

**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 TN (CO3094)**

**LAB 5**

**Wireshark: ICMP v8.0**

**HK: 241 - LỚP: L09**

**GVHD: Bùi Xuân Giang**

**Sinh viên thực hiện**

**Nguyễn Tấn Tài : 2212990**

Thành phố Hồ Chí Minh, tháng 11 năm 2024

## Wireshark: ICMP v8.0

Trong bài lab này, chúng ta sẽ khám phá một số khía cạnh của giao thức ICMP:

- Các thông điệp ICMP được tạo ra bởi chương trình Ping;
- Các thông điệp ICMP được tạo ra bởi chương trình Traceroute;
- Định dạng và nội dung của một thông điệp ICMP.

### 1. ICMP và Ping

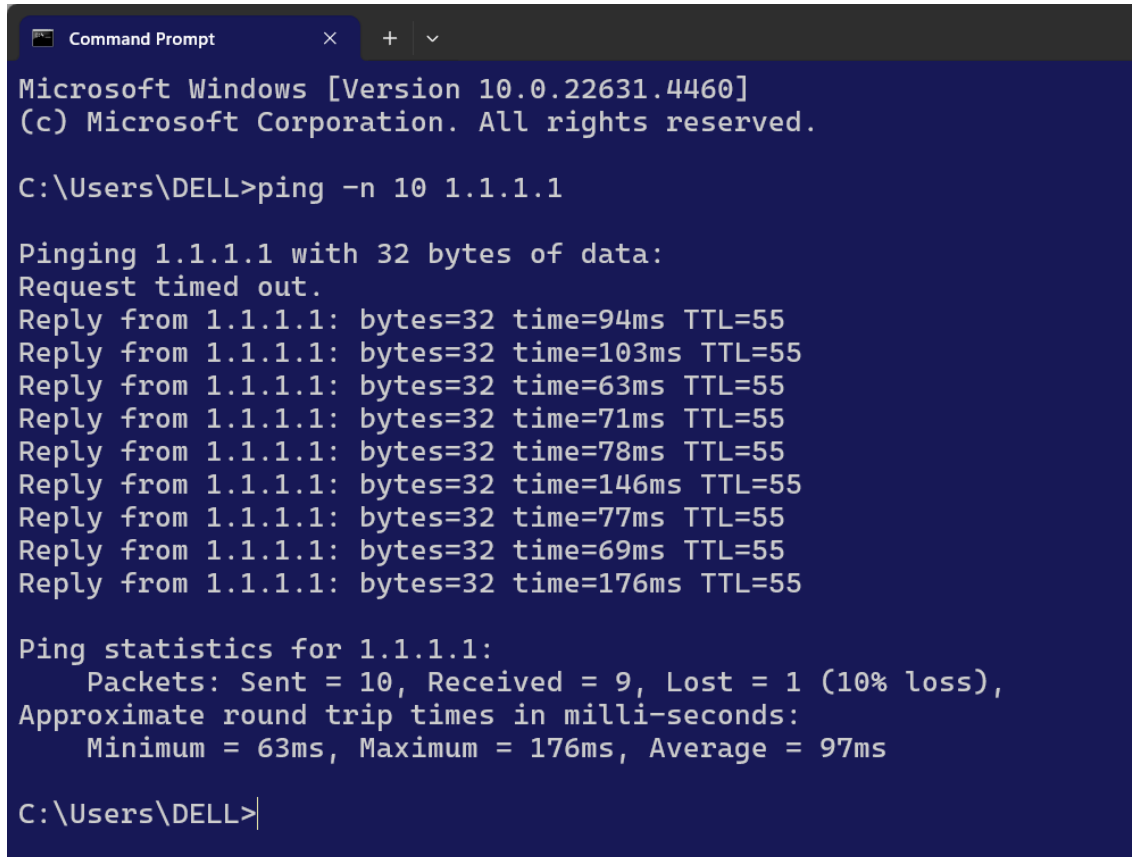
Hãy bắt đầu cuộc khám phá về ICMP của chúng ta bằng cách ghi lại các gói tin được tạo ra bởi chương trình Ping. Bạn có thể nhớ rằng chương trình Ping rất đơn giản, cho phép bất kỳ ai (ví dụ, một quản trị viên mạng) kiểm tra xem một máy chủ có hoạt động hay không. Chương trình Ping trên máy chủ nguồn sẽ gửi một gói tin đến địa chỉ IP mục tiêu; nếu máy đích đang hoạt động, chương trình Ping trên máy đích sẽ phản hồi bằng cách gửi lại một gói tin đến máy chủ nguồn. Như bạn có thể đoán (vì bài lab này liên quan đến ICMP), cả hai gói tin Ping này đều là gói ICMP.

Các bước thực hiện:

- Hãy bắt đầu bằng cách mở ứng dụng Command Prompt của Windows (có thể tìm thấy nó trong thư mục Accessories).
- Khởi động trình thu gói tin Wireshark và bắt đầu thu gói tin trong Wireshark.
- Lệnh *ping* nằm trong *c:\windows\system32*, do đó hãy nhập một trong các lệnh sau: "*ping -n 10 hostname*" hoặc "*c:\windows\system32\ping -n 10 hostname*" trong dòng lệnh MS-DOS (không có dấu ngoặc kép), với *hostname* là tên máy chủ ở một châu lục khác. Nếu bạn ở ngoài khu vực châu Á, bạn có thể nhập *www.ust.hk* cho máy chủ Web của Đại học Khoa học và Công nghệ Hồng Kông. Đổi số *-n 10* chỉ định rằng 10 thông điệp Ping sẽ được gửi. Sau đó chạy chương trình Ping bằng cách nhấn *enter*.
- Khi chương trình Ping kết thúc, hãy dừng việc thu gói tin trong Wireshark.

Ở cuối thí nghiệm, cửa sổ Command Prompt của bạn sẽ trông giống như Hình 1. Trong ví dụ này, chương trình Ping nguồn ở Massachusetts và chương trình Ping đích ở

Hồng Kông. Từ cửa sổ này, chúng ta thấy rằng chương trình Ping nguồn đã gửi 10 gói truy vấn và nhận được 10 phản hồi. Cũng lưu ý rằng đối với mỗi phản hồi, nguồn tính toán thời gian vòng hồi (RTT), và đối với 10 gói tin này, trung bình là 375 ms.



```
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>ping -n 10 1.1.1.1

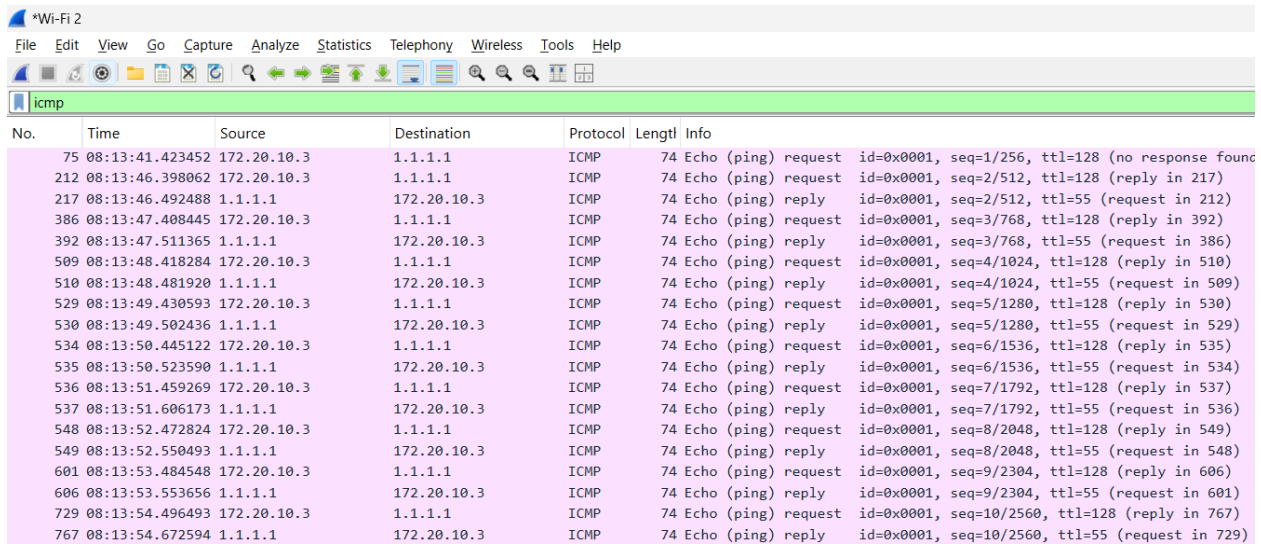
Pinging 1.1.1.1 with 32 bytes of data:
Request timed out.
Reply from 1.1.1.1: bytes=32 time=94ms TTL=55
Reply from 1.1.1.1: bytes=32 time=103ms TTL=55
Reply from 1.1.1.1: bytes=32 time=63ms TTL=55
Reply from 1.1.1.1: bytes=32 time=71ms TTL=55
Reply from 1.1.1.1: bytes=32 time=78ms TTL=55
Reply from 1.1.1.1: bytes=32 time=146ms TTL=55
Reply from 1.1.1.1: bytes=32 time=77ms TTL=55
Reply from 1.1.1.1: bytes=32 time=69ms TTL=55
Reply from 1.1.1.1: bytes=32 time=176ms TTL=55

Ping statistics for 1.1.1.1:
    Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 63ms, Maximum = 176ms, Average = 97ms

C:\Users\DELL>
```

Hình 1. Command Prompt window after entering Ping command.

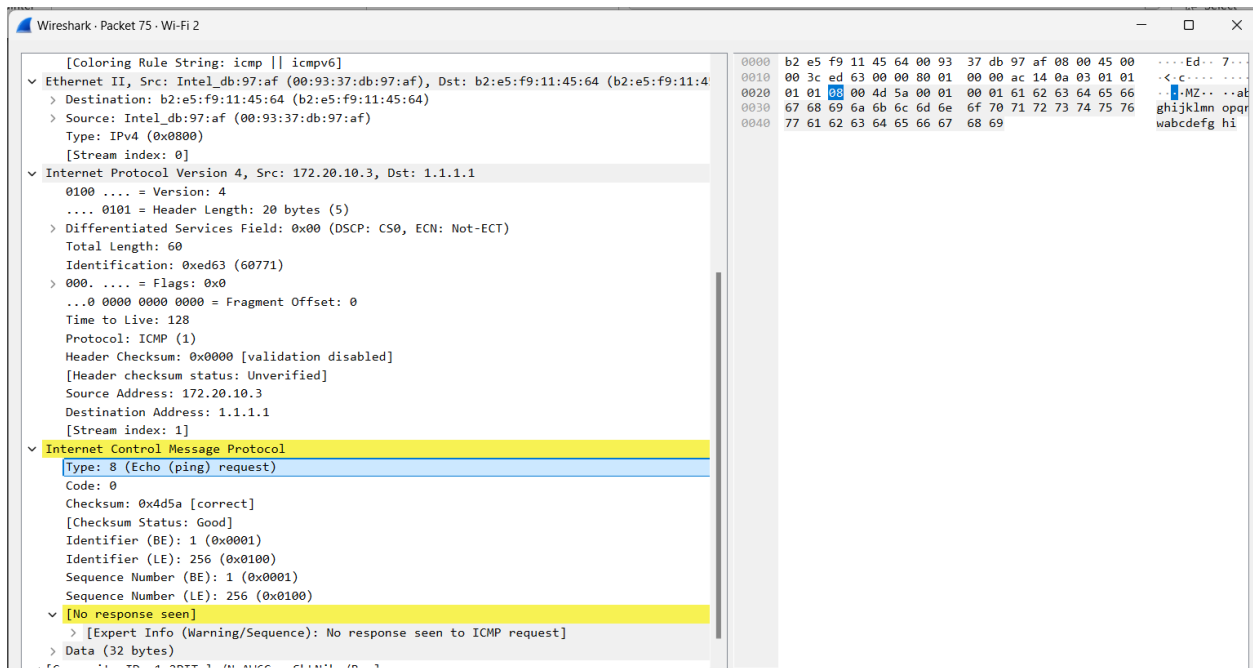
Hình 2 cung cấp một ảnh chụp màn hình của đầu ra Wireshark, sau khi “icmp” đã được nhập vào ô bộ lọc hiển thị. Lưu ý rằng danh sách gói tin hiển thị 20 gói tin: 10 truy vấn Ping được gửi bởi nguồn và 10 phản hồi Ping nhận được từ nguồn. Cũng lưu ý rằng địa chỉ IP của nguồn là một địa chỉ IP riêng (nằm sau NAT) có dạng 192.168/12; địa chỉ IP của đích là địa chỉ của máy chủ Web tại HKUST. Giờ hãy phóng to gói tin đầu tiên (được gửi bởi máy khách); trong hình dưới đây, khu vực chứa nội dung của gói tin cung cấp thông tin về gói tin này. Chúng ta thấy rằng datagram IP trong gói tin này có số hiệu giao thức là 01, là số hiệu giao thức dành cho ICMP. Điều này có nghĩa là tải trọng của datagram IP là một gói ICMP.



No.	Time	Source	Destination	Protocol	Length	Info
75	08:13:41.423452	172.20.10.3	1.1.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (no response found)
212	08:13:46.398062	172.20.10.3	1.1.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 217)
217	08:13:46.492488	1.1.1.1	172.20.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=55 (request in 212)
386	08:13:47.408445	172.20.10.3	1.1.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 392)
392	08:13:47.511365	1.1.1.1	172.20.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=55 (request in 386)
509	08:13:48.418284	172.20.10.3	1.1.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 510)
510	08:13:48.481920	1.1.1.1	172.20.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=55 (request in 509)
529	08:13:49.430593	172.20.10.3	1.1.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 530)
530	08:13:49.502436	1.1.1.1	172.20.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=55 (request in 529)
534	08:13:50.445122	172.20.10.3	1.1.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 535)
535	08:13:50.523590	1.1.1.1	172.20.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=55 (request in 534)
536	08:13:51.459269	172.20.10.3	1.1.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 537)
537	08:13:51.606173	1.1.1.1	172.20.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=55 (request in 536)
548	08:13:52.472824	172.20.10.3	1.1.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 549)
549	08:13:52.550493	1.1.1.1	172.20.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=55 (request in 548)
601	08:13:53.484548	172.20.10.3	1.1.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 606)
606	08:13:53.553656	1.1.1.1	172.20.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=55 (request in 601)
729	08:13:54.496493	172.20.10.3	1.1.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 767)
767	08:13:54.672594	1.1.1.1	172.20.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=55 (request in 729)

Hình 2. Wireshark output for Ping program with Internet Protocol expanded.

Hình 3 tập trung vào cùng gói ICMP đó nhưng đã mở rộng thông tin về giao thức ICMP trong cửa sổ nội dung của gói tin. Hãy quan sát rằng gói ICMP này thuộc loại Type 8 và Code 0 - một gói tin gọi là ICMP “yêu cầu hồi đáp” (echo request). (Xem Hình 5.19 trong sách giáo khoa.) Cũng lưu ý rằng gói tin ICMP này chứa một mã kiểm tra (checksum), một trường định danh (identifier), và một số thứ tự (sequence number).



Wireshark - Packet 75 - Wi-Fi 2	
[Coloring Rule String: icmp    icmpv6]	
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64) Destination: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64) Source: Intel_db:97:af (00:93:37:db:97:af) Type: IPv4 (0x0800) [Stream index: 0]	
Internet Protocol Version 4, Src: 172.20.10.3, Dst: 1.1.1.1 0100 .... = Version: 4 ... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 60 Identification: 0xed63 (60771) 000. .... = Flags: 0x0 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: ICMP (1) Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source Address: 172.20.10.3 Destination Address: 1.1.1.1 [Stream index: 1]	
Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0x4d5a [correct] [Checksum Status: Good] Identifier (BE): 1 (0x0001) Identifier (LE): 256 (0x0100) Sequence Number (BE): 1 (0x0001) Sequence Number (LE): 256 (0x0100) [No response seen] [Expert Info (Warning/Sequence): No response seen to ICMP request] Data (32 bytes)	

Hình 3. Wireshark capture of ping packet with ICMP packet expanded.

## Trả lời câu hỏi

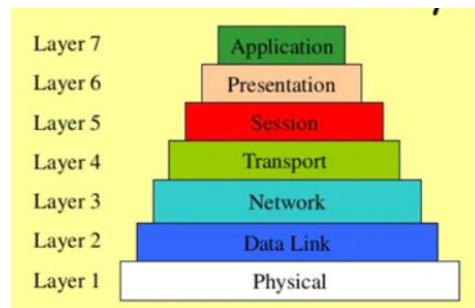
**Câu hỏi 1:** Địa chỉ IP của máy chủ của bạn là gì? Địa chỉ IP của máy đích là gì?

Địa chỉ IP của máy chủ (Source): 172.20.10.3

Địa chỉ IP của máy đích (Destination): 1.1.1.1

**Câu hỏi 2:** Tại sao một gói tin ICMP không có các số cổng nguồn và đích?

ICMP hoạt động ở lớp Internet của mô hình OSI (lớp 3), trong khi các số cổng được sử dụng trong lớp Transport (lớp 4) bởi các giao thức như TCP và UDP. Do đó, ICMP không sử dụng các số cổng vì nó không thuộc lớp vận chuyển; thay vào đó, ICMP sử dụng số loại (Type) và mã (Code) để xác định loại thông báo ICMP.



**Câu hỏi 3:** Kiểm tra một trong các gói tin yêu cầu Ping được gửi bởi máy chủ của bạn.

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4d59 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 2 (0x0002)
Sequence Number (LE): 512 (0x0200)
[Response frame: 217]
Data (32 bytes)
0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70  abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
[Community ID: 1:2PITyle/NuAW6CrnqShLNiba/Bs=]
```

Loại (Type): 8 (Echo (ping) request)

Mã (Code): 0

Các trường khác:

- Checksum: 0x4d59
- Identifier (ID): 0x0001
- Sequence Number: 512 (0x0200)

Số byte:

- Checksum: 2 bytes
- Identifier: 2 bytes
- Sequence Number: 2 bytes

**Câu hỏi 4:** Kiểm tra gói tin phản hồi Ping tương ứng.

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x5559 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 2 (0x0002)

Sequence Number (LE): 512 (0x0200)

[Request frame: 212]

[Response time: 94.426 ms]

Data (32 bytes)

0000 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefghijklmnop

0010 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi

Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

[Length: 32]

[Community ID: 1:2PITyle/NuAW6CrnqShLNiba/Bs=]

Loại (Type): 0 (Echo (ping) reply)

Mã (Code): 0

Các trường khác:

- Checksum: 0x55f9
- Identifier (ID): 0x0001
- Sequence Number: 512 (0x0200)

Số byte:

- Checksum: 2 bytes
- Identifier: 2 bytes
- Sequence Number: 2 bytes

## 2. ICMP và Traceroute

Bây giờ hãy tiếp tục cuộc phiêu lưu ICMP của chúng ta bằng cách ghi lại các gói tin được tạo ra bởi chương trình Traceroute. Bạn có thể nhớ rằng chương trình Traceroute có thể được sử dụng để xác định đường đi mà một gói tin thực hiện từ nguồn đến đích. Traceroute được thảo luận trong Mục 1.4 và Mục 5.6 của sách giáo khoa.

Traceroute được triển khai theo các cách khác nhau trong Unix/Linux/macOS và Windows. Trong Unix/Linux, nguồn gửi một loạt các gói tin UDP đến địa chỉ đích bằng cách sử dụng một số cổng đích không hợp lệ; trong Windows, nguồn gửi một loạt các gói tin ICMP đến đích. Đối với cả hai hệ điều hành, chương trình gửi gói đầu tiên với TTL=1, gói thứ hai với TTL=2, v.v. Hãy nhớ rằng mỗi bộ định tuyến sẽ giảm giá trị TTL của gói khi gói đi qua bộ định tuyến. Khi một gói đến một bộ định tuyến có TTL=1, bộ định tuyến sẽ gửi một gói lỗi ICMP trở lại nguồn. Trong phần tiếp theo, chúng ta sẽ sử dụng chương trình Traceroute gốc của Windows là *tracert*. Phiên bản phần mềm chia sẻ của một chương trình Traceroute tốt cho Windows là *pingplotter* ([www.pingplotter.com](http://www.pingplotter.com)). Chúng ta sẽ sử dụng *pingplotter* trong bài lab IP Wireshark của chúng ta vì nó cung cấp các tính năng bổ sung mà chúng ta cần.

Thực hiện các bước sau:

- Hãy bắt đầu bằng cách mở ứng dụng Command Prompt của Windows (có thể tìm thấy trong thư mục Accessories).
- Khởi động trình thu gói tin Wireshark và bắt đầu thu gói tin.
- Lệnh *tracert* nằm trong *c:\windows\system32*, do đó hãy nhập *tracert hostname* hoặc *c:\windows\system32\tracert hostname* trong dòng lệnh MS-DOS (không có dấu ngoặc kép), với *hostname* là một máy chủ ở một châu lục khác. (Lưu ý rằng trên máy Windows, lệnh là “tracert” chứ không phải “traceroute”.) Nếu bạn ở ngoài châu Âu, bạn có thể muốn nhập [www.inria.fr](http://www.inria.fr) cho máy chủ Web của INRIA, một viện nghiên cứu khoa học máy tính ở Pháp. Sau đó chạy chương trình Traceroute bằng cách nhấn phím *enter*.

```
C:\Users\DELL>tracert 1.1.1.1

Tracing route to one.one.one.one [1.1.1.1]
over a maximum of 30 hops:

  1    13 ms    7 ms    35 ms  172.20.10.1
  2   149 ms   63 ms   38 ms  1.3.7.249
  3   153 ms   36 ms   28 ms  10.204.87.57
  4    80 ms   39 ms   34 ms  10.204.87.58
  5   173 ms   42 ms   67 ms  10.203.227.162
  6    48 ms   23 ms   47 ms  10.203.227.237
  7     *      *      *    Request timed out.
  8   162 ms   65 ms   96 ms  DESKTOP-26T57VF [27.68.250.208]
  9   213 ms   60 ms   56 ms  162.158.160.218
 10    81 ms  202 ms  138 ms  162.158.160.141
 11   288 ms  174 ms  274 ms  one.one.one.one [1.1.1.1]

Trace complete.
```

Hình 4. Command Prompt window displays the results of the Traceroute program.

- Khi chương trình Traceroute kết thúc, hãy dừng thu gói tin trong Wireshark.

Kết thúc thí nghiệm, cửa sổ Command Prompt của bạn sẽ trông giống như Hình 4. Trong hình này, chương trình Traceroute chạy trên máy khách ở Massachusetts và đích đến là ở Pháp. Từ hình này, chúng ta thấy rằng với mỗi giá trị TTL, chương trình nguồn gửi ba gói dò. Traceroute hiển thị các RTT cho mỗi gói dò, cũng như địa chỉ IP (và có thể là tên) của bộ định tuyến đã trả về thông báo ICMP TTL-exceeded.

**Hình 5** hiển thị cửa sổ Wireshark cho một gói ICMP được trả về bởi một bộ định tuyến. Lưu ý rằng gói lỗi ICMP này chứa nhiều trường hơn các gói ICMP Ping.

### Trả lời câu hỏi

**Câu 5:** Địa chỉ IP của máy chủ của bạn là gì? Địa chỉ IP của máy đích là gì?

Địa chỉ IP của máy chủ (Source): 172.20.10.3

Địa chỉ IP của máy đích (Destination): 1.1.1.1

**Câu 6:** Nếu ICMP gửi các gói UDP thay thế (như trong Unix/Linux), số giao thức IP sẽ vẫn là 01 cho các gói dò không? Nếu không, nó sẽ là gì?





Số giao thức IP cho ICMP là 01. Nếu Traceroute sử dụng các gói UDP thay thế, số giao thức IP sẽ không còn là 01.

Thay vào đó, số giao thức IP sẽ là 17, vì 17 là số giao thức dành cho UDP (User Datagram Protocol).

**Câu 7:** Kiểm tra gói tin ICMP echo trong ảnh chụp màn hình của bạn. Gói tin này có khác với các gói truy vấn Ping ICMP trong phần đầu của bài lab này không? Nếu có, tại sao?

[illegible]

Gói tin ICMP echo trong ảnh chụp màn hình có Type là 8 và Code là 0, tương ứng với một gói Ping Request (yêu cầu hồi đáp).

Gói tin này tương tự với các gói truy vấn Ping ICMP trước đó trong bài lab. Nó không có sự khác biệt vì gói tin ICMP echo luôn có cùng Type và Code (Type = 8, Code = 0) cho yêu cầu Ping.

**Lý do:** Traceroute trên Windows sử dụng gói ICMP với Type = 8 và Code = 0 cho mỗi gói dò, tương tự như các gói Ping.

**Câu 8:** Kiểm tra gói tin ICMP lỗi trong ảnh chụp màn hình của bạn. Gói tin này có nhiều trường hơn gói tin ICMP echo. Những gì được bao gồm trong các trường này?

Gói tin ICMP lỗi trong ảnh chụp màn hình có Type là 11 và Code là 0, tương ứng với lỗi "Time-to-live exceeded" (thời gian tồn tại đã vượt quá).

```
[Checksum Index: 4]
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xf4ff [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 172.20.10.3, Dst: 1.1.1.1
  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: 92
  Identification: 0xed6d (60781)
  000. .... = Flags: 0x0
    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: 1
    [Expert Info (Note/Sequence): "Time To Live" only 1]
      ["Time To Live" only 1]
      [Severity level: Note]
      [Group: Sequence]
  Protocol: ICMP (1)
  Header Checksum: 0x141b [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.20.10.3
```

Các trường bổ sung trong gói ICMP lỗi:

- Gói tin chứa toàn bộ phần tiêu đề IP và phần đầu của gói tin ICMP yêu cầu ban đầu (Echo Request) đã gây ra lỗi TTL.
- Điều này bao gồm:
  - Địa chỉ IP nguồn và đích ban đầu.
  - Thông tin về gói tin ICMP yêu cầu (Ping Request) ban đầu, bao gồm các trường như Checksum, Identifier, và Sequence Number.

Mục đích của các trường bổ sung này: Các trường này cho phép máy nguồn biết được gói tin nào đã hết thời gian TTL và tại đâu, giúp ích cho việc theo dõi đường đi của gói tin đến đích.

**Câu 9:** Kiểm tra ba gói ICMP cuối cùng nhận được bởi máy nguồn. Những gói này khác với các gói lỗi ICMP như thế nào? Tại sao chúng khác nhau?

[illegible]

Gói tin 2661: Đây là gói tin ICMP echo reply (hồi đáp) với địa chỉ nguồn là 1.1.1.1 (máy đích) và địa chỉ đích là 172.20.10.3 (máy nguồn). Gói tin này có Type là 0 và Code là 0, là một phản hồi cho gói yêu cầu Ping cuối cùng.

[illegible]

Gói tin 2662: Đây là gói tin ICMP echo request (yêu cầu hồi đáp) từ máy nguồn 172.20.10.3 đến máy đích 1.1.1.1, với Type là 8 và Code là 0. Gói này có Sequence Number là 43.

[illegible]

Gói tin 2663: Đây là gói tin ICMP echo reply từ máy đích 1.1.1.1 đến máy nguồn 172.20.10.3, với Type là 0 và Code là 0. Gói này cũng là một phản hồi cho yêu cầu Ping với Sequence Number là 43.

## Sự Khác Biệt Giữa Các Gói ICMP Cuối Cùng và Các Gói Lỗi ICMP:

- Ba gói tin cuối cùng này là các gói ICMP echo request và echo reply dùng trong Ping, trong khi các gói lỗi ICMP trong Traceroute có Type = 11 và Code = 0 (Time-to-live exceeded).
- Lý do chúng khác nhau:
  - Trong Traceroute, các gói ICMP lỗi được gửi khi TTL (Time to Live) của gói tin giảm đến 0 tại các bộ định tuyến trên đường đi, khiến bộ định tuyến trả về thông báo lỗi TTL.
  - Trong các gói tin cuối cùng này, gói tin đã đến đích (1.1.1.1), và máy đích đã trả lời lại bằng gói ICMP echo reply thay vì thông báo lỗi. Điều này xảy ra vì TTL đã không giảm đến 0 trước khi đến đích, nên không có lỗi TTL nào được trả về.

**Câu 10:** Trong các phép đo Traceroute, có liên kết nào mà độ trễ của nó dài hơn đáng kể so với các liên kết khác không? Dựa trên ảnh chụp màn hình trong Hình 4, có liên kết nào mà độ trễ của nó dài hơn đáng kể không? Dựa trên tên của các bộ định tuyến, bạn có thể đoán vị trí của hai bộ định tuyến ở hai đầu của liên kết này không?

Từ kết quả Traceroute trong Command Prompt, chúng ta có thể thấy thời gian phản hồi (RTT) cho từng bước nhảy (hop) trên đường đi đến đích (1.1.1.1). Dưới đây là một số nhận xét:

- Bước nhảy 2: Độ trễ tăng đột ngột lên khoảng 149 ms ở hop này, điều này có thể là do khoảng cách địa lý lớn hơn hoặc thời gian xử lý tại bộ định tuyến này.
- Bước nhảy 7: Tất cả các yêu cầu tại bước nhảy này đều bị timeout (Request timed out), có thể do firewall hoặc thiết lập của bộ định tuyến không cho phép trả lời ICMP.

Phát hiện liên kết có độ trễ cao: bước nhảy 9 và 10, thời gian phản hồi cho bước nhảy 9 và 10 khá cao so với các bước khác, với RTT trung bình khoảng 213 ms và 202 ms. Độ trễ cao này có thể là do các bộ định tuyến đang nằm ở một khoảng cách xa hơn so với các bộ định tuyến khác trong hành trình, hoặc các bước này có thể nằm ở một khu vực có tốc độ kết nối thấp hơn.

Đoán vị trí của các bộ định tuyến dựa trên tên

- Bước nhảy 8 là nơi kết nối đến địa chỉ 27.68.250.208, là địa chỉ IP công cộng của mạng mà máy tôi đang kết nối (tức là mạng của ISP). Điều này cho thấy các bộ định tuyến ở bước nhảy 8 và các bước sau có thể là các điểm giao tiếp giữa mạng của ISP của bạn và mạng của Cloudflare.
- Bước nhảy 9 và 10 có các địa chỉ 162.158.160.218 và 162.158.160.141, đây là các địa chỉ IP thuộc mạng của Cloudflare, gần với máy chủ đích (1.1.1.1).

### 3. Extra Credit

Trong một bài tập lập trình, bạn đã tạo một chương trình ping UDP. Chương trình ping này, không giống như chương trình ping tiêu chuẩn, gửi các gói dò UDP thay vì các gói dò ICMP. Sử dụng chương trình khách hàng để gửi một gói UDP với một số cổng đích

bất thường đến một máy chủ trực tuyến. Đồng thời, sử dụng Wireshark để thu lại bất kỳ phản hồi nào từ máy chủ. Nộp ảnh chụp màn hình Wireshark của phản hồi cũng như phân tích phản hồi đó.

```
main.go U x
1 package main
2
3 import (
4     "fmt"
5     "net"
6     "os"
7     "time"
8 )
9
10 func main() {
11     // Địa chỉ IP của máy chủ trực tuyến và cổng đích không tồn tại
12     serverAddr := "1.1.1.1:9999" // Cổng 9999 là một cổng không phổ biến
13
14     // Tạo UDP address
15     addr, err := net.ResolveUDPAddr("udp", serverAddr)
16     if err != nil {
17         fmt.Println("Error resolving address:", err)
18         os.Exit(1)
19     }
20
21     // Kết nối tới địa chỉ UDP
22     conn, err := net.DialUDP("udp", nil, addr)
23     if err != nil {
24         fmt.Println("Error connecting:", err)
25         os.Exit(1)
26     }
27     defer conn.Close()
28
29     // Gửi một gói UDP rỗng
30     message := []byte("ping")
31     _, err = conn.Write(message)
32     if err != nil {
33         fmt.Println("Error sending message:", err)
34         os.Exit(1)
35     }
36     fmt.Println("UDP packet sent to", serverAddr)
37
38     // Chờ một thời gian để thu lại phản hồi ICMP trong Wireshark
39     time.Sleep(5 * time.Second) // Chờ 5 giây
40 }
41
```

Đoạn mã trên gửi một gói UDP đến 1.1.1.1 trên cổng 9999, đây là một cổng "bất thường" mà thường không có dịch vụ nào lắng nghe, do đó có thể gây ra phản hồi ICMP lỗi "Port Unreachable".

Capturing from Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp || udp

No.	Time	Source	Destination	Protocol	Length	Info
3	09:00:18.606029	172.20.10.3	8.8.8.8	UDP	46	59714 → 33434 Len=4
4	09:00:18.703646	8.8.8.8	172.20.10.3	ICMP	70	Destination unreachable (Port unreachable)

Windows PowerShell

```
PS D:\HCMUT\HK241\C03093-Computer-Networks-HK241\Lab\Lab_03\src> go run .\main.go
UDP packet sent to 1.1.1.1:9999
PS D:\HCMUT\HK241\C03093-Computer-Networks-HK241\Lab\Lab_03\src> go run .\main.go
UDP packet sent to 8.8.8.8:9999
PS D:\HCMUT\HK241\C03093-Computer-Networks-HK241\Lab\Lab_03\src> go run .\main.go
UDP packet sent to 8.8.8.8:33434
PS D:\HCMUT\HK241\C03093-Computer-Networks-HK241\Lab\Lab_03\src> |
```

Chúng ta dùng net.DialUDP để tạo kết nối UDP đến máy chủ đích. Gửi một gói tin chứa chuỗi "ping" đến máy chủ đích. Sau khi gửi gói tin, chương trình chờ khoảng 5 giây để đảm bảo ta có thể thu lại phản hồi ICMP trong Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
4	09:00:18.703646	8.8.8.8	172.20.10.3	ICMP	70	Destination unreachable (Port unreachable)

Frame 4: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF\_{E8972303-5AC7-4ADA-9205-681936D705B5}, id 0

Section number: 1

Interface id: 0 (\Device\NPF\_{E8972303-5AC7-4ADA-9205-681936D705B5})

Interface name: \Device\NPF\_{E8972303-5AC7-4ADA-9205-681936D705B5}

Interface description: Wi-Fi 2

Encapsulation type: Ethernet (1)

Arrival Time: Nov 16, 2024 09:00:18.703646000 SE Asia Standard Time

UTC Arrival Time: Nov 16, 2024 02:00:18.703646000 UTC

Epoch Arrival Time: 1731722418.703646000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.097617000 seconds]

[Time delta from previous displayed frame: 0.097617000 seconds]

[Time since reference or first frame: 0.257936000 seconds]

Frame Number: 4

Frame Length: 70 bytes (560 bits)

Capture Length: 70 bytes (560 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:icmp:ip:udp]

[Coloring Rule Name: ICMP errors]

[Coloring Rule String: icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }]



```

Internet Control Message Protocol
Type: 3 (Destination unreachable)
Code: 3 (Port unreachable)
Checksum: 0x1d9a [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 172.20.10.3, Dst: 8.8.8.8
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x80 (DSCP: CS4, ECN: Not-ECT)
    1000 00.. = Differentiated Services Codepoint: Class Selector 4 (32)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 32
  Identification: 0x5801 (22529)
  000. .... = Flags: 0x0
    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: 118
  Protocol: UDP (17)
  Header Checksum: 0x2625 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.20.10.3
  Destination Address: 8.8.8.8
  [Stream index: 0]
User Datagram Protocol, Src Port: 59714, Dst Port: 33434
  Source Port: 59714
  Destination Port: 33434

Length: 12
Checksum: 0x7379 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Community ID: 1:6nTm3Xiwd0Hp3q+CUgqncURX2/A=]

```

Ta nhận được gói phản hồi ICMP Destination Unreachable (Port Unreachable) từ máy chủ khi gửi gói UDP đến một cổng không lắng nghe.

Phản hồi ICMP: Máy chủ 8.8.8.8 không có dịch vụ nào đang lắng nghe trên cổng 33434, vì vậy nó trả về một gói ICMP với Type = 3 và Code = 3 (Destination Unreachable - Port Unreachable). Đây là một phản hồi cho biết rằng cổng UDP đích không khả dụng.'