

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



MẠNG MÁY TÍNH THỰC HÀNH - CO3094

Báo cáo:

Lab 5

Giảng viên hướng dẫn: Vũ Thành Tài

Sinh viên: Lê Đức Cường

Thành phố Hồ Chí Minh, tháng 3 năm 2025



1 Question 1

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

ANS:

```
Microsoft Windows [Version 10.0.22631.5039]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping -n 10 www.google.com

Pinging www.google.com [142.251.12.99] with 32 bytes of data:
Reply from 142.251.12.99: bytes=32 time=49ms TTL=57
Reply from 142.251.12.99: bytes=32 time=43ms TTL=57
Reply from 142.251.12.99: bytes=32 time=46ms TTL=57
Reply from 142.251.12.99: bytes=32 time=45ms TTL=57
Reply from 142.251.12.99: bytes=32 time=45ms TTL=57
Reply from 142.251.12.99: bytes=32 time=44ms TTL=57
Reply from 142.251.12.99: bytes=32 time=41ms TTL=57
Reply from 142.251.12.99: bytes=32 time=44ms TTL=57
Reply from 142.251.12.99: bytes=32 time=42ms TTL=57
Reply from 142.251.12.99: bytes=32 time=45ms TTL=57

Ping statistics for 142.251.12.99:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 41ms, Maximum = 49ms, Average = 44ms

C:\Users\Admin>
```

No.	Time	Source	Destination	Protocol	Length	Info
1174	18.183594	192.168.31.87	142.251.12.99	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 1177)
1177	18.233275	142.251.12.99	192.168.31.87	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=57 (request in 1174)
1184	19.206591	192.168.31.87	142.251.12.99	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 1186)
1186	19.250065	142.251.12.99	192.168.31.87	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=57 (request in 1184)
1193	20.227486	192.168.31.87	142.251.12.99	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 1194)
1194	20.273696	142.251.12.99	192.168.31.87	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=57 (request in 1193)
1209	21.256500	192.168.31.87	142.251.12.99	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 1210)
1210	21.301529	142.251.12.99	192.168.31.87	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=57 (request in 1209)
1240	22.276839	192.168.31.87	142.251.12.99	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 1241)
1241	22.322194	142.251.12.99	192.168.31.87	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=57 (request in 1240)
1242	23.303537	192.168.31.87	142.251.12.99	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 1243)
1243	23.348318	142.251.12.99	192.168.31.87	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=57 (request in 1242)
1419	24.328343	192.168.31.87	142.251.12.99	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 1420)
1420	24.369541	142.251.12.99	192.168.31.87	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=57 (request in 1419)

Frame 1174: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{68272D8F-0FB6-459B-ABCF-000000000000} cc 08 00 4d 5a 00 00 00 00
Ethernet II, Src: Intel_93:30:aa (54:00:14:93:30:aa), Dst: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41:1f) 0010 00 3c a5 9d 0020 0c e3 08 00 0030 67 68 69 6a 0040 77 61 62 63

Internet Protocol Version 4, Src: 192.168.31.87, Dst: 142.251.12.99
Internet Control Message Protocol

IP address of the host: 192.168.31.87

IP address of the destination host: 142.251.12.99

2 Question 2

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

ANS:

ICMP operates at the Network Layer in the OSI model, not the Transport Layer like TCP or UDP. Therefore, it does not use source and destination port numbers because:

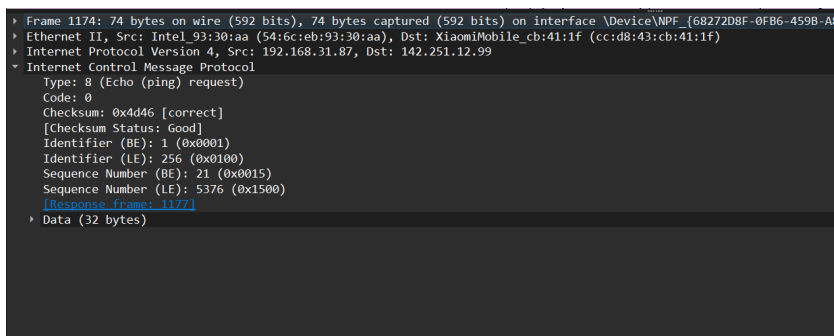
- ICMP is designed for network diagnostics and error reporting, not for data transmission between applications.
- Transport layer protocols like TCP/UDP require port numbers to identify specific applications on the receiving device, whereas ICMP communicates between network devices (routers, hosts).
- ICMP works directly over IP and uses Type and Code fields to identify the message type instead of port numbers.

Thus, ICMP does not require source and destination port numbers like transport layer protocols.

3 Question 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?

ANS:



```

> Frame 1174: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{68272DBF-0FB6-459B-A8...}
> Ethernet II, Src: Intel_93:30:aa (54:6c:eb:93:30:aa), Dst: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41:1f)
> Internet Protocol Version 4, Src: 192.168.31.87, Dst: 142.251.12.99
> Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d46 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 21 (0x0015)
  Sequence Number (LE): 5376 (0x1500)
  [Response from: 1177]
> Data (32 bytes)
```

ICMP Type: 8 (Echo Request)

ICMP Code: 0

Each field contains 2 bytes.

4 Question 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?

ANS:

1209	21.256500	192.168.31.87	142.251.12.99	ICMP	74 Echo (ping) request	id=0x0001, seq=24/6144, ttl=128 (reply in 1210)
1210	21.301529	142.251.12.99	192.168.31.87	ICMP	74 Echo (ping) reply	id=0x0001, seq=24/6144, ttl=57 (request in 1209)
1240	22.276839	192.168.31.87	142.251.12.99	ICMP	74 Echo (ping) request	id=0x0001, seq=25/6400, ttl=128 (reply in 1241)
1241	22.322194	142.251.12.99	192.168.31.87	ICMP	74 Echo (ping) reply	id=0x0001, seq=25/6400, ttl=57 (request in 1240)
1242	23.303537	192.168.31.87	142.251.12.99	ICMP	74 Echo (ping) request	id=0x0001, seq=26/6656, ttl=128 (reply in 1243)
1243	23.348318	142.251.12.99	192.168.31.87	ICMP	74 Echo (ping) reply	id=0x0001, seq=26/6656, ttl=57 (request in 1242)
1419	24.328343	192.168.31.87	142.251.12.99	ICMP	74 Echo (ping) request	id=0x0001, seq=27/6912, ttl=128 (reply in 1420)
1420	24.369541	142.251.12.99	192.168.31.87	ICMP	74 Echo (ping) reply	id=0x0001, seq=27/6912, ttl=57 (request in 1419)
1421	25.355069	192.168.31.87	142.251.12.99	ICMP	74 Echo (ping) request	id=0x0001, seq=28/7168, ttl=128 (reply in 1422)
1422	25.399582	142.251.12.99	192.168.31.87	ICMP	74 Echo (ping) reply	id=0x0001, seq=28/7168, ttl=57 (request in 1421)
1425	26.382485	192.168.31.87	142.251.12.99	ICMP	74 Echo (ping) request	id=0x0001, seq=29/7424, ttl=128 (reply in 1426)
1426	26.424789	142.251.12.99	192.168.31.87	ICMP	74 Echo (ping) reply	id=0x0001, seq=29/7424, ttl=57 (request in 1425)
1433	27.403417	192.168.31.87	142.251.12.99	ICMP	74 Echo (ping) request	id=0x0001, seq=30/7680, ttl=128 (reply in 1434)
1434	27.449180	142.251.12.99	192.168.31.87	ICMP	74 Echo (ping) reply	id=0x0001, seq=30/7680, ttl=57 (request in 1433)

0100 = Version: 4
.... 0101	= Header Length: 20 bytes (5)
Differentially Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)	
Total Length: 60	
Identification: 0x0000 (0)	
0000 = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0	
Time to Live: 57	
Protocol: ICMP (1)	
Header Checksum: 0xb644 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 142.251.12.99	
Destination Address: 192.168.31.87	
[Stream index: 38]	
Internet Control Message Protocol	
Type: 0 (Echo (ping) reply)	
Code: 0	
Checksum: 0x5543 [correct]	
[Checksum Status: Good]	
Identifier (BE): 1 (0x0001)	
Identifier (LE): 256 (0x0100)	
Sequence Number (BE): 34 (0x001A)	
Sequence Number (LE): 10 (0x000A)	

Other fields in the ICMP Echo Request packet:

- Checksum – Used for error checking.
- Identifier (ID) – Helps match requests with replies.
- Sequence Number – Tracks the order of Echo Requests and Replies.
- Payload – Contains additional data (often includes a timestamp for round-trip time calculation).

5 Question 5

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

ANS:

```
Command Prompt
2 * * * Request timed out.
3 6 ms 9 ms 16 ms adsl.hnpt.com.vn [203.210.144.132]
4 12 ms 3 ms 7 ms 172.17.100.73
5 15 ms 8 ms 8 ms static.vnpt.vn [113.171.146.149]
6 29 ms 29 ms 28 ms static.vnpt.vn [113.171.49.193]
7 31 ms 32 ms 31 ms static.vnpt.vn [113.171.143.22]
8 29 ms 34 ms 28 ms static.vnpt.vn [113.171.31.33]
9 50 ms 48 ms 67 ms 72.14.219.148
10 56 ms 60 ms 70 ms 142.251.67.15
11 53 ms 56 ms 51 ms 74.125.245.2
12 56 ms 61 ms 64 ms 216.239.63.216
13 55 ms 56 ms 70 ms 142.251.231.3
14 53 ms 50 ms 55 ms 142.251.231.198
15 62 ms 59 ms 55 ms 142.251.52.239
16 * * * Request timed out.
17 * * * Request timed out.
18 * * * Request timed out.
19 * * * Request timed out.
20 * * * Request timed out.
21 * * * Request timed out.
22 * * * Request timed out.
23 * * * Request timed out.
24 * * * Request timed out.
25 * * * Request timed out.
26 * * * Request timed out.
27 133 ms 83 ms 77 ms sd-in-f147.1e100.net [142.251.10.147]

Trace complete.
C:\Users\Admin>
```

```
Internet Protocol Version 4, Src: 192.168.31.87, Dst: 142.251.10.147
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xc60e (50702)
  000. .... = Flags: 0x0
    ..0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.31.87
    Destination Address: 142.251.10.147
    [Stream index: 23]
  Internet Control Message Protocol
```

IP address of the host: 192.168.31.87

IP address of the destination host: 142.251.10.147

6 Question 6

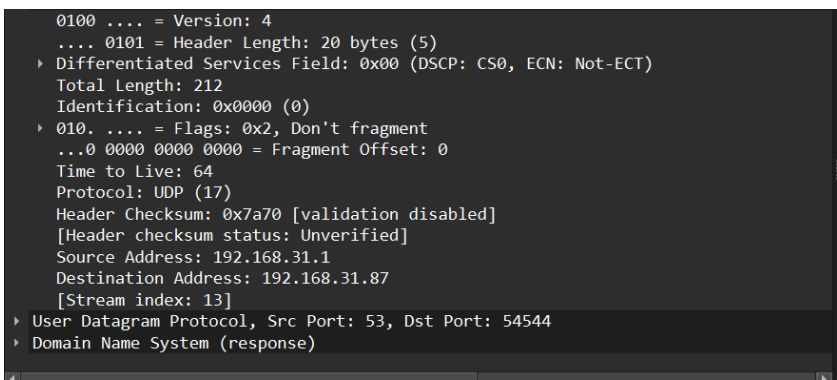
If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

ANS:

No, the IP protocol number would not be 01 if ICMP sent UDP packets instead.

- IP protocol number 01 is specifically assigned to ICMP.
- UDP packets use IP protocol number 17 (0x11 in hexadecimal)

So, if ICMP were replaced by UDP for probe packets (as seen in Unix/Linux traceroute), the IP protocol number would be 17 instead of 01.



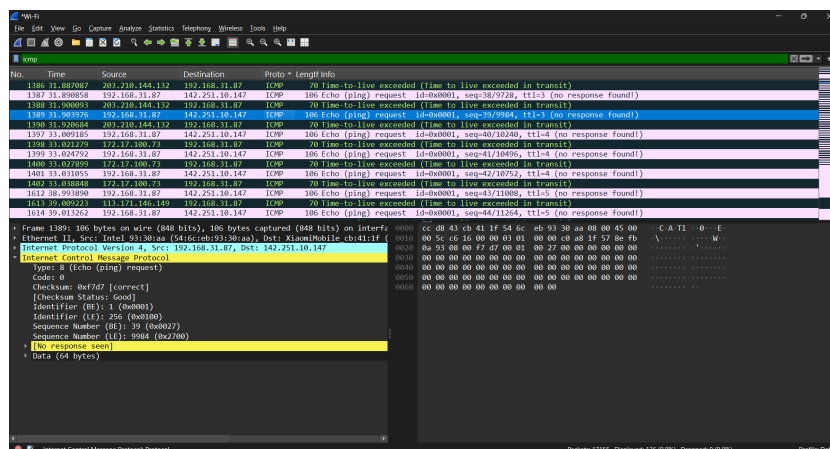
```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 212
    Identification: 0x0000 (0)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x7a70 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.31.1
    Destination Address: 192.168.31.87
    [Stream index: 13]
  ▸ User Datagram Protocol, Src Port: 53, Dst Port: 54544
  ▸ Domain Name System (response)
```

7 Question 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?

ANS: The ICMP echo packets are the same as the ping query packets in terms of structure and key fields, including:

- Type and Code: Echo Request (Type 8, Code 0) and Echo Reply (Type 0, Code 0).
- Checksum, Identifier, and Sequence Number: These fields remain the same in both request and reply packets.



- Payload: Contains the same data in both packets, often including a timestamp for round-trip time measurement.

However, the difference is in their function and direction:

- The ping query (ICMP Echo Request) is sent from the host to the destination.
- The ICMP Echo Reply is sent back from the destination to the host, confirming receipt.

8 Question 8

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

ANS:

The ICMP error packet contains additional fields compared to the ICMP echo packet. Specifically, it includes:

- ICMP Type and Code: Identifies the type of error (e.g., Destination Unreachable, Time Exceeded).
- Checksum: Used for error detection.
- Unused/Reserved Fields: Some ICMP error messages have extra fields that are set to zero or contain additional information.

- Original IP Header: The header of the original packet that caused the error.
- First 8 Bytes of the Original Packet's Data: Includes the source and destination port numbers (if the original packet was UDP or TCP), helping the sender identify the connection that triggered the error.

This extra information allows the sender to diagnose and respond to network issues.

9 Question 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?

ANS:

The last three ICMP packets are Type 0 (Echo Reply) instead of Type 11 (Time Exceeded - TTL Expired). They differ from ICMP error packets in the following ways:

- ICMP Echo Reply (Type 0) Packets:
 - Indicate that the probe packets successfully reached the destination host.
 - Contain the original Identifier and Sequence Number to match the request.
 - Do not include the original IP header and first 8 bytes of the original packet.
- ICMP Error (Type 11 - TTL Expired) Packets:
 - Are sent by intermediate routers when a packet's TTL reaches zero before reaching the destination.
 - Include the original IP header and the first 8 bytes of the original packet for troubleshooting.

These packets differ because the Echo Reply messages confirm successful delivery, whereas TTL Expired messages indicate that the packet was discarded before reaching the destination.

10 Question 10

Within the tracert 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?

ANS:

Yes, the link between hop 26 and hop 27 has a significantly higher delay (133ms compared to previous values around 60ms). The last router, sd-in-f147.1e100.net [142.251.10.147], is likely a Google data center, possibly in the US. The previous router did not respond, making its exact location unknown, but it could be an intermediate Google server or a trans-oceanic connection point. The increased delay is likely due to the long-distance connection, possibly crossing an ocean or involving multiple network hops.

```
Command Prompt
Tracing route to www.google.com [142.251.10.147]
over a maximum of 30 hops:
  1    2 ms    1 ms    1 ms    XiaoQiang [192.168.31.1]
  2    *      *      *      Request timed out.
  3    6 ms    9 ms    16 ms    adsl.hnpt.com.vn [203.210.144.132]
  4    12 ms   3 ms    7 ms    172.17.100.73
  5    15 ms   8 ms    8 ms    static.vnpt.vn [113.171.146.149]
  6    29 ms   29 ms   28 ms    static.vnpt.vn [113.171.49.193]
  7    31 ms   32 ms   31 ms    static.vnpt.vn [113.171.143.22]
  8    29 ms   34 ms   28 ms    static.vnpt.vn [113.171.31.33]
  9    50 ms   48 ms   67 ms    72.14.219.148
 10   56 ms   60 ms   70 ms    142.251.67.15
 11   53 ms   56 ms   51 ms    74.125.245.2
 12   56 ms   61 ms   64 ms    216.239.63.216
 13   55 ms   56 ms   70 ms    142.251.231.3
 14   53 ms   50 ms   55 ms    142.251.231.198
 15   62 ms   59 ms   55 ms    142.251.52.239
 16    *      *      *      Request timed out.
 17    *      *      *      Request timed out.
 18    *      *      *      Request timed out.
 19    *      *      *      Request timed out.
 20    *      *      *      Request timed out.
 21    *      *      *      Request timed out.
 22    *      *      *      Request timed out.
 23    *      *      *      Request timed out.
 24    *      *      *      Request timed out.
 25    *      *      *      Request timed out.
 26    *      *      *      Request timed out.
 27  133 ms   83 ms   77 ms    sd-in-f147.1e100.net [142.251.10.147]

Trace complete.
C:\Users\Admin>
```