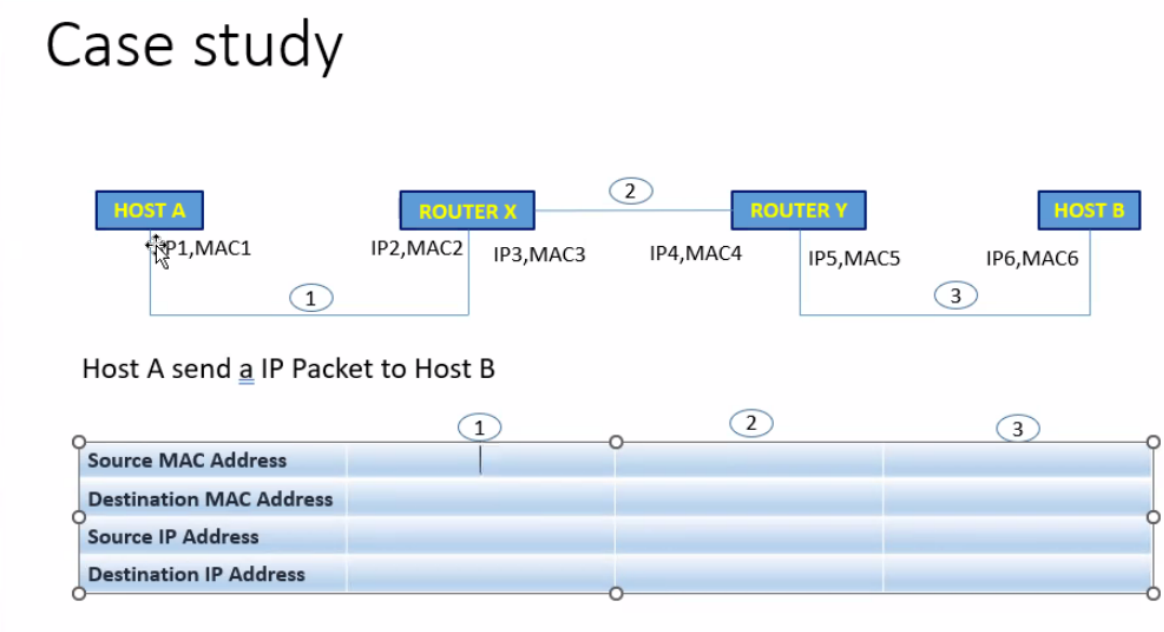
MÔN: TRIỂN KHAI AN NINH HỆ THỐNG

LT05 – 06/09/2024

Phúc Lâm

Case Study



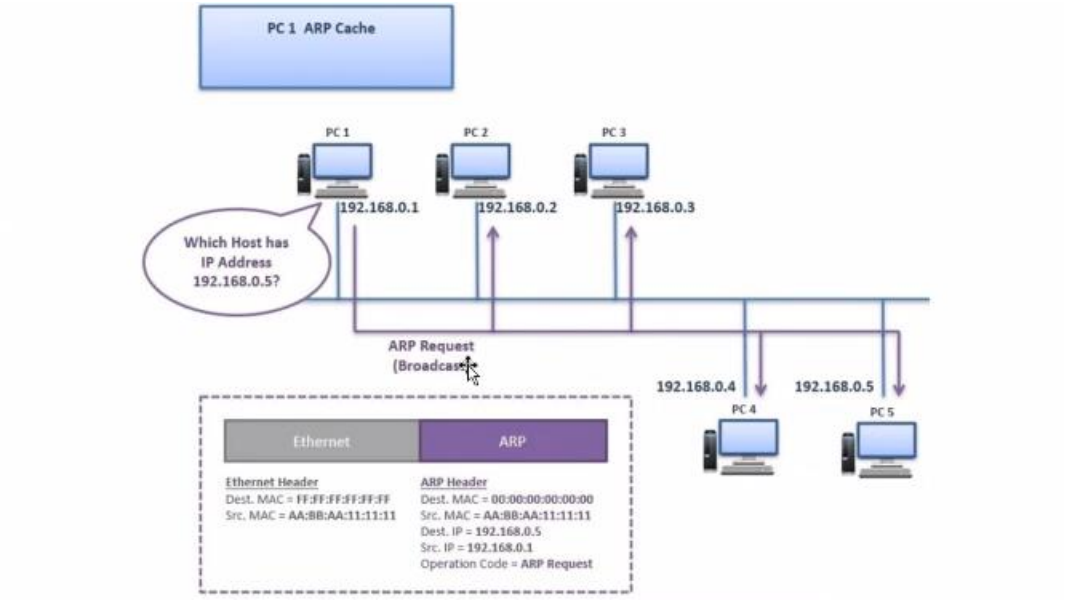
BÀI LÀM

	1	2	3
Source MAC address	MAC1	MAC3	MAC5
Destination MAC address	MAC2	MAC4	MAC6
Source IP Address	IP1	IP1	IP1
Destination IP Address	IP6	IP6	IP6

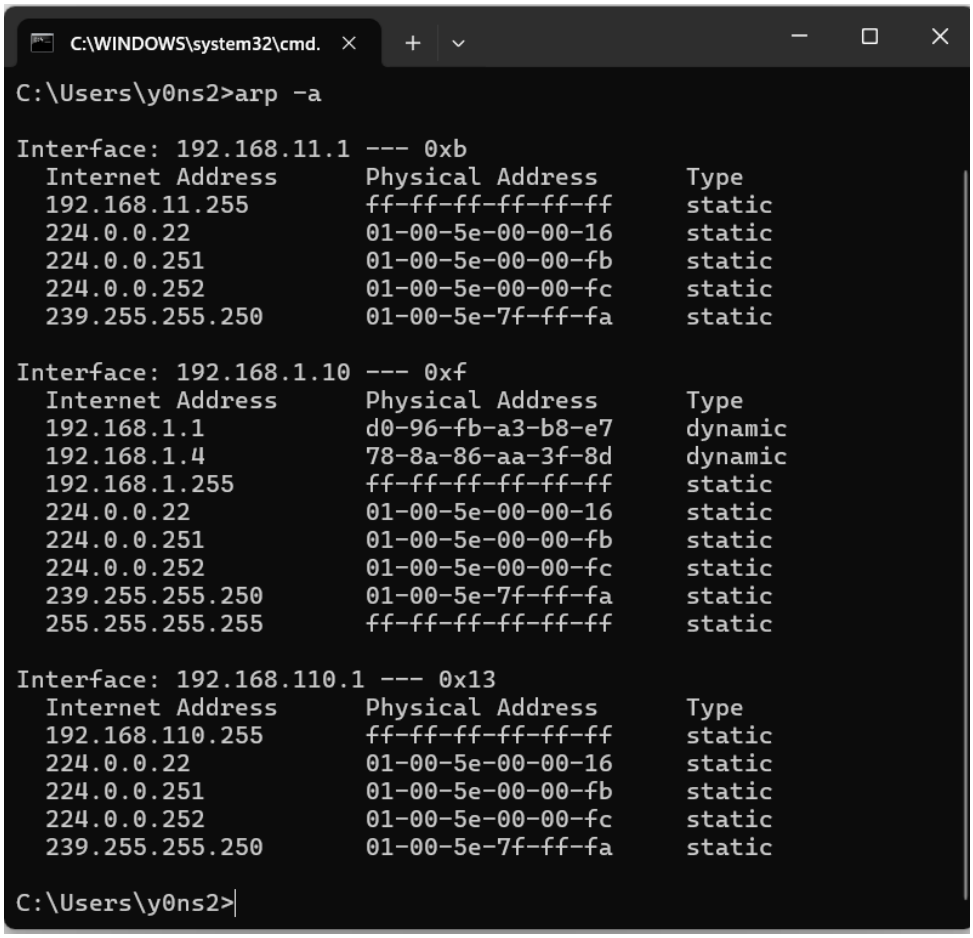
IP nguồn và đích sẽ không thay đổi trong quá trình

Địa chỉ MAC nguồn và đích sẽ thay đổi theo môi trường trong quá trình

Gói ARP Request (broadcast): sẽ gửi tới các máy

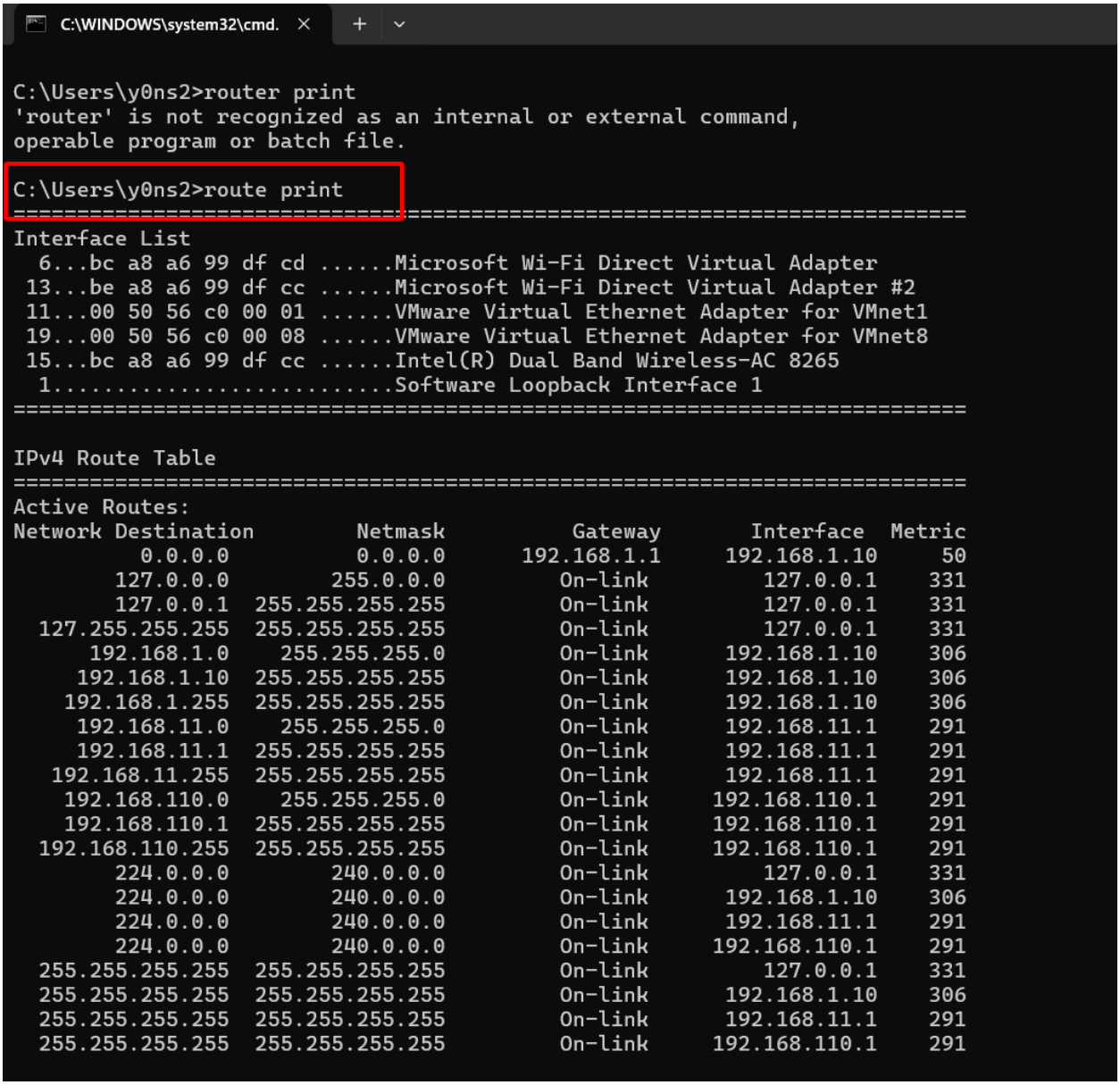


Xem bằng lệnh arp -a



```
C:\Users\y0ns2>arp -a

Interface: 192.168.11.1 --- 0xb
  Internet Address      Physical Address      Type
  192.168.11.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.1.10 --- 0xf
  Internet Address      Physical Address      Type
  192.168.1.1           d0-96-fb-a3-b8-e7     dynamic
  192.168.1.4           78-8a-86-aa-3f-8d     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.110.1 --- 0x13
  Internet Address      Physical Address      Type
  192.168.110.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\y0ns2>ping 192.168.1.4 -4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=66ms TTL=64
Reply from 192.168.1.4: bytes=32 time=4ms TTL=64
Reply from 192.168.1.4: bytes=32 time=8ms TTL=64
Reply from 192.168.1.4: bytes=32 time=6ms TTL=64

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

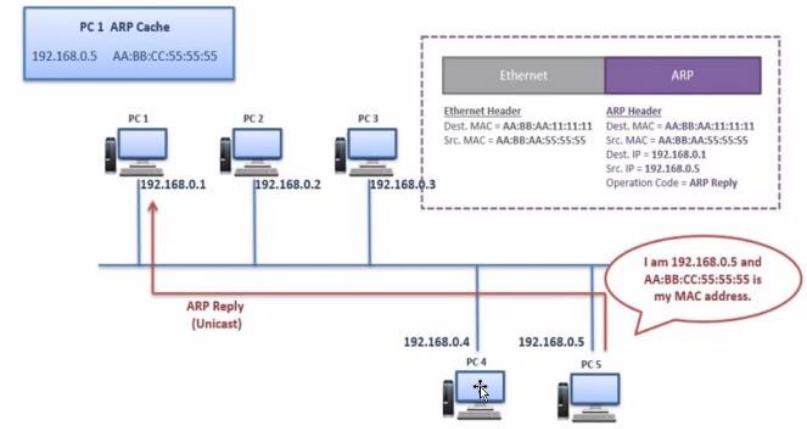
Xem khác mạng



//on link là cùng mạng, khác mạng thì đi ra bằng gateway

TẤN CÔNG BẺ LÁI ĐƯỜNG TRUYỀN

1. **Tấn công ARP**
2. **Tấn công DHCP**
3. **Tấn công DNS**



1. Tấn công ARP

Kẻ tấn công ngồi ở PC4 và tấn công PC1, khi pc1 gửi arp ra tới pc5 mà pc4 đã gửi ARP rely trước PC5

Pc1 gửi cho PC5 mà PC4 đã lấy được.(bẻ lái đường truyền, ăn cắp thông tin)

Giả sử pc5 kết nối cổng ra internet, pc4 giả mạo mac của pc5 làm cho pc1 gửi nhầm sang pc4 và sau đó pc4 gửi sang pc5 để ra cổng internet

2. Tấn công DHCP server

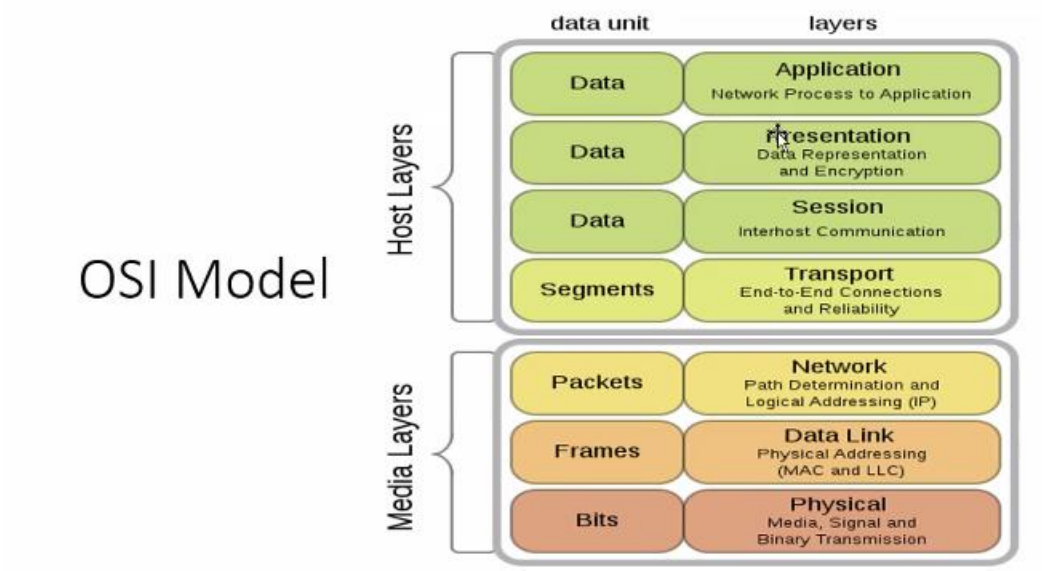
DHCP server cấp ip, subnet, mask cho các máy, kẻ tấn công tiến hành cướp hoặc sửa thông tin ip, mac.

3. Tấn công DNS

Pc1 muốn truy cập internet thì phải truy cập pc3 để phân giải miền dns, pc4 tiến hành truy cập vào cơ sở dữ liệu của pc3 để sửa hoặc làm cho khi truy cập vào miền máy chủ khác, giả mạo nhằm đánh cắp thông tin đăng nhập,v.v

II. OSI Model

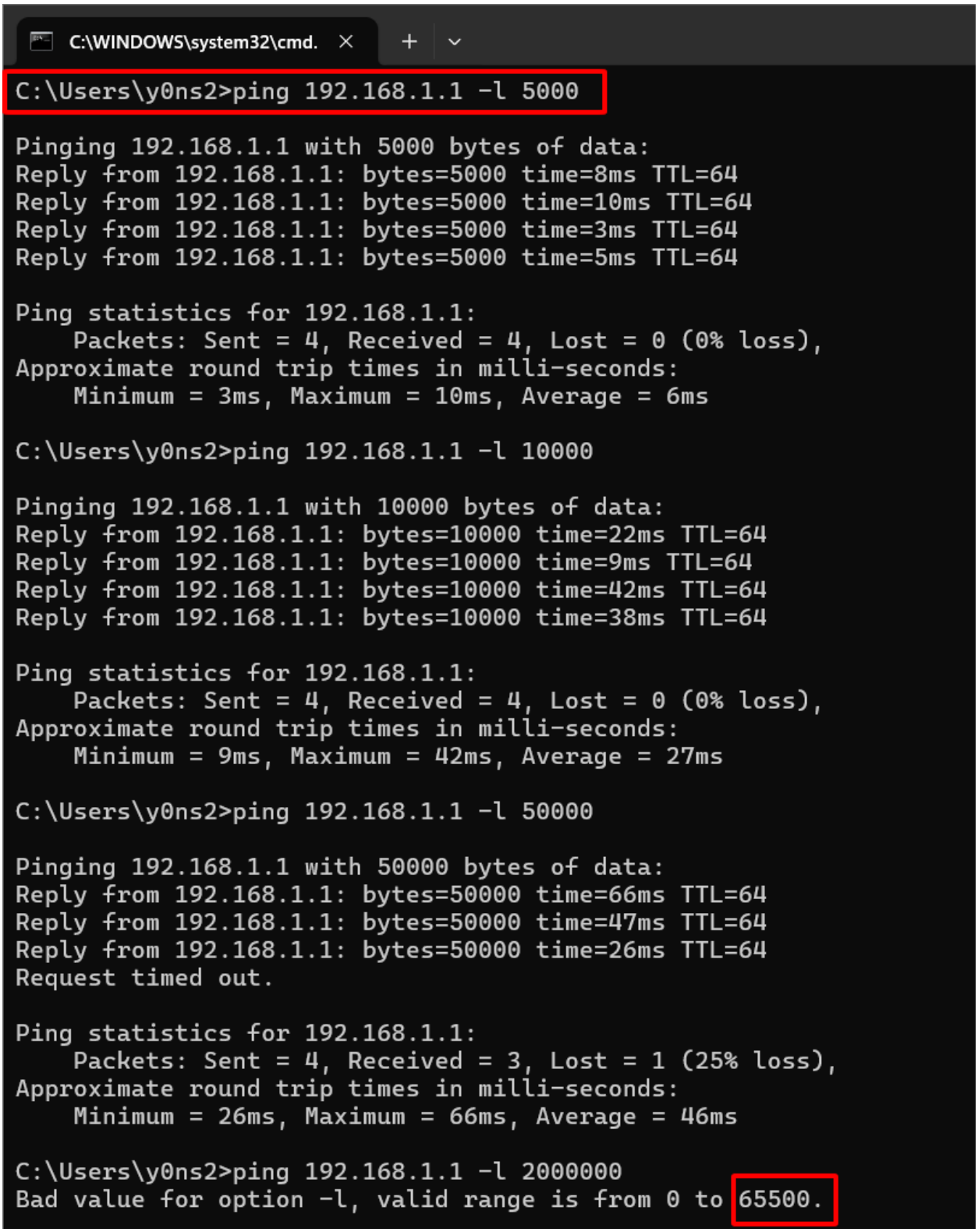
OSI gồm 7 tầng



Demo việc chuyển gói tin

```
C:\Users\y0ns2>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

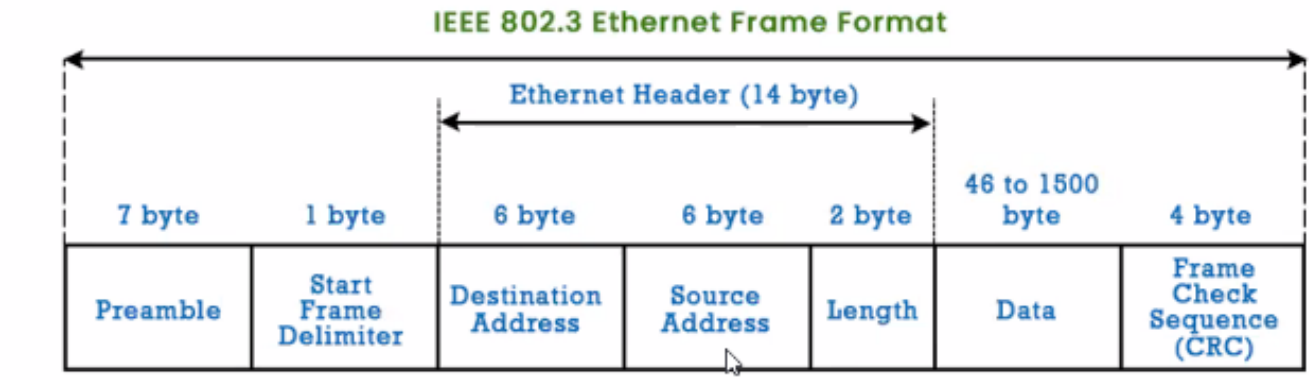
32 bytes


C:\WINDOWS\system32\cmd.
C:\Users\y0ns2>ping 192.168.1.1 -l 5000
Pinging 192.168.1.1 with 5000 bytes of data:
Reply from 192.168.1.1: bytes=5000 time=8ms TTL=64
Reply from 192.168.1.1: bytes=5000 time=10ms TTL=64
Reply from 192.168.1.1: bytes=5000 time=3ms TTL=64
Reply from 192.168.1.1: bytes=5000 time=5ms TTL=64
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 10ms, Average = 6ms
C:\Users\y0ns2>ping 192.168.1.1 -l 10000
Pinging 192.168.1.1 with 10000 bytes of data:
Reply from 192.168.1.1: bytes=10000 time=22ms TTL=64
Reply from 192.168.1.1: bytes=10000 time=9ms TTL=64
Reply from 192.168.1.1: bytes=10000 time=42ms TTL=64
Reply from 192.168.1.1: bytes=10000 time=38ms TTL=64
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 9ms, Maximum = 42ms, Average = 27ms
C:\Users\y0ns2>ping 192.168.1.1 -l 50000
Pinging 192.168.1.1 with 50000 bytes of data:
Reply from 192.168.1.1: bytes=50000 time=66ms TTL=64
Reply from 192.168.1.1: bytes=50000 time=47ms TTL=64
Reply from 192.168.1.1: bytes=50000 time=26ms TTL=64
Request timed out.
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 26ms, Maximum = 66ms, Average = 46ms
C:\Users\y0ns2>ping 192.168.1.1 -l 2000000
Bad value for option -l, valid range is from 0 to 65500.

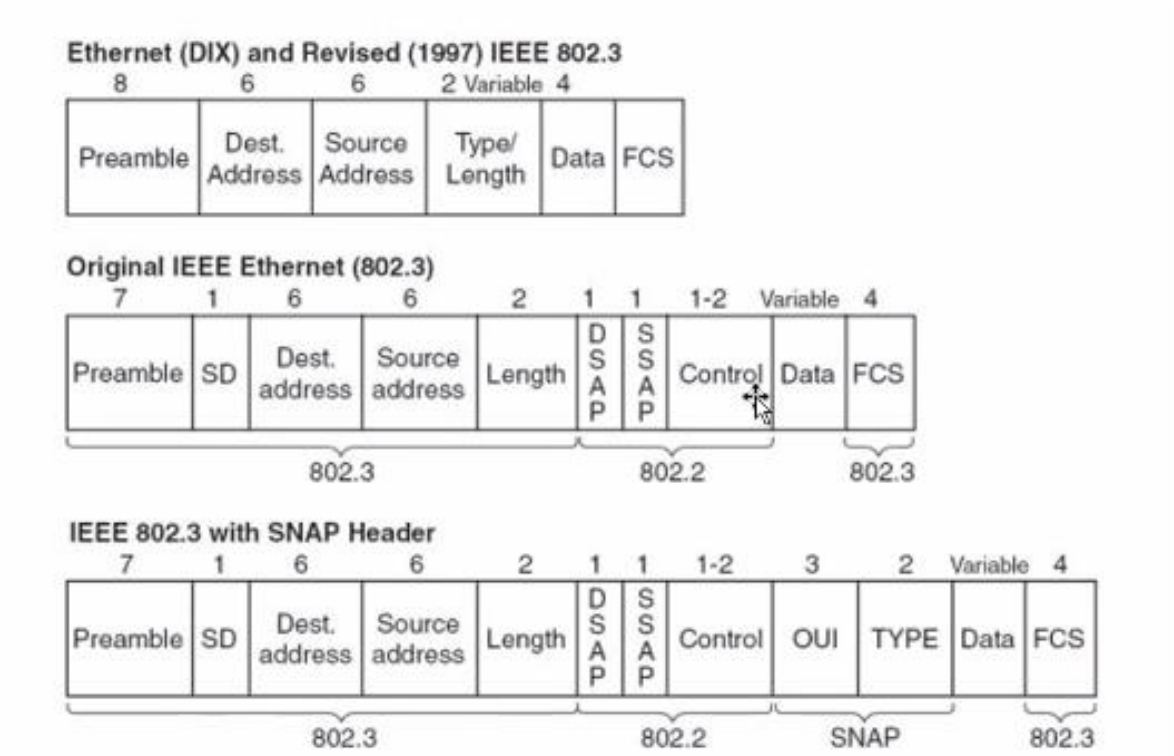
```
C:\Users\y0ns2>ping 192.168.1.1 -f -l 1000

Pinging 192.168.1.1 with 1000 bytes of data:
Reply from 192.168.1.1: bytes=1000 time=23ms TTL=64
Reply from 192.168.1.1: bytes=1000 time=2ms TTL=64
Reply from 192.168.1.1: bytes=1000 time=7ms TTL=64
Reply from 192.168.1.1: bytes=1000 time=4ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 23ms, Average = 9ms

C:\Users\y0ns2>ping 192.168.1.1 -f -l 2000

Pinging 192.168.1.1 with 2000 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\y0ns2>ping 192.168.1.1 -f -l 1472

Pinging 192.168.1.1 with 1472 bytes of data:
Reply from 192.168.1.1: bytes=1472 time=1ms TTL=64
Reply from 192.168.1.1: bytes=1472 time=3ms TTL=64
Reply from 192.168.1.1: bytes=1472 time=2ms TTL=64
Reply from 192.168.1.1: bytes=1472 time=5ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\Users\y0ns2>
```

kích thước dữ liệu lớn nhất để gửi

Kích thước khuôn



Chuẩn khác



Ping -l 2000

(2000 bytes)

Tính gói tin

2000 bytes + 8 (đầu ICMP) = 2008

2008 / 1480 = 1.3567

- ⇨ Cần 2 frame
- ⇨ Frame 1: 1480 (Phần dữ liệu) + 20 + 14 = 1514
- ⇨ Frame 2: 2008 – 1480 = 528 + 20 +14 = 562 bytes

Ping -l 1500

1500 bytes: 1500 + 8 = 1508 bytes

1508/1480 = 1,0189 => cần 2 Frame

Frame 1: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 2: 28+20+14 = 62 < 64 bytes

Frame 2: 64 bytes

1480 bytes dữ liệu (payload).

20 bytes IP header.

14 bytes Ethernet header.

4 bytes FCS (Frame Check Sequence).

14+4+1472 =1500

1472 là giá trị lớn nhất trong lệnh ping 192.168.1.1 -f -l 1472

Nếu lớn hơn giá trị này thì sẽ không truyền đi được gói tin nếu không phân mảnh

BÀI TẬP 30 PHÚT

a) **Ping x.x.x.x -l 7500**

b) **Ping x.x.x.x -l 5930**

c) **Lệnh ping có phần mảnh:**

- **Frame 1,2,3,4,5,6,7: 1518**
- **Frame 8: 800**

⇨ **Xác định kích thước dữ liệu**

Bài làm

a) Ping x.x.x.x -l 7500

Kích thước gói ping: 7500 bytes + 8 (đầu ICMP) = 7508

Tính số Frame: 7508/1480 = 5,072 => cần 6 Frame

Frame 1: 1480 + 20 (IP header) + 14 (Ethernet header) + 4 = 1518 bytes

Frame 2: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 3: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 4: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 5: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 6: 7508 - (1480*5) = 108 + 20 + 14 + 4= 146 bytes

b) Ping x.x.x.x -l 5930

Kích thước gói ping: 5930 bytes + 8 (đầu ICMP) = 5938 bytes

Tính số Frame: 5938/1480 = 4,012 => cần 5 Frame

Frame 1: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 2: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 3: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 4: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 5: 5938 – (1480*4) = 18 + 20 + 14 + 4 = 56 bytes

Mà 1 Frame tối thiểu 64 bytes nên cộng thêm vào cho đủ nên là 56 + 8 = 64 bytes

⇨ Vậy Frame 5: 64 bytes

c) Lệnh ping có phần mảnh:

- Frame 1,2,3,4,5,6,7: 1518
- Frame 8: 800

⇨ Xác định kích thước dữ liệu

Frame 1: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 2: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 3: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 4: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 5: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 6: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 7: 1480 + 20 + 14 + 4 = 1518 bytes

Frame 8: 762 + 20 + 14 + 4 = 800 bytes

⇨ **Tổng kích thước tất cả các Frame: 11426 bytes**

⇨ Trong mỗi frame, tổng header (IP, Ethernet, FCS) chiếm: 20 + 14 + 4 = 38 bytes

⇨ Tổng kích thước dữ liệu:

- Frame 1-7 chứa: 1480 × 7 = 10360 bytes
- Frame 8 chứa: 762

⇨ **Tổng kích thước dữ liệu là:** 10360+762=11122 bytes