Thực hành Lập trình mạng

HW2

Nguyễn Thành Vinh 20225779

Bài 2 :

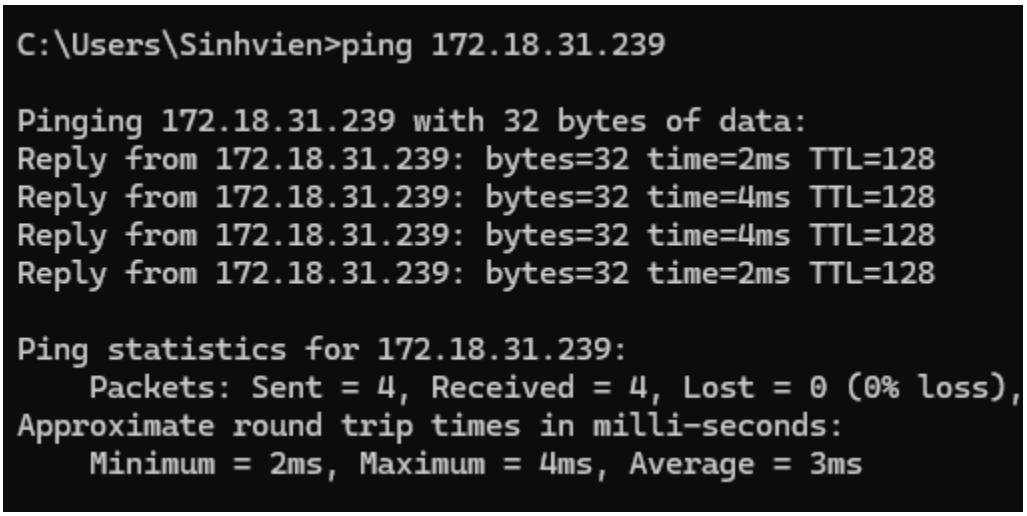
Câu 1 : Trình bày các bước (các lệnh) để thực hiện quá trình cấu hình mạng sao cho các máy nằm trong cùng một mạng đó.

- Bước 1 vào Control Panel → Network and Sharing Center
- Bước 2 chuột phải vào mạng mình dùng chọn properties
- Bước 3 chọn Internet Protocol Version 4 (TCP/IPv4) → Properties
- Bước 4 sau đó chọn Alternate Configuration rồi chọn UserConfig
- Bước 5 sau đó nhập
  Máy A : 172.18.36.249 Subnet: 255.255.255.0
  Máy B : 172.18.36.239 Subnet: 255.255.255.0
  Máy C : 172.18.36.192 Subnet: 255.255.255.0

Câu 2 : Em thực hiện lệnh nào để biết các máy đã được kết nối trong cùng một mạng?

Em thực hiện lênh : ping + ip của máy mà đã cấu hình cùng mạng với máy thực hiện lệnh

Vd : ping 172.18.36.239



Nếu thấy Reply from... thì các máy đã kết nối cùng mạng

Bài 3 : Cài đặt wireshark cho máy A. Thử kết nối giữa các máy. Quan sát màn hình wireshark của máy A khi được B và C thực hiện lệnh ping.

Thực hiện bắt các gói tin với wireshark:

- Ấn vào nút Capture
- Lựa chọn giao diện mạng (interface) phù hợp (chú ý: phải chọn đúng giao diện đang có kết nối giữa các máy)

Câu hỏi 3: Thực hiện lệnh ping giữa các máy. Những dòng thông tin nào trên cửa sổ wireshark cho thấy thông tin của lệnh ping đó?

- Lệnh **ping** sử dụng **ICMP (Internet Control Message Protocol)** nên sẽ thấy các dòng mà có **Protocol** là "ICMP" và **Info** là "Echo (ping) request" hoặc "Echo (ping) reply"

50	4.533272	172.18.31.239	172.18.31.249	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 51)
54	5.545233	172.18.31.239	172.18.31.249	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 55)
59	6.561479	172.18.31.239	172.18.31.249	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=128 (reply in 60)
61	7.578700	172.18.31.239	172.18.31.249	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=128 (reply in 62)
51	4.533494	172.18.31.249	172.18.31.239	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=128 (request in 50)
55	5.545431	172.18.31.249	172.18.31.239	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=128 (request in 54)
60	6.561673	172.18.31.249	172.18.31.239	ICMP	74	Echo (ping) reply id=0x0001, seq=17/4352, ttl=128 (request in 59)
62	7.578899	172.18.31.249	172.18.31.239	ICMP	74	Echo (ping) reply id=0x0001, seq=18/4608, ttl=128 (request in 61)

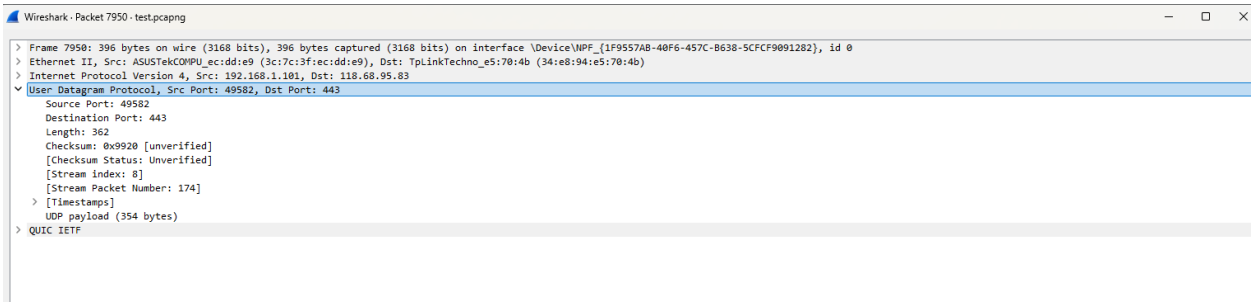
Câu hỏi 4: Dùng trình duyệt của máy đang chạy wireshark truy cập vào các trang web khác nhau. Những dòng thông tin nào trên cửa sổ wireshark cho thấy thông tin của quá trình duyệt web đó (các gói tin liên quan HTTP/HTTPS traffic).

- Nếu trang web HTTP (không mã hóa):
  - Cột Protocol hiển thị HTTP
  - Trong Info có dòng GET / HTTP/1.1

⇨ Đây là các gói tin yêu cầu/trả lời của quá trình duyệt web

- Nếu trang web HTTPS (mã hóa):
  - Cột Protocol hiển thị TLSv1.2 hoặc TLSv1.3
  - Quá trình bắt tay TLS : Client Hello, Server Hello\
  - Sau khi handshake xong, dữ liệu mã hóa sẽ hiển thị là Application Data (không đọc được nội dung)
  - Trước khi TLS diễn ra, luôn có 3 gói TCP handshake (SYN, SYN-ACK, ACK)

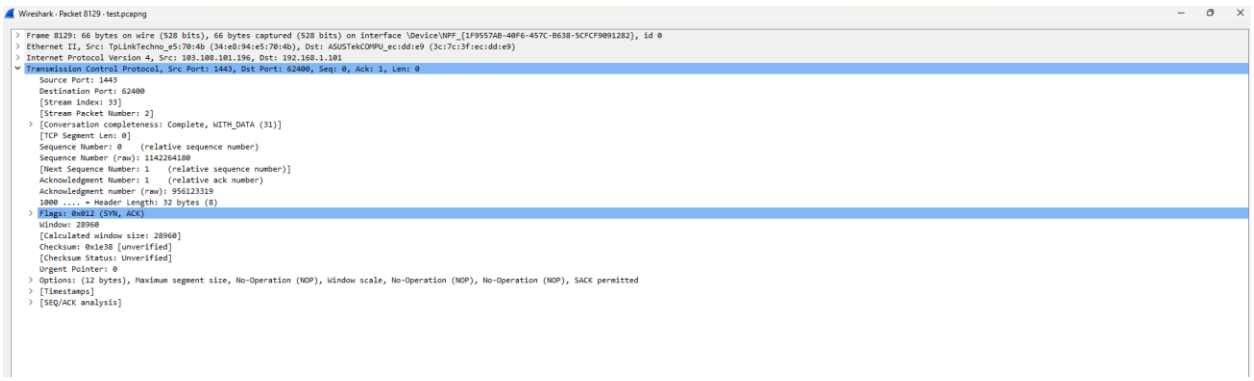
Câu hỏi 5: Quan sát UDP packet trên wireshark, phân tích về tính đơn giản của UDP. Gợi ý: không có kết nối, do đó không có cờ (flags) để thiết lập hoặc hủy kết nối.



- UDP header chỉ có 4 trường chính: Source Port, Destination Port, Length, Checksum
- Ko có cơ chế kết nối, Không có flags như SYN, ACK, FIN, Không đảm bảo tin cậy (không có xác nhận, không retransmission)

⇨ UDP rất đơn giản, nhẹ, nhanh, thích hợp cho ứng dụng thời gian thực (video call, game online)

Câu hỏi 6: Ấn vào trường thông tin TCP, quan sát sẽ thấy nhiều trường hơn so với UDP. Đó là những trường nào? Ý nghĩa của từng trường là gì?



- Sequence Number : Số thứ tự byte đầu tiên của dữ liệu trong gói tin, giúp sắp xếp lại dữ liệu theo đúng thứ tự
- Acknowledgment Number : Cho biết byte tiếp theo mà máy nhận mong đợi, Dùng để xác nhận đã nhận dữ liệu trước đó thành công
- Urgent Pointer : Chỉ vị trí dữ liệu “khẩn cấp” trong gói tin (khi URG = 1)
- Window : cho biết dung lượng bộ đệm (buffer) còn trống ở phía nhận, giúp kiểm soát luồng
- Header length : Độ dài header TCP
- Flags : điều khiển kết nối

Bài 4 : Trên máy A, nghiên cứu lựa chọn để sử dụng câu lệnh phân giải tên miền (ví dụ tên miền hust.edu.vn hoặc vnexpress.net), ghi lại địa chỉ IP tương ứng và so sánh kết quả nhiều lần phân giải

Khi chạy lệnh " nslookup hust.edu.vn " thì được kết quả

```
Name:    hust.edu.vn
Address:  202.191.59.134
```

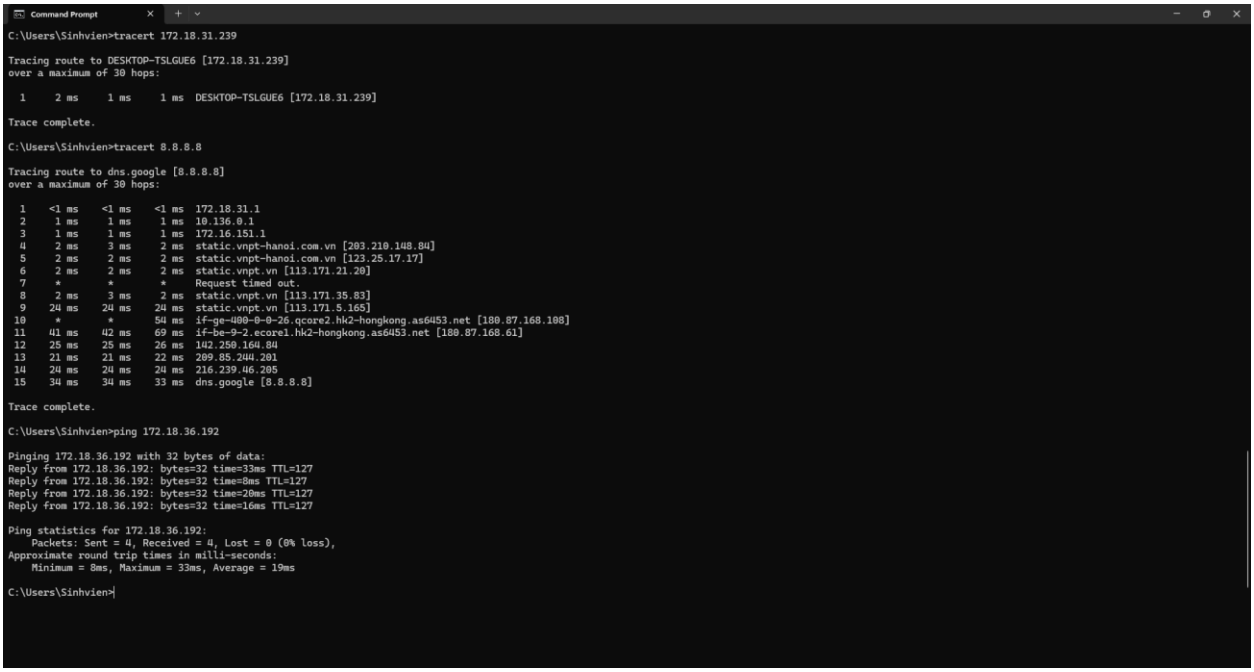
Câu hỏi 7: Khi dùng câu lệnh phân giải tên miền mà em đã lựa chọn thì thông tin nào trong output cho biết địa chỉ IP của tên miền?

- Khi dùng câu lệnh phân giải tên miền mà em đã lựa chọn thì thông tin của Address trong output cho biết địa chỉ IP của tên miền

Câu hỏi 8: Tại sao khi phân giải nhiều lần cùng tên miền, đôi khi kết quả trả về lại khác nhau?

- Có một số nguyên nhân chính:
    - Cơ chế Load Balancing (cân bằng tải) : Các trang lớn (như vnexpress.net, google.com) thường có nhiều server, mỗi lần phân giải DNS có thể trả về IP khác nhau để chia tải
    - CDN (Content Delivery Network) : DNS có thể trỏ đến server gần với vị trí địa lý vì vậy IP thay đổi theo lần phân giải và theo khu vực
    - DNS Cache & TTL (Time To Live) : Nếu bản ghi DNS hết hạn (TTL hết), khi phân giải lại thì DNS server sẽ trả về IP mới (có thể khác)
    - Anycast IP : Một số dịch vụ (ví dụ 8.8.8.8 của Google) dùng công nghệ Anycast: nhiều server dùng chung một IP, nhưng tuyến đường sẽ dẫn đến server gần nhất

Bài 5 : Sử dụng câu lệnh traceroute để hiển thị đường đi từ máy A đến máy B và máy C



Câu hỏi 9 : Output của lệnh traceroute thể hiện những gì? Giải thích ý nghĩa của từng cột trong kết quả (nếu có)

- Chỉ có 1 hop duy nhất → gói tin đi thẳng đến máy đích
- Các giá trị 2 ms, 1 ms, 1 ms là thời gian phản hồi ICMP (Round Trip Time).

Câu hỏi 10: Khi traceroute ra Internet (ví dụ đến 8.8.8.8) liệu có gì khác với mạng nội bộ không?

- Khi traceroute ra Internet (ví dụ đến 8.8.8.8) phải đi qua nhiều hop : có hop quốc tế, IP public, qua ISP → backbone → server đích, delay cao hơn và đôi khi có hop không trả lời.