Lab W2
Nguyễn Khánh Nam - 20225749

Bài 1: Cài đặt các máy kết nối cùng mạng.

- Chúng em đã làm nhóm và thực hiện trên cả 3 máy đều kết nối chung mạng của phòng Lab.
- Và 3 máy có địa chỉ IPv4 như sau:

  Máy A: 172.18.38.121

  Máy B: 172.18.38.127

  Máy C: 172.18.39.0

Bài 2: Cấu hình mạng cho các máy

- Câu hỏi 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. Em thực hiện lệnh nào để biết các máy đã được kết nối trong cùng một mạng?

+ Trong trường hợp cần thực hiện quá trình cấu hình mạng cho từng máy nằm trên cùng một mạng, cần để ý tới thông số subnet mask và dải địa chỉ IP mạng và thực hiện các lệnh sau trên từng máy:
Giả sử setup cho cả 3 máy nằm trên mạng có địa chỉ mạng 192.168.1.0 với X là 3 giá trị khác nhau từ 1 đến 254.

  sudo ifconfig eth0 192.168.1.X netmask 255.255.255.0 up

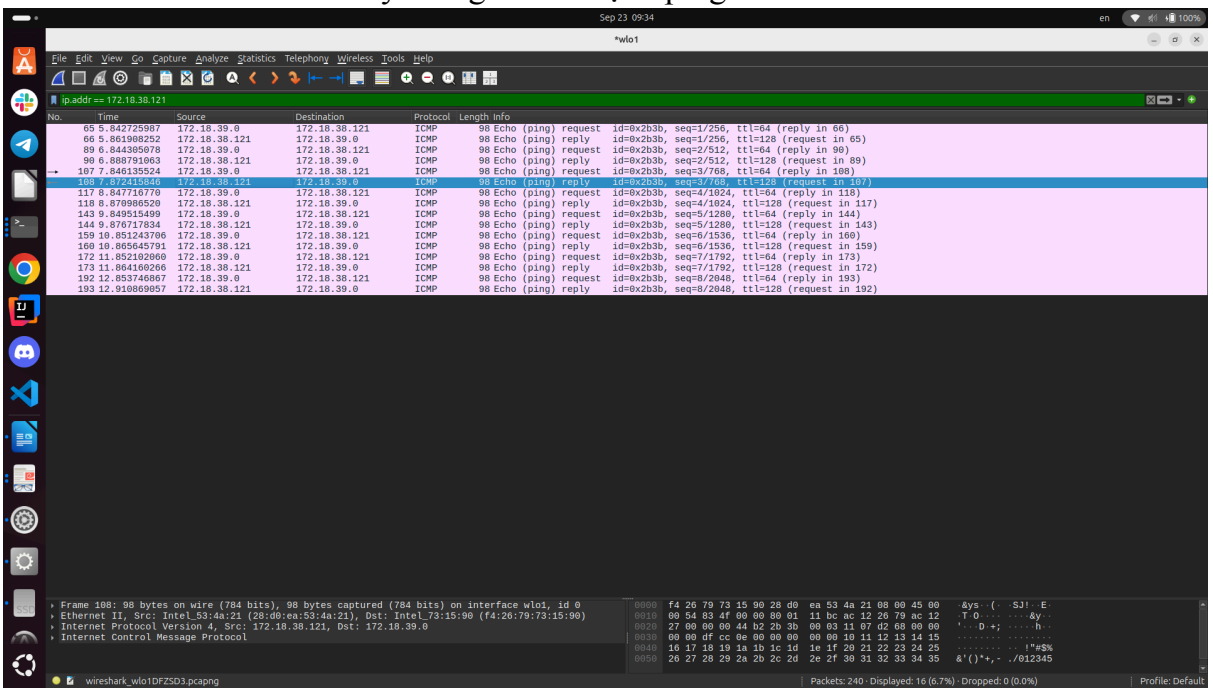
+ Để kiểm tra các máy đã kết nối trong cùng 1 mạng sử dụng lệnh ping đến từng địa chỉ IP của 3 máy host.

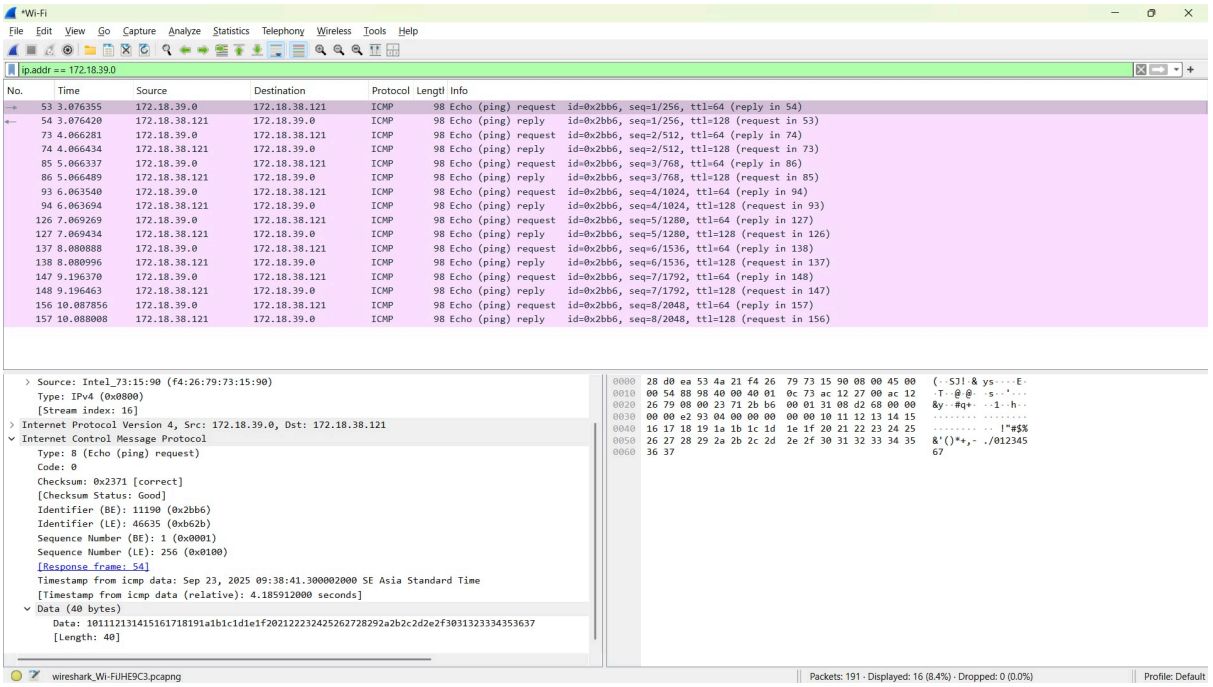
- Câu hỏi 2: Em thực hiện lệnh nào để biết các máy đã được kết nối trong cùng một mạng?

+ Để kiểm tra các máy đã kết nối trong cùng 1 mạng sử dụng lệnh ping đến từng địa chỉ IP của 3 máy host.

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.

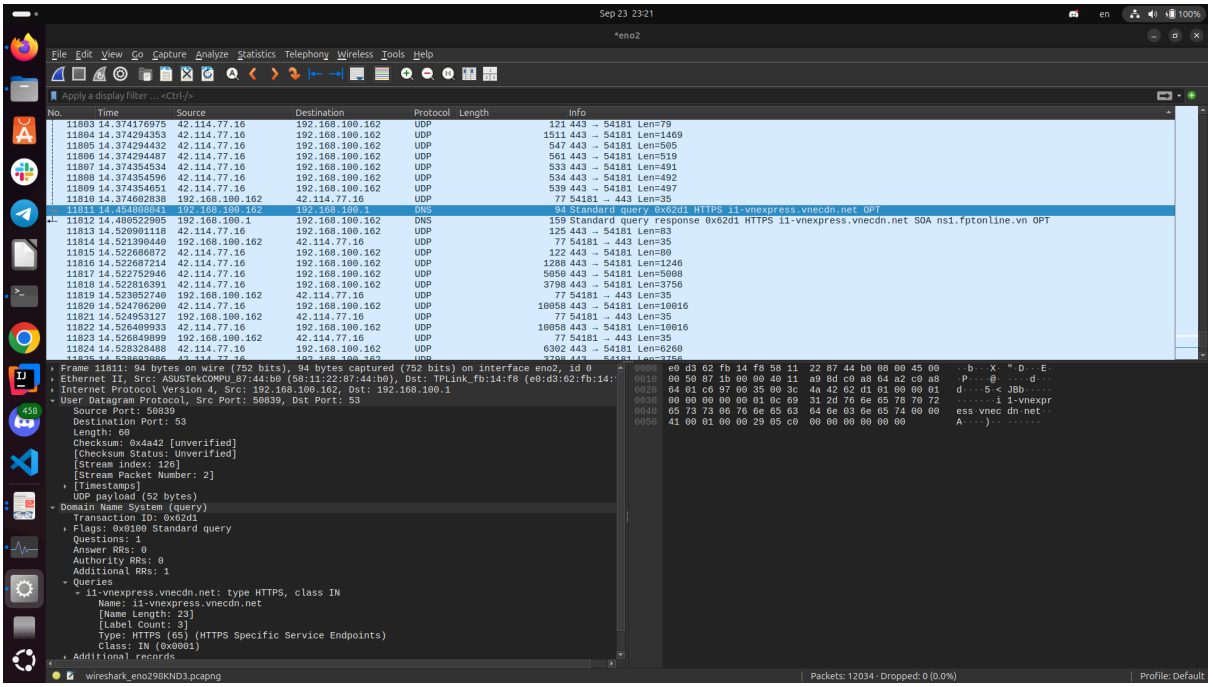
- Câu 3: Thực hiện lệnh ping giữa các máy. Những dòng thông tin nào trên cửa sổ wireshark cho thấy thông tin của lệnh ping đó?



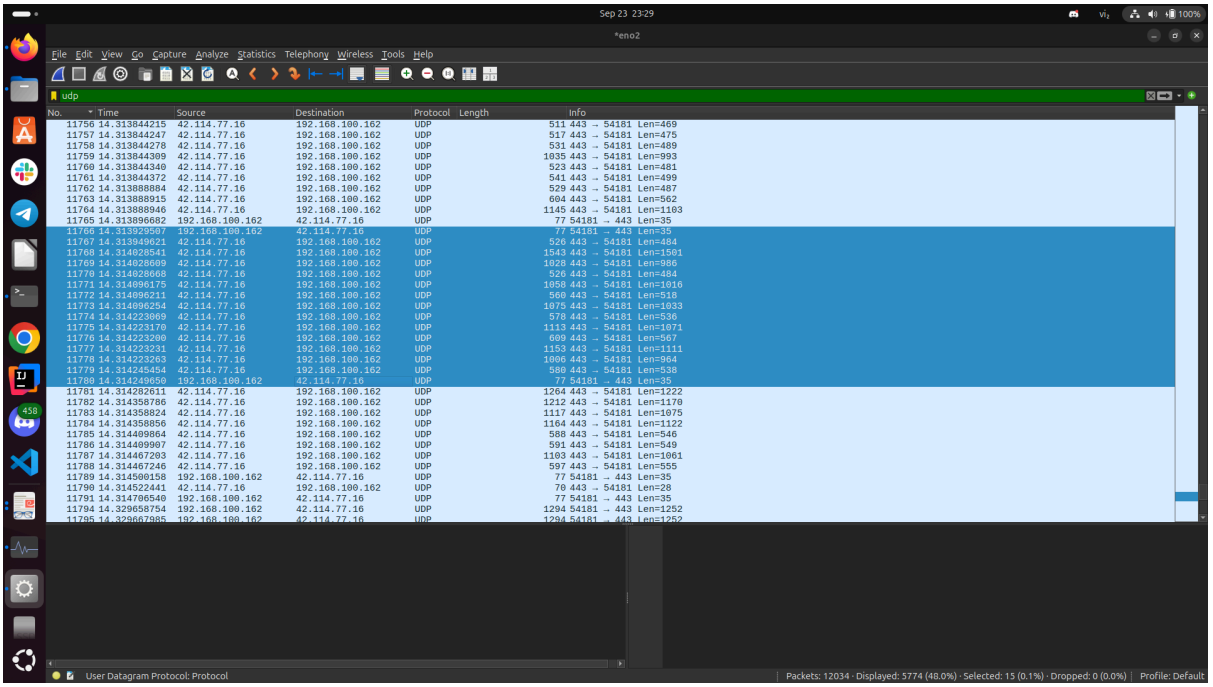


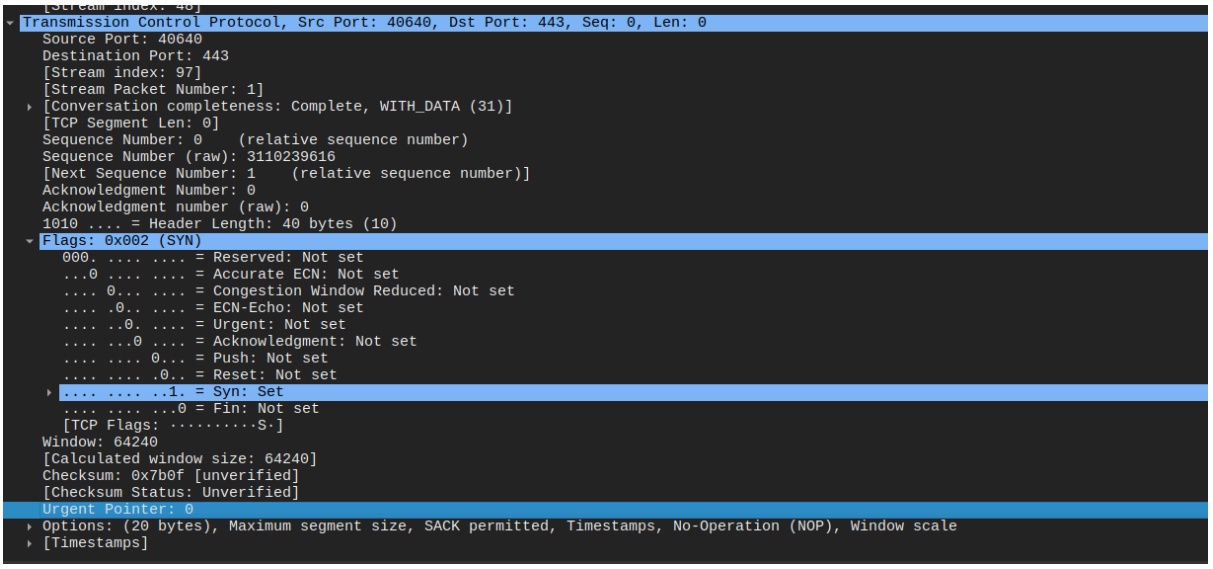
- Câu hỏi 4: Dùng trình duyệt của máy đang chạy wireshark truy cập vào các trang web khác nhau. Những dòng thông tin nào trên cửa sổ wireshark cho thấy thông tin của quá trình duyệt web đó (các gói tin liên quan HTTP/HTTPS traffic).

Web: https://vnexpress.net/



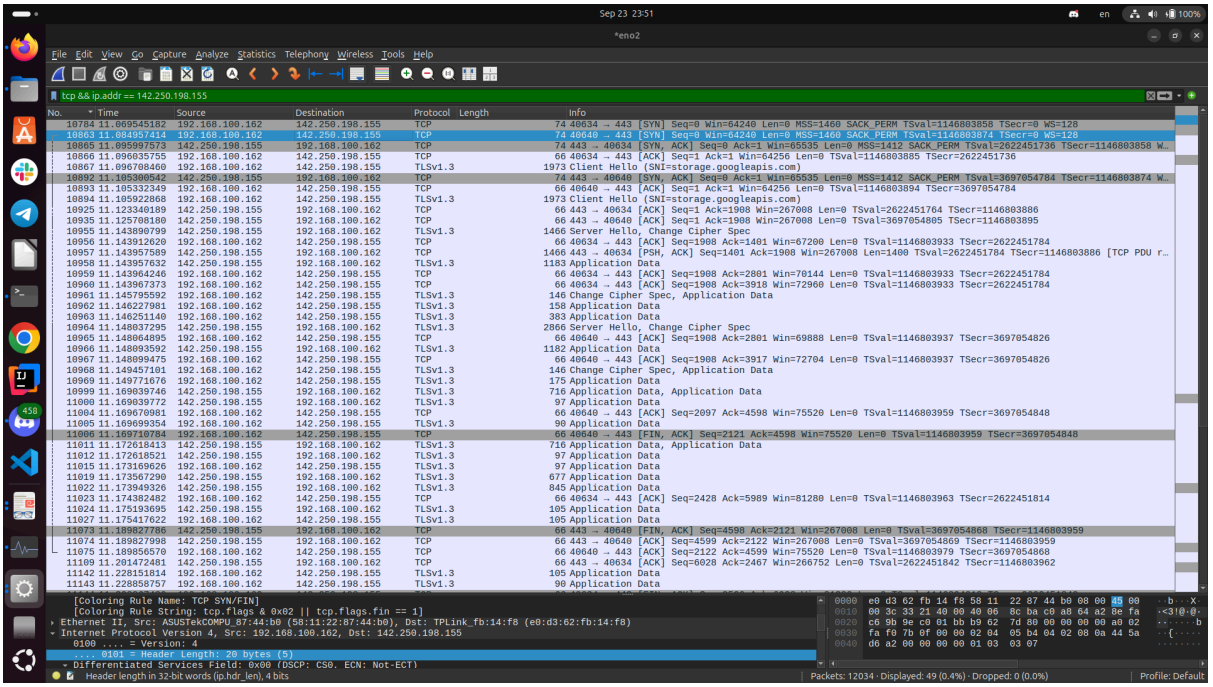
- Câu hỏi 5: Quan sát UDP packet trên wireshark, phân tích về tính đơn giản của UDP. Gợi ý: không có kết nối, do đó không có cờ (flags) để thiết lập hoặc hủy kết nối.

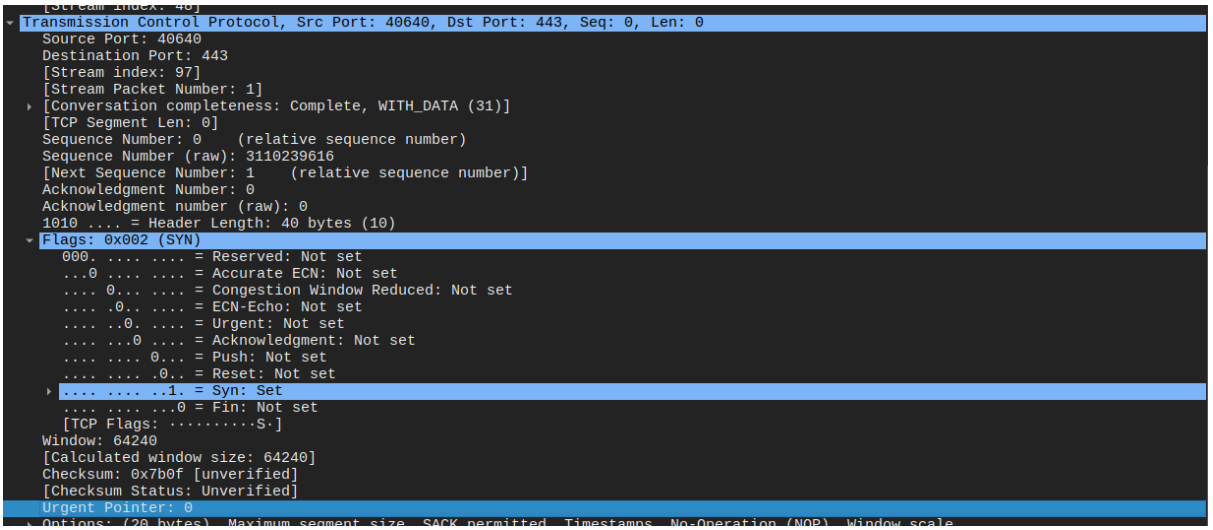




+ UDP không có cơ chế thiết lập hay hủy đường truyền kết nối
+ Không có cờ flags để đánh dấu trạng thái gói tin
+ UDP liên tục gửi gói tin đến đích nhưng không kiểm tra đích có nhận được hay không, nếu mất gói tin sẽ không tự truyền lại

- 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?





+ Trong TCP:

Source Port: Cổng nguồn của tiến trình gửi dữ liệu.

Destination Port: Cổng đích của tiến trình nhận dữ liệu.

Sequence Number: Đánh số thứ tự byte trong luồng dữ liệu TCP. Giúp đảm bảo dữ liệu đến đúng thứ tự và không bị trùng lặp.

Acknowledgment Number: Số thứ tự byte tiếp theo mà phía nhận mong đợi. Dùng để xác nhận đã nhận đủ dữ liệu từ bên kia.

Data Offset: Độ dài phần header TCP (tính bằng 32-bit word). Cho biết phần data bắt đầu từ đâu.

Reserved: Dành cho sử dụng trong tương lai, thường là 0.

Flags:

SYN: bắt đầu kết nối (handshake).
ACK: xác nhận dữ liệu.
FIN: kết thúc kết nối.
Reset: reset kết nối.
Push: yêu cầu đẩy dữ liệu lên ứng dụng ngay.
Urgent: đánh dấu dữ liệu khẩn cấp.
ECN - Echo /Congestion Window Reduced: liên quan điều khiển tắc nghẽn.

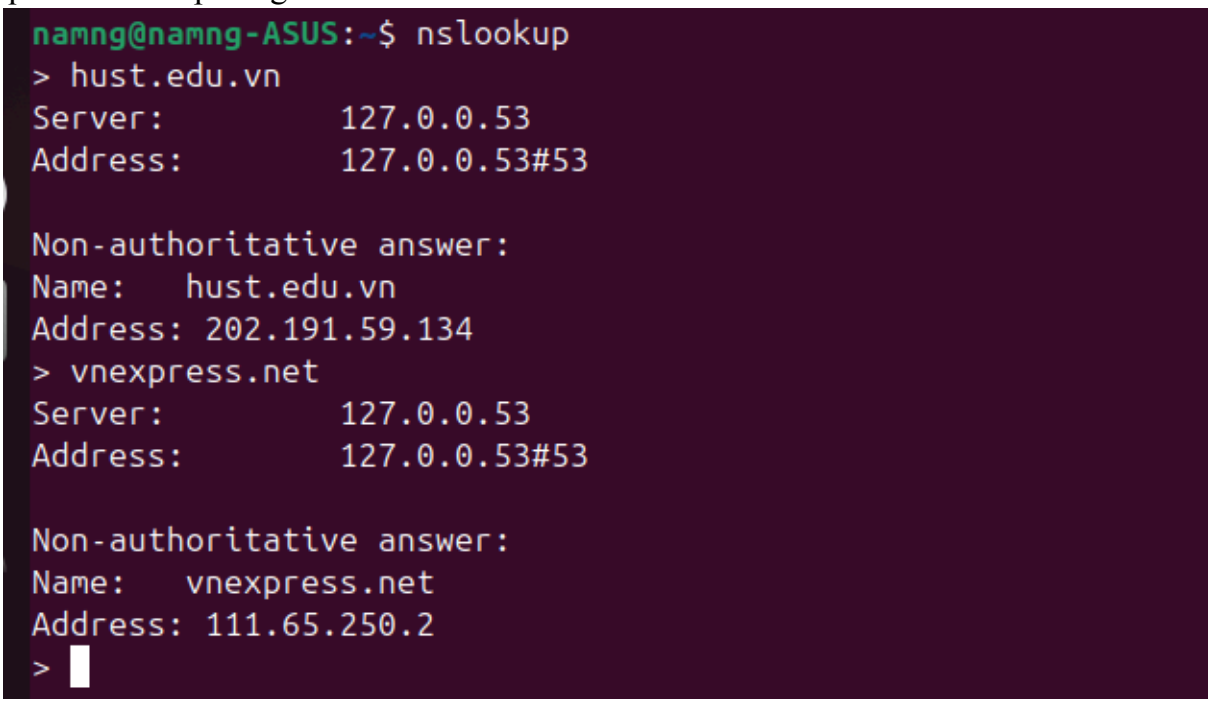
Window Size: Cho biết dung lượng buffer phía nhận còn trống. Dùng để điều khiển luồng dữ liệu (flow control).

Checksum: Kiểm tra lỗi TCP header và data.

Urgent Pointer: Nếu cờ Urgent = 1, chỉ định byte dữ liệu nào là khẩn cấp.

Options: Một số tùy chọn mở rộng:

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



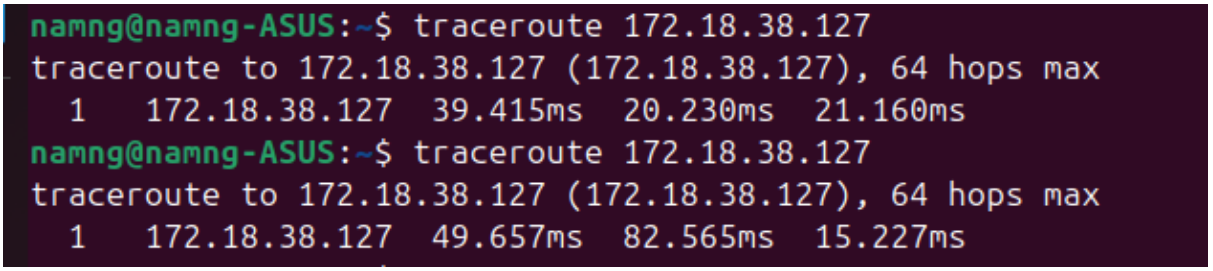
- Câu hỏi 7: Khi dùng câu lệnh phân giải tên miền mà em đã lựa chọn thì thông tin nào trong output cho biết địa chỉ IP của tên miền?

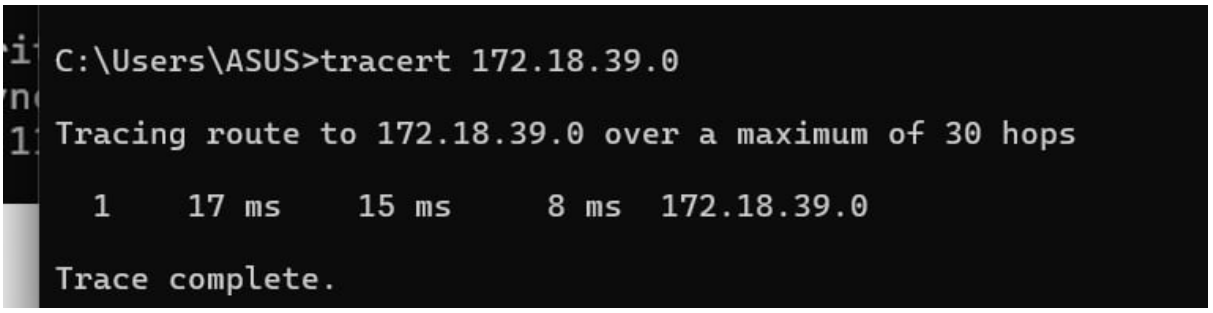
+ Thông tin Address.

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

+ Do có DNS load balancing cân bằng tải cho server của các máy chủ dịch vụ lớn có nhiều truy cập nên để tránh quá tải cho 1 máy chủ thì cần đổi sang IP của các máy chủ khác
+ Ngoài ra còn có giá trị TTL (Time To Live) cho mỗi địa chỉ IP nên việc phân lại địa chỉ IP khác là do có giá trị TTL hết hạn

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)

Địa chỉ đích: 172.18.38.127

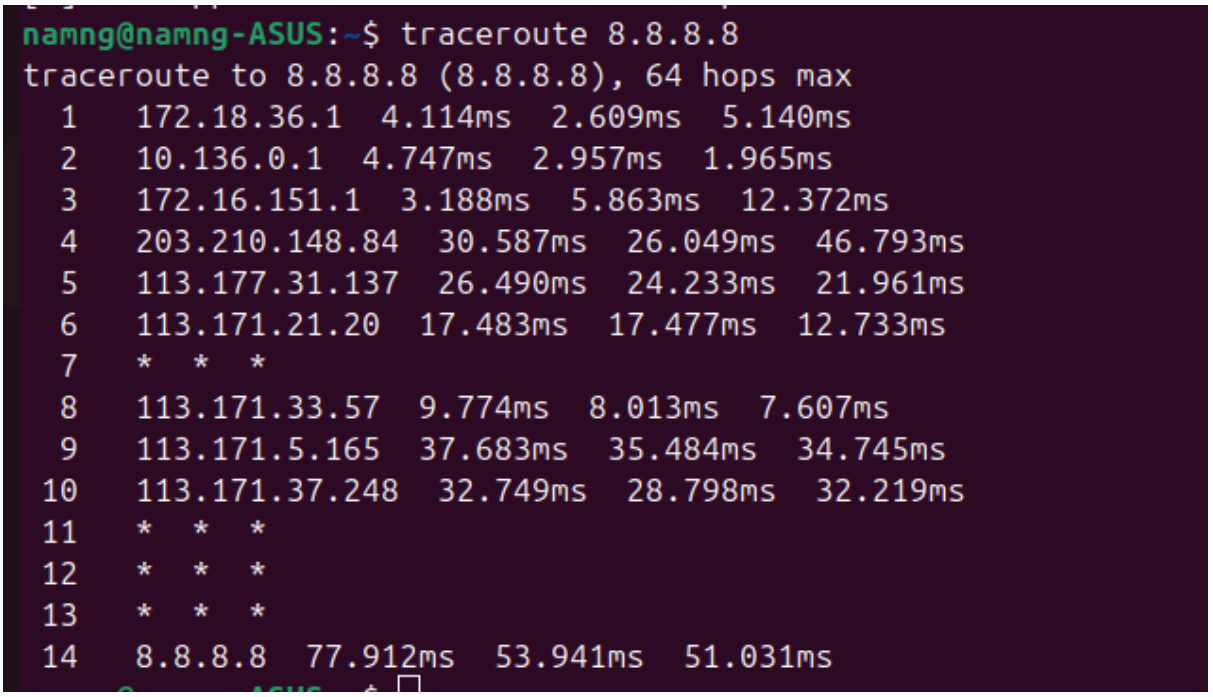
Số hop tối đa: 64 (mặc định traceroute gửi gói với TTL từ 1- 64).

Cột 1 (hop number): số thứ tự hop → ở đây là 1 nghĩa là gói đến đích ngay ở hop đầu tiên (cùng subnet, không phải qua router trung gian).

Cột 2 (IP hoặc hostname): địa chỉ của router/host ở hop đó → ở đây là 172.18.38.127 (chính là IP đích).

Các cột sau (thời gian ms): 3 lần đo RTT (Round-Trip Time) cho 3 gói probe mà traceroute gửi đi. Ví dụ: 39.415ms, 20.230ms, 21.160ms là thời gian đi-về cho mỗi gói.

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



+ Nhiều hop trung gian
    - Mỗi hop là một router hoặc gateway ISP/Internet backbone.

+ Thời gian RTT tăng dần
    - Hop gần thì ~2–5ms.
    - Hop xa hơn thì lên 20–40ms.
    - Phản ánh độ trễ tích lũy khi đi qua nhiều router và khoảng cách vật lý xa hơn.

+ Có dấu * (timeout) ở một số hop (Không trả lời)