

Student Name: Gökay Gülsoy
Student Number: 270201072

-CENG312-ASSIGNMENT 3 IP, ICMP, NAT, DHCP-

1.)

a.) When we look at the packet traffic “Fragmentation needed” ICMP messages are triggered in case amount of data that should be carried by datagram exceeds the maximum amount of data can be carried within the datagram.

b.) When endpoints receive the “Fragmentation needed” message endpoints can divide or in other words fragment datagram into smaller IPv4 packets. To identify fragments 16-bit field is used as an identification field and this identification field is copied to fragmented packet header so that on the destination side receiver will be able to reassemble the fragments that belong to a particular frame. In the packet traffic there is a problem related to fragmentation, because even though endpoint with IP address 62.177.254.141 has received ICMP message “Destination unreachable (Fragmentation needed)” three times it was not able to perform fragmentation. (Figure 1 and 2)

No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
1	2005-10-12 05:11:48, 326590	62.177.254.141	62.177.254.1	DNS	78		Standard query 0x0e69 A scsc.msg.yahoo.com
2	2005-10-12 05:11:48, 327329	100.100.100.100	62.177.254.141	ICMP	78		Destination unreachable (Fragmentation needed)
3	2005-10-12 05:11:49, 327191	62.177.254.141	62.177.254.1	DNS	78		Standard query 0x0e69 A scsc.msg.yahoo.com
4	2005-10-12 05:11:50, 327263	62.177.254.141	62.177.254.1	DNS	78		Standard query 0x0e69 A scsc.msg.yahoo.com
5	2005-10-12 05:11:52, 327711	62.177.254.141	62.177.254.1	DNS	78		Standard query 0x0e69 A scsc.msg.yahoo.com
6	2005-10-12 05:11:54, 329648	08:05:5d:7d:1..	Broadcast	ARP	60		Who has 62.177.254.141? Tell 62.177.254.1
7	2005-10-12 05:11:54, 329673	Sony_f4:3a:09	08:05:5d:7d:1..	ARP	42		62.177.254.141 is at 08:00:46:f4:3a:09
8	2005-10-12 05:11:56, 328481	62.177.254.141	62.177.254.1	DNS	78		Standard query 0x0e69 A scsc.msg.yahoo.com
9	2005-10-12 05:11:56, 329135	100.100.100.100	62.177.254.141	ICMP	78		Destination unreachable (Fragmentation needed)
10	2005-10-12 05:12:03, 329481	62.177.254.141	62.177.254.1	DNS	78		Standard query 0xb16b A scsc.msg.yahoo.com
11	2005-10-12 05:12:03, 330124	100.100.100.100	62.177.254.141	ICMP	78		Destination unreachable (Fragmentation needed)
12	2005-10-12 05:12:04, 329919	62.177.254.141	62.177.254.1	DNS	78		Standard query 0xb16b A scsc.msg.yahoo.com
13	2005-10-12 05:12:05, 330114	62.177.254.141	62.177.254.1	DNS	78		Standard query 0xb16b A scsc.msg.yahoo.com
14	2005-10-12 05:12:07, 330481	62.177.254.141	62.177.254.1	DNS	78		Standard query 0xb16b A scsc.msg.yahoo.com
15	2005-10-12 05:12:09, 593433	08:05:5d:7d:1..	Broadcast	ARP	60		Who has 62.177.254.141? Tell 62.177.254.1
16	2005-10-12 05:12:09, 593453	Sony_f4:3a:09	08:05:5d:7d:1..	ARP	42		62.177.254.141 is at 08:00:46:f4:3a:09
17	2005-10-12 05:12:11, 331277	62.177.254.141	62.177.254.1	DNS	78		Standard query 0xb16b A scsc.msg.yahoo.com
18	2005-10-12 05:12:11, 332056	100.100.100.100	62.177.254.141	ICMP	78		Destination unreachable (Fragmentation needed)

Frame 2: 78 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface unknown, id 0
Ethernet II, Src: 08:05:5d:7d:1b:a0 (08:05:5d:7d:1b:a0), Dst: Sony_f4:3a:09 (08:00:46:f4:3a:09)
Internet Protocol Version 4, Src: 100.100.100.100, Dst: 62.177.254.141
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 56
Identification: 0x310e (12558)
Flags: 0x00
0... = Reserved bit: Not set
..0... = Don't fragment: Not set
..0... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x03b0 [validation disabled]
[Header checksum status: Unverified]
Source Address: 100.100.100.100
Destination Address: 62.177.254.141
Internet Control Message Protocol
Type: 3 (Destination unreachable)
Code: 4 (Fragmentation needed)
Checksum: 0x417a [correct]
Checksum Status: Correct

Also when we look at the "More fragments" bit we can see that it is not set, normally it should be set to 1 in order to indicate fragmentation. This also indicates that there is a problem in fragmentation process.

When we look at the traffic "Destination unreachable" (Fragmentation needed) ICMP message was sent three times which indicates that IP fragmentation couldn't be performed.

Figure 1: Fragmentation problem in the traffic

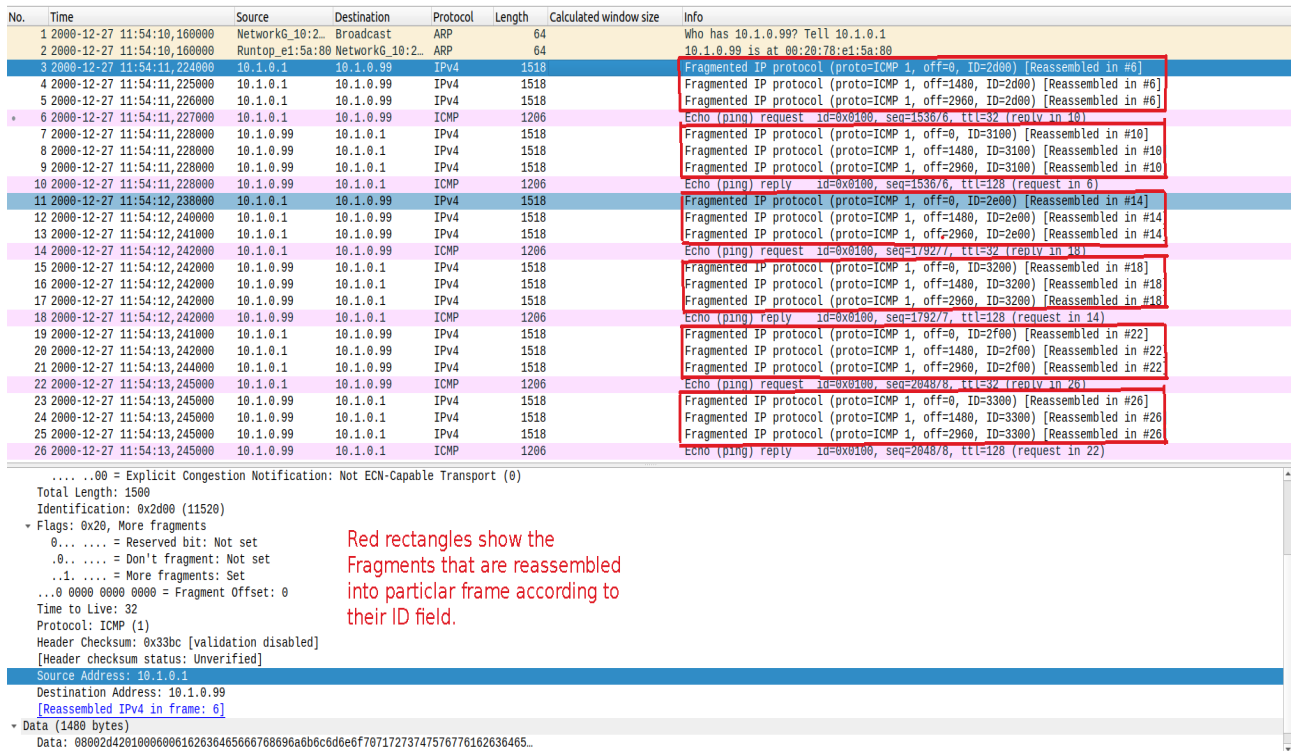


Figure 2: Reassembly operation on fragments is done according to id fields

2.)

a.) In the packet capture Info column, there is an information saying that

“Fragmented IP protocol” with fragment’s offset number. (Figure 3)

b.) Purpose of IP fragmentation is to divide large datagrams into smaller packets

which does not fit into a single datagram previously. Later, fragments will be reassembled at the destination according to identification fields.

c.) When we look at the line numbers 3,4, and 5 fragments with the ID=2d00 are all reassembled into number #6 frame. In the lines 7,8, and 9 fragments with ID=3100 are all reassembled into number #10 frame. In the lines 11,12, and 13 fragments with ID=2e00 are all reassembled into number #14 frame. In the lines 15,16, and 17 fragments with ID=3200 are all reassembled into number #18 frame.

In the lines 19,20, and 21 fragments with ID=2f00 are all reassembled into number #22 (Figure 3 and Figure 4)

frame. In the lines 23,24, and 25 with ID=3300 are all reassembled into number #26.

c.) If we look at the line numbers 3,4, and 5, fragments which have ID=2d00 belong to

to frame with number #6. Each Fragment has a total length of 1500, so total length is 4500. We can also compute the original packet size by using offset values. First packet's offset is 0 and second packet's offset is 1480, so data length of first packet should be 1480. Second packet offset is 1480 and third packet offset is 2960, so data length of second packet is 1480. Third packet also has the data length 1480, so total data length is 4440 and also each fragment has 20 byte header field so total 60 bytes for headers. Indeed $4440 + 60 = 4500$ is the original IP packet length which conforms to total length information in Wireshark bottom panel. (Figure 4 and Figure 6)

d.) For the fragments whose ID's are 2d00, 2e00, and 2f00 Time to live field is 32 whereas, fragments whose ID's are 3100, 3200, and 3300 have Time to live field value 128. So TTL value is different for some fragments. Reason that's why TTL value for some fragments is longer than others can be attributed to importance of fragment, may be some fragments some fragments are given more importance due to role of data they carry. (Figure 5)

No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
1	2000-12-27 11:54:10	160000 NetworkG_10:22:1b	Broadcast	ARP	64		Who has 10.1.0.99? Tell 10.1.0.1
2	2000-12-27 11:54:10	160000 Runtop_e1:5a:80	NetworkG_10:22:1b	ARP	64		10.1.0.99 is at 00:20:78:e1:5a:80
3	2000-12-27 11:54:11	224000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2d00) [Reassembled in #6]
4	2000-12-27 11:54:11	225000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2d00) [Reassembled in #6]
5	2000-12-27 11:54:11	226000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2d00) [Reassembled in #6]
6	2000-12-27 11:54:11	227000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=1536/6, ttl=32 (reply in 10)
7	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3100) [Reassembled in #10]
8	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3100) [Reassembled in #10]
9	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3100) [Reassembled in #10]
10	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=1536/6, ttl=128 (request in 6)
11	2000-12-27 11:54:12	238000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2e00) [Reassembled in #14]
12	2000-12-27 11:54:12	240000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2e00) [Reassembled in #14]
13	2000-12-27 11:54:12	241000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2e00) [Reassembled in #14]
14	2000-12-27 11:54:12	242000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=1792/7, ttl=32 (reply in 18)
15	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3200) [Reassembled in #18]
16	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3200) [Reassembled in #18]
17	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3200) [Reassembled in #18]
18	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=1792/7, ttl=128 (request in 14)
19	2000-12-27 11:54:13	241000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2f00) [Reassembled in #22]
20	2000-12-27 11:54:13	242000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2f00) [Reassembled in #22]
21	2000-12-27 11:54:13	244000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2f00) [Reassembled in #22]
22	2000-12-27 11:54:13	245000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=2048/8, ttl=32 (reply in 26)
23	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3300) [Reassembled in #26]
24	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3300) [Reassembled in #26]
25	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3300) [Reassembled in #26]
26	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=2048/8, ttl=128 (request in 22)

Flags: 0x20, More fragments
0... .. = Reserved bit: Not set
0... .. = Don't fragment: Not set
...1... .. = More fragments: Set
...0 0101 1100 1000 = Fragment Offset: 1480
Time to Live: 32
Protocol: ICMP (1)
Header Checksum: 0x3303 (validation disabled)
[Header checksum status: Unverified]
Source Address: 10.1.0.1
Destination Address: 10.1.0.99
[Reassembled IPv4 in frame: 6]
Data (1480 bytes)
Data: 61b2636465666768696a6b6c6d6e6f70717273747576776162636465666768696a6b6c6d...
[Length: 1480]

Each fragment with ID=2d00 has the data part length 1480 bytes. So the total data part length of these three fragments is 4440. Also each fragment has an header field of 20 bytes, so in total $4440 + 3 \times 20 = 4500$ should be the length of original IP packet.

Figure 3: Calculating original packet length with help of offset information

No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
1	2000-12-27 11:54:10	160000 NetworkG_10:22:1b	Broadcast	ARP	64		Who has 10.1.0.99? Tell 10.1.0.1
2	2000-12-27 11:54:10	160000 Runtime_e1:5a:80	NetworkG_10:22:1b	ARP	64		10.1.0.99 is at 00:20:78:e1:5a:80
3	2000-12-27 11:54:11	224000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2d00) [Reassembled in #6]
4	2000-12-27 11:54:11	225000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2d00) [Reassembled in #6]
5	2000-12-27 11:54:11	226000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2d00) [Reassembled in #6]
6	2000-12-27 11:54:11	227000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=1536/6, ttl=32 (reply in 10)
7	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3100) [Reassembled in #10]
8	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3100) [Reassembled in #10]
9	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3100) [Reassembled in #10]
10	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=1536/6, ttl=128 (request in 6)
11	2000-12-27 11:54:12	238000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2e00) [Reassembled in #14]
12	2000-12-27 11:54:12	240000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2e00) [Reassembled in #14]
13	2000-12-27 11:54:12	241000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2e00) [Reassembled in #14]
14	2000-12-27 11:54:12	242000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=1792/7, ttl=32 (reply in 18)
15	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3200) [Reassembled in #18]
16	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3200) [Reassembled in #18]
17	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3200) [Reassembled in #18]
18	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=1792/7, ttl=128 (request in 14)
19	2000-12-27 11:54:13	241000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2f00) [Reassembled in #22]
20	2000-12-27 11:54:13	242000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2f00) [Reassembled in #22]
21	2000-12-27 11:54:13	244000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2f00) [Reassembled in #22]
22	2000-12-27 11:54:13	245000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=2048/8, ttl=32 (reply in 26)
23	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3300) [Reassembled in #26]
24	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3300) [Reassembled in #26]
25	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3300) [Reassembled in #26]
26	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=2048/8, ttl=128 (request in 22)

Frame 4: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits) on interface unknown, id 0
Ethernet II, Src: NetworkG_10:22:1b (00:08:65:10:22:1b), Dst: Runtime_e1:5a:80 (00:20:78:e1:5a:80)
Internet Protocol Version 4, Src: 10.1.0.1, Dst: 10.1.0.99
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 1500
Identification: 0x2d00 (11520)
Flags: 0x20, More fragments
0... = Reserved bit: Not set
0... = Don't fragment: Not set
..1. = More fragments: Set
...0 0101 1100 1000 = Fragment Offset: 1480

Total length of each fragment
with ID=2d00 is 1500 bytes and
each fragment has an header field
of 20 bytes

Figure 4: Total length and header length fields of fragments

No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
1	2000-12-27 11:54:10	160000 NetworkG_10:22:1b	Broadcast	ARP	64		Who has 10.1.0.99? Tell 10.1.0.1
2	2000-12-27 11:54:10	160000 Runtime_e1:5a:80	NetworkG_10:22:1b	ARP	64		10.1.0.99 is at 00:20:78:e1:5a:80
3	2000-12-27 11:54:11	224000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2d00) [Reassembled in #6]
4	2000-12-27 11:54:11	225000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2d00) [Reassembled in #6]
5	2000-12-27 11:54:11	226000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2d00) [Reassembled in #6]
6	2000-12-27 11:54:11	227000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=1536/6, ttl=32 (reply in 10)
7	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3100) [Reassembled in #10]
8	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3100) [Reassembled in #10]
9	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3100) [Reassembled in #10]
10	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=1536/6, ttl=128 (request in 6)
11	2000-12-27 11:54:12	238000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2e00) [Reassembled in #14]
12	2000-12-27 11:54:12	240000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2e00) [Reassembled in #14]
13	2000-12-27 11:54:12	241000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2e00) [Reassembled in #14]
14	2000-12-27 11:54:12	242000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=1792/7, ttl=32 (reply in 18)
15	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3200) [Reassembled in #18]
16	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3200) [Reassembled in #18]
17	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3200) [Reassembled in #18]
18	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=1792/7, ttl=128 (request in 14)
19	2000-12-27 11:54:13	241000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2f00) [Reassembled in #22]
20	2000-12-27 11:54:13	242000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2f00) [Reassembled in #22]
21	2000-12-27 11:54:13	244000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2f00) [Reassembled in #22]
22	2000-12-27 11:54:13	245000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=2048/8, ttl=32 (reply in 26)
23	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3300) [Reassembled in #26]
24	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3300) [Reassembled in #26]
25	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3300) [Reassembled in #26]
26	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=2048/8, ttl=128 (request in 22)

Total Length: 1500
Identification: 0x2d00 (11520)
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: 32
Protocol: ICMP (1)
Header Checksum: 0x33bc [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.1.0.1
Destination Address: 10.1.0.99
[Reassembled IPv4 in frame: 6]
Data (1480 bytes)

Fragments whose ID's are
2d00,2e00, and 2f00 respectively
have Time to live field value of 32

Figure 5: Time to live fields of fragments with ID's 2d00,2e00,2f00 is 32

No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
1	2000-12-27 11:54:10	160000 NetworkK	10:22:1b Broadcast	ARP	64		Who has 10.1.0.99? Tell 10.1.0.1
2	2000-12-27 11:54:10	160000 Runtime	e1:5a:80 NetworkK	10:22:1b ARP	64		10.1.0.99 is at 00:20:78:e1:5a:80
3	2000-12-27 11:54:11	224000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2d00) [Reassembled in #6]
4	2000-12-27 11:54:11	225000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2d00) [Reassembled in #6]
5	2000-12-27 11:54:11	226000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2d00) [Reassembled in #6]
6	2000-12-27 11:54:11	227000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=1536/6, ttl=32 (reply in 18)
7	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3100) [Reassembled in #10]
8	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3100) [Reassembled in #10]
9	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3100) [Reassembled in #10]
10	2000-12-27 11:54:11	228000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=1536/6, ttl=128 (request in 6)
11	2000-12-27 11:54:12	240000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2e00) [Reassembled in #14]
12	2000-12-27 11:54:12	240000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2e00) [Reassembled in #14]
13	2000-12-27 11:54:12	241000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2e00) [Reassembled in #14]
14	2000-12-27 11:54:12	242000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=1792/7, ttl=32 (reply in 18)
15	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3200) [Reassembled in #18]
16	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3200) [Reassembled in #18]
17	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3200) [Reassembled in #18]
18	2000-12-27 11:54:12	242000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=1792/7, ttl=128 (request in 14)
19	2000-12-27 11:54:13	241000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=2f00) [Reassembled in #22]
20	2000-12-27 11:54:13	242000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2f00) [Reassembled in #22]
21	2000-12-27 11:54:13	244000 10.1.0.1	10.1.0.99	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2f00) [Reassembled in #22]
22	2000-12-27 11:54:13	245000 10.1.0.1	10.1.0.99	ICMP	1206		Echo (ping) request id=8x0100, seq=2048/8, ttl=32 (reply in 26)
23	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=0, ID=3300) [Reassembled in #26]
24	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3300) [Reassembled in #26]
25	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	IPv4	1518		Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3300) [Reassembled in #26]
26	2000-12-27 11:54:13	245000 10.1.0.99	10.1.0.1	ICMP	1206		Echo (ping) reply id=8x0100, seq=2048/8, ttl=128 (request in 22)

Total Length: 1500
Identification: 0x3100 (12544)
Flags: 0x20, More fragments
0... = Reserved bit: Not set
0... = Don't fragment: Not set
1... = More fragments: Set
...00000000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0xcfb5 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.1.0.99
Destination Address: 10.1.0.1
[Reassembled IPv4 in frame: 10]
Data (1480 bytes)

Fragments whose ID's are 3100,3200, and 3300 respectively have Time to live field of 128

Figure 6: Time to live fields of fragments with ID's 3100,3200,3300 is 128

3.) If we look at the line number 8 we can see in the packet comments section that “IPv6 packets are encapsulated in IPv4” this is the method of tunnelling and encapsulation where IPv6 datagrams are embedded inside IPv4 datagram to sent to destination address. Also when we look at the Internet protocol version 4 part below the packet capture table we can see that Protocol field is also IPv6.

No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
1	2011-05-30 20:29:16	097200	2002:1806:addr...	2002:f0d0:200...	TCP	106	8192 52004 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1220 WS=4 SACK_PERM=1
2	2011-05-30 20:29:16	294201	2002:f0d0:200...	2002:1806:addr...	TCP	106	5760 80 - 52004 [SYN, ACK] Seq=0 Ack=1 Win=5760 Len=0 MSS=1440 SACK_PERM=1 WS=512
3	2011-05-30 20:29:16	295000	2002:1806:addr...	2002:f0d0:200...	TCP	94	17080 52004 - 80 [ACK] Seq=1 Ack=1 Win=17080 Len=0
4	2011-05-30 20:29:16	296339	2002:1806:addr...	2002:f0d0:200...	HTTP	758	17080 GET /image/ipv6.gif?id=2007997724 HTTP/1.1
5	2011-05-30 20:29:16	506624	2002:f0d0:200...	2002:1806:addr...	TCP	94	7168 80 - 52004 [ACK] Seq=1 Ack=665 Win=7168 Len=0
6	2011-05-30 20:29:16	507834	2002:f0d0:200...	2002:1806:addr...	HTTP	498	7168 HTTP/1.1 200 OK (GIF89a)
7	2011-05-30 20:29:16	704527	2002:1806:addr...	2002:f0d0:200...	TCP	94	16676 52004 - 80 [ACK] Seq=665 Ack=405 Win=16676 Len=0
8	2011-05-30 20:29:19	758768	2002:1806:addr...	2002:f0d0:200...	HTTP	778	16676 GET /image/ipv6.gif?id=1541349170 HTTP/1.1
9	2011-05-30 20:29:19	963078	2002:f0d0:200...	2002:1806:addr...	HTTP	502	8704 HTTP/1.1 200 OK (GIF89a)
10	2011-05-30 20:29:20	167760	2002:1806:addr...	2002:f0d0:200...	TCP	94	16268 52004 - 80 [ACK] Seq=1349 Ack=813 Win=16268 Len=0
11	2011-05-30 20:29:21	702919	fe80::5083:65...	ff02::1:2	DHCPv6	147	Solicit XID: 0xc37c88 CID: 0001000114294f3cd48564a3b133
12	2011-05-30 20:29:22	702904	fe80::5083:65...	ff02::1:2	DHCPv6	147	Solicit XID: 0xc37c88 CID: 0001000114294f3cd48564a3b133
13	2011-05-30 20:29:24	703065	fe80::5083:65...	ff02::1:2	DHCPv6	147	Solicit XID: 0xc37c88 CID: 0001000114294f3cd48564a3b133
14	2011-05-30 20:29:28	703206	fe80::5083:65...	ff02::1:2	DHCPv6	147	Solicit XID: 0xc37c88 CID: 0001000114294f3cd48564a3b133
15	2011-05-30 20:29:34	973212	2002:f0d0:200...	2002:1806:addr...	TCP	94	8704 80 - 52004 [FIN, ACK] Seq=813 Ack=1349 Win=8704 Len=0
16	2011-05-30 20:29:34	973527	2002:1806:addr...	2002:f0d0:200...	TCP	94	16268 52004 - 80 [ACK] Seq=1349 Ack=814 Win=16268 Len=0
17	2011-05-30 20:29:36	703973	fe80::5083:65...	ff02::1:2	DHCPv6	147	Solicit XID: 0xc37c88 CID: 0001000114294f3cd48564a3b133

Packet comments
Notice that these IPv6 packets are encapsulated in IPv4 - the packet is routed based on the IPv4 header through an IPv4 network.
[Expert Info (Comment/Comment): Notice that these IPv6 packets are encapsulated in IPv4 - the packet is routed based on the IPv4 header through an IPv4 network.]
[Notice that these IPv6 packets are encapsulated in IPv4 - the packet is routed based on the IPv4 header through an IPv4 network.]
[Severity level: Comment]
[Group: Comment]
Frame 8: 778 bytes on wire (6224 bits), 778 bytes captured (6224 bits) on interface unknown, id 0
Ethernet II, Src: HewlettP...a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 192.88.99.1
0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 764
Identification: 0x2d40 (11584)
Flags: 0x00
...00000000 = Fragment Offset: 0
Time to Live: 128
Protocol: IPv6 (41)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 24.6.173.220
Destination Address: 192.88.99.1
Internet Protocol Version 6, Src: 2002:1806:addr..., Dst: 2002:f0d0:2001e:1::120
Transmission Control Protocol, Src Port: 52004, Dst Port: 80, Seq: 665, Ack: 405, Len: 684
Hypertext Transfer Protocol

When we look at the get request line we can see a packet comment and protocol information which indicates that IPv6 datagrams are encapsulated inside IPv4 packets before sent to destination

Figure 7: IPv6 packets encapsulated inside IPv4 datagrams

4.)

a.) We can observe two ICMP message types as a result of executing traceroute command from terminal. First one is Type 11 which gives the time exceeded message when a router receives a datagram with TTL of 0 or 1. So by using this TTL value infinite routing loops are prevented. Routers can not forward a datagram that has a TTL of 0 or 1 and packet is dropped. ICMP message of code 0 indicates Time-to-live became equal to 0 during transit not during reassembly. Second is Type 3 ICMP message which indicates that the router cannot find the destination network. Code 3 which says “port unreachable” indicates that transport layer protocol we are attempting to communicate is not available on the arriving side.

b.) As a result of executing traceroute google.com command, intermediate network devices are same in both cases because when we look at the hop IP addresses, in the Wireshark and in the output of traceroute they are same. It is intuitive to get same intermediate device IP addresses because we have captured packets during the same traceroute execution. (Figure 10)

c.) Routers with IP addresses given inside blue rectangle in the screenshot below have been sent 3 packets. Routers with the IP addresses given inside the red rectangle have been sent 1 packet. (Figure 8 and Figure 9)

586	2023-06-08	14:14:58	288758348	192.168.0.1	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
588	2023-06-08	14:14:58	289102705	192.168.0.1	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
589	2023-06-08	14:14:58	289102726	192.168.0.1	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
591	2023-06-08	14:14:58	217327353	172.25.7.17	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
592	2023-06-08	14:14:58	218113868	172.25.7.114	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
593	2023-06-08	14:14:58	218727055	172.25.7.17	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
594	2023-06-08	14:14:58	218727877	172.25.7.17	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
595	2023-06-08	14:14:58	220863597	172.25.7.114	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
596	2023-06-08	14:14:58	221198316	172.25.7.113	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
597	2023-06-08	14:14:58	221596315	172.25.7.114	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
599	2023-06-08	14:14:58	229579486	172.25.7.113	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
600	2023-06-08	14:14:58	230043268	172.25.7.113	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
601	2023-06-08	14:14:58	230094468	195.175.76.165	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
621	2023-06-08	14:14:58	273732066	195.175.76.165	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
623	2023-06-08	14:14:58	274173616	195.175.76.165	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
624	2023-06-08	14:14:58	274184568	81.212.209.173	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
625	2023-06-08	14:14:58	274184599	81.212.209.173	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
626	2023-06-08	14:14:58	274184618	81.212.209.173	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
631	2023-06-08	14:14:58	274229874	81.212.39.28	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
632	2023-06-08	14:14:58	274229897	81.212.39.28	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
633	2023-06-08	14:14:58	274229131	81.212.39.28	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
637	2023-06-08	14:14:58	283354802	195.175.166.32	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
639	2023-06-08	14:14:58	286381725	195.175.166.32	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
640	2023-06-08	14:14:58	286381748	195.175.166.32	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
641	2023-06-08	14:14:58	286384715	81.212.217.121	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
642	2023-06-08	14:14:58	286384753	81.212.217.121	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
648	2023-06-08	14:14:58	293656387	81.212.217.121	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
651	2023-06-08	14:14:58	308808509	212.156.104.152	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
652	2023-06-08	14:14:58	3088081801	212.156.104.152	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
655	2023-06-08	14:14:58	311156104	212.156.104.152	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
660	2023-06-08	14:14:58	323231373	200.95.108.140	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)

Figure 8: Routers with IP addresses given inside blue rectangle have been sent 3 packets

665	2023-06-08 14:14:58,333821273	209.85.168.140	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
667	2023-06-08 14:14:58,334399051	72.14.222.58	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
669	2023-06-08 14:14:58,335308721	74.125.51.44	192.168.0.32	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
670	2023-06-08 14:14:58,343530413	142.251.61.242	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
671	2023-06-08 14:14:58,344754740	142.251.92.65	192.168.0.32	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
672	2023-06-08 14:14:58,345201851	142.251.227.252	192.168.0.32	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
674	2023-06-08 14:14:58,349824901	209.85.254.243	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
684	2023-06-08 14:14:58,365977146	142.251.92.2	192.168.0.32	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
685	2023-06-08 14:14:58,366764923	142.251.92.67	192.168.0.32	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
690	2023-06-08 14:14:58,390165271	142.250.187.174	192.168.0.32	ICMP	70	Destination unreachable (Port unreachable)
693	2023-06-08 14:14:58,401546910	142.251.243.28	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
711	2023-06-08 14:14:58,521040648	142.250.187.174	192.168.0.32	ICMP	70	Destination unreachable (Port unreachable)
712	2023-06-08 14:14:58,521191387	142.251.243.28	192.168.0.32	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
713	2023-06-08 14:14:58,523857302	142.251.242.230	192.168.0.32	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)

Figure 9: Routers with IP address given inside the red rectangle have been sent 1 packet

```

gokay@gokaycomputer:~$ traceroute google.com
traceroute to google.com (142.250.187.174), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  3.315 ms  3.622 ms  3.609 ms
 2  * * *
 3  172.25.7.17 (172.25.7.17)  11.801 ms  13.193 ms  13.187 ms
 4  172.25.7.114 (172.25.7.114)  12.565 ms  15.308 ms  16.035 ms
 5  172.25.7.113 (172.25.7.113)  15.630 ms  24.005 ms  24.449 ms
 6  195.175.76.165.static.turktelekom.com.tr (195.175.76.165)  24.492 ms  12.128 ms  11.630 ms
 7  07-kiziltoprak-t3-3---07-calli-t3-r.statik.turktelekom.com.tr (81.212.209.173)  12.074 ms  12.069 ms  12.064 ms
 8  07-kiziltoprak-sr12e-t2-2---07-kiziltoprak-t3-3.statik.turktelekom.com.tr (81.212.30.28)  12.103 ms  12.098 ms  12.093 ms
 9  06-ulus-sr14s-t2-2---07-kiziltoprak-sr12e-t2-2.statik.turktelekom.com.tr (195.175.166.32)  24.239 ms  24.235 ms  21.203 ms
10  06-ebgp-ulus-sr12e-k---06-ulus-sr14s-t2-2.statik.turktelekom.com.tr (81.212.217.121)  24.227 ms  24.222 ms  19.585 ms
11  307-sof-col-1---06-ebgp-ulus-sr12e-k.statik.turktelekom.com.tr (212.156.104.152)  34.611 ms  34.655 ms  36.944 ms
12  72.14.222.58 (72.14.222.58)  60.181 ms  209.85.168.140 (209.85.168.140)  58.774 ms  74.125.51.44 (74.125.51.44)  61.054 ms
13  * * *
14  142.251.61.242 (142.251.61.242)  57.106 ms  142.251.227.252 (142.251.227.252)  58.770 ms  142.251.92.65 (142.251.92.65)  58.318 ms
15  209.85.254.243 (209.85.254.243)  56.073 ms  142.251.92.67 (142.251.92.67)  57.860 ms  142.251.92.2 (142.251.92.2)  57.053 ms
16  142.251.243.28 (142.251.243.28)  90.306 ms  sof02s46-in-f14.1e100.net (142.250.187.174)  57.040 ms  142.251.243.28 (142.251.243.28)  59.883 ms
gokay@gokaycomputer:~$

```

IP addresses given inside the blue rectangle match with the IP addresses given inside the blue rectangles in Wireshark. Similarly, IP addresses given inside the red rectangle match with the IP addresses given inside the red rectangle in Wireshark

Figure 10: traceroute command output and the hops along with their IP addresses and packets they received

NAT SECTION

1.) NAT protocol stands for Network address translation which allows all devices inside local area network to share just one IP address as far as outer networks are

considered , so all datagrams leaving from local network share same NAT IP address, but they are distinguished by different port numbers. The mapping between datagram source IP address and NAT IP address, is implemented in the form of NAT table. NAT protocol also helps IPv4 address exhaustion because just one IP address is needed from ISP for all devices in local network.

2.) When we look at the lan-packets screenshot below, scenario might be as follows:

host with IP address 10.142.154.239 and destination with IP address 8.8.8.8 are located in the same local area network and host is trying to establish a TCP connection with server whose IP address is 8.8.8.8. When we look at the wan-packets screenshot below, scenario might be as follows: host with IP address 136.102.83.11 and destination with IP address 8.8.8.8 are located in different networks and host is trying to establish a TCP connection with server whose IP address is 8.8.8.8. This scenarios can be related to NAT protocol as follows: Actual IP address of host may be 10.142.154.239 inside it's local area network but let's say as in WAN scenario server with IP address 8.8.8.8 is located outside the LAN and any host when connecting to any server in LAN is using IP address 10.142.154.139, but when server for which host is going to establish connection is outside the LAN, there is a NAT router which translates IP address of host from 10.142.154.239 to 136.102.83.11. Thus when server sends response to host it sees it's NAT IP which is 136.102.83.11 not it's actual local network IP address which is 10.142.154.239. (Figure 11 and Figure 12)

No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
1	2023-06-08 17:32:21,448502	10.142.154.239	8.8.8.8	TCP	54	8192 5000 → 80	[SYN] Seq=0 Win=8192 Len=0
2	2023-06-08 17:32:21,448502	8.8.8.8	10.142.154.239	TCP	54	8192 80 → 5000	[SYN, ACK] Seq=0 Ack=0 Win=8192 Len=0
3	2023-06-08 17:32:21,452502	10.142.154.239	8.8.8.8	TCP	54	8192 [TCP Window Update] 5001 → 443	[ACK] Seq=1 Ack=1 Win=8192 Len=0
4	2023-06-08 17:32:21,454502	8.8.8.8	10.142.154.239	TCP	54	8192 [TCP Window Update] 443 → 5001	[PSH, ACK] Seq=1 Ack=1 Win=8192 Len=0
5	2023-06-08 17:32:21,466502	10.142.154.239	8.8.8.8	UDP	42	3000 → 53	Len=0

<p>Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)</p> <p>Ethernet II, Src: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa), Dst: Broadcast (ff:ff:ff:ff:ff:ff)</p> <p>Internet Protocol Version 4, Src: 10.142.154.239, Dst: 8.8.8.8</p> <p>0100 ... = Version: 4</p> <p>... 0101 = Header Length: 20 bytes (5)</p> <p>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</p> <p>Total Length: 40</p> <p>Identification: 0x0001 (1)</p> <p>Flags: 0x00</p> <p>... 0 0000 0000 0000 = Fragment Offset: 0</p> <p>Time to Live: 64</p> <p>Protocol: TCP (6)</p> <p>Header Checksum: 0xc542 [validation disabled]</p> <p>[Header checksum status: Unverified]</p> <p>Source Address: 10.142.154.239</p> <p>Destination Address: 8.8.8.8</p>	<p><i>Host with IP address 10.142.154.239 and server with IP address 8.8.8.8 are located inside the same local area network scenario</i></p>
--	--

Figure 11: Scenario in which host with IP address 10.142.154.239 and destination with IP 8.8.8.8 in same LAN

No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
1	2023-06-08 17:32:21,448502	136.102.83.11	8.8.8.8	TCP	54	8192 5000 → 80	[SYN] Seq=0 Win=8192 Len=0
2	2023-06-08 17:32:21,448502	8.8.8.8	136.102.83.11	TCP	54	8192 80 → 5000	[SYN, ACK] Seq=0 Ack=0 Win=8192 Len=0
3	2023-06-08 17:32:21,452502	136.102.83.11	8.8.8.8	TCP	54	8192 [TCP Window Update] 5001 → 443	[ACK] Seq=1 Ack=1 Win=8192 Len=0
4	2023-06-08 17:32:21,454502	8.8.8.8	136.102.83.11	TCP	54	8192 [TCP Window Update] 443 → 5001	[PSH, ACK] Seq=1 Ack=1 Win=8192 Len=0
5	2023-06-08 17:32:21,466502	136.102.83.11	8.8.8.8	UDP	42	3000 → 53	Len=0

▶ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
 ▶ Ethernet II, Src: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Internet Protocol Version 4, Src: 136.102.83.11, Dst: 8.8.8.8
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 Total Length: 40
 Identification: 0x0001 (1)
 ▶ Flags: 0x00
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 64
 Protocol: TCP (6)
 Header Checksum: 0x8f4e [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 136.102.83.11
 Destination Address: 8.8.8.8

*Host with IP address 136.102.83.11
 and server with IP address 8.8.8.8
 are located in different local are networks
 scenario*

Figure 12: Scenario in which host with IP address 136.102.83.11 and destination with IP 8.8.8.8 in different LANs

DHCP SECTION

1.) `ipconfig /release` command will inform the DHCP server that we don't want to use previously assigned IP address any larger and we release it. After releasing the previously assigned IP address we can request new IP address from DHCP server with `ipconfig /renew` command. Note: As I am using **UBUNTU** distribution of Linux, I have used **dhclient** program for releasing and obtaining new IP address with DHCP which is equivalent to `ipconfig` program on Windows.

2.) When we look at the packet capture on Wireshark 1 DHCP packet was captured for the release command, 4 DHCP packets were captured for first renew command. 2 DHCP packets were captured for second renew command.

3.) If we look at the Wireshark packet capture when I made two new requests respectively to DHCP server both newly assigned IP address in both situation were same as we can see in the below screenshots. In both situations requested IP address was 192.138.0.1, but this may not always be the case, IP address can differ from previous one.

4.) When we look at the packets as a result of first renew command, we can see

four different DHCP message types which are DISCOVER, OFFER, REQUEST, and ACK respectively. DHCP DISCOVER message is sent by client to locate DHCP server when client attempts to connect network for the first time. DHCP OFFER message is sent by server in response to DHCP discover message of client, and it carries configuration information along with the new IP address. DHCP REQUEST message is sent by server. Finally DHCP ACK message is sent by server to acknowledge DHCP REQUEST message sent from DHCP client. After receiving DHCP ACK message client obtains configuration parameters including new IP address.

5.) For first dhclient command (which is equivalent to piconfig /renew on Windows) common option fields to all packets are as follows: subnet mask which defines the subnet IP of computer that belongs to particular LAN, IP address of DHCP server, and DHCP message type option which indicates the sending purpose of DHCP packet that I have explained detaily in the previous question (4) it can be of type DISCOVER, OFFER, REQUEST, ACK, etc.. to indicate what client wants from DHCP server and DHCP servers response.

dhcp							
Interface phy0.mon		Channel 1 · 2.412 GHz		20 MHz			
No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
48	2023-06-09 00:27:36	348738880 192.168.0.32	192.168.0.1	DHCP	342		DHCP Release - Transaction ID 0x3360402a
55	2023-06-09 00:27:45	998970668 0.0.0.0	255.255.255.255	DHCP	342		DHCP Discover - Transaction ID 0x7a0be129
56	2023-06-09 00:27:46	004771527 192.168.0.1	192.168.0.32	DHCP	342		DHCP Offer - Transaction ID 0x7a0be129
57	2023-06-09 00:27:46	004949305 0.0.0.0	255.255.255.255	DHCP	342		DHCP Request - Transaction ID 0x7a0be129
60	2023-06-09 00:27:47	052505494 192.168.0.1	192.168.0.32	DHCP	342		DHCP ACK - Transaction ID 0x7a0be129
417	2023-06-09 00:27:55	747096965 0.0.0.0	255.255.255.255	DHCP	342		DHCP Request - Transaction ID 0x16149207
421	2023-06-09 00:27:56	789598365 192.168.0.1	192.168.0.32	DHCP	342		DHCP ACK - Transaction ID 0x16149207

▶ Frame 55: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlo1, id 0 ▶ Ethernet II, Src: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa), Dst: Broadcast (ff:ff:ff:ff:ff:ff) ▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255 ▶ User Datagram Protocol, Src Port: 68, Dst Port: 67 ▶ Dynamic Host Configuration Protocol (Discover)							
Message type: Boot Request (1) Hardware type: Ethernet (0x01) Hardware address length: 6 Hops: 0 Transaction ID: 0x7a0be129 Seconds elapsed: 0 ▶ Bootp flags: 0x0000 (Unicast) 0... .. = Broadcast flag: Unicast .000 0000 0000 0000 = Reserved flags: 0x0000 Client IP address: 0.0.0.0 Your (client) IP address: 0.0.0.0 Next server IP address: 0.0.0.0 Relay agent IP address: 0.0.0.0 Client MAC address: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa) Client hardware address padding: 00000000000000000000 Server host name not given Boot file name not given Magic cookie: DHCP							
▶ Option: (53) DHCP Message Type (Discover) Length: 1 DHCP: Discover (1) ▶ Option: (50) Requested IP Address (192.168.0.32) Length: 4 Requested IP Address: 192.168.0.32 ▶ Option: (12) Host Name Length: 13 Host Name: gokaycomputer							

DHCP message type discover

Figure 13: DHCP Discover message

dhcpc							
Interface		Channel					
phy0.mon		1 · 2.412 GHz		20 MHz			
No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
48	2023-06-09 00:27:36,348738880	192.168.0.32	192.168.0.1	DHCP	342		DHCP Release - Transaction ID 0x3360402a
55	2023-06-09 00:27:45,998970668	0.0.0.0	255.255.255.255	DHCP	342		DHCP Discover - Transaction ID 0x7a0be129
56	2023-06-09 00:27:46,004771527	192.168.0.1	192.168.0.32	DHCP	342		DHCP Offer - Transaction ID 0x7a0be129
57	2023-06-09 00:27:46,004949305	0.0.0.0	255.255.255.255	DHCP	342		DHCP Request - Transaction ID 0x7a0be129
60	2023-06-09 00:27:47,052505494	192.168.0.1	192.168.0.32	DHCP	342		DHCP ACK - Transaction ID 0x7a0be129
417	2023-06-09 00:27:55,747096965	0.0.0.0	255.255.255.255	DHCP	342		DHCP Request - Transaction ID 0x16149207
421	2023-06-09 00:27:56,789598365	192.168.0.1	192.168.0.32	DHCP	342		DHCP ACK - Transaction ID 0x16149207
▶ Frame 56: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlo1, id 0 ▶ Ethernet II, Src: Broadcom_de:ad:a5 (00:10:18:de:ad:a5), Dst: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa) ▶ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.32 ▶ User Datagram Protocol, Src Port: 67, Dst Port: 68 ▶ Dynamic Host Configuration Protocol (Offer) Message type: Boot Reply (2) Hardware type: Ethernet (0x01) Hardware address length: 6 Hops: 0 Transaction ID: 0x7a0be129 Seconds elapsed: 0 Bootp flags: 0x0000 (Unicast) 0... .. = Broadcast flag: Unicast .000 0000 0000 0000 = Reserved flags: 0x0000 Client IP address: 0.0.0.0 Your (client) IP address: 192.168.0.32 Next server IP address: 192.168.0.1 Relay agent IP address: 0.0.0.0 Client MAC address: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa) Client hardware address padding: 00000000000000000000 Server host name not given Boot file name not given Magic cookie: DHCP							
▶ Option: (53) DHCP Message Type (Offer) Length: 1 DHCP: Offer (2) ▶ Option: (1) Subnet Mask (255.255.255.0) Length: 4 Subnet Mask: 255.255.255.0 ▶ Option: (2) Time Offset Length: 4 Time Offset: (0s) 0 seconds							

DHCP offer message type

Figure 14: DHCP Offer message type

dhcpc							
Interface		Channel					
phy0.mon		1 · 2.412 GHz		20 MHz			
No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
48	2023-06-09 00:27:36,348738880	192.168.0.32	192.168.0.1	DHCP	342		DHCP Release - Transaction ID 0x3360402a
55	2023-06-09 00:27:45,998970668	0.0.0.0	255.255.255.255	DHCP	342		DHCP Discover - Transaction ID 0x7a0be129
56	2023-06-09 00:27:46,004771527	192.168.0.1	192.168.0.32	DHCP	342		DHCP Offer - Transaction ID 0x7a0be129
57	2023-06-09 00:27:46,004949305	0.0.0.0	255.255.255.255	DHCP	342		DHCP Request - Transaction ID 0x7a0be129
60	2023-06-09 00:27:47,052505494	192.168.0.1	192.168.0.32	DHCP	342		DHCP ACK - Transaction ID 0x7a0be129
417	2023-06-09 00:27:55,747096965	0.0.0.0	255.255.255.255	DHCP	342		DHCP Request - Transaction ID 0x16149207
421	2023-06-09 00:27:56,789598365	192.168.0.1	192.168.0.32	DHCP	342		DHCP ACK - Transaction ID 0x16149207
▶ Frame 57: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlo1, id 0 ▶ Ethernet II, Src: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa), Dst: Broadcast (ff:ff:ff:ff:ff:ff) ▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255 ▶ User Datagram Protocol, Src Port: 68, Dst Port: 67 ▶ Dynamic Host Configuration Protocol (Request) Message type: Boot Request (1) Hardware type: Ethernet (0x01) Hardware address length: 6 Hops: 0 Transaction ID: 0x7a0be129 Seconds elapsed: 0 Bootp flags: 0x0000 (Unicast) 0... .. = Broadcast flag: Unicast .000 0000 0000 0000 = Reserved flags: 0x0000 Client IP address: 0.0.0.0 Your (client) IP address: 0.0.0.0 Next server IP address: 0.0.0.0 Relay agent IP address: 0.0.0.0 Client MAC address: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa) Client hardware address padding: 00000000000000000000 Server host name not given Boot file name not given Magic cookie: DHCP							
▶ Option: (53) DHCP Message Type (Request) Length: 1 DHCP: Request (3) ▶ Option: (54) DHCP Server Identifier (192.168.0.1) Length: 4 DHCP Server Identifier: 192.168.0.1 ▶ Option: (50) Requested IP Address (192.168.0.32) Length: 4 Requested IP Address: 192.168.0.32							

DHCP request message type

Figure 15: DHCP Request message type

```

gokay@gokaycomputer:~$ sudo dhclient -v -r wlo1
Killed old client process
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlo1/3c:58:c2:a5:ff:aa
Sending on LPF/wlo1/3c:58:c2:a5:ff:aa
Sending on Socket/fallback
DHCPRELEASE of 192.168.0.32 on wlo1 to 192.168.0.1 port 67 (xid=0x629a7f54)
gokay@gokaycomputer:~$ sudo dhclient -v wlo1
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlo1/3c:58:c2:a5:ff:aa
Sending on LPF/wlo1/3c:58:c2:a5:ff:aa
Sending on Socket/fallback
DHCPDISCOVER on wlo1 to 255.255.255.255 port 67 interval 3 (xid=0x7a0be129)
DHCPOFFER of 192.168.0.32 from 192.168.0.1
DHCPREQUEST for 192.168.0.32 on wlo1 to 255.255.255.255 port 67 (xid=0x29e10b7a)
DHCPACK of 192.168.0.32 from 192.168.0.1 (xid=0x7a0be129)
bound to 192.168.0.32 -- renewal in 243054 seconds.
gokay@gokaycomputer:~$ sudo dhclient -v wlo1
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlo1/3c:58:c2:a5:ff:aa
Sending on LPF/wlo1/3c:58:c2:a5:ff:aa
Sending on Socket/fallback
DHCPREQUEST for 192.168.0.32 on wlo1 to 255.255.255.255 port 67 (xid=0x7921416)
DHCPACK of 192.168.0.32 from 192.168.0.1 (xid=0x16149207)
RTNETLINK answers: File exists
bound to 192.168.0.32 -- renewal in 235556 seconds.
gokay@gokaycomputer:~$

```

Figure 16: dhclient command equivalent to ipconfig in Windows for releasing IP address and obtaining new IP address

dhcp

Interface phy0.mon Channel 1 · 2.412 GHz 20 MHz

No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
48	2023-06-09 00:27:36,348738880	192.168.0.32	192.168.0.1	DHCP	342		DHCP Release - Transaction ID 0x3360402a
55	2023-06-09 00:27:45,998970668	0.0.0.0	255.255.255.255	DHCP	342		DHCP Discover - Transaction ID 0x7a0be129
56	2023-06-09 00:27:46,004771527	192.168.0.1	192.168.0.32	DHCP	342		DHCP Offer - Transaction ID 0x7a0be129
57	2023-06-09 00:27:46,004949305	0.0.0.0	255.255.255.255	DHCP	342		DHCP Request - Transaction ID 0x7a0be129
60	2023-06-09 00:27:47,052505494	192.168.0.1	192.168.0.32	DHCP	342		DHCP ACK - Transaction ID 0x7a0be129
417	2023-06-09 00:27:55,747096965	0.0.0.0	255.255.255.255	DHCP	342		DHCP Request - Transaction ID 0x16149207
421	2023-06-09 00:27:56,789598365	192.168.0.1	192.168.0.32	DHCP	342		DHCP ACK - Transaction ID 0x16149207

Frame 60: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlo1, id 0

Ethernet II, Src: Broadcom_de:ad:05 (00:10:18:de:ad:05), Dst: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.32

User Datagram Protocol, Src Port: 67, Dst Port: 68

Dynamic Host Configuration Protocol (ACK)

Message type: Boot Reply (2)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x7a0be129

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

0... .. = Broadcast flag: Unicast

.000 0000 0000 0000 = Reserved flags: 0x0000

Client IP address: 0.0.0.0

Your (client) IP address: 192.168.0.32

Next server IP address: 192.168.0.1

Relay agent IP address: 0.0.0.0

Client MAC address: IntelCor_a5:ff:aa (3c:58:c2:a5:ff:aa)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option: (53) DHCP Message Type (ACK)

Length: 1

DHCP: ACK (5)

Option: (1) Subnet Mask (255.255.255.0)

Length: 4

Subnet Mask: 255.255.255.0

Option: (2) Time Offset

Length: 4

Time Offset: (0s) 0 seconds

Figure 17: DHCP ACK message for second dhclient command (same as ipconfig /renew)