中国科学技术大学
University of Science and Technology of China

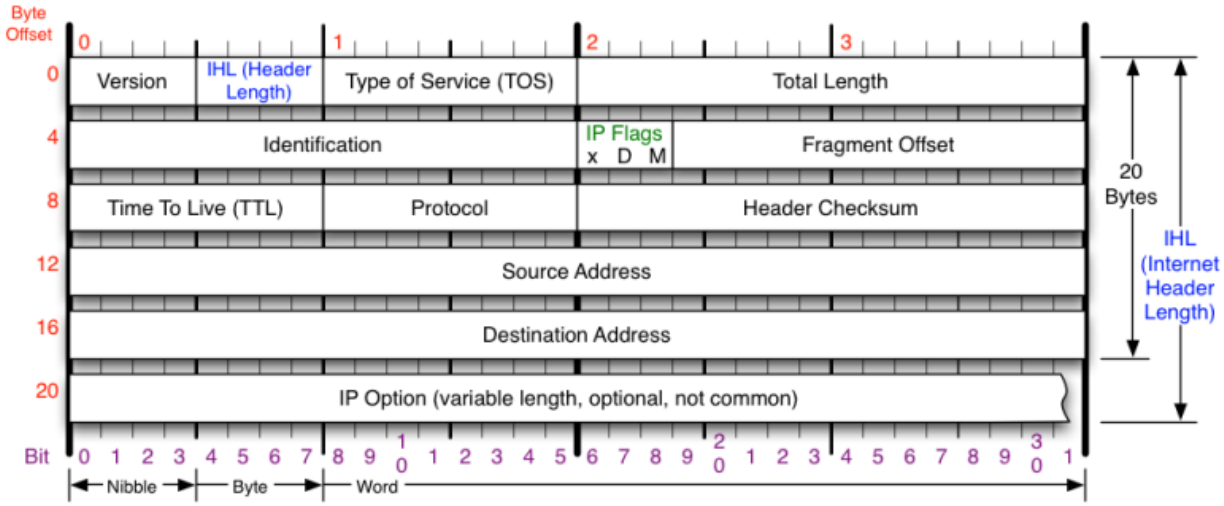
第四次实验

利用Wireshark观察IP数据报

2020年12月4日

IPv4报文

Internet Protocol Version 4 ——网络层协议



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

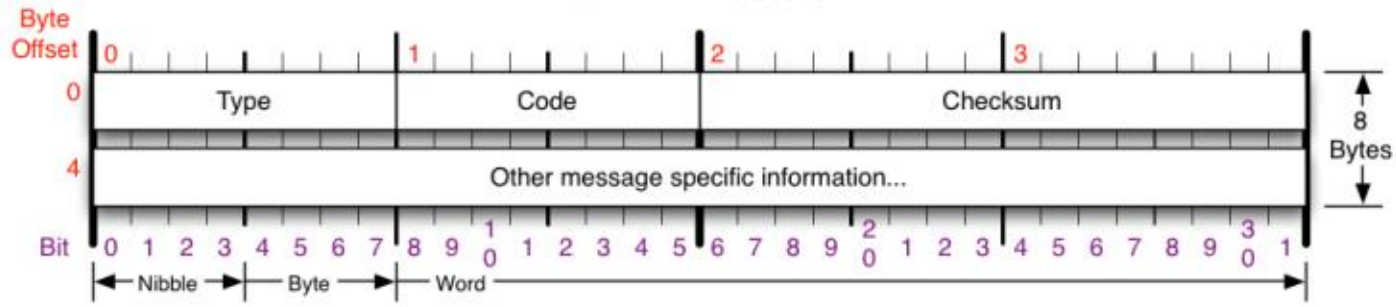
x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

ICMP报文

Internet Control Message Protocol——传输层协议



ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Checksum

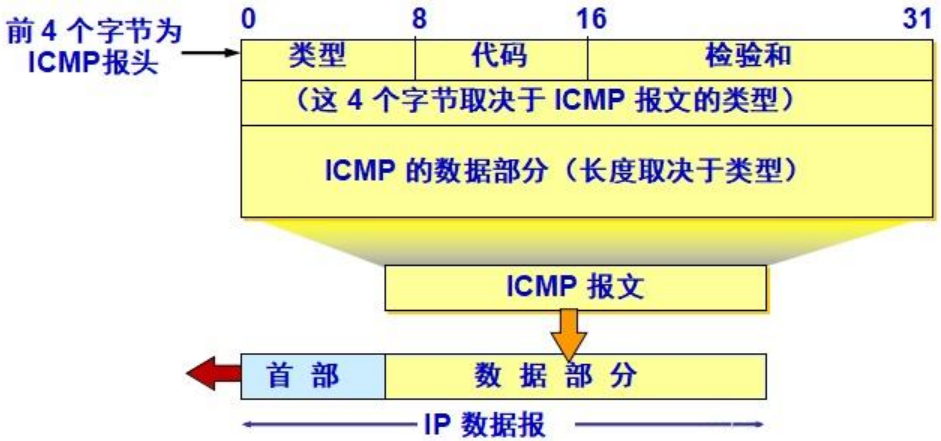
Checksum of ICMP header

RFC 792

Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

报文演示


```
Internet Protocol Version 4, Src:                , Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0,
    Total Length: 240
    Identification: 0x80fa (33018)
  v Flags: 0x01
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 2960
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.81
    Destination Address: 128.59.23.100
  > [3 IPv4 Fragments (3180 bytes): #84(1480), #85(1480), #86(220)]
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xd0a4 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 8275 (0x2053)
    Sequence Number (LE): 21280 (0x5320)
  > [No response seen]
  > Data (3172 bytes)
```



IP报文分片

- MTU： Maximum Transmit Unit，最大传输单元，即物理接口（数据链路层）提供给其上层（通常是IP层）最大一次传输数据的大小；以普遍使用的以太网接口为例，缺省MTU=1500 Byte，这是以太网接口对IP层的约束，如果IP层有<=1500 byte 需要发送，只需要一个IP包就可以完成发送任务；如果IP层有> 1500 byte 数据需要发送，需要分片才能完成发送，这些分片有一个共同点，即

- 标识：唯一的标识主机发送的每一份数据报。通常每发送一个报文，它的值加一。当IP报文长度超过传输网络的MTU（最大传输单元）时必须分片，这个标识字段的值被复制到所有数据分片的标识字段中，使得这些分片在达到最终目的地时可以依照标识字段的内容重新组成原先的数据。

TTL

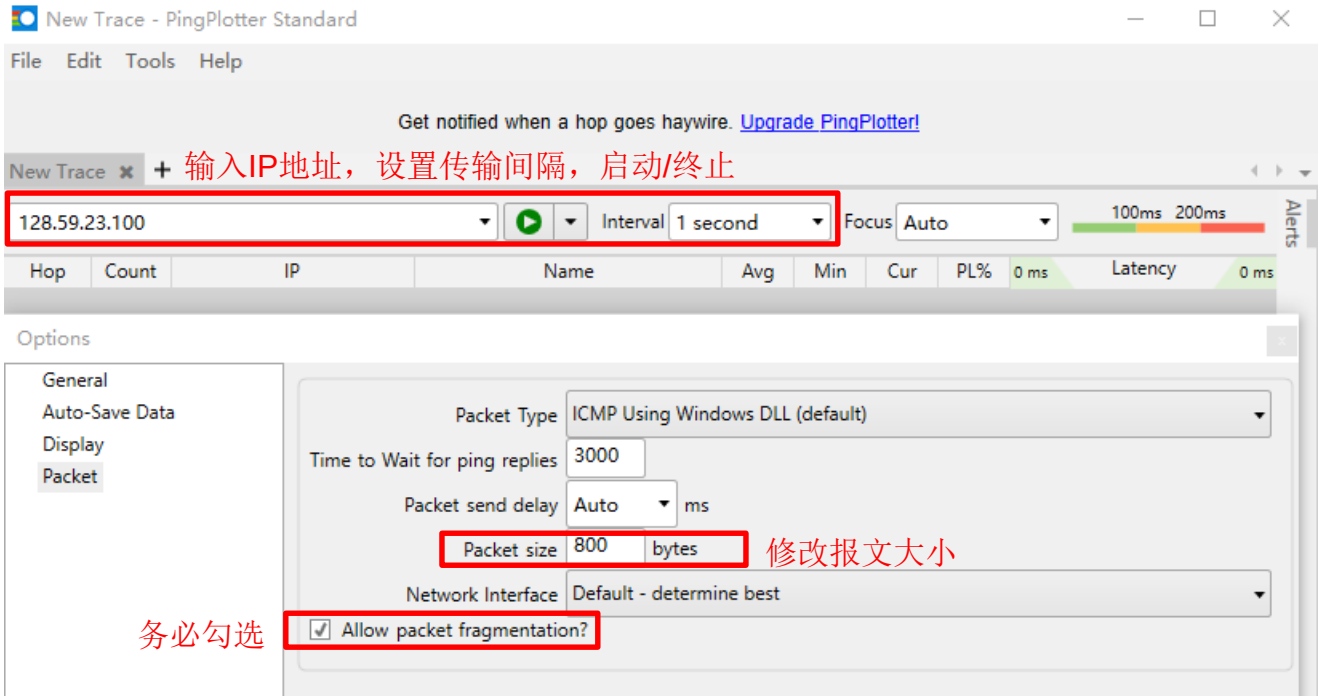
- TTL是IP数据包在计算机网络中可以转发的最大跳数。TTL字段由IP数据包的发送者设置，在IP数据包从源到目的的整个转发路径上，每经过一个路由器，路由器都会修改这个TTL字段值，具体的做法是把该TTL的值减1，然后再将IP包转发出去。如果在IP包到达目的IP之前，TTL减少为0，路由器将会丢弃收到的TTL=0的IP包并向IP包的发送者发送 ICMP time exceeded消息。

- TTL的主要作用是避免IP包在网络中的无限循环和收发，节省了网络资源，并能使IP包的发送者能收到告警消息。

- TTL 是由发送主机设置的，以防止数据包不断在IP互联网络上永不终止地循环。转发IP数据包时，要求路由器至少将 TTL 减小 1。

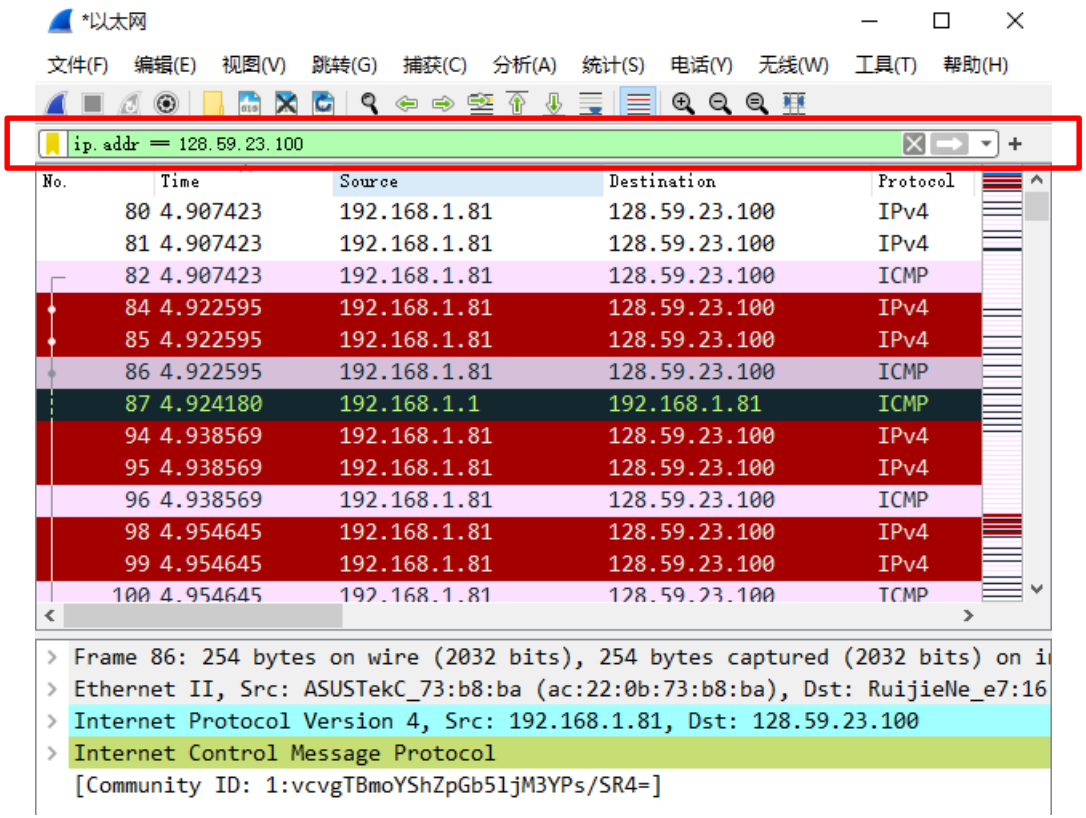
PingPlotter

- IP报文大小设置：Edit→Options→Packet
- 本次实验建议设置IP地址为128.59.23.100，便于批改，不作为强制要求
- 本次实验设置包大小为800、1600、3200，替换pdf中的56、2000、3500



Wireshark

- 显示过滤条件设置



实验要求

- 捕获观察并分析IP数据报的结构。
- 掌握traceroute的使用(Windows下替换为PingPlotter)。
- 回答pdf中的question部分的问题。本次实验由同学们自己在电脑上完成，实验参考PDF文件会上传QQ群，请同学们自行下载。
- 在回答部分问题时需要将自己的报文截图下来作为答题依据，并添加必要的分析过程，但不必按照文件上介绍的将报文打印下来。
- 本次实验设置包大小为800、1600、3200，替换pdf中的56、2000、3500，单位Byte
- 对于报文分片的问题，请给出详细计算。
- 请务必使用自己捕获的报文(参考前面软件使用相关设置)回答相关问题，否则本次实验计分减0.5(计分满分为10)

- 建议但不作为强制要求
  - 本次实验建议设置IP地址为128.59.23.100，便于批改
  - Wireshark使用过滤功能

实验报告

- 报告提交邮箱：
  - network_2020@163.com
- 第四次次实验报告提交截止时间：
  - 2020年12月31日23:59:59
- 邮箱主题及报告格式：
  - 姓名 +学号+第四次计算机网络实验
  - 提交pdf文档