

IP实验

Q1

Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

8	2004-08-22 09:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
9	2004-08-22 09:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
10	2004-08-22 09:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100

0100 = Version: 4

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

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

IP为192.168.1.102

Q2

Within the IP packet header, what is the value in the upper layer protocol field?

> Time to Live: 1

Protocol: ICMP (1)

Header Checksum: 0x2d2c [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.102

ICMP (1)

Q3

How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

```
.... 0101 = Header Length: 20 bytes (5) ←
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84 ←
Identification: 0x32d0 (13008)
> 000. .... = Flags: 0x0
```

报头20字节，总共84字节，所以payload bytes是84-20=64字节

Q4

Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented

```
✓ 000. .... = Flags: 0x0
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set ←
  ...0 0000 0000 0000 = Fragment Offset: 0
```

flags字段中的More fragments没有置位，为0，所以没有分片

Q5

Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

```

    Identification: 0x32d0 (13008) ←
> 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
> Time to Live: 1 ←
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled] ←

    Identification: 0x32d1 (13009) ←
> 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
> Time to Live: 2 ←
    Protocol: ICMP (1)
    Header Checksum: 0x2c2b [validation disabled] ←

```

identification（标识符）、time to live（存在时间）、header checksum（首部检验和）在改变

Q6

Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

```

✓ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x32d1 (13009)
> 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
> Time to Live: 2
  Protocol: ICMP (1)
  Header Checksum: 0x2c2b [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 128.59.23.100

```

- 图中所示，除了Q5中所改变，其余Version,Header Length,Differentiated Services Field,Total Length,Flags Fragment Offset,Protocol,Source Address,Destination Address 保持不变

- 其中必须保持不变的有：Version, Header Length, Differentiated Services Field, Protocol, Source Address, Destination Address
- 必须改变的是Q5中提到的Identification、Time to Live、Header Checksum，因为Identification用来唯一标识数据报，Time to Live是因为traceroute程序会发送该字段递增的报文，在跳数计数器的作用下来避免报文永远存在，Header Checksum是因为该字段是首部检验和，只要有首部字段发生改变，该字段就会变化

Q7

Describe the pattern you see in the values in the Identification field of the IP datagram

还是Q5中的图可以看出是递增1的

Q8

What is the value in the Identification field and the TTL field?

```
Identification: 0x9d7c (40316) ←
> 000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255 ←
```

Identification为0x9d7c (40316)

TTL为255

Q9

Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why

```
9 2004-08-22 09:48:02.835178 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
40 2004-08-22 09:48:07.832847 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
Identification: 0x9d7c (40316)
> 000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Identification: 0x9d98 (40344)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
```

ID改变了，TTL没有变，因为ID是对数据报的唯一标识，而TTL不变是因为它们都是第一跳路由器发出的，具有相同的寿命

Q10

Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

93	2004-08-22 09:48:25.100537	192.168.1.102	128.59
94	2004-08-22 09:48:25.120616	10.216.228.1	192.16
95	2004-08-22 09:48:25.129020	192.168.1.102	128.59
96	2004-08-22 09:48:25.129600	192.168.1.102	128.59


```

Total Length: 548
Identification: 0x32f9 (13049)
> 000. .... = Flags: 0x0
...0 0000 1011 1001 = Fragment Offset: 1480
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2a7a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
  [Frame: 92, payload: 0-1479 (1480 bytes)]
  [Frame: 93, payload: 1480-2007 (528 bytes)]
  [Fragment count: 2]
  [Reassembled IPv4 length: 2008]
  [Reassembled IPv4 data: 0800d0c603007703373620aaaaaaaaa]

```

分为了2片

Q11

Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram

打印结果如下:

```

No.      Time           Source           Destination      Protocol Length Info
 92 28.441511      192.168.1.102    128.59.23.100    IPv4      1514    Fragmented IP protocol
(proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x32f9 (13049)
Flags: 0x20, More fragments
 0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..1. .... = More fragments: Set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x077b [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[Reassembled IPv4 in frame: 93]

```

More fragments为set说明数据报被分片

Fragment Offset为0说明没有偏移，为第一个分片

数据报长度为1500字节

Q12

Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

打印结果如下：

```

No.      Time           Source           Destination      Protocol Length Info
 93 28.442185      192.168.1.102    128.59.23.100    ICMP      562     Echo (ping) request
id=0x0300, seq=30467/887, ttl=1 (no response found!)
Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 548
Identification: 0x32f9 (13049)
Flags: 0x00
 0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 1011 1001 = Fragment Offset: 1480
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2a7a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
Internet Control Message Protocol

```

Fragment Offset为1480说明有偏移，则不是第一个分片

More fragments为Not set说明没有更多分片

Q13

What fields change in the IP header between the first and second fragment?

比较上面两题的图即可知道，Total Length,More fragments,Fragment Offset,Header Checksum有变化

Q14

How many fragments were created from the original datagram?

```
→ 218 43.467629 192.168.1.102 128.59.23.100 ICMP 582 Ec
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0001 0111 0010 = Fragment Offset: 2960
> Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x2983 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 128.59.23.100
> [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)] ←
▼ Internet Control Message Protocol
```

3个分片

Q15

What fields change in the IP header among the fragments?

```
Total Length: 1500 ←
Identification: 0x3323 (13091)
v Flags: 0x20, More fragments
  0... .. = Reserved bit: Not set
  .0.. .. = Don't fragment: Not set
  ..1. .... = More fragments: Set ←
  ...0 0000 0000 0000 = Fragment Offset: 0 ←

Total Length: 1500 ←
Identification: 0x3323 (13091)
v Flags: 0x20, More fragments
  0... .. = Reserved bit: Not set
  .0.. .. = Don't fragment: Not set
  ..1. .... = More fragments: Set ←
  ...0 0000 1011 1001 = Fragment Offset: 1480 ←

Total Length: 568 ←
Identification: 0x3323 (13091)
v Flags: 0x01
  0... .. = Reserved bit: Not set
  .0.. .. = Don't fragment: Not set
  ..0. .... = More fragments: Not set ←
  ...0 0001 0111 0010 = Fragment Offset: 2960 ←
```

Total Length, More fragments, Fragment Offset 变化, 所以 Header Checksum 也会变化