

CS305-2022Spring Lab11 Report

Name: Yitong WANG 11910104@mail.sustech.edu.cn

Student ID: 11910104

Lab Time: Thursday 10:20 a.m. to 12:10 p.m.

Lab Teacher: Qing WANG wangq9@mail.sustech.edu.cn

Lab SA:


- Siyu LIU 11912935@mail.sustech.edu.cn
- Xingying ZHENG 11912039@mail.sustech.edu.cn

Practice11.1: ICMP

- Q1: How to initiate an ICMP Echo request with 2021B length?

A1: type the following commands in cmd:

```
ping www.example.com -4 -l 2021
```

 命令提示符

```
C:\Users\16011>ping www.example.com -4 -l 2021

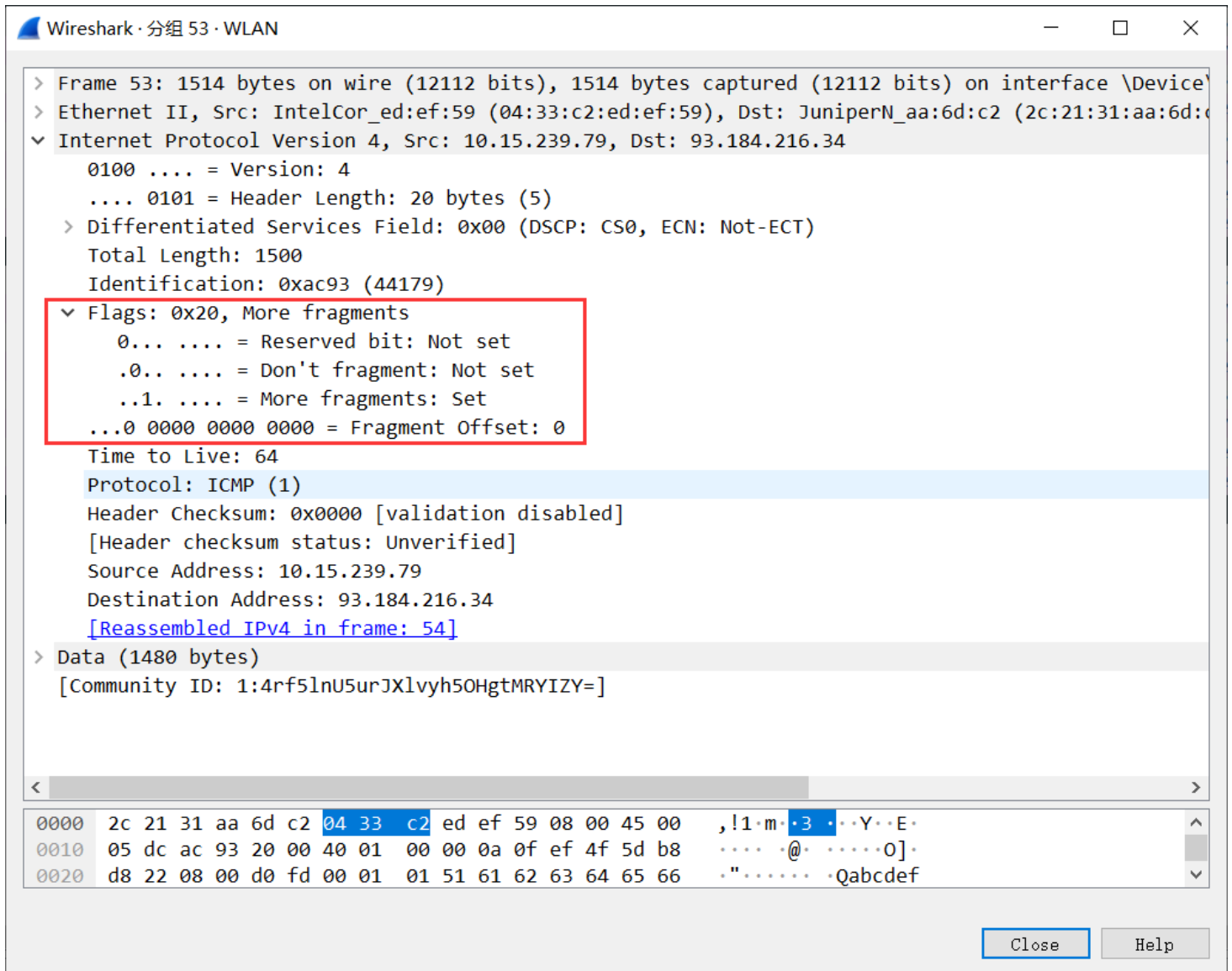
正在 Ping www.example.com [93.184.216.34] 具有 2021 字节的数据:
来自 93.184.216.34 的回复: 字节=2021 时间=169ms TTL=49
来自 93.184.216.34 的回复: 字节=2021 时间=169ms TTL=49
来自 93.184.216.34 的回复: 字节=2021 时间=169ms TTL=49
来自 93.184.216.34 的回复: 字节=2021 时间=170ms TTL=49

93.184.216.34 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 169ms, 最长 = 170ms, 平均 = 169ms

C:\Users\16011>
```

- Q2: Is there any fragmentation on the IP packets, how to find them?

A2: We can see that these packets have fragmentation.



Wireshark · 分组 53 · WLAN

- > Frame 53: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF...
- > Ethernet II, Src: IntelCor_ed:ef:59 (04:33:c2:ed:ef:59), Dst: JuniperN_aa:6d:c2 (2c:21:31:aa:6d:c2)
- ▼ Internet Protocol Version 4, Src: 10.15.239.79, Dst: 93.184.216.34
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 1500
 - Identification: 0xac93 (44179)
 - ▼ 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: 64
 - Protocol: ICMP (1)
 - Header Checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 10.15.239.79
 - Destination Address: 93.184.216.34
 - [\[Reassembled IPv4 in frame: 54\]](#)
- > Data (1480 bytes)
 - [Community ID: 1:4rf5lnU5urJXlvh5OHgtMRYIZY=]

0000	2c 21 31 aa 6d c2 04 33 c2 ed ef 59 08 00 45 00	,!1.m.3...Y..E.
0010	05 dc ac 93 20 00 40 01 00 00 0a 0f ef 4f 5d b8@.....O]..
0020	d8 22 08 00 d0 fd 00 01 01 51 61 62 63 64 65 66	.."......Qabcdef

Close Help

- Q3: How many fragments are the 2021-Byte-length IP packet divided into?

A3: It is divided into two fragments, for each of 2021-Byte-length ip packet.

This is because for two consecutive packets, one is IPv4 and one is ICMP.

WLAN

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

ip.addr == 93.184.216.34

No.	Time	Source	Destination	Protocol	Length	Info
40	5.339346	93.184.216.34	10.15.239.79	ICMP	590	Time-to-live exceeded (Fragment reassembly time exceeded)
53	7.523349	10.15.239.79	93.184.216.34	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ac93) [Reassembled in #54]
54	7.523349	10.15.239.79	93.184.216.34	ICMP	583	Echo (ping) request id=0x0001, seq=337/20737, ttl=64 (reply in 56)
55	7.692541	93.184.216.34	10.15.239.79	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2c13) [Reassembled in #56]
56	7.692541	93.184.216.34	10.15.239.79	ICMP	583	Echo (ping) reply id=0x0001, seq=337/20737, ttl=49 (request in 54)
143	8.534561	10.15.239.79	93.184.216.34	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ac94) [Reassembled in #144]
144	8.534561	10.15.239.79	93.184.216.34	ICMP	583	Echo (ping) request id=0x0001, seq=338/20993, ttl=64 (reply in 146)
145	8.704181	93.184.216.34	10.15.239.79	IPv4	583	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2cc80) [Reassembled in #146]
146	8.704181	93.184.216.34	10.15.239.79	ICMP	1514	Echo (ping) reply id=0x0001, seq=338/20993, ttl=49 (request in 144)
148	9.435972	93.184.216.34	10.15.239.79	ICMP	590	Time-to-live exceeded (Fragment reassembly time exceeded)
149	9.542675	10.15.239.79	93.184.216.34	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ac95) [Reassembled in #150]
150	9.542675	10.15.239.79	93.184.216.34	ICMP	583	Echo (ping) request id=0x0001, seq=339/21249, ttl=64 (reply in 153)
152	9.711500	93.184.216.34	10.15.239.79	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2cc8) [Reassembled in #153]
153	9.711500	93.184.216.34	10.15.239.79	ICMP	583	Echo (ping) reply id=0x0001, seq=339/21249, ttl=49 (request in 150)
176	10.563204	10.15.239.79	93.184.216.34	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ac96) [Reassembled in #177]
177	10.563204	10.15.239.79	93.184.216.34	ICMP	583	Echo (ping) request id=0x0001, seq=340/21505, ttl=64 (reply in 179)
178	10.732155	93.184.216.34	10.15.239.79	IPv4	583	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2d41) [Reassembled in #179]
179	10.732155	93.184.216.34	10.15.239.79	ICMP	1514	Echo (ping) reply id=0x0001, seq=340/21505, ttl=49 (request in 177)
247	21.724096	93.184.216.34	10.15.239.79	ICMP	590	Time-to-live exceeded (Fragment reassembly time exceeded)

[illegible]

A4: It could be seen in the type information of the packet:

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 569
Identification: 0xac93 (44179)
> Flags: 0x00
...0 0101 1100 1000 = Fragment Offset: 1480
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.15.239.79
Destination Address: 93.184.216.34
> [2 IPv4 Fragments (2029 bytes) · #53(1480), #54(549)]
✓ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xd0fd [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 337 (0x0151)
Sequence Number (LE): 20737 (0x5101)
[\[Response frame: 56\]](#)
> Data (2021 bytes)
[Community ID: 1:9C6ZH01LaGdULAh0jGsiimezGR0=]

< Frame (583 bytes) Reassembled IPv4 (2029 bytes) >

[Close](#)[Help](#)

Wireshark · 分组 56 · WLAN

> Flags: 0x00
 ...0 0101 1100 1000 = Fragment Offset: 1480
 Time to Live: 49
 Protocol: ICMP (1)
 Header Checksum: 0x2bbf [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 93.184.216.34
 Destination Address: 10.15.239.79
 > [2 IPv4 Fragments (2029 bytes): #55(1480), #56(549)]

✓ Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0xd8fd [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 337 (0x0151)
 Sequence Number (LE): 20737 (0x5101)
[\[Request frame: 54\]](#)
 [Response time: 169.192 ms]

> Data (2021 bytes)
 [Community ID: 1:9C6ZH01LaGdULAh0jGsiiMezGR0=]

0000	04 33 c2 ed ef 59 2c 21 31 aa 6d c2 08 00 45 00	·3···Y, ! 1·m···E·
0010	02 39 2c 13 00 b9 31 01 2b bf 5d b8 d8 22 0a 0f	·9,···1· +·]··"··
0020	ef 4f 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e	·0abcdef ghijklmn
0030	6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67	opqrstuv wabcdefg

Frame (583 bytes) Reassembled IPv4 (2029 bytes)

- Q5: For the ICMP Echo request, which fragment is the first one, which is the last ? How to identify them?

A5: In the captured packets, the #53 is the first one, and #177 is the last one. This can be identified by the epoch time.

Wireshark · 分组 53 · WLAN

▼ Frame 53: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{89B88E7E-F07A-4F3E-969E-18F5F268FB76}

> Interface id: 0 (\Device\NPF_{89B88E7E-F07A-4F3E-969E-18F5F268FB76})

Encapsulation type: Ethernet (1)

Arrival Time: Apr 28, 2022 11:29:29.517886000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1651116569.517886000 seconds

[Time delta from previous captured frame: 0.018331000 seconds]

[Time delta from previous displayed frame: 2.184003000 seconds]

[Time since reference or first frame: 7.523349000 seconds]

Frame Number: 53

Frame Length: 1514 bytes (12112 bits)

Capture Length: 1514 bytes (12112 bits)

0000	2c 21 31 aa 6d c2 04 33 c2 ed ef 59 08 00 45 00	,!1.m..3 ...Y..E.
0010	05 dc ac 93 20 00 40 01 00 00 0a 0f ef 4f 5d b8@.O].
0020	d8 22 08 00 d0 fd 00 01 01 51 61 62 63 64 65 66	..".Qabcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f	wabcdefg hijklmno
0050	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68	pqrstuvw abcdefgh
0060	69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61	ijklmnop qrstuvwa
0070	62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71	bcdefghi jklmnopq
0080	72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a	rstuvwab cdefghij
0090	6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63	klmnopqr stuvwabc
00a0	64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73	defghijk lmnopqrs
00b0	74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c	tuvwabcd efghijkl
00c0	6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65	mnopqrst uvwabcde
00d0	66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75	fghijklm nopqrstu
00e0	76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e	vwabcdef ghijklmn
00f0	6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67	opqrstuv wabcdefg

No.: 53 · Time: 7.523349 · Source: 10.15.239.79 · Destination: 93.184.21...agmented IP protocol (proto=ICMP 1, off=0, ID=ac93) [Reassembled in #54]

Close Help

- Q6: What's the length of each IP fragment? Is the sum of each fragment's length equal to the original IP packet?

A6: Take 1 IPv4 and 1 ICMP packet as an example.

Wireshark · 分组 53 · WLAN

▼ Ethernet II, Src: IntelCor_ed:ef:59 (04:33:c2:ed:ef:59), Dst: JuniperN_aa:6d:c2 (2c:21:31:aa:6d:c2)

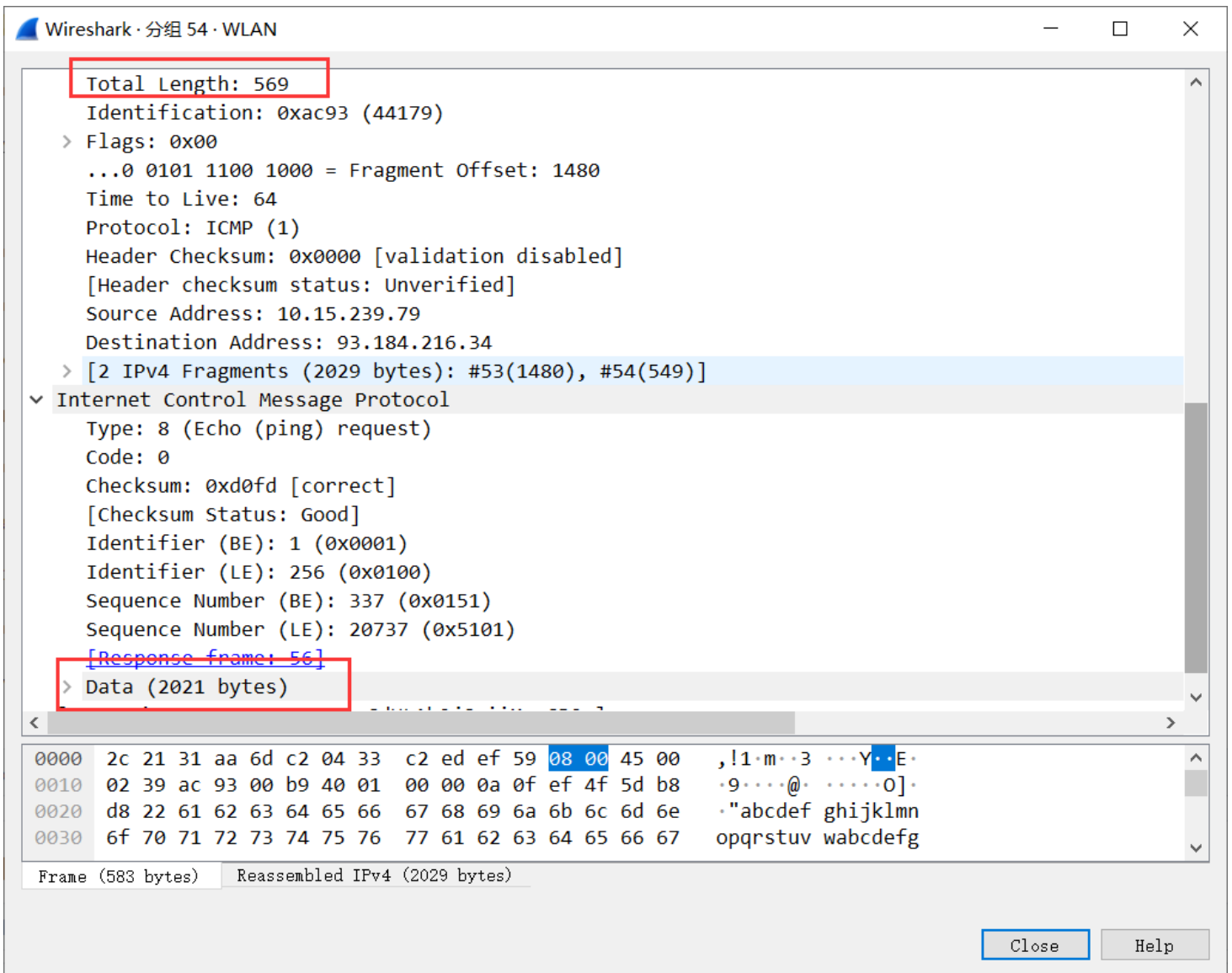
- > Destination: JuniperN_aa:6d:c2 (2c:21:31:aa:6d:c2)
- > Source: IntelCor_ed:ef:59 (04:33:c2:ed:ef:59)
- Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 10.15.239.79, Dst: 93.184.216.34

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 1500
- Identification: 0xac93 (44179)
- > Flags: 0x20, More fragments
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 64
- Protocol: ICMP (1)
- Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
- Source Address: 10.15.239.79
- Destination Address: 93.184.216.34
- [Reassembled IPv4 in frame: 54]
- Data (1480 bytes)
[Community ID: 1:4rf5lnU5urJXlvh5OHgtMRYIZY=]

Offset	Hex	ASCII
0000	2c 21 31 aa 6d c2 04 33 c2 ed ef 59 08 00 45 00	,!1.m.3 ...Y..E.
0010	05 dc ac 93 20 00 40 01 00 00 0a 0f ef 4f 5d b8 @.O].
0020	d8 22 08 00 d0 fd 00 01 01 51 61 62 63 64 65 66	."..... Qabcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f	wabcdefg hijklmno
0050	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68	pqrstuvw abcdefgh

The length of the IPv4 fragment is 1500, with 20 header length and 1480 data length.



The length of ICMP fragment is 569, with 20 header length and 2021 data length.

The sum is not equal, $1500 + 569 = 2069 \neq 2021$.

Practice11.2: tracert and ICMP

Commands:

```
tracert -4 www.sustech.edu.cn
```

- Q1: Is there any 'Time-to-live exceeded' ICMP packets?

A1: We can see that there are some 'TTL exceeded' ICMP packets.

No.	Time	Source	Destination	Protocol	Length	Info
133	17.046611	10.15.239.79	172.18.1.3	ICMP	106	Echo (ping) request id=0x0001, seq=357/25857, ttl=1 (no response found!)
134	17.050166	10.10.10.10	10.15.239.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
135	17.050648	10.15.239.79	172.18.1.3	ICMP	106	Echo (ping) request id=0x0001, seq=358/26113, ttl=1 (no response found!)
136	17.054365	10.10.10.10	10.15.239.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
137	17.054691	10.15.239.79	172.18.1.3	ICMP	106	Echo (ping) request id=0x0001, seq=359/26369, ttl=1 (no response found!)
138	17.064159	10.10.10.10	10.15.239.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
208	27.102965	10.15.239.79	172.18.1.3	ICMP	106	Echo (ping) request id=0x0001, seq=360/26625, ttl=2 (reply in 210)
210	27.108259	172.18.1.3	10.15.239.79	ICMP	106	Echo (ping) reply id=0x0001, seq=360/26625, ttl=63 (request in 208)
211	27.108731	10.15.239.79	172.18.1.3	ICMP	106	Echo (ping) request id=0x0001, seq=361/26881, ttl=2 (reply in 212)
212	27.113268	172.18.1.3	10.15.239.79	ICMP	106	Echo (ping) reply id=0x0001, seq=361/26881, ttl=63 (request in 211)
213	27.113705	10.15.239.79	172.18.1.3	ICMP	106	Echo (ping) request id=0x0001, seq=362/27137, ttl=2 (reply in 214)
214	27.117542	172.18.1.3	10.15.239.79	ICMP	106	Echo (ping) reply id=0x0001, seq=362/27137, ttl=63 (request in 213)

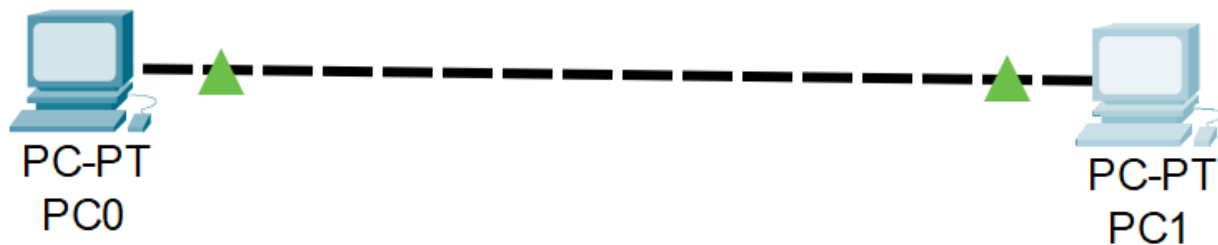
- Q2: What's the difference between these ICMP packets which are invoked by 'tracert' and ICMP echo request/replay packets which are invoked by 'ping'?

A2: Differences:

1. The total length of packets caused by `tracert` is much smaller than those by `ping`. The total length is 56 in `tracert` while 1500 in `ping`.
2. The packet by `ping` will contain a original packet(2021 bytes), while not by `tracert`
3. The TTL is not the same.

Practice11.3: Packet-tracer and ICMP

Build connection first:



- Q1: What's link-local unicast IPv6 address of these 2 PCs?

A1: Check the ip configuration of these two PCs.

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0 ▾

IP Configuration

☐ DHCP ☒ StaticIPv4 Address Subnet Mask

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☒ Automatic ☐ Static Ipv6 request failed.IPv6 Address / Link Local Address FE80::230:F2FF:FEBA:D0EC Default Gateway DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5 ▾

Username Password ☐ Top

PC1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address

Subnet Mask

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address

Link Local Address FE80::2D0:97FF:FE23:5B1C

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

We can get the IPv6 address:

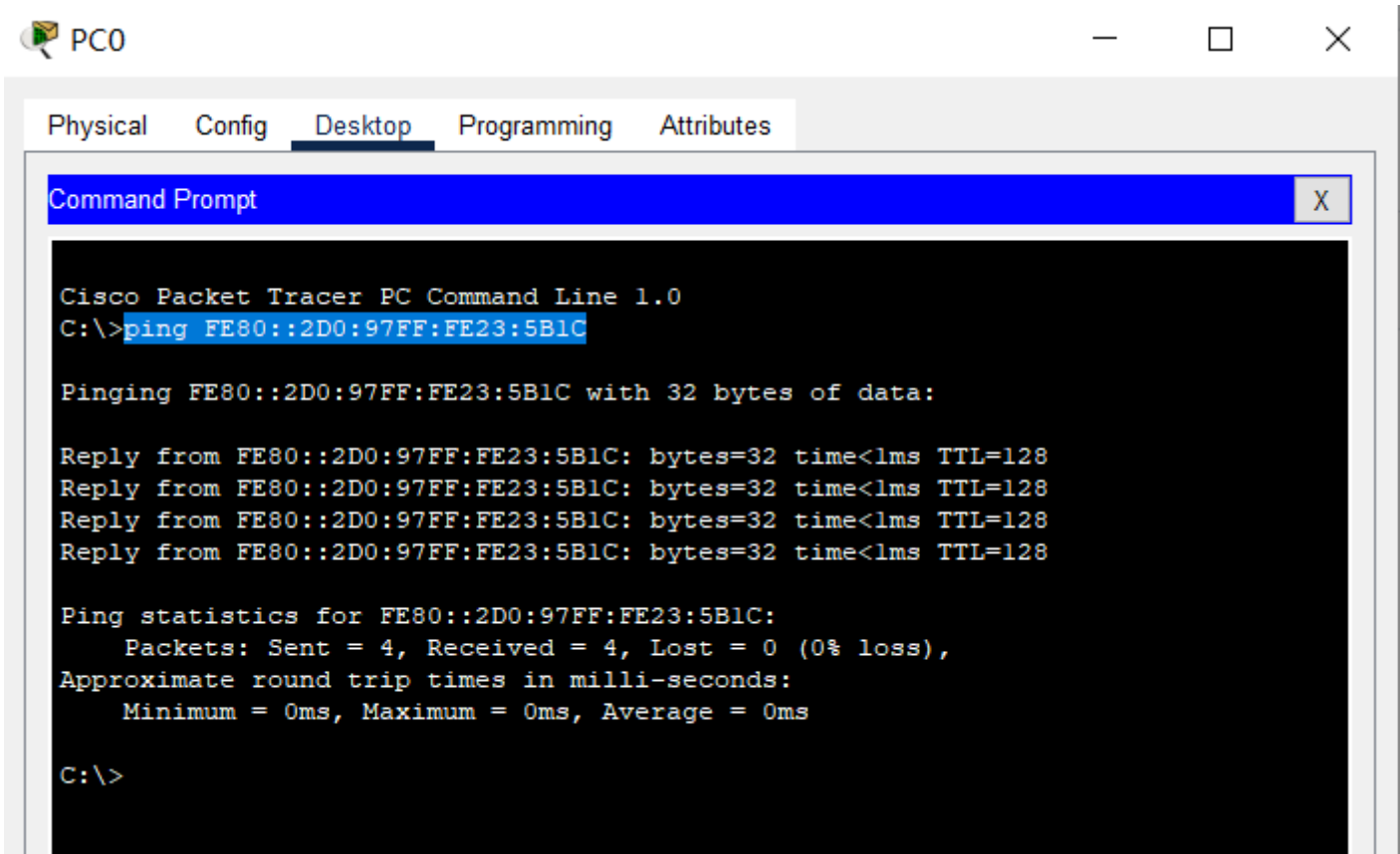
PC0: FE80::230:F2FF:FEBA:D0EC

PC1: FE80::2D0:97FF:FE23:5B1C

- Q2: Initiates an ICMPv6 session on PC0 to PC1, capture the packets

A2: Open a command prompt and type the following commands:

```
ping FE80::2D0:97FF:FE23:5B1C
```



- Q3: What's the difference between IPv4 datagram and IPv6 datagram? List at least 3 aspects.

A3: get the ipv6 packet under the simulation mode:

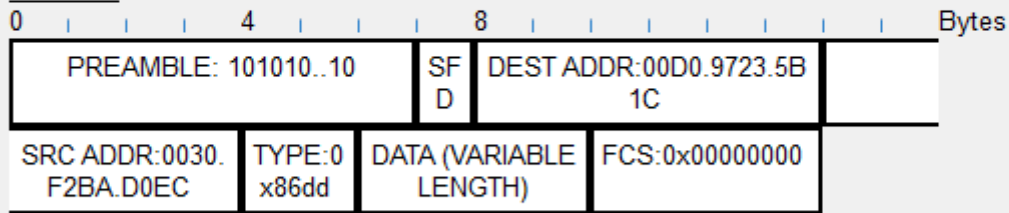
PDU Information at Device: PC1



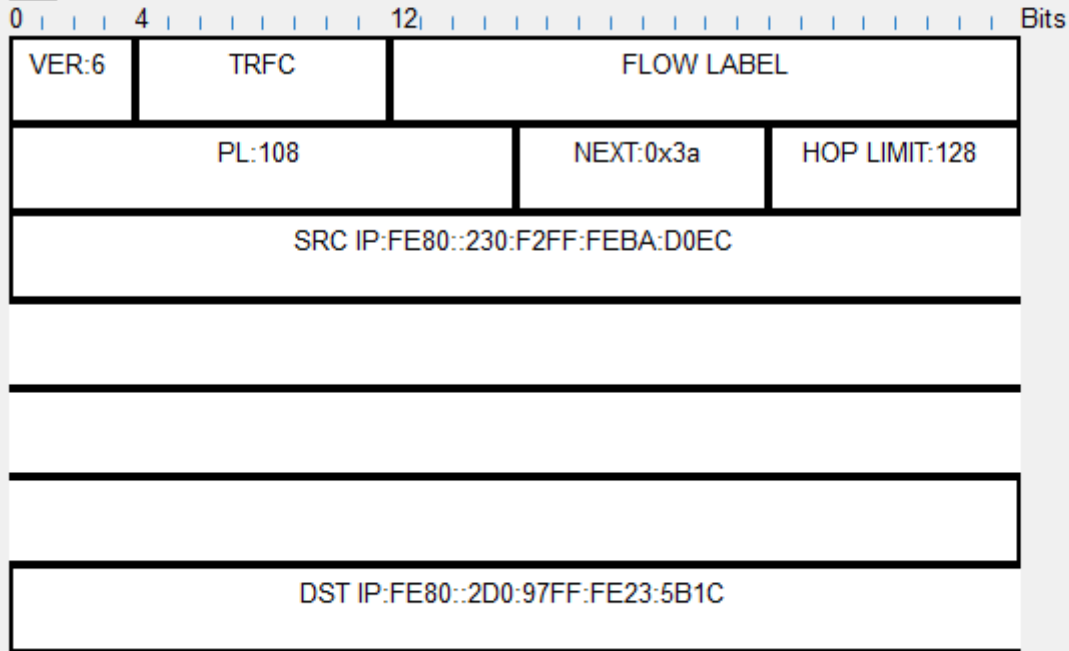
OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

EthernetII

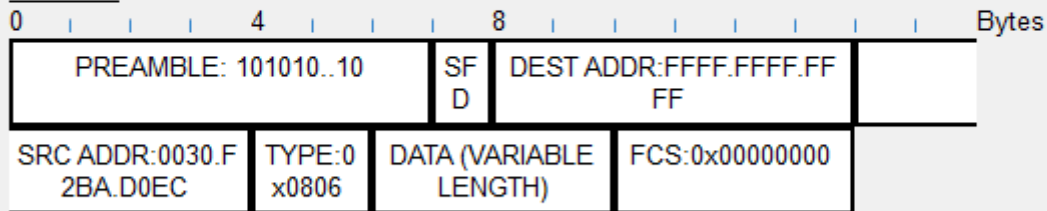
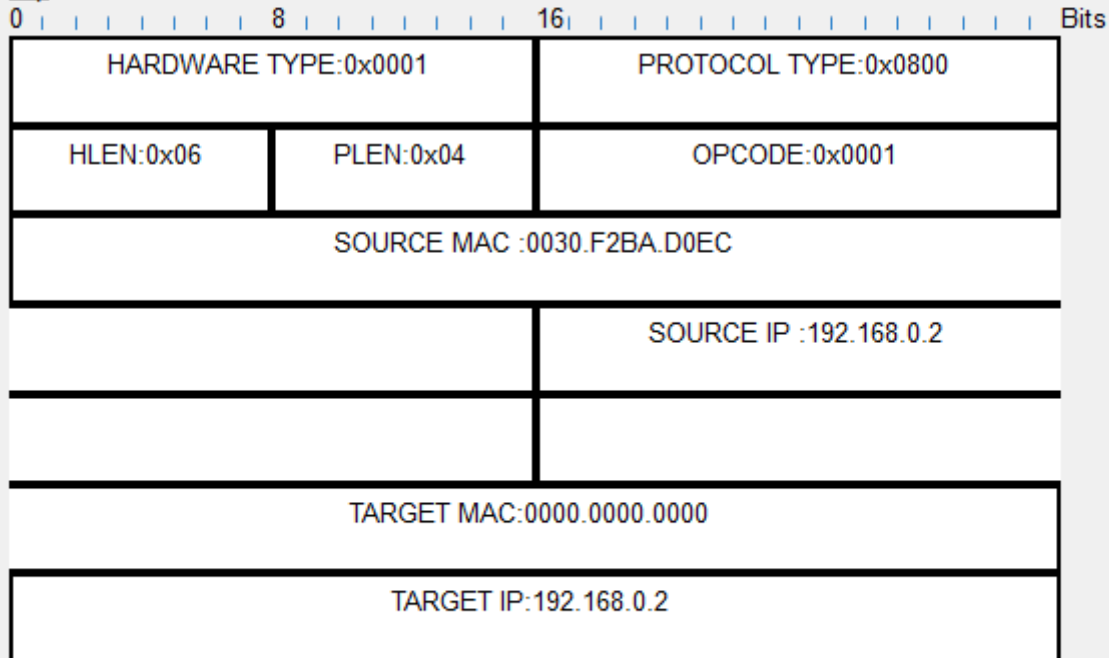


IPv6



get the ipv4 packet under the simulation mode:

PDU Formats

EthernetIIArp

We can see there are several differences:

1. ipv6 contains hardware information, while ipv4 not
2. ipv6 omits the protocol type information
3. ipv6 omits opcode and adds hop limit in the datagram

- Q4: Does these two IPv6 addresses belong to the same sub-net, what is the sub-net ID of these two IPv6 addresses?

A4: use ipconfig to get the subnet mask.

Subnet mask

PC0: 255.255.255.0

PC1: 255.255.255.0

IP address

PC0: 192.168.0.2

PC1: 192.168.0.1

We do the AND operation between subnet mask and IP address. The result is same: 192.168.0.0

Thus they belong to the same sub-net, and their sub-net ID is 192.168.0.0.