

Computer Networks

LAB 6

Author: Tran Dinh Dang Khoa
2211649

November 16, 2024

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

No.	Time	Source	Destination	Protocol	Length	Info
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!)
20	3.127841	24.128.0.101	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
21	3.127945	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=44545/430, ttl=4 (no response found!)
22	3.144138	24.128.0.101	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
23	3.144406	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=44801/431, ttl=4 (no response found!)
24	3.159699	24.128.0.101	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
25	4.158711	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0200, seq=45057/432, ttl=5 (no response found!)

IP address of my host: 192.168.1.101. IP address of the destination host: 138.96.146.2

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

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

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?

→	97	17.893746	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request
←	98	18.007202	138.96.146.2	192.168.1.101	ICMP	106	Echo (ping) reply
	99	18.007380	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request
	100	18.121745	138.96.146.2	192.168.1.101	ICMP	106	Echo (ping) reply
	101	18.121876	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request
	102	18.234596	138.96.146.2	192.168.1.101	ICMP	106	Echo (ping) reply

>	Frame 97: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)	00
>	Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysGroup_da:af:73 (00:06:00:00:00:00)	00
>	Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2	00
>	Internet Control Message Protocol	00
	Type: 8 (Echo (ping) request)	00
	Code: 0	00
	Checksum: 0x21fe [correct]	00
	[Checksum Status: Good]	00
	Identifier (BE): 512 (0x0200)	00
	Identifier (LE): 2 (0x0002)	00
	Sequence Number (BE): 54273 (0xd401)	00
	Sequence Number (LE): 468 (0x01d4)	00
	[Response frame: 98]	
>	Data (64 bytes)	

The ICMP type is 8, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

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?

 - The ICMP type is 0, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

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

 - IP address of my host: 192.168.1.101. IP address of the destination host: 138.96.146.2

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?

 - No. If ICMP sent UDP packets instead, the IP protocol number should be 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?

```

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 0.023551 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!)

> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysGroup_da:af:73 (00:06:00:00:00:00)
> 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)
  
```

The ICMP echo packet has the same fields as the ping query packets.

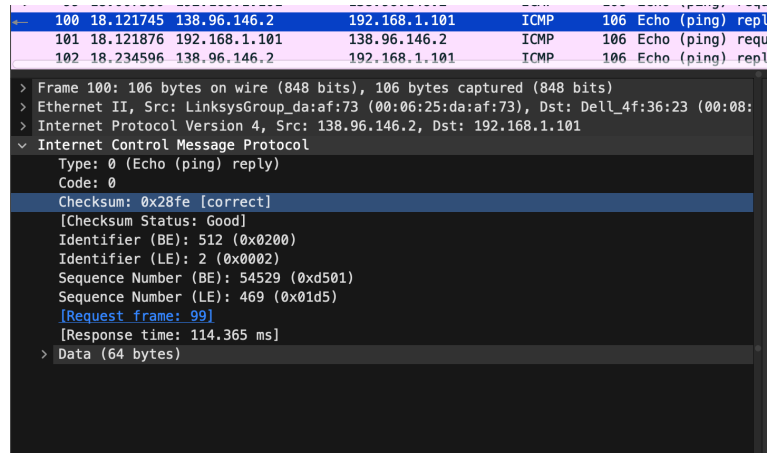
8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

```

> Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: LinksysGroup_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: 10.216.228.1, 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: 0x51fe [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]
  Identifier (BE): 512 (0x0200)
  Identifier (LE): 2 (0x0002)
  Sequence Number (BE): 41985 (0xa401)
  Sequence Number (LE): 420 (0x01a4)
  
```

The ICMP error packet is not the same as the ping query packets. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.

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?



The screenshot shows a Wireshark packet capture with three ICMP Echo (ping) reply packets at the bottom. The packet list shows:

- 100: 18.121745 138.96.146.2 → 192.168.1.101 ICMP 106 Echo (ping) repl
- 101: 18.121876 192.168.1.101 → 138.96.146.2 ICMP 106 Echo (ping) requ
- 102: 18.234596 138.96.146.2 → 192.168.1.101 ICMP 106 Echo (ping) repl

The packet details for packet 100 are expanded, showing:

- Frame 100: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
- Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:00:04:5e:36:23)
- Internet Protocol Version 4, Src: 138.96.146.2, Dst: 192.168.1.101
- Internet Control Message Protocol
 - Type: 0 (Echo (ping) reply)
 - Code: 0
 - Checksum: 0x28fe [correct] (Checksum Status: Good)
 - Identifier (BE): 512 (0x0200)
 - Identifier (LE): 2 (0x0002)
 - Sequence Number (BE): 54529 (0xd501)
 - Sequence Number (LE): 469 (0x01d5)
 - Request frame: 99
 - Response time: 114.365 ms
- Data (64 bytes)

The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL expired.

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?
- In the tracer measurements to google.com, there is indeed one link whose delay is significantly longer than the others. The hop from router6.ispnet.com to edge1.lon.uk.google.com shows a jump in delay from 24ms on previous hops to 179ms. This substantial increase suggests a long-distance link, likely an intercontinental connection.
 - Based on the router names, it appears that router6.ispnet.com could be located in a region near the trace's origin, potentially in a local data center, while edge1.lon.uk.google.com suggests it is a router based in London, United Kingdom. The significant delay likely arises from the physical distance and the network complexity associated with crossing international boundaries or a major internet exchange.