

LAB 4 : Giao thức ICMP, địa chỉ IP và kỹ thuật chia mạng con

Phần 1 : Giao thức ICMP và lệnh Ping

1. Cho biết địa chỉ IP của máy tính mà sinh viên đang dùng và địa chỉ IP của Host đích đã chọn? Tại sao một gói tin ICMP không có số cổng (port number) của Host nguồn và đích?

- Địa chỉ IP của máy tính đang sử dụng là : 192.168.1.4
- Địa chỉ IP của Host đích đã chọn là : 23.76.235.227 (mit.edu)

Source	Destination
23.76.235.227	192.168.1.4

- Lí do 1 gói tin ICMP không có số cổng của Host nguồn và Host đích vì : Giao thức **ICMP** nằm ở tầng network nên không hề có khái niệm về cổng . Vì muốn sử dụng cổng phải nằm ở tầng **Transport** như giao thức TCP/UDP

2. Xem xét chi tiết thông tin (quan sát trong phần Internet Control Message Protocol - ICMP) của 1 gói tin Ping Request được gửi bởi Host mà SV đang dùng và 1 gói tin Ping Reply tương ứng: So sánh thông tin về ICMP Type và các Code Number của 2 gói tin trên. Gói tin ICMP có các trường thông tin nào khác? Các trường thông tin Checksum, Sequence Number và định danh có bao nhiêu byte?

So sánh về ICMP Type và Code Number của gói Request và Reply

	Request	Reply
Type	8	0
Code Number	0	0

- Ngoài ra còn có các trường như Checksum , Identifier, Sequence Number

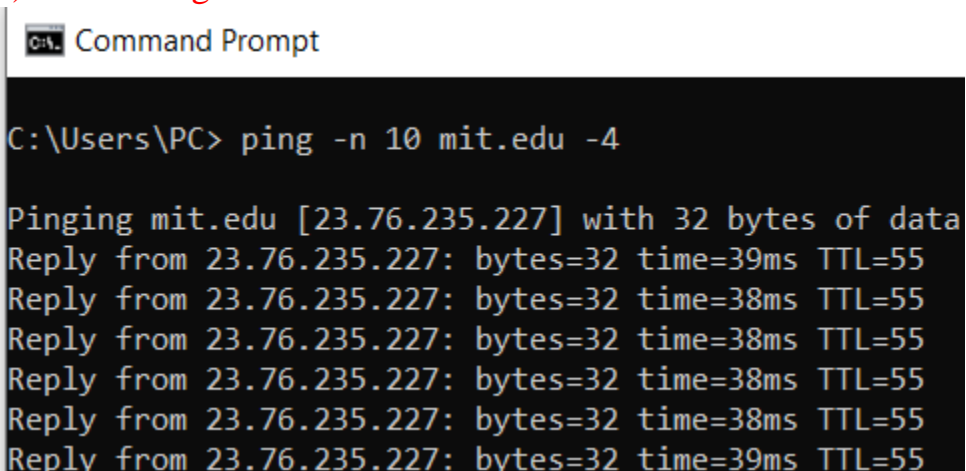
```
Checksum: 0x1229 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 15154 (0x3b32)
Sequence Number (LE): 12859 (0x323b)
[Response frame: 351]
Data (32 bytes)
```

- +) Checksum gồm 2 bytes
- +) Sequence Number (BE) : 2 bytes
- +) Sequence Number (LE) : 2 Bytes
- +) Identifier (BE) : 2 Bytes
- +) Identifier (LE) : 2 Bytes

3. Tìm hiểu và thử nghiệm, cho biết khi sử dụng lệnh ping thì có thể có những loại kết quả trả về nào? Giải thích ý nghĩa từng loại kết quả trả về và cho ví dụ minh họa. Tiến hành ping đến website uit.edu.vn và kiểm tra, giải thích kết quả.

Có 3 loại kết quả có thể trả về

A) Thành công



```
Command Prompt

C:\Users\PC> ping -n 10 mit.edu -4

Pinging mit.edu [23.76.235.227] with 32 bytes of data:
Reply from 23.76.235.227: bytes=32 time=39ms TTL=55
Reply from 23.76.235.227: bytes=32 time=38ms TTL=55
Reply from 23.76.235.227: bytes=32 time=38ms TTL=55
Reply from 23.76.235.227: bytes=32 time=38ms TTL=55
Reply from 23.76.235.227: bytes=32 time=38ms TTL=55
Reply from 23.76.235.227: bytes=32 time=39ms TTL=55
```

B) Lỗi Request Timeout :

```
C:\Users\PC> ping 10.3.3.3

Pinging 10.3.3.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.3.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Lỗi Request Timeout là lỗi khi thực hiện gửi gói tin thành công nhưng không nhận được gói phản hồi
 - Nguyên nhân gây ra lỗi
 - +) Thiết bị định tuyến bị tắt
 - +) Địa chỉ máy đích đang bị tắt hoặc không có thật , cấm ping
 - +) Máy tính khác đường mạng với máy nguồn thì nguyên nhân có thể do định tuyến ngược trở lại máy nguồn
- Ping đến website uit.edu.vn

```
C:\Users\PC> ping uit.edu.vn

Pinging uit.edu.vn [45.122.249.78] with 32 bytes of data:
Reply from 45.122.249.78: bytes=32 time=4ms TTL=54
Reply from 45.122.249.78: bytes=32 time=3ms TTL=54
Reply from 45.122.249.78: bytes=32 time=3ms TTL=54
Reply from 45.122.249.78: bytes=32 time=3ms TTL=54

Ping statistics for 45.122.249.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

- Ping đến thành công (không có lỗi Request Timeout và Destination host unreachable)
- Không gói nào bị mất (0 % loss)
- C) Không tìm thấy host

```
C:\Users\PC> ping uitvn.edu
Ping request could not find host uitvn.edu. Please check the name and try again.
```

4. Tìm hiểu các thông số mở rộng của lệnh ping và thử nghiệm: Mở CMD, dùng lệnh ping /? để xem các thông số mở rộng của lệnh ping:

1) Lệnh ping -t

```
C:\Users\PC> ping 1.1.1.1 -t

Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54
Reply from 1.1.1.1: bytes=32 time=38ms TTL=54
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54
Reply from 1.1.1.1: bytes=32 time=38ms TTL=54
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54

Ping statistics for 1.1.1.1:
    Packets: Sent = 13, Received = 13, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 37ms, Maximum = 38ms, Average = 37ms
Control-C
^C
```

- Lệnh ping -t (Ping được ngừng cho tới khi được dừng lại) bằng **Control + C**
- 2) Lệnh ping -i (Time to live) (Khoảng cách giữa máy chủ và máy đích)

```

C:\Users\PC> ping -n 10 1.1.1.1 -i 60

Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54
Reply from 1.1.1.1: bytes=32 time=37ms TTL=54

Ping statistics for 1.1.1.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 37ms, Maximum = 37ms, Average = 37ms
Control-C
^C
C:\Users\PC> ping -n 10 1.1.1.1 -i 1

Pinging 1.1.1.1 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 1.1.1.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Control-C
^C
C:\Users\PC>

```

- Ở đây ta thấy sự khác biệt khi dùng -i 60 và -i 1
 - + I 60 sẽ thành công và xuất ra
 - + I 1 sẽ lỗi (expired in transit)
 - Phân tích ra thì theo em – I (N) với n là số lượng route có thể phân bổ đi được , 1 ở đây lỗi vì chưa tới đích đã hết số lượng TTL
- 3) **Lệnh Ping – I**

```
C:\Users\PC> ping -n 10 1.1.1.1 -l 90

Pinging 1.1.1.1 with 90 bytes of data:
Reply from 1.1.1.1: bytes=90 time=37ms TTL=54
Reply from 1.1.1.1: bytes=90 time=38ms TTL=54
Reply from 1.1.1.1: bytes=90 time=37ms TTL=54
Reply from 1.1.1.1: bytes=90 time=37ms TTL=54
Reply from 1.1.1.1: bytes=90 time=37ms TTL=54
Reply from 1.1.1.1: bytes=90 time=38ms TTL=54
Reply from 1.1.1.1: bytes=90 time=37ms TTL=54
Reply from 1.1.1.1: bytes=90 time=37ms TTL=54
Reply from 1.1.1.1: bytes=90 time=37ms TTL=54
Reply from 1.1.1.1: bytes=90 time=37ms TTL=54
```

- -L 90 là gói tin nào có số bytes = 90 thì sẽ xuất ra

*** Công cụ Ping có thể dùng để thực hiện Tấn công từ chối dịch vụ (Dos)

- Phương thức tấn công sử dụng Ping là Ping of Death
 - +) Có 2 phần quan trọng trong 1 gói ICMP là ECHO_REQUEST và ECHO_RESPONSE
 - + Khi máy tính gửi thông điệp request đến máy nào đó , nếu nó hoạt động sẽ trả về thông điệp response . Ta biết rằng kích thước cho phép của TCP/IP là 65536 bytes , hacker đã sử dụng sơ hở đó , gửi gói tin lớn hơn 65536 bytes
 - +) Gói tin sẽ chia nhỏ và được ráp lại ở máy đích và do lúc này kích thước quá lớn so với Buffer nên bên nhận không thể quản lí dẫn đến reboot hoặc bị treo

Phần 2 : Giao thức ICMP và công cụ Tracert

1. Cho biết địa chỉ IP của máy tính đang sử dụng? Địa chỉ IP của Host đích mà sinh viên đã chọn?
- Địa chỉ IP của máy là 192.168.1.4

- Địa chỉ IP của Host là 23.76.235.227

Source	Destination
23.76.235.227	192.168.1.4

2. Giá trị Time-To-Live (TTL) có ý nghĩa gì? TTL với website đã tracert bằng bao nhiêu? Khi dùng lệnh Ping thì giá trị TTL tương ứng bằng bao nhiêu? Giải thích sự khác biệt ?

- Giá trị Time – To – Live mang ý nghĩa khoảng cách giữa máy chủ và máy đích tính theo router (dài 8 bit , giá trị tối đa 255 , giảm 1 khi đi qua 1 router)

- TTL khi dùng tracert là 14

518	139.062710	23.76.235.227	192.168.1.4	ICMP	106 Echo (ping) reply	id=0x0001, seq=16596/54336, ttl=53 (request in 517)
519	139.063805	192.168.1.4	23.76.235.227	ICMP	106 Echo (ping) request	id=0x0001, seq=16597/54592, ttl=14 (reply in 520)
520	139.106577	23.76.235.227	192.168.1.4	ICMP	106 Echo (ping) reply	id=0x0001, seq=16597/54592, ttl=53 (request in 519)

- > Frame 519: 106 bytes on wire (848 bits). 106 bytes captured (848 bits) on interface \Device\NPF {0A752F4D-CD1D-460F-9B3B-3F1C7B4FF036}. id 0

- Khi sử dụng lệnh Ping thì giá trị TTL với trang web trên là 53

```
C:\Users\PC> ping mit.edu

Pinging mit.edu [23.77.14.148] with 32 bytes of data:
Reply from 23.77.14.148: bytes=32 time=45ms TTL=53
```

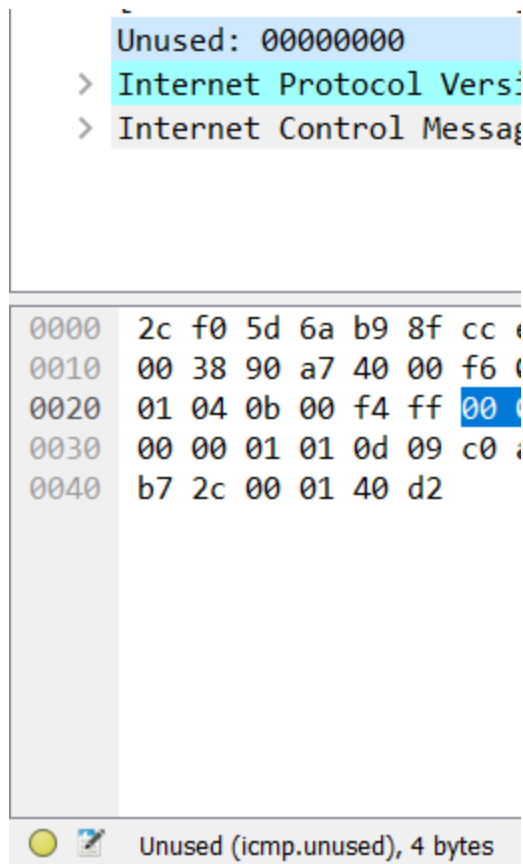
- Ở đây ta thấy lệnh ping có TTL lớn hơn rất nhiều so với Tracert , lí do là vì ở lệnh ping chúng ta sẽ cho sẵn 1 số TTL định trước và khi gặp 1 hop sẽ trừ đi 1 , còn ở Tracert sẽ bắt đầu từ 0 và gặp 1 hop sẽ tăng lên 1 , vì vậy ở đây tạo ra sự khác biệt này

3. Liệt kê IP của các router và phân tích đường đi của gói tin từ nguồn đến đích thông qua lệnh tracert.

Địa chỉ IP và TTL	Đường đi
1) 192.168.1.1	Router tại nhà (Việt Nam)
2) 100.123.1.131	Không có địa chỉ cụ thể
3) 113.22.4.177	Hồ Chí Minh (Việt Nam)
4) 100.123.0.251	Không có địa chỉ cụ thể
5) 118.69.241.177	Hồ Chí Minh (Việt Nam)
6) 42.117.11.158	Hồ Chí Minh (Việt Nam)

7)	42.117.11.157	Hồ Chí Minh (Việt Nam)
8)	183.80.133.146	Hà Chí Minh (Việt Nam)
9)	118.70.1.173	Hà Nội (Việt Nam)
10)	118.69.249.26	Hồ Chí Minh (Việt Nam)
11)	42.112.0.255	Hồ Chí Minh (Việt Nam)
12)	Request timed out.	-
13)	23.56.133.153	Cambrigde (USA)
14)	23.76.235.227	HongKong

4. Xem chi tiết 1 cặp gói tin ICMP Request và Reply thành công khi thực hiện tracert và so sánh với 1 cặp gói ICMP Request và Reply khi thực hiện ping ở bài 1, cặp gói tin này có khác gì nhau không? Nếu có, hãy giải thích?
 - Có sự khác nhau ở đây là ở gói Request và Reply của tracert có data là 64 bytes và data của Ping là 32 bytes
5. Xem chi tiết 1 gói tin ICMP lỗi (Time-to-live Exceeded) trong kết quả Wireshark, nó có nhiều trường thông tin hơn gói tin ICMP Reply thông thường. Những trường thông tin này bao gồm những gì và kích thước của chúng thế nào?
 - Ở phần Internet Control Message Protocol có sự khác biệt ngoài checksum thì những phần khác không có mà thay vào đó là Unused (kích thước 4 bytes)



6. Trong quá trình Tracert, có đường liên kết (link) nào mà có thời gian trễ dài hơn đáng kể so với các link khác hay không? Căn cứ vào các tên Router có thể đoán biết được vị trí của 2 Router ở điểm kết thúc ở link này hay không?
- Trong quá trình Tracert, có đường liên kết có thời gian trễ dài hơn đáng kể so với các link

6	78 ms	77 ms	78 ms
7	3 ms	2 ms	3 ms
8	*	22 ms	22 ms
9	23 ms	22 ms	23 ms
10	47 ms	46 ms	47 ms
11	84 ms	*	*
12	*	*	*
13	*	2366 ms	1104 ms
14	42 ms	42 ms	42 ms

- 6 và 13 : 77ms và 2366 ms

- Vị trí 6 nằm ở HCM và vị trí 13 nằm ở USA

Phần 3 : Địa chỉ IP và chia mạng con

1. Địa chỉ IP dùng để làm gì? IP Private và IP Public là gì và được sử dụng trong trường hợp nào? Liệt kê các dãy IP Private.

- Địa chỉ IP dùng như 1 địa chỉ trên Internet để người dùng có thể kết nối đến , nhận biết mỗi máy tính
- IP Private là : IP được dành riêng cho việc sử dụng nội bộ thông qua router hoặc NAT , cô lập với các mạng bên ngoài
- IP Private dùng để cung cấp địa chỉ hoàn toàn riêng biệt , cho nên được dùng để phân biệt các máy tính và thiết bị trong 1 mạng riêng như trường học , gia đình hay tổ chức , công ty
- IP Public là : Là địa chỉ mà mỗi nhà mạng mang đến dịch vụ Internet (ISP) sử dụng giúp chuyển tiếp những yêu cầu Internet đến một doanh nghiệp hoặc gia đình.
- Các dãy IP Private :
 - +) Lớp A : từ 10.0.0.0 đến 10.255.255.255
 - +) Lớp B : từ 172.16.0.0 đến 172.31.255.255
 - +) Lớp C: từ 192.168.0.0 đến 192.168.255.255

2. Mạng con (subnet) là gì? Tại sao cần phải chia mạng con

- Mạng con là 1 vùng mạng độc lập , mà mạng độc lập là từ việc tách mỗi interface từ host hoặc router của nó tạo thành .
- Chia mạng con có rất nhiều mạng lợi như sau :
 - +) Giảm nghẽn mạng bằng tái định hướng các giao vận và giới hạn phạm vi các thông điệp quảng bá
 - +) Giới hạn phạm vi trong từng mạng con các trục trặc có thể xảy ra

- +) Giảm % sử dụng CPU do giảm lưu lượng các giao vận
- +) Tăng cường bảo mật
- +) Cho phép áp dụng các cấu hình khác nhau cho từng mạng con

3. Subnet Mask là gì? Địa chỉ Broadcast là gì?

- Subnet Mask là một số dạng 32 bit được tạo bằng cách đặt tất cả các host bit thành số 0 và đặt tất cả các network bit thành các số 1. Bằng cách này, subnet mask phân tách địa chỉ IP thành địa chỉ mạng và địa chỉ host.
- Địa chỉ Broadcast là đại diện cho tất cả các thiết bị kết nối cùng mạng

IP ban đầu : 172.25.0.0/16

Bước 1 : Mượn 3 bit của Host ID

+) Subnet Mask mới : 255.255.224.0/19

Bước 2 :

Subnet	IP Address	Subnet Mask	IP khả dụng đầu tiên	IP khả dụng cuối cùng
LAN1	172.25.0.0/19	255.255.224.0	172.25.0.1	172.25.31.254
LAN2	172.30.32.0/19	255.255.224.0	172.25.32.1	172.25.63.254
LAN3	172.30.64.0/19	255.255.224.0	172.25.64.1	172.25.95.254
LAN4	172.30.96.0/19	255.255.224.0	172.25.96.1	172.25.127.254
WAN1	172.30.128.0/19	255.255.224.0	172.25.128.1	172.25.159.254
WAN2	172.30.160.0/19	255.255.224.0	172.25.160.1	172.25.191.254
WAN3	172.30.192.0/19	255.255.224.0	172.25.192.1	172.25.223.254