

CSC358 Wireshark Assignment 4 Solution

1. What is the client ip on the home side? And what is the client ip on the ISP side? What's the relationship between them?

Solution:

client ip on the home side: 192.168.1.100

client ip on the ISP side: 71.192.34.104

relationship: 71.192.34.104 is the external IP of internal host 192.168.1.100.

2. For the first packet of this TCP stream, is there anything changed in the TCP header between home side and ISP side? If so, name the header field(s).

Solution:

The “Checksum” field is different.

ISP side:

```

> Frame 82: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
> Internet Protocol Version 4, Src: 71.192.34.104 (71.192.34.104), Dst: 64.233.169.104 (64.233.169.104)
< Transmission Control Protocol, Src Port: 4335 (4335), Dst Port: 80 (80), Seq: 0, Len: 0
  Source Port: 4335 (4335)
  Destination Port: 80 (80)
  [Stream index: 2]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 0
  Header Length: 32 bytes
  < ... 0000 0000 0010 = Flags: 0x002 (SYN)
  Window size value: 65535
  [Calculated window size: 65535]
  < Checksum: 0xda46 [validation disabled]
  Urgent pointer: 0
  < Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted

```

home side:

```

> Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco_Li_45:1f:1b (00:22:6b:45:1f:1b)
> Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 64.233.169.104 (64.233.169.104)
< Transmission Control Protocol, Src Port: 4335 (4335), Dst Port: 80 (80), Seq: 0, Len: 0
  Source Port: 4335 (4335)
  Destination Port: 80 (80)
  [Stream index: 2]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 0
  Header Length: 32 bytes
  < ... 0000 0000 0010 = Flags: 0x002 (SYN)
  Window size value: 65535
  [Calculated window size: 65535]
  < Checksum: 0x8262 [validation disabled]
  Urgent pointer: 0
  < Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted

```

3. Focus on the same packet, is there anything changed in the IP header? If so, name the header field(s), and explain why they are changed?

Solution:

Different fields: Time to live, Header checksum, Source.

Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed.

ISP side:

```
> Frame 82: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
> Internet Protocol Version 4, Src: 71.192.34.104 (71.192.34.104), Dst: 64.233.169.104 (64.233.169.104)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 52
  Identification: 0xa2aa (41642)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 127
  Protocol: TCP (6)
  Header checksum: 0x04a0 [validation disabled]
  Source: 71.192.34.104 (71.192.34.104)
  Destination: 64.233.169.104 (64.233.169.104)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
> Transmission Control Protocol, Src Port: 4335 (4335), Dst Port: 80 (80), Seq: 0, Len: 0
```

home side:

```
> Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
> Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 64.233.169.104 (64.233.169.104)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 52
  Identification: 0xa2aa (41642)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0xabbb [validation disabled]
  Source: 192.168.1.100 (192.168.1.100)
  Destination: 64.233.169.104 (64.233.169.104)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
> Transmission Control Protocol, Src Port: 4335 (4335), Dst Port: 80 (80), Seq: 0, Len: 0
```

4. For the first packet of this UDP stream, is there anything changed in the UDP header between home side and ISP side? If so, name the header field(s). Is any other udp header or data changed? If not, explain why udp checksum changed.

Solution:

The field of “Checksum” is different.

UDP has a checksum that covers all the data they carry, as well as the UDP header, plus a "pseudo-header" that contains the source and destination IP addresses of the packet carrying the TCP/UDP header. Since the source IP contained in the “pseudo-header” changes, the checksum is also changed correspondingly. It is worth mentioning that no other headers or data is changed.

ISP side:

```
▶ Frame 3: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits)
▶ Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)
▶ Internet Protocol Version 4, Src: 68.87.71.230 (68.87.71.230), Dst: 71.192.34.104 (71.192.34.104)
▼ User Datagram Protocol, Src Port: 53 (53), Dst Port: 51554 (51554)
    Source Port: 53 (53)
    Destination Port: 51554 (51554)
    Length: 177
    ▶ Checksum: 0x5738 [validation disabled]
      [Stream index: 0]
▶ Domain Name System (response)
```

home side:

```
▶ Frame 3: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits)
▶ Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
▶ Internet Protocol Version 4, Src: 68.87.71.230 (68.87.71.230), Dst: 192.168.1.100 (192.168.1.100)
▼ User Datagram Protocol, Src Port: 53 (53), Dst Port: 51554 (51554)
    Source Port: 53 (53)
    Destination Port: 51554 (51554)
    Length: 177
    ▶ Checksum: 0xff53 [validation disabled]
      [Stream index: 1]
▶ Domain Name System (response)
```

5. For the tcp and udp streams we discussed above, for all the packets that the client sent, is the tcp/udp source port ever changed by the router? If not, is it mandatory to keep the same port before and after NAT translation?

Solution:

It is not mandatory to preserve port number for both TCP and UDP, as long as the router can distinguish each stream and forward packet to corresponding internal hosts.

6. Why is it that an ICMP packet does not have source and destination port number?

Solution:

The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes. Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

7. Choose one of the ping request packets sent by your host, what are the ICMP type and code numbers? Find the corresponding ping reply, what are the type and code numbers?

Solution:

ping request:

type: 8

code number: 0

ping reply:

type: 0

code number: 0

ping request:

```
▶ Frame 234: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Apple_b2:bc:fd (78:ca:39:b2:bc:fd), Dst: Sagemcom_dc:f4:50 (18:62:2c:dc:f4:50)
▶ Internet Protocol Version 4, Src: 192.168.2.12 (192.168.2.12), Dst: 128.119.245.12 (128.119.245.12)
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4e6a [correct]
  Identifier (BE): 27654 (0x6c06)
  Identifier (LE): 1644 (0x066c)
  Sequence number (BE): 0 (0x0000)
  Sequence number (LE): 0 (0x0000)
  [Response frame: 235]
  Timestamp from icmp data: Mar  5, 2016 23:06:06.347901000 EST
  [Timestamp from icmp data (relative): 0.000059000 seconds]
▶ Data (48 bytes)
```

ping reply:

```
▶ Frame 235: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Sagemcom_dc:f4:50 (18:62:2c:dc:f4:50), Dst: Apple_b2:bc:fd (78:ca:39:b2:bc:fd)
▶ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.2.12 (192.168.2.12)
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x566a [correct]
  Identifier (BE): 27654 (0x6c06)
  Identifier (LE): 1644 (0x066c)
  Sequence number (BE): 0 (0x0000)
  Sequence number (LE): 0 (0x0000)
  [Request frame: 234]
  [Response time: 39.385 ms]
  Timestamp from icmp data: Mar  5, 2016 23:06:06.347901000 EST
  [Timestamp from icmp data (relative): 0.039444000 seconds]
▶ Data (48 bytes)
```

8. During the browser trying to loading the page, did your host receive any ICMP. If yes, what are the type and code of these ICMP packets?

Solution:

Yes.

Type: 3

code: 10

```

▶ Frame 232: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
▶ Ethernet II, Src: Sagemcom_dc:f4:50 (18:62:2c:dc:f4:50), Dst: Apple_b2:bc:fd (78:ca:39:b2:bc:fd)
▶ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.2.12 (192.168.2.12)
▼ Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 10 (Host administratively prohibited)
  Checksum: 0x3561 [correct]
▶ Internet Protocol Version 4, Src: 192.168.2.12 (192.168.2.12), Dst: 128.119.245.12 (128.119.245.12)
▶ Transmission Control Protocol, Src Port: 50390 (50390), Dst Port: 81 (81), Seq: 787161744
```

9. Apart from the ICMP headers, what is in the data field of these ICMP packets?

Solution:

The data field contains the IP header and first 8 bytes of original datagram's data.

```

    ▶ Frame 403: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
    ▶ Ethernet II, Src: Sagemcom_dc:f4:50 (18:62:2c:dc:f4:50), Dst: Apple_b2:bc:fd (78:ca:39:b2:bc:fd)
    ▶ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.2.12 (192.168.2.12)
    ▼ Internet Control Message Protocol
      Type: 3 (Destination unreachable)
      Code: 10 (Host administratively prohibited)
      Checksum: 0x3561 [correct]
    ▶ Internet Protocol Version 4, Src: 192.168.2.12 (192.168.2.12), Dst: 128.119.245.12 (128.119.245.12)
    ▶ Transmission Control Protocol, Src Port: 51072 (51072), Dst Port: 81 (81), Seq: 1832505291
  
```

```

0000  78 ca 39 b2 bc fd 18 62 2c dc f4 50 08 00 45 00  x.9...b ,..P..E.
0010  00 5c 63 4c 00 00 32 01 ed 1c 80 77 f5 0c c0 a8  .\cL..2. ...w...
0020  02 0c 03 0a 35 61 00 00 00 00 45 00 00 40 08 e9  ...5a...E...@..
0030  40 00 33 06 06 97 c0 a8 02 0c 80 77 f5 0c c7 80  @.3.....w...
0040  00 51 6d 39 cf cb 00 00 00 00 b0 02 ff ff 16 f0  .Qm9.....
0050  00 00 02 04 05 ac 01 03 03 05 01 01 08 0a 2c ef  .....
0060  b6 16 00 00 00 00 04 02 00 00  .....
  
```

From wiki:

Destination unreachable message^{[3]:3}

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type = 3								Code								Header checksum															
unused																Next-hop MTU															
IP header and first 8 bytes of original datagram's data																															

10. Imagine the case when a NAT router receives one of the above ICMP packets on its external interface, how does the router know which internal host to forward this packet to?

Solution:

For ICMP query/reply type messages like Echoes (pings), NAT uses the ICMP Query ID (sometimes just called the ICMP ID) the same way it would use a TCP or UDP port number. For ICMP error messages such as Destination Unreachable, it uses the ICMP packet's internal copy of the headers of the frame that caused the error to figure out which mapping in the NAT table to use to translate it.