

HO CHI MINH UNIVERSITY OF TECHNOLOGY
Faculty of Computer Science and Engineering



Computer Networks

Report for lab 5

Lecturer: Nguyễn Mạnh Thìn
Student name: Đặng Trần Khánh-1852037



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

Answer: The IP address of my host is 192.168.1.101. The IP address of the destination host is 143.89.14.34.

No.	Time	Source	Destination	Protocol	Length	Info
3	01:28:40.830479	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26369/359, ttl=128 (reply in 4)
4	01:28:41.243921	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26369/359, ttl=231 (request in 3)
5	01:28:41.835102	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26625/360, ttl=128 (reply in 6)
6	01:28:42.260507	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26625/360, ttl=231 (request in 5)
7	01:28:42.835151	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26881/361, ttl=128 (reply in 8)
8	01:28:43.153302	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26881/361, ttl=231 (request in 7)
9	01:28:43.835179	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27137/362, ttl=128 (reply in 10)
10	01:28:44.149944	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27137/362, ttl=231 (request in 9)

> 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

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0xd1fd (53757)

Flags: 0x0000

Fragment offset: 0

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0x093b [validation disabled]

[Header checksum status: Unverified]

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

Answer: 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. Instead it uses the type and code message to specify the message received. The network decodes all ICMP messages so port numbers are unnecessary.

No.	Time	Source	Destination	Protocol	Length	Info
3	01:28:40.830479	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26369/359, ttl=128 (reply in 4)
4	01:28:41.243921	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26369/359, ttl=231 (request in 3)
5	01:28:41.835102	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26625/360, ttl=128 (reply in 6)
6	01:28:42.260507	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26625/360, ttl=231 (request in 5)
7	01:28:42.835151	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26881/361, ttl=128 (reply in 8)
8	01:28:43.153302	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26881/361, ttl=231 (request in 7)
9	01:28:43.835179	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27137/362, ttl=128 (reply in 10)
10	01:28:44.149944	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27137/362, ttl=231 (request in 9)

> 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

> 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)

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?

Answer: The ICMP type is 8 and the code number is 0. Other fields in this packet are checksum, identifier, sequence number and data field. The checksum, identifier and sequence number are 2 bytes each. The data field is 32 bytes

No.	Time	Source	Destination	Protocol	Length	Info
3	01:28:40.830479	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26369/359, ttl=128 (reply in 4)
4	01:28:41.243921	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26369/359, ttl=231 (request in 3)
5	01:28:41.835102	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26625/360, ttl=128 (reply in 6)
6	01:28:42.260507	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26625/360, ttl=231 (request in 5)
7	01:28:42.835151	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26881/361, ttl=128 (reply in 8)
8	01:28:43.153302	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26881/361, ttl=231 (request in 7)
9	01:28:43.835179	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27137/362, ttl=128 (reply in 10)
10	01:28:44.149944	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27137/362, ttl=231 (request in 9)

> 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
> 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)

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?

Answer: The ICMP type is 0 and the code number is 0. Other fields in this packet are checksum, identifier, sequence number and data field. The checksum, identifier and sequence number are 2 bytes each. The data field is 32 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
3	01:28:40.830479	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26369/359, ttl=128 (reply in 4)
4	01:28:41.243921	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26369/359, ttl=231 (request in 3)
5	01:28:41.835102	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26625/360, ttl=128 (reply in 6)
6	01:28:42.260507	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26625/360, ttl=231 (request in 5)
7	01:28:42.835151	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26881/361, ttl=128 (reply in 8)
8	01:28:43.153302	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26881/361, ttl=231 (request in 7)
9	01:28:43.835179	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27137/362, ttl=128 (reply in 10)
10	01:28:44.149944	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27137/362, ttl=231 (request in 9)

> 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
> 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)
Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
[Length: 32]

0000	00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00	..t06#..%..s..E..
0010	00 3c b3 63 40 00 e7 01 80 d4 8f 59 0e 22 c0 a8	..<.c@... ..Y."..
0020	01 65 00 00 ec 5a 02 00 67 01 61 62 63 64 65 66	..e...Z...g..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	..ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	..wabcdefg hi

5/ What is the IP address of your host? What is the IP address of the target destination host?

Answer: The IP address of my host is 192.168.1.101. The IP address of the destination host is 138.96.146.2.

No.	Time	Source	Destination	Protocol	Length	Info
1	01:47:39.264781	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=41985/420, ttl=1 (no r
2	01:47:39.277932	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3	01:47:39.278039	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=42241/421, ttl=1 (no r
4	01:47:39.290332	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5	01:47:39.290415	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=42497/422, ttl=1 (no r
6	01:47:39.303952	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7	01:47:40.298318	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=42753/423, ttl=2 (no r
8	01:47:40.319323	24.218.0.153	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
9	01:47:40.319427	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=43009/424, ttl=2 (no r
10	01:47:40.333427	24.218.0.153	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
11	01:47:40.333532	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=43265/425, ttl=2 (no r
12	01:47:40.347289	24.218.0.153	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
13	01:47:41.345243	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=43521/426, ttl=3 (no r
14	01:47:41.357554	24.128.190.197	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> 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
> Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x51fe [correct]
[Checksum Status: Good]
Identifier (BE): 512 (0x0200)

6/ 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?

Answer: It would actually be different if ICMP sent UDP packets. Instead of 01 it would be switched to 0X11.

7/ 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?

Answer: The echo packets have the same ones as the ping query.

No.	Time	Source	Destination	Protocol	Length	Info
1	01:47:39.264781	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=41985/420, ttl=1 (no response found!)
2	01:47:39.277932	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3	01:47:39.278039	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=42241/421, ttl=1 (no response found!)
4	01:47:39.290332	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5	01:47:39.290415	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=42497/422, ttl=1 (no response found!)
6	01:47:39.303952	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7	01:47:40.298318	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=42753/423, ttl=2 (no response found!)
8	01:47:40.319323	24.218.0.153	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
9	01:47:40.319427	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=43009/424, ttl=2 (no response found!)
10	01:47:40.333427	24.218.0.153	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
11	01:47:40.333532	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=43265/425, ttl=2 (no response found!)
12	01:47:40.347289	24.218.0.153	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
13	01:47:41.345243	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=43521/426, ttl=3 (no response found!)
14	01:47:41.357554	24.128.190.197	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

>	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: Linksys_G_d:af:73 (00:06:25:da:af:73)
>	Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
▼	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)

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

Answer: The ICMP error packet is not the same as the ping query packets. It has the IP header and the first 8 bytes of the original ICMP packet.



9/ *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?*

ICMP packet sent by the host:

6 | Page

ICMP error packet:

96 01:47:56.271288 193.51.181.137	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
97 01:47:57.158527 192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=54273/468, ttl=17 (reply in 98)
98 01:47:57.271983 138.96.146.2	192.168.1.101	ICMP	106 Echo (ping) reply id=0x0200, seq=54273/468, ttl=238 (request in 97)
99 01:47:57.272161 192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=54529/469, ttl=17 (reply in 100)
100 01:47:57.386526 138.96.146.2	192.168.1.101	ICMP	106 Echo (ping) reply id=0x0200, seq=54529/469, ttl=238 (request in 99)
101 01:47:57.386657 192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=54785/470, ttl=17 (reply in 102)
102 01:47:57.499377 138.96.146.2	192.168.1.101	ICMP	106 Echo (ping) reply id=0x0200, seq=54785/470, ttl=238 (request in 101)

> Frame 96: 70 bytes on wire (560 bits), 70 bytes captured (560 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: 193.51.181.137, Dst: 192.168.1.101
> Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0x2c16 [correct]
[Checksum Status: Good]
Unused: 00000000
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
> Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x22fe [unverified] [in ICMP error packet]
[Checksum Status: Unverified]
Identifier (BE): 512 (0x0200)
Identifier (LE): 2 (0x0002)

10/ Within the tracer measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

Answer: There is a link between steps 9 and 10 that has a significantly longer delay. The location of the link is from New York City to Pastourelle, France.

```

C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>tracert www.inria.fr

Tracing route to www.inria.fr [138.96.146.2]
over a maximum of 30 hops:

 1  13 ms  12 ms  13 ms  10.216.228.1
 2  21 ms  14 ms  13 ms  24.218.0.153
 3  12 ms  11 ms  13 ms  bar01-p4-0.wsfdhe1.ma.attbb.net [24.128.190.197]
 4  16 ms  16 ms  15 ms  bar02-p6-0.ndhmhe1.ma.attbb.net [24.128.0.101]
 5  15 ms  15 ms  15 ms  12.125.47.49
 6  17 ms  17 ms  17 ms  12.123.40.218
 7  22 ms  23 ms  22 ms  tbr2-cll.n54ny.ip.att.net [12.122.10.22]
 8  23 ms  23 ms  23 ms  ggr2-p3120.n54ny.ip.att.net [12.123.3.109]
 9  26 ms  21 ms  25 ms  att-gw.nyc.opentransit.net [192.205.32.138]
10 98 ms  98 ms  96 ms  P4-0.PASCR1.Pastourelle.opentransit.net [193.251.241.133]
11 97 ms  98 ms  98 ms  P9-0.AUUCR1.Aubervilliers.opentransit.net [193.251.243.29]
12 98 ms  98 ms  108 ms  P6-0.BAGCR1.Bagnolet.opentransit.net [193.251.241.93]
13 104 ms  106 ms  103 ms  193.51.185.30
14 114 ms  114 ms  117 ms  grenoble-pos1-0.cssi.renater.fr [193.51.179.238]
15 114 ms  115 ms  114 ms  nice-pos2-0.cssi.renater.fr [193.51.180.34]
16 129 ms  114 ms  118 ms  inria-nice.cssi.renater.fr [193.51.181.137]
17 113 ms  114 ms  112 ms  www.inria.fr [138.96.146.2]

Trace complete.
C:\WINDOWS\SYSTEM32>

```