

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：PB15111604

姓 名：金泽文

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

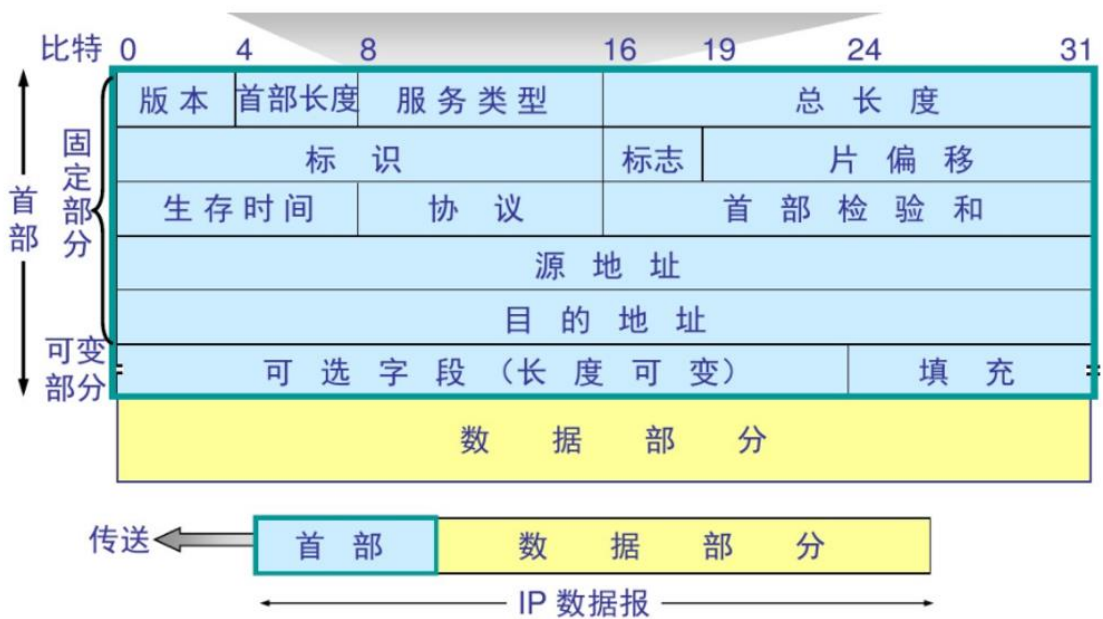
2017 年 12 月 27 日

一、实验目的

1、通过捕获观察并分析 IP 报文，理解 IP 的细节，掌握 traceroute 的使用。

二、实验原理

Wireshark 是一个 packet 分析工具，可以抓取 packet，并分析出详细信息。Wireshark 使用 wincap 作为接口，直接与网卡进行 packet 交换，监听共享网络上传送的 packet。



IP 数据报首部的 TTL(Time to live)表示数据报的生存时间,每经过路由器转发一次,就至少减少 1,当减少到 0 的时候,会被路由器丢弃,并返回 ICMP 消息.

Traceroute 通过巧妙的设置 ttl,通过一次次的重传,与 ttl+1 来得到到目的

地址的路径上的路由器的信息.

三、 实验条件

1、 硬件条件： 联想 Y700:

i5-6300HQ 2.30GHz

16G 内存

Intel(R) Dual Band Wireless-AC 3165

2、 软件条件： Win10 Professional 1703

Wireshark2.4.2

以及 WSL(Windows Subsystem for Linux) (如下)

```
Reaper@KZ:/mnt/d/USTC/algorithm$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.3 LTS
Release:        16.04
Codename:       xenial
```

traceroute for Linux, 2.0.21

```
Reaper@KZ:/mnt/d/USTC/algorithm$ traceroute -V
Modern traceroute for Linux, version 2.0.21
Copyright (c) 2008 Dmitry Butskoy, License: GPL v2 or any later
```

四、 实验过程

1、 安装 traceroute

```
Reaper@KZ:/mnt/d/USTC/algorithm$ traceroute
程序 'traceroute' 已包含在下列软件包中:
 * inetutils-traceroute
 * traceroute
请尝试: sudo apt install <选定的软件包>
Reaper@KZ:/mnt/d/USTC/algorithm$ sudo apt-get install traceroute
[sudo] Reaper 的密码:
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列【新】软件包将被安装:
  traceroute
升级了 0 个软件包, 新安装了 1 个软件包, 要卸载 0 个软件包, 有 0 个软件包未被升级。
需要下载 45.5 kB 的归档。
解压缩后会消耗 177 kB 的额外空间。
获取:1 https://mirrors.ustc.edu.cn/ubuntu xenial/universe amd64 traceroute amd64 1:2.0.21-1 [45.5 kB]
已下载 45.5 kB, 耗时 1秒 (40.8 kB/s)
正在选中未选择的软件包 traceroute。
(正在读取数据库 ... 系统当前共安装有 42618 个文件和目录。)
正准备解包 .../traceroute_1%3a2.0.21-1_amd64.deb ...
正在解包 traceroute (1:2.0.21-1) ...
正在处理用于 man-db (2.7.5-1) 的触发器 ...
正在设置 traceroute (1:2.0.21-1) ...
update-alternatives: 使用 /usr/bin/traceroute.db 来在自动模式中提供 /usr/bin/traceroute (traceroute)
update-alternatives: 使用 /usr/bin/lft.db 来在自动模式中提供 /usr/bin/lft (lft)
update-alternatives: 使用 /usr/bin/traceproto.db 来在自动模式中提供 /usr/bin/traceproto (traceproto)
update-alternatives: 使用 /usr/sbin/tcptraceproto.db 来在自动模式中提供 /usr/sbin/tcptraceproto (tcptraceproto)
```

```
Reaper@KZ:/mnt/d/USTC/algorithm$ traceroute -V
Modern traceroute for Linux, version 2.0.21
Copyright (c) 2008 Dmitry Butskoy, License: GPL v2 or any later
```

2、 利用 traceroute 发包并用 wireshark 查看.

用 wireshark 开始捕获, 用 traceroute 发送 3 个 56 字节, 2000 字节, 3500 字节的包.

```
Reaper@KZ:/mnt/d/USTC/algorithm$ traceroute gaia.cs.umass.edu 56
traceroute to gaia.cs.umass.edu (128.119.245.12), 30 hops max, 56 byte packets
 1 * * *
 2 * * *
 3 * * *
```

```
Reaper@KZ:/mnt/d/USTC/algorithm$ traceroute gaia.cs.umass.edu 2000
traceroute to gaia.cs.umass.edu (128.119.245.12), 30 hops max, 2000 byte packets
 1 * * *
```

```
Reaper@KZ:/mnt/d/USTC/algorithm$ traceroute gaia.cs.umass.edu 3500
traceroute to gaia.cs.umass.edu (128.119.245.12), 30 hops max, 3500 byte packets
 1 * * *
```

五、 结果分析

以下是 pdf 中 15 个问题对应的回答

(到第 4 题使用我自己抓的包, 之后由于我的电脑没有发 icmp 包出去, 所以用的是官网下载的包.)

1. 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?

答: 192.168.43.174

8	19:15:02.846761	192.168.43.1	192.168.43.174	ICMP	98 Time-to-live exceeded
9	19:15:02.846857	192.168.43.174	128.119.245.12	SKYPE	70 Payload Unk: 4
10	19:15:02.846869	192.168.43.1	192.168.43.174	ICMP	98 Time-to-live exceeded
11	19:15:02.847517	192.168.43.1	192.168.43.174	ICMP	98 Time-to-live exceeded
12	19:15:02.847553	192.168.43.174	128.119.245.12	SKYPE	70 Payload Unk: 4
13	19:15:02.848314	192.168.43.174	128.119.245.12	SKYPE	70 Payload Unk: 4

Source: 192.168.43.1
Destination: 192.168.43.174
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]

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

答: 1 (表示ICMP)

Time to live: 64
Protocol: ICMP (1)
Header checksum: 0x5f

3. 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.

答: 20 字节, $84-20=64$ 字节. payload 字节数就是总字节数减去 header 字节数.

Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.174
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
Total Length: 84
Identification: 0x465d (18557)

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

答： 没有被 fragmented.因为 more fragments 位没有被置为 1.如下：

```
✓ Internet Protocol Version 4, Src: 192.168.43.174, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x7fbb (32699)
  ✓ Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    Fragment offset: 0
```

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

答：

ip.addr == 192.168.43.174 && icmp						
No.	Time	Source	Destination	Protocol	Length	Info
303	19:15:48.672699	192.80.83.101	192.168.43.174	ICMP	70	Time
302	19:15:48.660497	192.80.83.101	192.168.43.174	ICMP	70	Time
90	19:15:13.894417	192.80.83.101	192.168.43.174	ICMP	70	Time
87	19:15:13.891006	192.80.83.101	192.168.43.174	ICMP	70	Time
86	19:15:13.890877	192.80.83.101	192.168.43.174	ICMP	70	Time
498	19:16:35.403341	192.168.43.1	192.168.43.174	ICMP	590	Time
497	19:16:35.402442	192.168.43.1	192.168.43.174	ICMP	590	Time
493	19:16:35.402296	192.168.43.1	192.168.43.174	ICMP	590	Time
180	19:15:38.060260	192.168.43.1	192.168.43.174	ICMP	590	Time
177	19:15:38.059426	192.168.43.1	192.168.43.174	ICMP	590	Time
176	19:15:38.058588	192.168.43.1	192.168.43.174	ICMP	590	Time
41	19:15:03.017517	192.168.43.1	192.168.43.174	ICMP	60	Time

↑ 由于我电脑没有抓到自己电脑发的 icmp,所以这部分题用官网下载好的 trace 文件.

从下面可以看出：

Header 中的 TTL,checksum,Identification 总改变

<pre> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.10 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 84 Identification: 0x32d0 (13008) > Flags: 0x00 Fragment offset: 0 > Time to live: 1 > [Expert Info (Note/Sequence): "Time To Live" only 1] Protocol: ICMP (1) Header checksum: 0x2d2c [validation disabled] [Header checksum status: Unverified] Source: 192.168.1.102 Destination: 128.59.23.100 [Source GeoIP: Unknown] [Destination GeoIP: Unknown] </pre>	<pre> 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) > Flags: 0x00 Fragment offset: 0 > Time to live: 2 > [Expert Info (Note/Sequence): "Time To Live" only 2] Protocol: ICMP (1) Header checksum: 0x2c2b [validation disabled] [Header checksum status: Unverified] Source: 192.168.1.102 Destination: 128.59.23.100 [Source GeoIP: Unknown] [Destination GeoIP: Unknown] </pre>
--	---

6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?

答: stay constant:

Version, header length, Differentiated Services Field, flags, fragment offset, protocol, source ip address, destination ip address.

必须不变的是

Version: 因为都是 ipv4.

Protocol: 都是 ICMP

Header length: 因为 protocol 不变, 是 icmp, 所以 header 不变

Differentiated Services: 理由同上, 都是 icmp 类型

source ip address, destination ip address: 源, 目的地址在这一过程不变

必须变的是:

TTL: 因为 traceroute 会改变 ttl

Identification: IP 数据报之间要有不一样的 id

Header checksum: 因为 header 每次都会不一样

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

答: 每个 id 会比前一个增加 1

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

答:

```
8 09:48:02.821397 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq
9 09:48:02.835178 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live
10 09:48:02.846981 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq

.... 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: 10.216.228.1
Destination: 192.168.1.102
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xd946 [correct]
[Checksum Status: Good]
v 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: 0x32d0 (13008)
> Flags: 0x00
Fragment offset: 0
> Time to live: 1
Protocol: ICMP (1)
```

第一跳的id为0x9d7c (40316), ttl为255

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

答: id变化, 因为id相同表示ip包是同一个大包的fragment, 这里的id需要独立. ttl不变. 因为在一段时间内(排除电脑转移或者网络环境彻底

变化), 电脑的第一跳路由是不变的, 其ttl的初始值已经是255了, 默认不会改变.

10. 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? [Note: if you find your packet has not been fragmented, you should download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the *ipethereal-trace-1* packet trace. If your computer has an Ethernet interface, a packet size of 2000 *should* cause fragmentation.³]

答： 是的, 被分成了2份fragments.

93 09:48:25.120616	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id
94 09:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (
96 09:48:25.129690	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id
98 09:48:25.149675	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id
100 09:48:25.179745	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id

```
Ethernet II, Src: PremaxPe_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
```

Fragment offset: 1480

```
> Time to live: 1
```

Protocol: ICMP (1)

```
Header checksum: 0x2a7a [validation disabled]
```

```
[Header checksum status: Unverified]
```

Source: 192.168.1.102

Destination: 128.59.23.100

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

✓ [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]
```

```
[Decomposed TDVA data: 0900d0c602007702273670cccccccccccccccccccccccccc]
```

11. 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?

答： 有上一题的图找到No. 92 frame, 得到：

```
91 09:48:19.611090 128.119.245.12 192.168.1.102 TCP 60 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Le
92 09:48:25.099863 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off
93 09:48:25.100537 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=30467
94 09:48:25.120616 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live excee
95 09:48:25.129020 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off
96 09:48:25.129690 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=30723
97 09:48:25.149015 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off
98 09:48:25.149675 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=30979
> Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: PremaxPe_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: 0x01 (More Fragments)
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..1... .... = More fragments: Set
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x077b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 93
> Data (1480 bytes)
```

其中flags中的 More fragments位被置为1.

这里的fragment offset为0,

整个ip包的长度为1500字节.

12. 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?

答： 如下图所示.与No.92 frame相同id的No.93 frame,其fragment offset为1480,非0,表示不是第一个.

不能根据more fragments位判断是不是第一个,因为最后一个fragment的more fragments位也是0.

91 09:48:25.011090	192.168.1.102	128.59.23.100
92 09:48:25.099863	192.168.1.102	128.59.23.100
93 09:48:25.100537	192.168.1.102	128.59.23.100
94 09:48:25.120616	10.216.228.1	192.168.1.102
95 09:48:25.129020	192.168.1.102	128.59.23.100
96 09:48:25.129690	192.168.1.102	128.59.23.100
97 09:48:25.149015	192.168.1.102	128.59.23.100
98 09:48:25.149675	192.168.1.102	128.59.23.100

```

.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-Set)
  Total Length: 548
  Identification: 0x32f9 (13049)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 1480
  Time to live: 1
  Protocol: ICMP (1)
  Header checksum: 0x2a7a [validation disabled]

```

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

答：就这两个fragment来说的话,变的有:

Total length, flags, fragment offset, header checksum

对于所有的第一个fragment与第二个fragment来说的话,一般肯定变的有:

Fragment offset和header checksum

14. How many fragments were created from the original datagram?

答： 3个

216 09:48:40.124488	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP pro
217 09:48:40.125160	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP pro
218 09:48:40.125981	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) reque
219 09:48:40.144138	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exce
220 09:48:40.150636	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP pro
221 09:48:40.151305	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP pro
222 09:48:40.152253	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) reque
223 09:48:40.170497	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP pro

```

[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
  [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
    [Frame: 216, payload: 0-1479 (1480 bytes)]
    [Frame: 217, payload: 1480-2959 (1480 bytes)]
    [Frame: 218, payload: 2960-3507 (548 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 3508]

```

15. What fields change in the IP header among the fragments?

答: header checksum, fragment offset.

第一个第二个的more fragments位是1, 第三个是0

第一个第二个的length是1500, 第三个是568

第一个第二个的