), Dst: 182.61.200.6 (182.61.200.6)
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 ⌄ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
   Total Length: 144
   Identification: 0x4979 (18809)
 › 010. .... = Flags: 0x2, Don't fragment
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 128
   Protocol: TCP (6)
   Header Checksum: 0xa1d9 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 172.30.228.178 (172.30.228.178)
   Destination Address: 182.61.200.6 (182.61.200.6)
```

图 19: Destination Address 字段

可以做出如下示意图来表示 IP 数据报的结构：

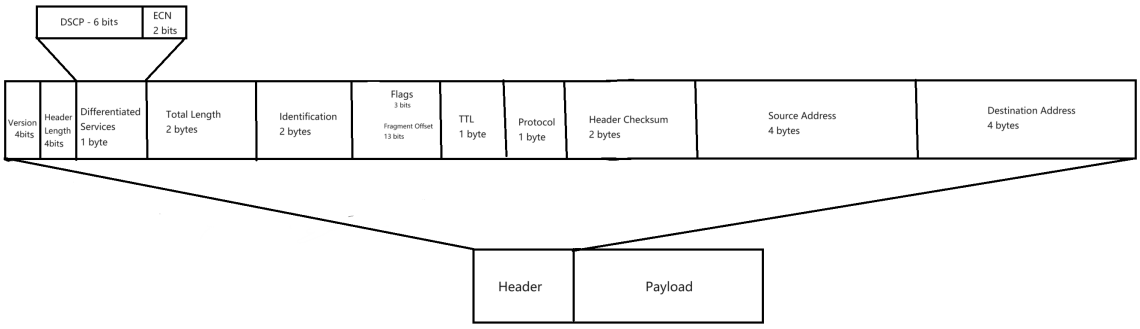

图 20: IP 数据报结构示意图

4.3 回答问题

1. What are the IP addresses of your computer and the remote server?
   我的电脑的 IP 地址为 172.30.228.178，远程服务器的 IP 地址为 182.61.200.6。
2. Does the Total Length field include the IP header plus IP payload, or just the IP payload?
   Total Length 字段包括 IP 报头和 IP 数据的总长度。
3. How does the value of the Identification field change or stay the same for different packets? For instance, does it hold the same value for all packets in a TCP connection or does it differ for each packet? Is it the same in both directions? Can you see any pattern if the value does change?
   标识字段的值在不同的数据包中不同。在同一个 TCP 连接中，标识字段的值不同。在同一个方向上，标识字段的值不同。在不同的方向上，标识字段的值不同。在这个数据报中，标识字段的值为 0x4979。
4. What is the initial value of the TTL field for packets sent from your computer? Is it the maximum possible value, or some lower value?
   我的电脑发送的数据包的生存时间字段的初始值为 128，不是最大值。
5. How can you tell from looking at a packet that it has not been fragmented? Most often IP packets in normal operation are not fragmented. But the receiver must have a way to be sure. Hint: you may need to read your text to confirm a guess.
   如果一个数据包没有被分段，那么它的标志字段的 DF 位为 1，且标志字段的 MF 位为 0。
6. What is the length of the IP Header and how is this encoded in the header length field? Hint: notice that only 4 bits are used for this field, as the version takes up the other 4 bits of the byte. You may guess and check your text.
   IP 报头的长度为 20 bytes，版本号和首部长度字段共占 8 bits，其中版本号占 4 bits，首部长度占 4 bits。

4.4 Internet Path

在命令行下使用 tracert 命令，查看到达 www.baidu.com 的路由路径。根据输出画出网络路径。（实验地点有所差别，顾目标 IP 地址略有不同）

```
lipen tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.a.shifen.com [182.61.200.7] 的路由:

  1     *        *        *     请求超时。
  2     5 ms     6 ms     6 ms  10.100.5.1
  3     7 ms     5 ms     7 ms  202.120.95.246
  4     5 ms     6 ms     7 ms  202.120.95.254
  5    10 ms    10 ms     7 ms  10.255.16.1
  6  1076 ms     6 ms     5 ms  10.255.249.253
  7     *        8 ms     8 ms  10.255.38.254
  8     *        *       10 ms  202.112.27.1
  9     9 ms     8 ms     5 ms  101.4.115.105
 10   532 ms    45 ms    29 ms  101.4.115.201
 11    38 ms    42 ms    35 ms  219.224.103.65
 12    32 ms    30 ms    33 ms  101.4.130.34
 13    32 ms    30 ms    32 ms  182.61.255.36
 14    34 ms    32 ms    34 ms  182.61.254.177
 15     *        *        *     请求超时。
 16     *        *        *     请求超时。
 17     *        *        *     请求超时。
 18    31 ms    70 ms    34 ms  182.61.200.7

跟踪完成。
```

图 21: `tracert` 命令输出

画出网络路径图如下:

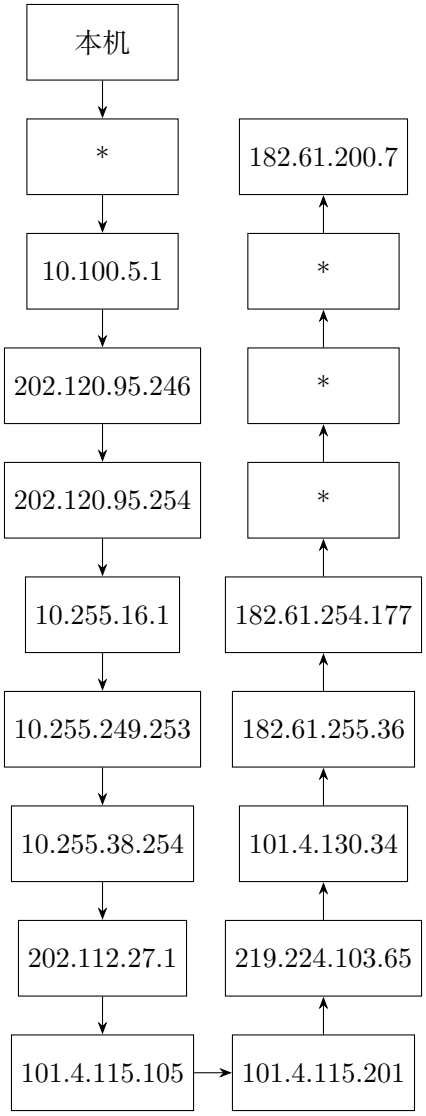

图 22: 网络路径图

4.5 计算 checksum

IP 报头的校验和可以用来验证一个数据包是否正确。我们选择刚才的 IP 报文，计算它的 checksum。将其校验和字段置为 0 后，数据如下：45 00 00 90 49 79 40 00 80 06 00 00 ac 1e e4 b2 b6 3d c8 06
将其分为两个字节一组，进行二进制求和，再将最高位的进位加到低 16 位，得到的结果如下：

```
     45 00
+    00 90
+    49 79
+    40 00
+    80 06
```

```
+     00 00
+     ac 1e
+     e4 b2
+     b6 3d
+     c8 06
---------------
   4 5e 22
+         4
---------------
     5e 26
```

取反后，得到 checksum 为 0xa1d9，与原数据报中的 checksum 字段相同。

```
  ff ff
- 5e 26
-----------
  a1 d9
```

4.6 问题讨论

1. Read about and experiment with IPv6. Modern operating systems already include support for IPv6so you may be able to capture IPv6 traffic on your network. You can also "join the IPv6'backbone by tunneling to an IPv6 provider.

   IPv6 是 IP 协议的下一代协议，它的主要特点是地址空间更大，报头更简单，安全性更好，支持多播和组播，支持流量标签，支持流量优先级，支持更多的选项和扩展，支持更多的协议。现代操作系统已经支持 IPv6，可以在网络上捕获 IPv6 流量。也可以通过隧道连接到 IPv6 提供者。

   我们使用 Wireshark 捕获 IPv6 数据包.

   在 Wireshark 的筛选器中输入 ipv6，可以看到捕获到的 IPv6 数据包。

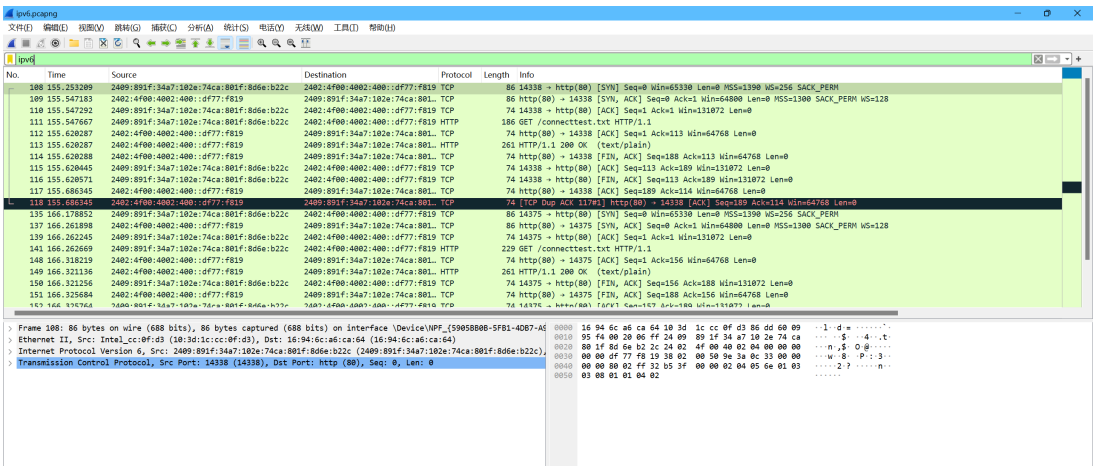

图 23: Wireshark 捕获 IPv6 数据包

选择其中的一个数据包，可以看到其结构如下：

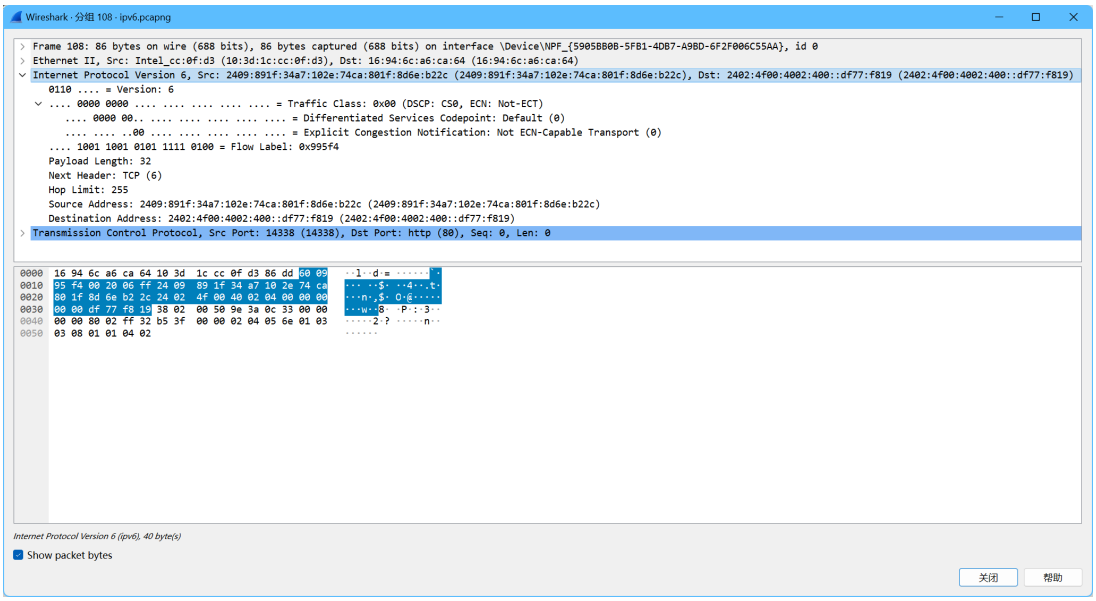

图 24: IPv6 数据包结构

可以发现，IPv6 数据包的结构与 IPv4 数据包的结构有所不同。其中，IPv6 数据包的首部长度为 40 bytes，地址均为 16 bytes，校验和字段被取消。增加了 Hop Limit 字段，用于替代 IPv4 中的 TTL 字段。

2. Learn about tunnels, which wrap an IP packet within another IP header.
   隧道是一种将一个 IP 数据包封装在另一个 IP 报头中的方法。隧道可以用于将 IPv6 数据包封装在 IPv4 数据包中，也可以用于将 IPv4 数据包封装在 IPv6 数据包中。
3. Read about IP geolocation, It is the process of assigning a geographical location to an IP addressusing measurements or clues from its name administrative databases. Try a geolocation service.
   IP 地理定位是将地理位置分配给 IP 地址的过程，可以使用测量或来自其名称管理数据库的线索。可以尝试使用 IP 地理定位服务。例如，https://www.iplocation.net/ 可以根据 IP 地址查询其地理位置。
4. Learn about IPsec or IP security. It provides confidentiality and authentication for IP packets, and isoften used as part of VPNs.
   IPsec 或 IP 安全是一种为 IP 数据包提供机密性和身份验证的协议，通常作为 VPN 的一部分使用。它提供了一种在网络层对数据包进行安全处理的方式，确保在传输过程中数据的机密性和完整性，并验证通信的参与方身份。

5 实验结果总结

本次实验中，我们使用 Wireshark 捕获 IP 数据包，并对其进行分析。我们分析了 IP 数据包的结构，回答了相关问题。我们使用 tracert 命令查看了到达 www.baidu.com 的路由路径，并画出了网络路径图。我们

选择了一个 IP 数据包，计算了其 checksum。最后，我们对实验中的问题进行了讨论，还捕获了 IPv6 数据包，并对其进行了分析。

6 附录

无