

**中国科学技术大学计算机学院**

## **计算机网络实验报告**

### **实验四**

#### **利用 Wireshark 观察 ip 报文**

**学 号： PB18081616**

**姓 名： 谭园**

**专 业： 计算机科学与技术**

**指导老师： 张信明**

**中国科学技术大学计算机学院**

**2020 年 12 月 21 日**

## 一、 实验目的

- 1、 利用 wireshark 观察 ip 报文

## 二、 实验原理

为了生成一系列 IP 数据报，我们将使用 traceroute 程序向不同的目的地发送不同大小的数据报。traceroute 通过首先发送一个或多个带有生存时间（TTL）字段设置为 1 的数据报；然后发送一个或多个带有 TTL 字段设置为 2 的数据报到同一个目的地；然后发送一个或多个带有 TTL 字段设置为 3 的数据报到同一个目的地，以此类推，直到目的地真正收到此数据报为止。路由器必须将每个接收到的数据报中的 TTL 减 1，如果 TTL 达到 0，路由器会向来源主机发送 ICMP 消息。由于这种行为，TTL 为 1 的数据报将导致距发送方一次跳跃的路由器，将 ICMP TTL 超出的消息发送回发送方主机；以 TTL 为 2 发送的数据报将导致距离为两次跳跃的路由器，将 ICMP 消息发送回发送方主机等等。以这种方式，执行 traceroute 的主机可以通过查看包含 ICMP TTL 超出消息的数据报中的来源 IP 地址来获知其自身与目的地之间的路由器的身份。

## 三、实验条件

- 1、 硬件条件：一台 PC 机

2、 软件条件：wireshar, chrome 浏览器，注意配置软件的环境条件

## 四、实验过程

1. 捕获执行 traceroute 的数据包
2. 分析数据包。此处我用的是官方的数据包。

## 五、结果分析

1.

No.	Time	Source	Destination	Protocol	Length	Info
70	16.243006	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=27907/877, ttl=4 (n
71	16.260058	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit
72	16.270515	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=28163/878, ttl=5 (n
73	16.288698	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit
74	16.293181	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=28419/879, ttl=6 (n
75	16.312871	12.123.40.218	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit
76	16.313040	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=28675/880, ttl=7 (n

> Frame 72: 98 bytes on wire (784 bits), 98 bytes captured (784 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: 84

Identification: 0x32ef (13039)

> Flags: 0x00

Fragment Offset: 0

Time to Live: 5

Protocol: ICMP (1)

Header Checksum: 0x290d [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.102

Destination Address: 128.59.23.100

192.168.1.102

2. Protocol: ICMP (1)

值就为 1

3. IP header 20 bytes, 数据报一共有 56 bytes, 因此有效负载中有 36 bytes。

Header Length: 20 bytes (5)

Total Length: 56

4. 没有分片, 原因: flag 和 offset 都为 0

▼ Flags: 0x00

0... .... = Reserved bit: Not set

.0... .... = Don't fragment: Not set

..0. .... = More fragments: Not set

Fragment Offset: 0

5. 标识符 (Identification)、存活时间 (Time To Live, TTL)、首部检验和 (Header Checksum) 一直在变。

```
> Frame 16: 98 bytes on wire (784 bits), 98 bytes captured (784 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: 84
    Identification: 0x32d4 (13012)
> Flags: 0x00
    Fragment Offset: 0
    Time to Live: 5
    Protocol: ICMP (1)
    Header Checksum: 0x2928 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
> Internet Control Message Protocol
```

```

> Frame 18: 98 bytes on wire (784 bits), 98 bytes captured (784 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: 84
    Identification: 0x32d5 (13013)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 6
    Protocol: ICMP (1)
    Header Checksum: 0x2827 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  > Internet Control Message Protocol

```

因为路由跟踪就是靠 TTL 来辨识路由的，每次的标识符和校验和也会不一样

6 保持不变：版本号 首部长度的，服务类型，标志，偏移，上层协议，目的和源 IP 地址

必须保持不变：必须保持不变的是：版本号 源和目的 IP 地址

必须变：标识，首部检验和，存活时间

7. 每一个 IP 数据报头部的标识号域都不一样，每次加一

8. 40316 255

```

> Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.102
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x9d7c (40316)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x6ca0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.216.228.1
    Destination Address: 192.168.1.102
  > Internet Control Message Protocol

```

9. 每一个固定的路由器都有一个固定的 TTL 值，所以最近的那个路由器回复的

所有的 ICMP TTL-exceeded 的 TTL 的值都不会改变

10. 可以很明显的看到原本的 IP 数据报已经被分段为三个部分，#363、#364、#365

361	53.728518	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=49667/962, ttl=11 (no response found!)
362	53.744006	21.128.190.197	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
363	53.757036	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
364	53.757703	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
365	53.758584	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (no response found!)
366	53.777161	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
367	53.777832	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]

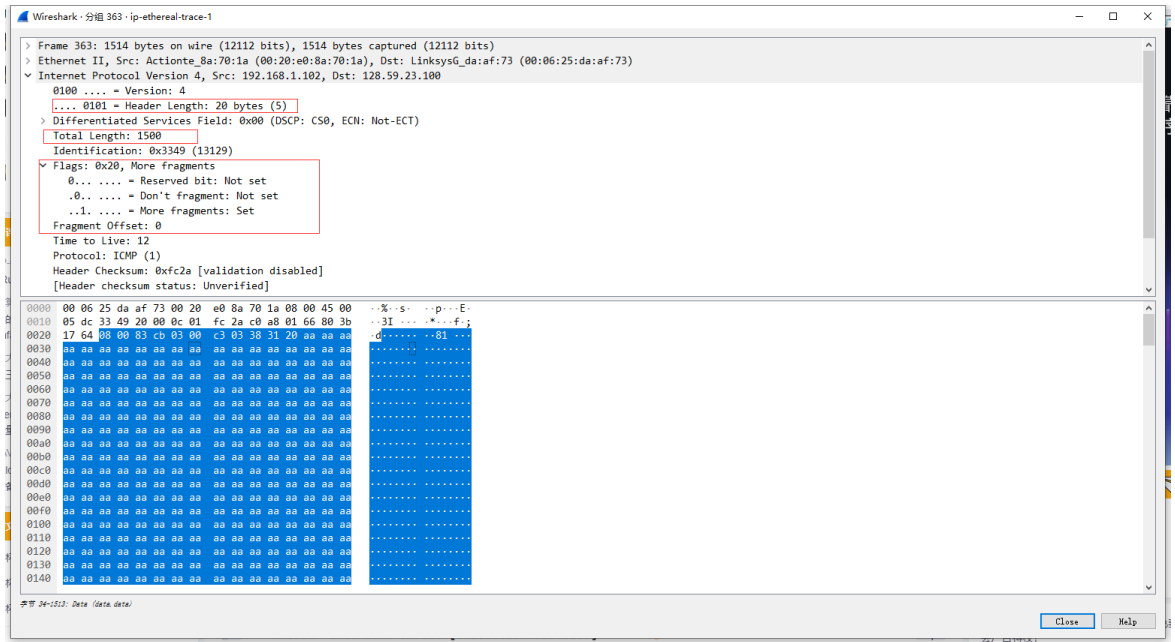
```

> Frame 365: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
> Ethernet II, Src: Actionte_Ba: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: 0xc0 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 568
    Identification: 0x3349 (13129)
  > Flags: 0x01
    Fragment Offset: 2960
    Time to Live: 12
    Protocol: ICMP (1)
    Header Checksum: 0x1e5d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  > [3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)]
> Internet Control Message Protocol

```

11. More fragments 字段为 1 表示 Set，即该数据包被分片。通

过 ID 字段判断这是第一个片段, 分片长度为 1480 bytes, 以及 20bytes 报头



12.

361	53.728518	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=49667/962, ttl=11 (no response found!)
362	53.744006	24.128.190.197	192.168.1.102	ICMP	70 Time-to-live exceeded (time to live exceeded in transit)
363	53.757036	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
364	53.757703	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
365	53.758584	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (no response found!)
366	53.777161	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
367	53.777832	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]

> Frame 364: 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: 0x3349 (13129)

> Flags: 0x20, More fragments

0... .... = Reserved bit: Not set

.0... .... = Don't fragment: Not set

..1. .... = More fragments: Set

Fragment Offset: 1480

Time to Live: 12

Protocol: ICMP (1)

Header Checksum: 0xf7b1 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.102

Destination Address: 128.59.23.100

[Reassembled IPv4 in frame: 365]

> Data (1480 bytes)

361	53.748518	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (no response found!)
362	53.744006	24.128.190.197	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
363	53.757036	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
364	53.757703	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
365	53.758584	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (no response found!)
366	53.777161	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
367	53.777832	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]

```

> Frame 365: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys_G_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: 568
  Identification: 0x3349 (13129)
  Flags: 0x01
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0... .... = More fragments: Not set
  Fragment Offset: 2960
  Time to Live: 12
  Protocol: ICMP (1)
  Header Checksum: 0x1e5d [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 128.59.23.100
  > [3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)]
> Internet Control Message Protocol

```

Fragment Offset 字段表示偏移量，1480 bytes 的偏移量表示是上一个片段的后续。没有更多片段了，因为 More fragments 字段为 Not set，表示后面没有分片了。

13. 全长 (Total Length)、标志 (Flags) 和分片偏移 (Fragment Offset)。

14. 3 个

TIME TO LIVE: 12
Protocol: ICMP (1)
Header Checksum: 0x1e5d [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
> [3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)]
[Frame: 363, payload: 0-1479 (1480 bytes)]
[Frame: 364, payload: 1480-2959 (1480 bytes)]
[Frame: 365, payload: 2960-3507 (548 bytes)]
[Fragment count: 3]
[Reassembled IPv4 length: 3508]



## 15. 总长度 Total Length、标志 Flags、首部校验和 Header checksum