**BÀI TẬP TUẦN 2 – IT4062**

Họ và tên: Đoàn Nhật Quang

MSSV: 20225911

Mã lớp: 161266

*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.*

- Bước 1: Kiểm tra card mạng, trên terminal gõ lệnh “ifconfig” để xem tên card mạng

**A screenshot of a computer

AI-generated content may be incorrect.**

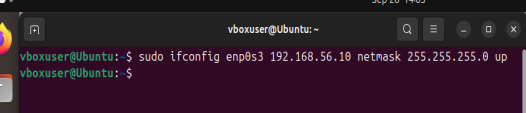
- Bước 2: Gán địa chỉ IP tĩnh cho từng máy (cùng subnet, khác số cuối)

A computer screen with numbers

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



- Bước 3: Kiểm tra lại IP đã gán, dùng lệnh “ifconfig”

A screenshot of a computer

AI-generated content may be incorrect.

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

- Dùng lệnh ping để kiểm tra kết nối giữa các máy

A screenshot of a computer screen

AI-generated content may be incorrect.

A screen shot of a computer program

AI-generated content may be incorrect.

- Như hình trên, đã có phản hồi, chứng minh các máy đã kết nối thành công trong cùng mạng

*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?*

- Các dòng có **Protocol = ICMP**, với nội dung **Echo (ping) request** và **Echo (ping) reply** trong cột Info, chính là gói tin ping giữa các máy. Như hình sau là khi ta thực hiện lệnh ping từ máy có IP 192.168.56.11 đến máy có IP 192.168.56.10

A screenshot of a computer

AI-generated content may be incorrect.

*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).*

A screen shot of a computer

AI-generated content may be incorrect.

- Khi máy A (IP 10.0.2.15 – IP khác so với trước đó do ở network của máy ảo Ubuntu đã chuyển từ Internal Network sang NAT) truy cập một website, Wireshark đã bắt được gói tin có giao thức HTTP.

- Trong gói tin này:

* IP nguồn (Source IP): 10.0.2.15
* IP đích (Destination IP): 34.107.221.82 (máy chủ web)
* Cổng nguồn (Source Port): 38842
* Cổng đích (Destination Port): 80 (cổng HTTP chuẩn)
* Phương thức HTTP: GET
* Resource yêu cầu: /canonical.html

- Ngoài ra, có gói trả lời từ server: HTTP/1.1 200 OK cho thấy web server đã phản hồi thành công.

=> Kết luận: Máy A đã gửi gói tin HTTP GET request đến server, chứng minh rằng nó đã thực hiện truy cập web thành công.

*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.*

A screenshot of a computer

AI-generated content may be incorrect.

- Không có kết nối (connectionless): UDP không cần quá trình bắt tay (3-way handshake) để thiết lập hay hủy kết nối như TCP. Mỗi gói được gửi độc lập.

- Không có flags (cờ điều khiển): Trong TCP có cờ SYN, ACK, FIN… để điều khiển kết nối. UDP hoàn toàn không có.

- Header rất ngắn (8 byte): Giúp giảm overhead, tốc độ truyền nhanh, thích hợp cho ứng dụng real-time.

- Không đảm bảo độ tin cậy: UDP không đảm bảo gói đến nơi, không có cơ chế kiểm soát luồng (flow control) hay phát hiện mất gói – cái này để ứng dụng tự xử lý.

*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?*

A screenshot of a computer

AI-generated content may be incorrect.

- Sequence Number (32 bits): Số thứ tự của byte đầu tiên trong gói tin này, dùng để sắp xếp lại dữ liệu.

- Acknowledgment Number (32 bits): Nếu cờ ACK bật, đây là số byte mà bên nhận mong đợi tiếp theo → cơ chế xác nhận.

- Flags (Control Bits) (9 bits): SYN: bắt đầu kết nối; ACK: xác nhận; FIN: kết thúc kết nối; RST: reset kết nối; PSH: đẩy dữ liệu ngay; URG: dữ liệu khẩn cấp.

- Window Size (16 bits): Dùng trong cơ chế kiểm soát luồng (flow control), cho biết bên nhận có thể nhận bao nhiêu byte tiếp theo.

- Urgent Pointer (16 bits): Chỉ ra byte cuối cùng của dữ liệu khẩn cấp (nếu URG flag bật).

- Options (nếu có, không bắt buộc): ví dụ như Window Scaling, Timestamps, MSS.

- Padding: căn chỉnh header về bội số của 32-bit.

*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?*

- Em dùng câu lệnh “dig vnexpress.net” để lấy địa chỉ IP từ output. Trong phần ANSWER SECTION sẽ chứa địa chỉ IP của tên miền

A screenshot of a computer

AI-generated content may be incorrect.

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

- DNS Round Robin: Nhiều website (như vnexpress.net, google.com) có nhiều server đặt ở nhiều nơi. DNS sẽ trả về các IP khác nhau để cân bằng tải.

- CDN (Content Delivery Network): Các dịch vụ lớn dùng CDN để đưa người dùng đến server gần nhất (theo địa lý). Vì vậy cùng một domain nhưng người ở Việt Nam sẽ nhận IP khác với người ở Mỹ.

- Caching và TTL (Time To Live): Bản ghi DNS có thời gian sống (TTL). Khi hết TTL, DNS server có thể trả về IP khác (server mới, hoặc cân bằng tải).

- Thay đổi hạ tầng DNS: Quản trị viên có thể thay đổi IP gắn với tên miền (ví dụ chuyển sang server khác), nên kết quả mới khác với lần cũ.

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

A screenshot of a computer screen

AI-generated content may be incorrect.

- Dòng đầu: thông báo đang traceroute tới địa chỉ đích (192.168.56.10 hoặc 192.168.56.12), giới hạn tối đa 30 hops, mỗi gói tin 60 byte.

- Cột 1: số thứ tự hop (ở đây chỉ có 1 hop → nghĩa là máy A có thể đi thẳng tới đích mà không qua router trung gian).

- Cột 2: địa chỉ IP (192.168.56.10 / 192.168.56.12) – chính là máy đích.

- 3 giá trị thời gian tiếp theo: round-trip time (RTT) tính bằng ms, kết quả của 3 gói tin gửi thử để đo độ trễ.

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

A screenshot of a computer

AI-generated content may be incorrect.

- Kết quả traceroute đến địa chỉ 8.8.8.8 (Google DNS) cho thấy:

* Ở hop 1: gói tin đi đến gateway (10.0.2.2), chính là router/gateway mặc định của máy ảo. Thời gian phản hồi khoảng 0.5 ms.
* Từ hop 2 trở đi: toàn bộ hiển thị \* \* \*. Điều này nghĩa là các router trung gian trên đường đi ra Internet không trả lời gói ICMP Time Exceeded hoặc bị chặn bởi chính sách bảo mật.

- Khác biệt so với traceroute trong mạng nội bộ:

* Trong mạng LAN, kết quả traceroute thường chỉ có 1–2 hop, thấy rõ IP đích và thời gian phản hồi rất thấp (vài ms).
* Khi ra Internet, gói tin phải đi qua nhiều router trung gian (của ISP, backbone, Google…). Tuy nhiên, một số router không phản hồi traceroute nên chỉ thấy \* \* \*. Vì vậy output dài hơn, nhiều dấu \*, và thường mất nhiều thời gian hơn.