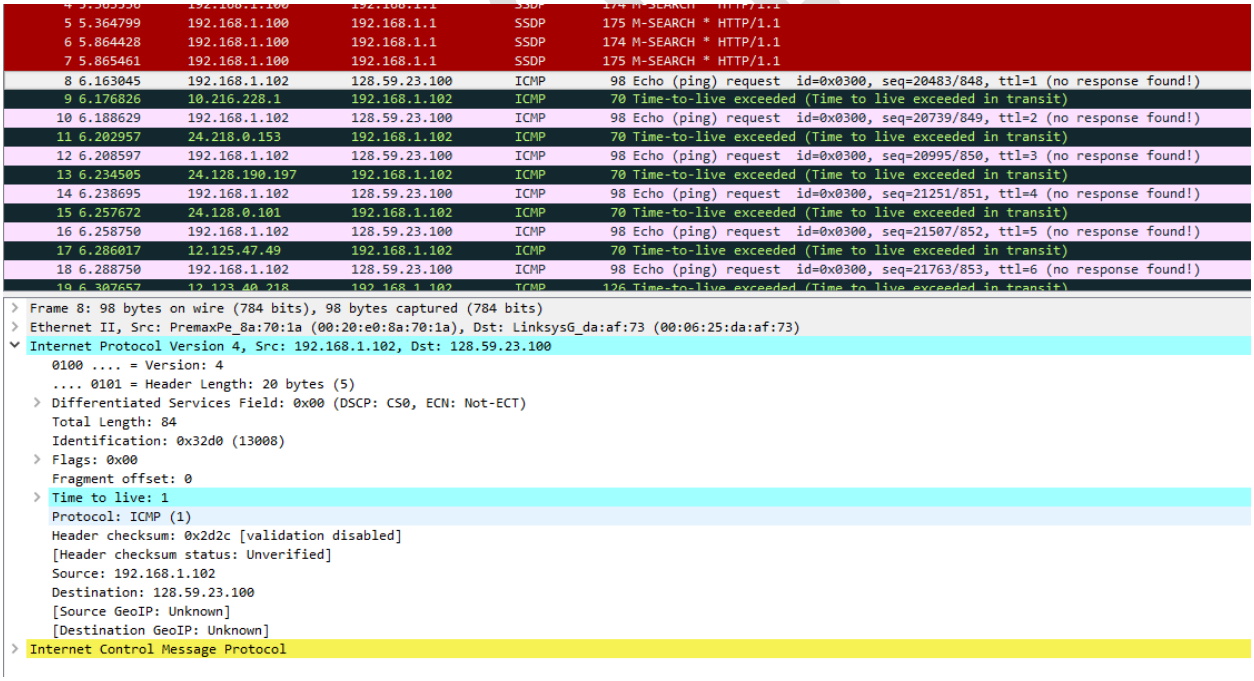
LAB 5: Analysis of IP packets through Wireshark and Introduction to static routing through packet tracer.

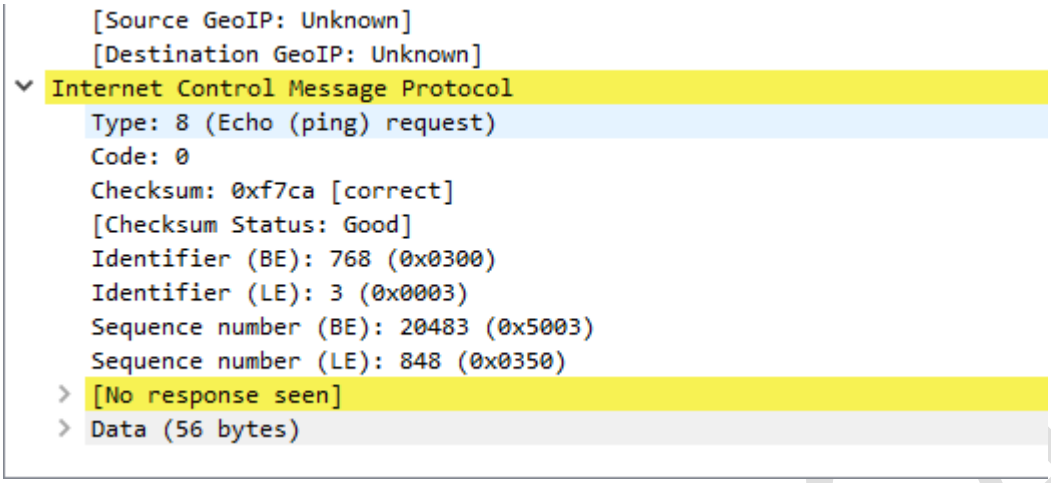
Name : Shubham Patel

ID: 202101464

Exercise:

1.2:





Answering below questions from the above screenshots

1. What is the IP address of your computer?

IP Address: 192.168.1.102.

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

Protocol: ICMP(1).

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.

The IP header length= 20 bytes.

The total length of the packet = 84 bytes

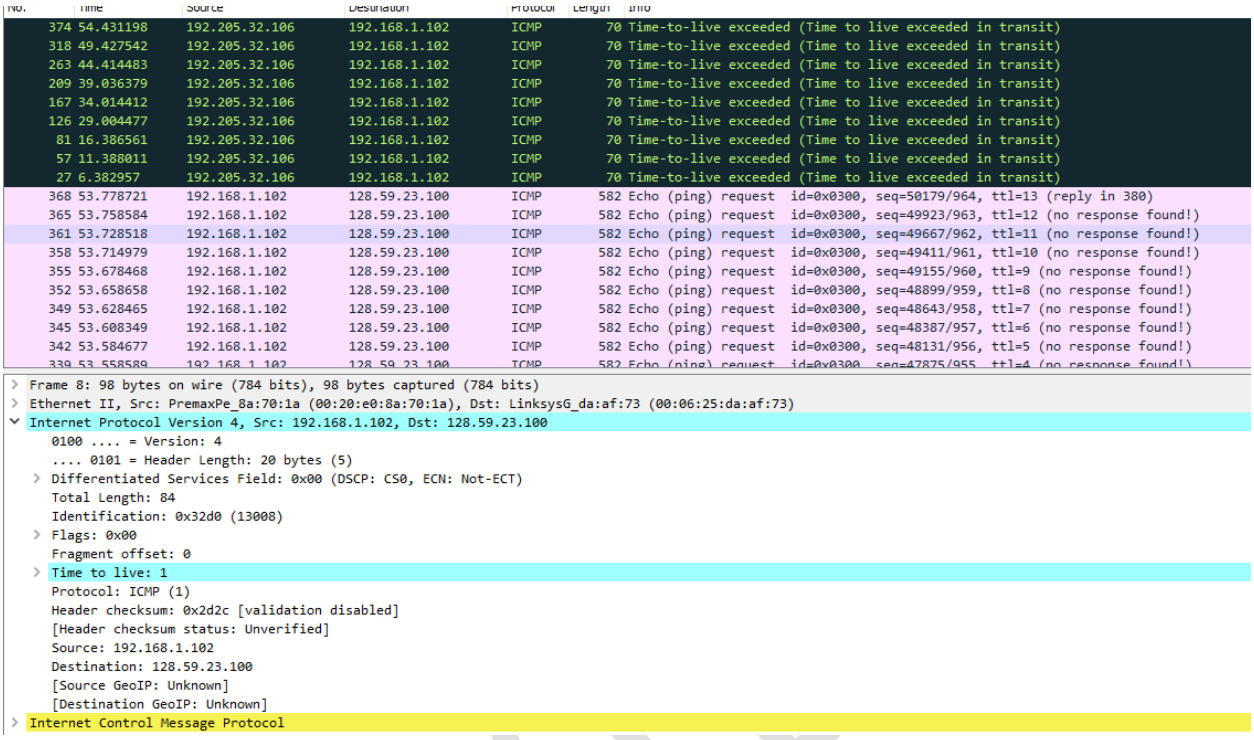
Payload -> 84 - 20 = 64 bytes.

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

Fragment Offset: 0

Therefore there is no fragmentation.

1.3:



No.	Time	Source	Destination	Protocol	Length	Info
374	54.431198	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
318	49.427542	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
263	44.414483	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
209	39.036379	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
167	34.014412	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
126	29.004477	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
81	16.386561	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
57	11.388011	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
27	6.382957	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
368	53.778721	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=50179/964, ttl=13 (reply in 380)
365	53.758584	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (no response found!)
361	53.728518	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49667/962, ttl=11 (no response found!)
358	53.714979	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49411/961, ttl=10 (no response found!)
355	53.678468	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49155/960, ttl=9 (no response found!)
352	53.658658	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=48899/959, ttl=8 (no response found!)
349	53.628465	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=48643/958, ttl=7 (no response found!)
345	53.608349	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=48387/957, ttl=6 (no response found!)
342	53.584677	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=48131/956, ttl=5 (no response found!)
339	53.558589	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=47875/955, ttl=4 (no response found!)

```
> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
> Internet Control Message Protocol
```

1.4:

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

3 fields change from one datagram to another: Identification , Time to live and Header Checksum.

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

The fields that stay and must remain constant are:

- Source IP: Source is the same computer.

- Destination IP: Destination remains same.

-Protocol: ICMP for all.

- Differentiated Services Field: All the packets are ICMP(they use the same types of services)

- Version: All the packets areIPv4

- Header Length: As we are using ICMP.

The fields that change are:

1. Identification:There should be a unique packet id.

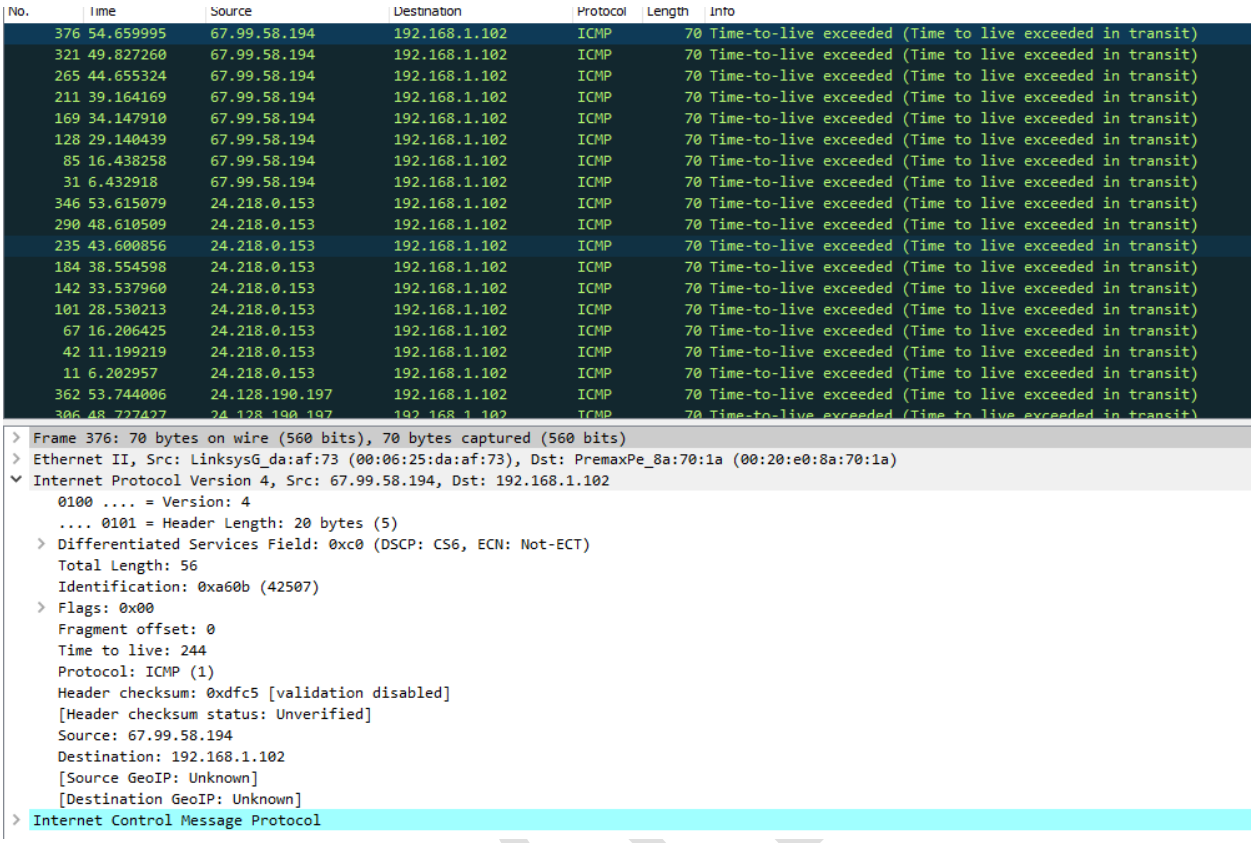
2. Time to live: It decreases as it is in descending order.

3. Header checksum: Checksum changes as headers change.

3. Describe the pattern you see in the values in the identification field of the IP datagram.

The values change by 1 in the identification field.

4. Next (with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to your computer by the nearest (first hop) router.



No.	Time	Source	Destination	Protocol	Length	Info
376	54.659995	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
321	49.827260	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
265	44.655324	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
211	39.164169	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
169	34.147910	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
128	29.140439	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	16.438258	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
31	6.432918	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
346	53.615079	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
290	48.610509	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
235	43.600856	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
184	38.554598	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
142	33.537960	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
101	28.530213	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
67	16.206425	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
42	11.199219	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
362	53.744006	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

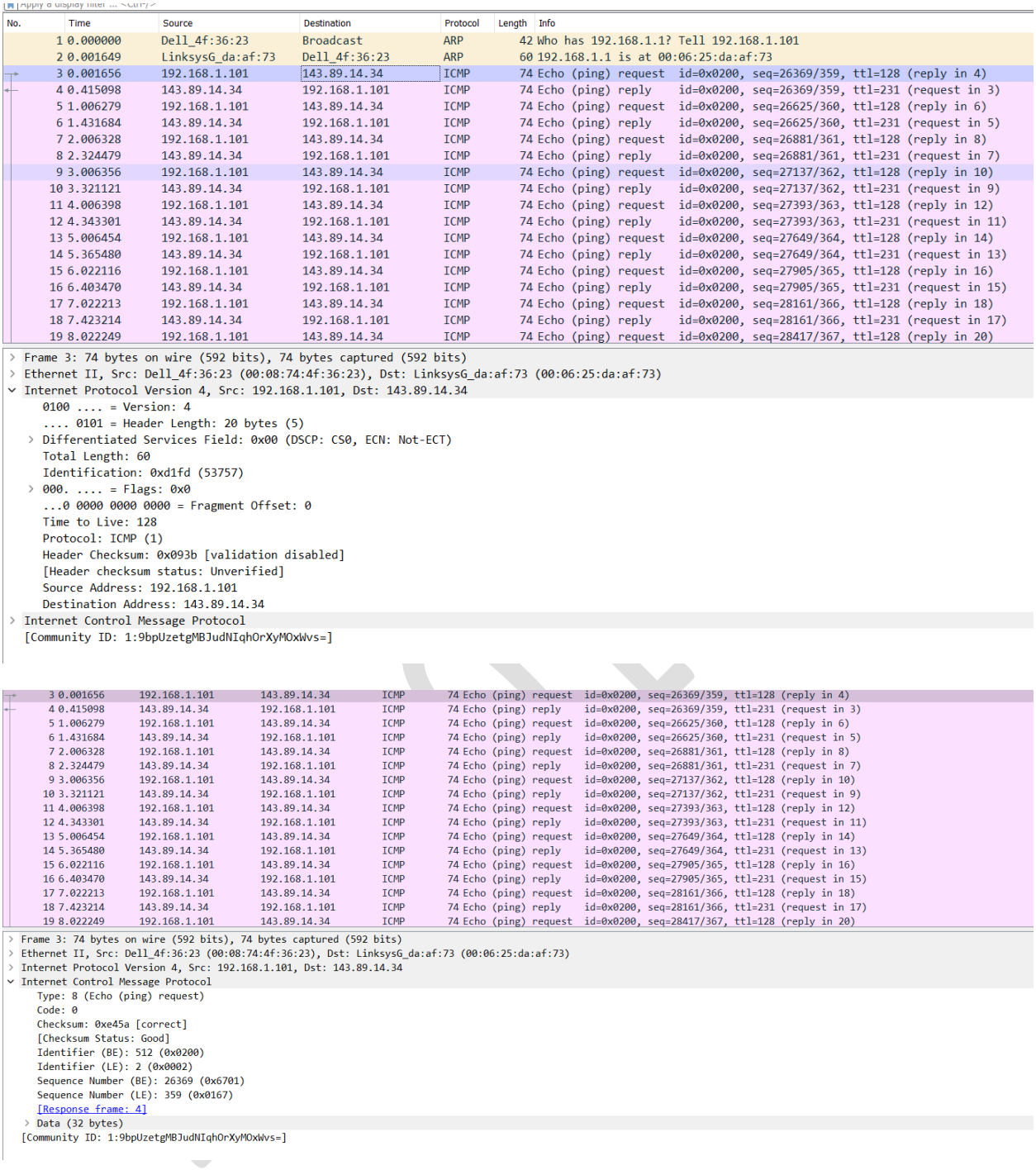
5. What is the value in the Identification field and the TTL field?

TTL= 244 and Identification = 0xa60b (42507)

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

Yes, for all ICMP TTL-exceeded answers from the closest router, the TTL and identification values stay unaltered. Since the first hop router is constant, the TTL does not vary. Since these IP datagrams are parts of a larger IP datagram, they all have the same identification value.

1.5:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Dell_4f:36:23	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.101
2	0.001649	LinksysG_da:af:73	Dell_4f:36:23	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001656	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26369/359, ttl=128 (reply in 4)
4	0.415098	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26369/359, ttl=231 (request in 3)
5	1.006279	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26625/360, ttl=128 (reply in 6)
6	1.431684	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26625/360, ttl=231 (request in 5)
7	2.006328	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26881/361, ttl=128 (reply in 8)
8	2.324479	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26881/361, ttl=231 (request in 7)
9	3.006356	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27137/362, ttl=128 (reply in 10)
10	3.321121	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27137/362, ttl=231 (request in 9)
11	4.006398	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27393/363, ttl=128 (reply in 12)
12	4.343301	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27393/363, ttl=231 (request in 11)
13	5.006454	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27649/364, ttl=128 (reply in 14)
14	5.365480	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27649/364, ttl=231 (request in 13)
15	6.022116	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27905/365, ttl=128 (reply in 16)
16	6.403470	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27905/365, ttl=231 (request in 15)
17	7.022213	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=28161/366, ttl=128 (reply in 18)
18	7.423214	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=28161/366, ttl=231 (request in 17)
19	8.022249	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=28417/367, ttl=128 (reply in 20)

```
> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.101, Dst: 143.89.14.34
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xd1fd (53757)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x093b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.101
    Destination Address: 143.89.14.34
> Internet Control Message Protocol
  [Community ID: 1:9bpUzetgMBJudNIqhOrXyMOxWvs=]
```

3	0.001656	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26369/359, ttl=128 (reply in 4)
4	0.415098	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26369/359, ttl=231 (request in 3)
5	1.006279	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26625/360, ttl=128 (reply in 6)
6	1.431684	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26625/360, ttl=231 (request in 5)
7	2.006328	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26881/361, ttl=128 (reply in 8)
8	2.324479	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26881/361, ttl=231 (request in 7)
9	3.006356	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27137/362, ttl=128 (reply in 10)
10	3.321121	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27137/362, ttl=231 (request in 9)
11	4.006398	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27393/363, ttl=128 (reply in 12)
12	4.343301	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27393/363, ttl=231 (request in 11)
13	5.006454	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27649/364, ttl=128 (reply in 14)
14	5.365480	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27649/364, ttl=231 (request in 13)
15	6.022116	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27905/365, ttl=128 (reply in 16)
16	6.403470	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27905/365, ttl=231 (request in 15)
17	7.022213	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=28161/366, ttl=128 (reply in 18)
18	7.423214	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=28161/366, ttl=231 (request in 17)
19	8.022249	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=28417/367, ttl=128 (reply in 20)

```
> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 143.89.14.34
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe45a [correct]
    [Checksum Status: Good]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence Number (BE): 26369 (0x6701)
    Sequence Number (LE): 359 (0x0167)
    [Response frame: 4]
  > Data (32 bytes)
  [Community ID: 1:9bpUzetgMBJudNIqhOrXyMOxWvs=]
```

1. What is the IP address of your host? What is the IP address of the destination host?

IP address of host = 192.168.1.101

IP address of destination host = 143.89.14.34.

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

The ICMP packet lacks source and destination port information since it was not intended to be used for application layer processes to exchange network-layer data. Its purpose was to facilitate information exchange at the network layer between hosts and routers. Each ICMP packet have type and code attached to it. They help to identify the message that is being received. No port numbers are required to route an ICMP message to an application layer process because the network software interprets all ICMP signals.

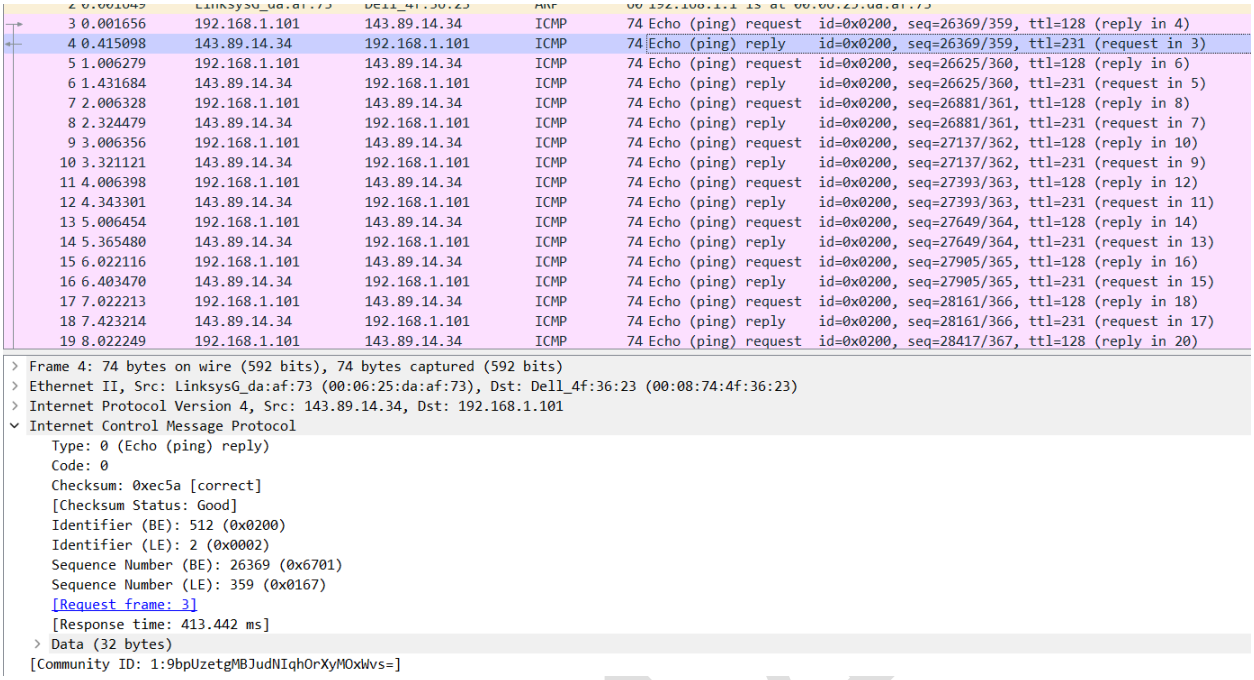
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

ICMP type = 8 and code number =0.

Some other fields in this ICMP packet are:

Checksum, identifier, sequence number, and data fields, each of 2 bytes

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?



3	0.001656	192.168.1.101	143.89.14.34	ICMP	74 Echo (ping) request id=0x0200, seq=26369/359, ttl=128 (reply in 4)
4	0.415098	143.89.14.34	192.168.1.101	ICMP	74 Echo (ping) reply id=0x0200, seq=26369/359, ttl=231 (request in 3)
5	1.006279	192.168.1.101	143.89.14.34	ICMP	74 Echo (ping) request id=0x0200, seq=26625/360, ttl=128 (reply in 6)
6	1.431684	143.89.14.34	192.168.1.101	ICMP	74 Echo (ping) reply id=0x0200, seq=26625/360, ttl=231 (request in 5)
7	2.006328	192.168.1.101	143.89.14.34	ICMP	74 Echo (ping) request id=0x0200, seq=26881/361, ttl=128 (reply in 8)
8	2.324479	143.89.14.34	192.168.1.101	ICMP	74 Echo (ping) reply id=0x0200, seq=26881/361, ttl=231 (request in 7)
9	3.006356	192.168.1.101	143.89.14.34	ICMP	74 Echo (ping) request id=0x0200, seq=27137/362, ttl=128 (reply in 10)
10	3.321121	143.89.14.34	192.168.1.101	ICMP	74 Echo (ping) reply id=0x0200, seq=27137/362, ttl=231 (request in 9)
11	4.006398	192.168.1.101	143.89.14.34	ICMP	74 Echo (ping) request id=0x0200, seq=27393/363, ttl=128 (reply in 12)
12	4.343301	143.89.14.34	192.168.1.101	ICMP	74 Echo (ping) reply id=0x0200, seq=27393/363, ttl=231 (request in 11)
13	5.006454	192.168.1.101	143.89.14.34	ICMP	74 Echo (ping) request id=0x0200, seq=27649/364, ttl=128 (reply in 14)
14	5.365480	143.89.14.34	192.168.1.101	ICMP	74 Echo (ping) reply id=0x0200, seq=27649/364, ttl=231 (request in 13)
15	6.022116	192.168.1.101	143.89.14.34	ICMP	74 Echo (ping) request id=0x0200, seq=27905/365, ttl=128 (reply in 16)
16	6.403470	143.89.14.34	192.168.1.101	ICMP	74 Echo (ping) reply id=0x0200, seq=27905/365, ttl=231 (request in 15)
17	7.022213	192.168.1.101	143.89.14.34	ICMP	74 Echo (ping) request id=0x0200, seq=28161/366, ttl=128 (reply in 18)
18	7.423214	143.89.14.34	192.168.1.101	ICMP	74 Echo (ping) reply id=0x0200, seq=28161/366, ttl=231 (request in 17)
19	8.022249	192.168.1.101	143.89.14.34	ICMP	74 Echo (ping) request id=0x0200, seq=28417/367, ttl=128 (reply in 20)

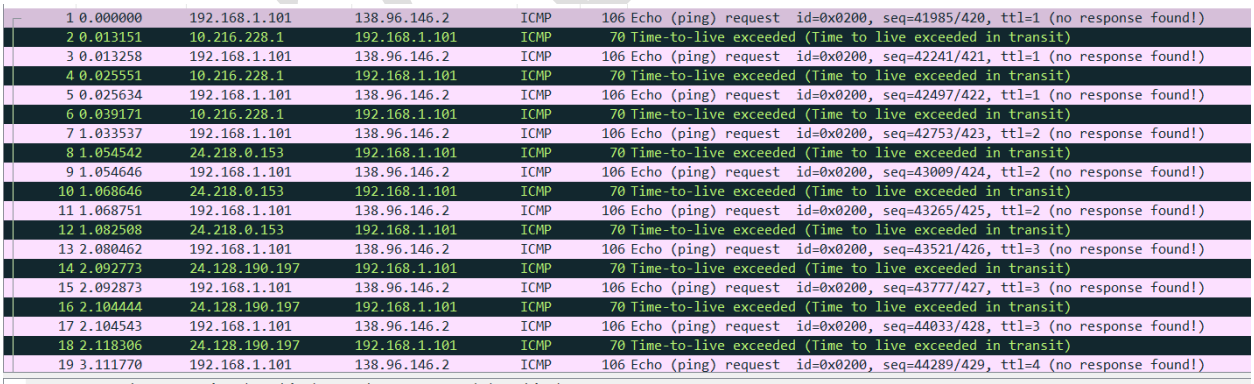
```
> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 143.89.14.34, Dst: 192.168.1.101
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xec5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence Number (BE): 26369 (0x6701)
    Sequence Number (LE): 359 (0x0167)
    [Request frame: 3]
    [Response time: 413.442 ms]
  > Data (32 bytes)
[Community ID: 1:9bpUzetgMBJudNIqhOrXyMOxWvs=]
```

ICMP type =0 and code number = 0.

Some other fields in this ICMP packet are:

Checksum, identifier, sequence number, and data fields, each of 2 bytes

1.6



1	0.000000	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=41985/420, ttl=1 (no response found!)
2	0.013151	10.216.228.1	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
3	0.013258	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=42241/421, ttl=1 (no response found!)
4	0.025551	10.216.228.1	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
5	0.025634	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=42497/422, ttl=1 (no response found!)
6	0.039171	10.216.228.1	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
7	1.033537	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=42753/423, ttl=2 (no response found!)
8	1.054542	24.218.0.153	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
9	1.054646	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=43009/424, ttl=2 (no response found!)
10	1.068646	24.218.0.153	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
11	1.068751	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=43265/425, ttl=2 (no response found!)
12	1.082508	24.218.0.153	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
13	2.080462	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=43521/426, ttl=3 (no response found!)
14	2.092773	24.128.190.197	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
15	2.092873	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=43777/427, ttl=3 (no response found!)
16	2.104444	24.128.190.197	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
17	2.104543	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=44033/428, ttl=3 (no response found!)
18	2.118306	24.128.190.197	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
19	3.111770	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=44289/429, ttl=4 (no response found!)

```
> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x51fe [correct]
    [Checksum Status: Good]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence Number (BE): 41985 (0xa401)
    Sequence Number (LE): 420 (0x01a4)
  > [No response seen]
  > Data (64 bytes)
[Community ID: 1:LH/pH1/Nmga6EyPvMWm4trAiKHY=]
```

1. What is the IP address of your host? What is the IP address of the target destination host?

The IP address of our host= 192.168.1.101

IP address of the target = 138.96.146.2.

2. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

No. The IP Protocol number would change to 0x11 if ICMP instead transmitted UDP packets.

3. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

The ICMP echo packet is not different and has the same fields.

```
> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xd2d5 (53973)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x085c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.101
    Destination Address: 138.96.146.2
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x51fe [correct]
    [Checksum Status: Good]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence Number (BE): 41985 (0xa401)
    Sequence Number (LE): 420 (0x01a4)
  > [No response seen]
  > Data (64 bytes)
```

4. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

Yes it is more than the echo packet as it contains both the IP header and the first 8 bytes of the original ICMP packet.

5. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

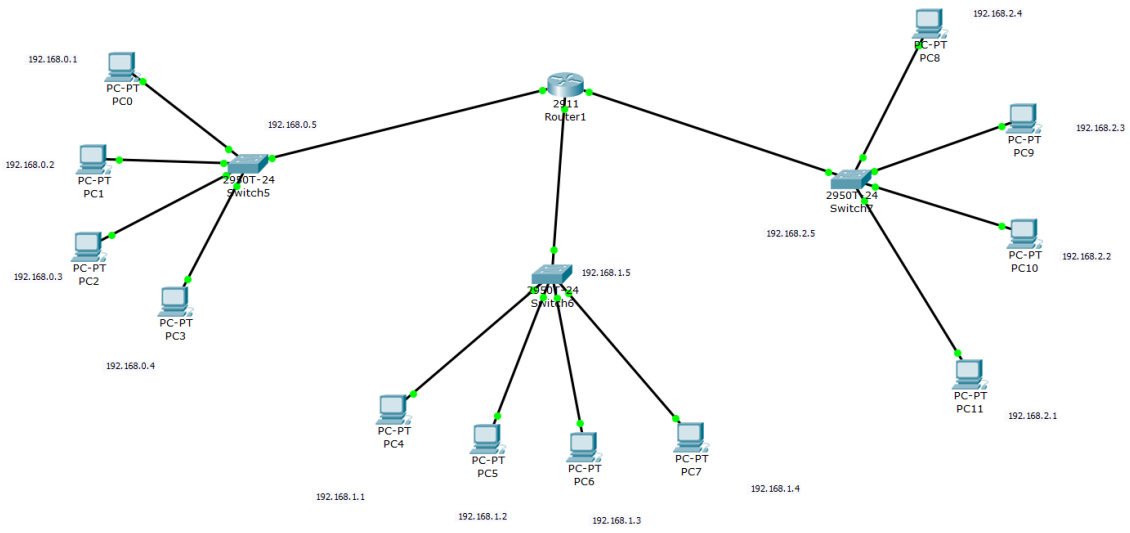
Type field = 0 (echo reply) and not 11 (TTL expired)

It also does not contain additional IP header information.

ICMP packets reach the destination before the TTL happens.

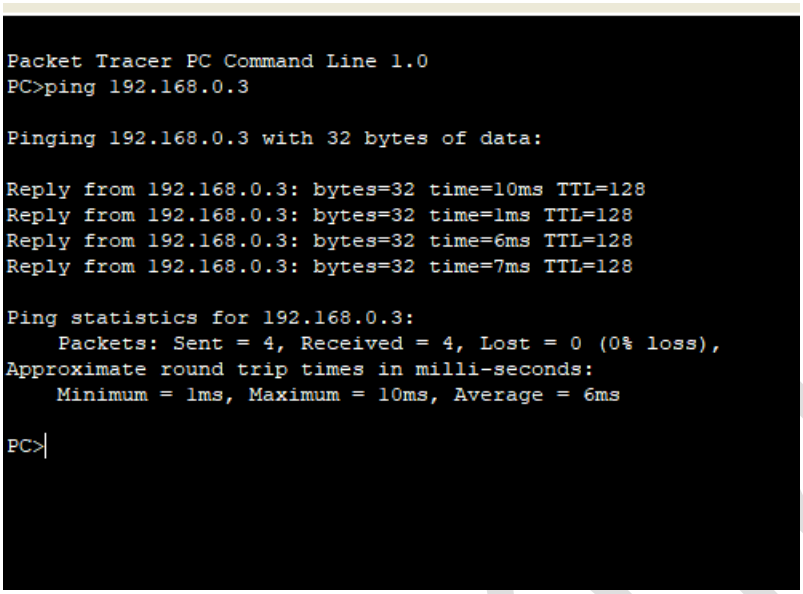
2.1

Design a topology which have three networks. Each network has 4 PCs and all three network are connected to each other. The suggested IP ranges are 192.168.0.1 to 192.168.2.4. All IP addresses of all network should be from the given range. Run the experiment and ping from each network to every other Network. Take a snapshot and submit. Also submit the snapshot of topology with IP assigned to each PC.

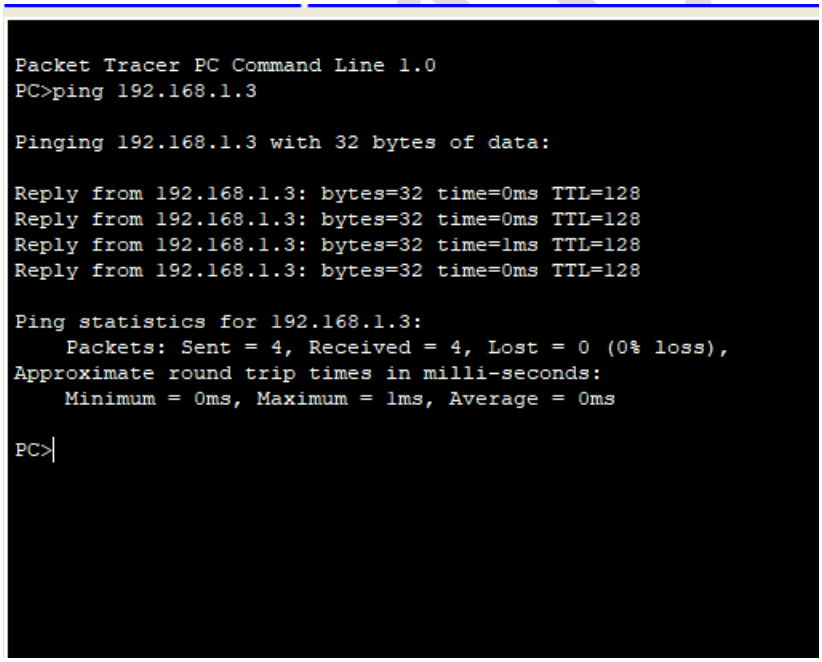


Here are the 3 cases of Ping from all the three different PC connected across another PC through the router.

Case 1



Case 2



Case 3

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=0ms TTL=128
Reply from 192.168.2.4: bytes=32 time=0ms TTL=128
Reply from 192.168.2.4: bytes=32 time=0ms TTL=128
Reply from 192.168.2.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```