

计算机网络实验报告_IP

PB20000219 李蔚林

计算机网络实验报告_IP

实验目的

实验过程

实验结果及问题

实验思考

实验目的

1. 了解IP协议,及分析IP数据包的方法
2. 了解ICMP协议和TTL的作用

实验过程

用pingplotter分别设置跟踪包大小为:56Byte, 2000Byte, 3500Byte.每个追踪包大小追踪3次,利用wireshark抓包.

实验结果及问题

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?

我的IP地址是:114.214.251.129

*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

icmp

No.	Time	Source	Destination	Protocol	Length	Info
103	2.177005	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
104	2.215477	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
105	2.220143	0.0.0.0	114.214.251.129	ICMP	70	Time-to-live exceeded
108	2.254528	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
109	2.257421	202.38.96.60	114.214.251.129	ICMP	70	Time-to-live exceeded
110	2.292674	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
112	2.294825	202.38.64.60	114.214.251.129	ICMP	98	Time-to-live exceeded
115	2.297031	202.38.96.60	114.214.251.129	ICMP	70	Destination unreachable
116	2.332298	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
117	2.335816	210.45.224.252	114.214.251.129	ICMP	70	Time-to-live exceeded
121	2.350211	202.38.64.60	114.214.251.129	ICMP	120	Destination unreachable
128	2.370347	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
129	2.373020	101.4.115.13	114.214.251.129	ICMP	70	Time-to-live exceeded
133	2.409996	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request

> Frame 103: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF...

> Ethernet II, Src: 6a:8a:9f:ae:a3:a3 (6a:8a:9f:ae:a3:a3), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)

> Internet Protocol Version 4, Src: 114.214.251.129, 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: 0xd6ff (55039)

> Flags: 0x00

Fragment Offset: 0

Internet Control M...Protocol: Protocol | 分组: 4702 · 已显示: 1004 (21.4%) · 已丢弃: 0 (0.0%) | 配置: Default

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

upper layer protocol field 字段为 ICMP, 值为1

*WLAN						
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)						
ip						
No.	Time	Source	Destination	Protocol	Length	Info
103	2.177005	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
104	2.215477	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
105	2.220143	0.0.0.0	114.214.251.129	ICMP	70	Time-to-live exceeded
108	2.254528	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
109	2.257421	202.38.96.60	114.214.251.129	ICMP	70	Time-to-live exceeded
110	2.292674	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
111	2.293018	114.214.251.129	202.38.64.56	DNS	85	Standard query 0x...
112	2.294825	202.38.64.56	114.214.251.129	ICMP	98	Time-to-live exceeded
113	2.294825	202.38.64.56	114.214.251.129	DNS	162	Standard query request
114	2.295047	114.214.251.129	202.38.96.60	NBNS	92	Name query NBSTA...
115	2.297031	202.38.96.60	114.214.251.129	ICMP	70	Destination unreachable
116	2.332298	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
117	2.335816	210.45.224.252	114.214.251.129	ICMP	70	Time-to-live exceeded
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 56 Identification: 0xd6ff (55039) > Flags: 0x00 Fragment Offset: 0 Time to Live: 255 Protocol: ICMP (1) Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source Address: 114.214.251.129						
Protocol (ip.proto), 1 byte(s) 分组: 4702 · 已显示: 2478 (52.7%) · 已丢弃: 0 (0.0%) 配置: Default						

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.

从图中可以看出IP 头20Byte,IP 报的总长度是56Byte,payload长度=IP总长度-IP头长度=36Byte.通过计算得出.

*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip

No.	Time	Source	Destination	Protocol	Length	Info
103	2.177005	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
104	2.215477	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
105	2.220143	0.0.0.0	114.214.251.129	ICMP	70	Time-to-live exceeded
108	2.254528	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
109	2.257421	202.38.96.60	114.214.251.129	ICMP	70	Time-to-live exceeded
110	2.292674	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
111	2.293018	114.214.251.129	202.38.64.56	DNS	85	Standard query response
112	2.294825	202.38.64.60	114.214.251.129	ICMP	98	Time-to-live exceeded
113	2.294825	202.38.64.56	114.214.251.129	DNS	162	Standard query response
114	2.295047	114.214.251.129	202.38.96.60	NBNS	92	Name query NBSTAT
115	2.297031	202.38.96.60	114.214.251.129	ICMP	70	Destination unreachable
116	2.332298	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
117	2.335816	210.45.224.252	114.214.251.129	ICMP	70	Time-to-live exceeded

> Frame 103: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF...
 > Ethernet II, Src: 6a:8a:9f:ae:a3:a3 (6a:8a:9f:ae:a3:a3), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
 > Internet Protocol Version 4, Src: 114.214.251.129, 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: 0xd6ff (55039)
 > Flags: 0x00
 > Fragment Offset: 0

Header length in 3...dr_len), 1 byte(s) | 分组: 4702 · 已显示: 2478 (52.7%) · 已丢弃: 0 (0.0%) | 配置: Default

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

没有分片.如下图.flag=0,且fragment offset=0.

*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip

No.	Time	Source	Destination	Protocol	Length	Info
103	2.177005	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
104	2.215477	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
105	2.220143	0.0.0.0	114.214.251.129	ICMP	70	Time-to-live exceeded
108	2.254528	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
109	2.257421	202.38.96.60	114.214.251.129	ICMP	70	Time-to-live exceeded
110	2.292674	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
111	2.293018	114.214.251.129	202.38.64.56	DNS	85	Standard query 0x...
112	2.294825	202.38.64.60	114.214.251.129	ICMP	98	Time-to-live exceeded
113	2.294825	202.38.64.56	114.214.251.129	DNS	162	Standard query request
114	2.295047	114.214.251.129	202.38.96.60	NBNS	92	Name query NBSTA...
115	2.297031	202.38.96.60	114.214.251.129	ICMP	70	Destination unreachable
116	2.332298	114.214.251.129	128.119.245.12	ICMP	70	Echo (ping) request
117	2.335816	210.45.224.252	114.214.251.129	ICMP	70	Time-to-live exceeded

Flags: 0x00

- 0... .. = Reserved bit: Not set
- .0.. = Don't fragment: Not set
- ..0. = More fragments: Not set

Fragment Offset: 0

Time to Live: 255

Protocol: ICMP (1)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 114.214.251.129

Header length in 3...dr_len), 1 byte(s) | 分组: 4702 · 已显示: 2478 (52.7%) · 已丢弃: 0 (0.0%) | 配置: Default

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?

Identification, TTL, Header Checksum.

*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

icmp

No.	Time	Source	Destination	Protocol	Length	Info
469	6.035575	128.119.3.32	114.214.251.129	ICMP	70	Time-to-live exce
272	3.545937	128.119.3.32	114.214.251.129	ICMP	70	Time-to-live exce
4631	88.778...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply
4486	87.214...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply
4427	86.275...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply
4237	83.775...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply
4093	82.213...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply
4024	80.022...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 540
Identification: 0x4e4e (20046)
Flags: 0x01
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment Offset: 2960
Time to Live: 33
Protocol: ICMP (1)
Header Checksum: 0x6445 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12

Frame (554 bytes) Reassembled IPv4 (3480 bytes)
Version (ip.version), 1 byte(s) || 分组: 4702 · 已显示: 1004 (21.4%) · 已丢弃: 0 (0.0%) || 配置: Default

*WLAN

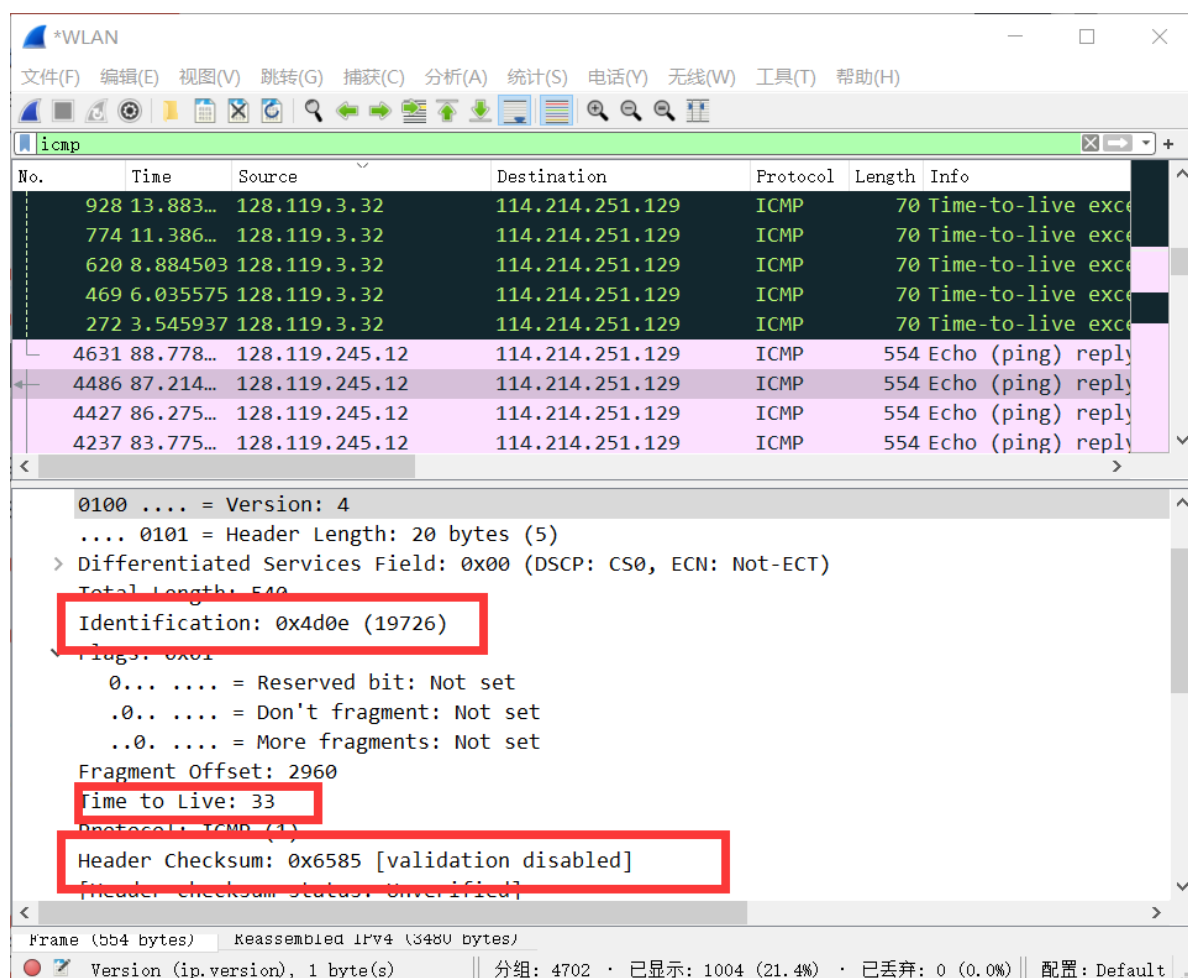
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

icmp

No.	Time	Source	Destination	Protocol	Length	Info
469	6.035575	128.119.3.32	114.214.251.129	ICMP	70	Time-to-live exce
272	3.545937	128.119.3.32	114.214.251.129	ICMP	70	Time-to-live exce
4631	88.778...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply
4486	87.214...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply
4427	86.275...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply
4237	83.775...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply
4093	82.213...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply
4024	80.022...	128.119.245.12	114.214.251.129	ICMP	554	Echo (ping) reply

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 540
Identification: 0x4d0e (19726)
Flags: 0x01
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment Offset: 2960
Time to Live: 33
Protocol: ICMP (1)
Header Checksum: 0x6585 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12

Frame (554 bytes) Reassembled IPv4 (3480 bytes)
Version (ip.version), 1 byte(s) || 分组: 4702 · 已显示: 1004 (21.4%) · 已丢弃: 0 (0.0%) || 配置: Default



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

本题由所学知识作答,无需截图.

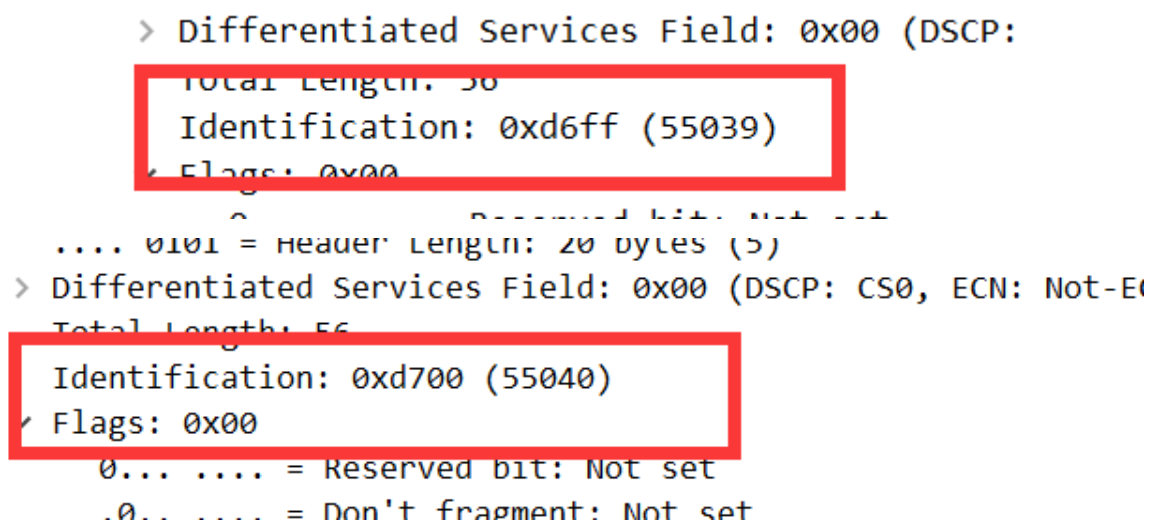
stay constant: 版本, 首部长度, 服务类型, 上层协议, 标志, 偏移,目的和源IP地址(对于分片的部分,标志,偏移可能变化)

must stay constant: 版本, 源IP地址, 目的IP地址.

must change: 首部检验和, 标识, 首部检验和, 数据,

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

identification中看到的值逐渐递增(如图,每次加1).用于区分每个IP数据.



```

.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0xd701 (55041)
✓ Flags: 0x00
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
Fragment Offset: 0
> Time to Live: 2

```

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

identification = 8439; TTL = 255

```

> Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2),
✓ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 114.214.2
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: N
Total Length: 56
Identification: 0x20f7 (8439)
✓ Flags: 0x00
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
Fragment Offset: 0
Time to Live: 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?

TTL不变,ID改变.因为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均保持不变.而ID是用来标识数据包的,改变.


```

> Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2),
✓ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 114.214.2
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: N
  Total Length: 56
  Identification: 0x20f7 (8439)
✓ Flags: 0x00
  0... .... = Reserved bit: Not set
  .0... .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  Fragment Offset: 0
  Time to Live: 255
<
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
  Total Length: 56
  Identification: 0x2168 (8552)
✓ Flags: 0x00
  0... .... = Reserved bit: Not set
  .0... .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  Fragment Offset: 0
  Time to Live: 255
<

```

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?

我的数据包在这题出现问题,所以分析作者提供的数据包.发现分片了.

ip-ethereal-trace-1

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip

No.	Time	Source	Destination	Protocol	Length	Info
152	33.648...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
153	33.648...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
154	33.677...	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exc
155	33.677...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
156	33.678...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
157	33.705...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
158	33.706...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
159	33.728...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
160	33.728...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
161	33.740...	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exc
162	33.748...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
163	33.748...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
164	33.809...	12.123.40.218	192.168.1.102	IPv4	554	Fragmented IP pro
165	33.885...	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP pro

Protocol: ICMP (1)
Header Checksum: 0xfe63 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[Reassembled IPv4 in frame: 156]
Data (1480 bytes)
Data: 0800bac503008d03373720aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
[Length: 1480]

Internet Protocol Version 4: Protocol | 分组: 380 · 已显示: 379 (99.7%) | 配置: Default

ip-ethereal-trace-1

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip

No.	Time	Source	Destination	Protocol	Length	Info
152	33.648...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
153	33.648...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
154	33.677...	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exc
155	33.677...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
156	33.678...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
157	33.705...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
158	33.706...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
159	33.728...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
160	33.728...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
161	33.740...	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exc
162	33.748...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
163	33.748...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
164	33.809...	12.123.40.218	192.168.1.102	IPv4	554	Fragmented IP pro
165	33.885...	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP pro

Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[2 IPv4 Fragments (2008 bytes): #155(1480), #156(528)]
[Frame: 155, payload: 0-1479 (1480 bytes)]
[Frame: 156, payload: 1480-2007 (528 bytes)]
[Fragment count: 2]
[Reassembled IPv4 length: 2008]
[Reassembled IPv4 data: 0800bac503008d03373720aaaaaaaaaaaaaaaaaaaaaaaaaaaaa...]
Internet Control Message Protocol

Frame (562 bytes) Reassembled IPv4 (2008 bytes)

Internet Protocol Version 4: Protocol | 分组: 380 · 已显示: 379 (99.7%) | 配置: Default

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?

通过IP头的flags部分可以看出已经被分段.通过offset=0可以看出这是第一个片段(长度1500Bytes)

The image shows a Wireshark packet capture analysis of a fragmented IP datagram. The packet list at the top shows several packets, with packet 154 highlighted. The packet details pane for packet 154 is expanded, showing the IP header and ICMP payload. Red boxes and arrows highlight specific fields in the IP header: 'Total Length: 1500', 'Identification: 0x3310 (13072)', and the 'Flags' section where 'More fragments' is set. The status bar at the bottom indicates the current filter is 'Internet Protocol Version 4: Protocol' and shows 380 groups with 379 packets displayed (99.7%).

No.	Time	Source	Destination	Protocol	Length	Info
152	33.648...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
153	33.648...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
154	33.677...	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exc
155	33.677...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
156	33.678...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
157	33.705...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
158	33.706...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ

Frame 155: 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:d...)
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: 0x3310 (13072)
Flags: 0x20, More fragments
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..1. = More fragments: Set
Fragment Offset: 0
Time to Live: 10
Protocol: ICMP (1)
Header Checksum: 0xf663 [validation disabled]

Internet Protocol Version 4: Protocol | 分组: 380 · 已显示: 379 (99.7%) | 配置: Default

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?

fragment offset=1480说明不是第一个分片.没有更多的了(因为flags=0)

ip-ethereal-trace-1

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip

No.	Time	Source	Destination	Protocol	Length	Info
152	33.648...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
153	33.648...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
154	33.677...	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exce
155	33.677...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
156	33.678...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ
157	33.705...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
158	33.706...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) requ

> Frame 156: 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:d)

> 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: 0x3310 (13072)

Flags: 0x00

0... = Reserved bit: Not set

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

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

Fragment Offset: 1480

Time to Live: 10

Protocol: ICMP (1)

Header Checksum: 0x2163 [validation disabled]

Frame (562 bytes) Reassembled IPv4 (2008 bytes)

Internet Protocol Version 4: Protocol 分组: 380 · 已显示: 379 (99.7%) 配置: Default

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

如图: fragment offset和header checksum字段变了.

ip-ethereal-trace-1

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip

No.	Time	Source	Destination	Protocol	Length	Info
292	48.620...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
293	48.621...	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) requ
294	48.649...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
295	48.650...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro

> Frame 294: 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:d)

> 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: 0x3337 (13111)

Flags: 0x20, More fragments

0... = Reserved bit: Not set

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

..1... = More fragments: Set

Fragment Offset: 0

Time to Live: 8

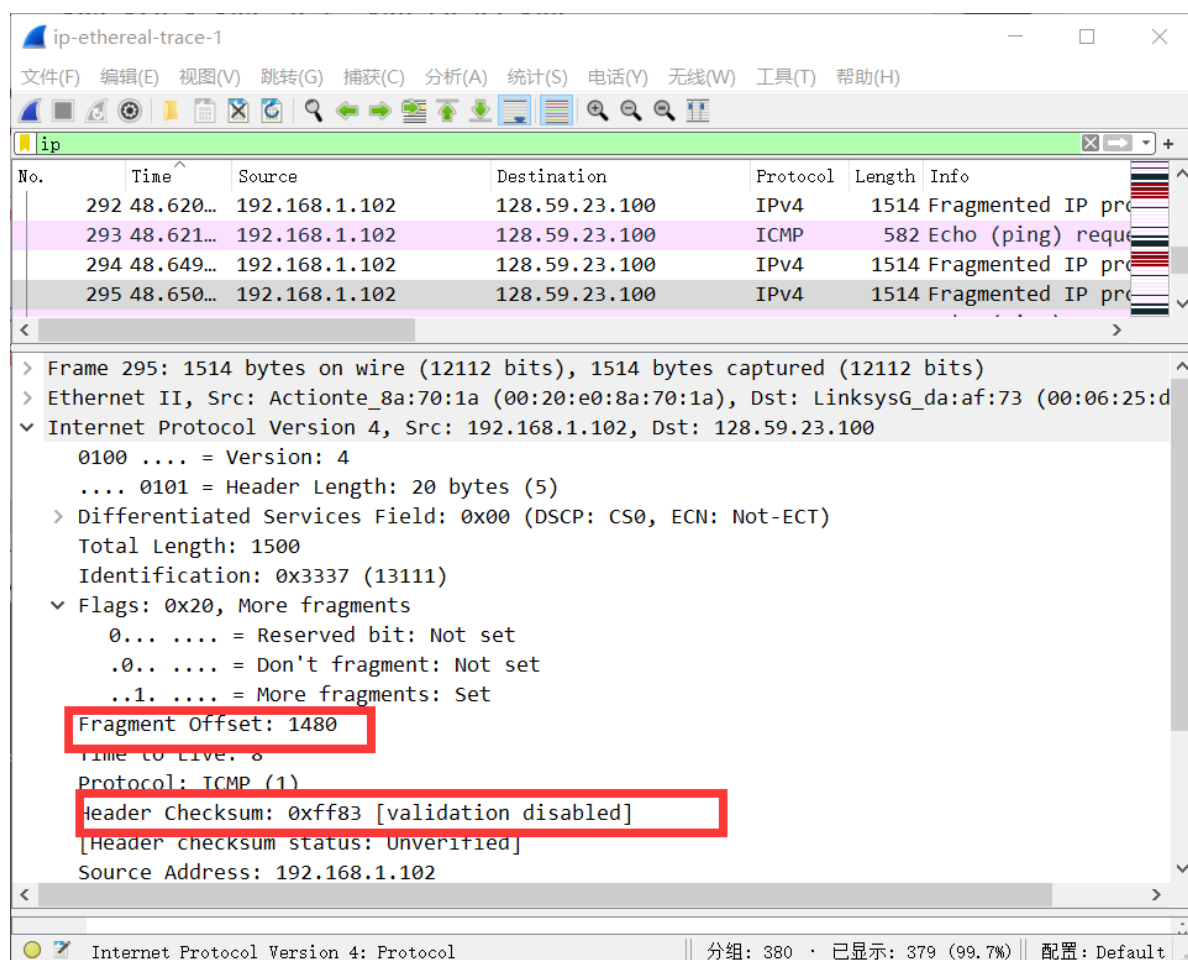
Protocol: ICMP (1)

Header Checksum: 0x003d [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.102

Internet Protocol Version 4: Protocol 分组: 380 · 已显示: 379 (99.7%) 配置: Default



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

创建了三个片段.(具体截图可由13,15题目看到)

→	294	48.649...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pr
→	295	48.650...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pr
→	296	48.651...	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) requ

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

Total Length, Flags, Fragment offset, Head checksum(第1,2个fragment截图见13题),下图为第3个

ip-ethereal-trace-1

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip

No.	Time	Source	Destination	Protocol	Length	Info
292	48.620...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro
293	48.621...	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) requ
294	48.649...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP pro

> Frame 296: 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: LinksysG_da:af:73 (00:06:25:d

▼ 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: 0x3337 (13111)
- ▼ Flags: 0x01
 - 0... = Reserved bit: Not set
 - .0.. = Don't fragment: Not set
 - ..0. = More fragments: Not set
- Fragment Offset: 2960
- Time to Live: 8
- Protocol: ICMP (1)
- Header Checksum: 0x226f | validation disabled |
- [Header checksum status: Unverified]
- Source Address: 192.168.1.102
- Destination Address: 128.59.23.100

Frame (582 bytes) Reassembled IPv4 (3508 bytes)

Internet Protocol Version 4: Protocol | 分组: 380 · 已显示: 379 (99.7%) | 配置: Default

实验思考

本次实验了解并在实践中应用了IP协议的相关知识,详细分析了IP数据报.