Họ và tên: Phạm Thùy Trang

MSSV: 1050080159

Lớp: 10DH\_CNPM2

**LAB 1**

Trước khi bắt đầu thực hành, sinh viên hãy trả lời các câu hỏi sau:

**Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng (kèm ảnh minh họa).**

Các thiết bị mạng phổ biến gồm có:

* Router (Bộ định tuyến)
* Switch (Bộ chuyển mạch)
* Modem (Thiết bị điều chế/tách sóng)
* Access Point (AP) (Điểm truy cập không dây)
* Network Interface Card (NIC) (Card mạng)
* Hub (Bộ tập trung) Firewall (Tường lửa)



**Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?**

* Không thể truy cập các dịch vụ trực tuyến như email, mạng xã hội, học tập và làm việc trực tuyến.
* Gián đoạn trong các cuộc gọi hoặc hội nghị trực tuyến.
* Mất khả năng tra cứu thông tin trên Google hoặc các công cụ tìm kiếm.
* Ảnh hưởng đến các hệ thống IoT (nhà thông minh, thiết bị điều khiển từ xa, camera giám sát,...).
* Các ứng dụng yêu cầu Internet (game online, lưu trữ đám mây, dịch vụ phát trực tuyến,...) bị gián đoạn.

**Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là gì?**

* Hiểu được các khái niệm cơ bản về mạng máy tính và mô hình OSI.
* Biết cách thiết lập, cấu hình và bảo trì mạng cục bộ (LAN).
* Nắm được cách hoạt động của các giao thức mạng như TCP/IP, HTTP, FTP, DNS, DHCP.
* Có khả năng khắc phục các sự cố mạng đơn giản.
* Hiểu và áp dụng các nguyên tắc bảo mật mạng để bảo vệ dữ liệu và hệ thống.

1. Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?

A screenshot of a computer

AI-generated content may be incorrect.

2. Liệt kê ít nhất 5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol) khi không áp dụng bộ lọc “http” khi truy cập 2 website. Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.

- UDP (User Datagram Protocol): UDP là giao thức truyền tải không kết nối, cung cấp giao tiếp nhanh nhưng không đảm bảo độ tin cậy. Nó thường được sử dụng cho các ứng dụng yêu cầu tốc độ cao như phát trực tuyến (streaming), trò chuyện video, và trò chơi trực tuyến.

- ARP (Address Resolution Protocol): ARP là giao thức phân giải địa chỉ, dùng để chuyển đổi địa chỉ IP thành địa chỉ MAC trong một mạng cục bộ (LAN). Khi một thiết bị muốn giao tiếp với thiết bị khác trong cùng mạng, nó sử dụng ARP để tìm địa chỉ MAC của thiết bị đó.

- ICMP (Internet Control Message Protocol): ICMP được sử dụng để gửi thông điệp chẩn đoán và kiểm soát lỗi trong mạng, chẳng hạn như xác định xem một máy chủ có hoạt động hay không (dùng trong lệnh ping). Nó giúp quản trị viên kiểm tra và giám sát tình trạng mạng.

- TCP (Transmission Control Protocol): TCP là giao thức truyền tải có kết nối, đảm bảo dữ liệu được gửi đi một cách đáng tin cậy, không bị mất hoặc trùng lặp. Nó thường được sử dụng trong các ứng dụng yêu cầu tính toàn vẹn dữ liệu như trình duyệt web, email, và truyền tệp.

- mDNS (Multicast DNS): mDNS là một giao thức dùng để phân giải tên miền trong mạng cục bộ mà không cần máy chủ DNS trung tâm. Nó thường được sử dụng trong các thiết bị IoT, máy in, và hệ thống mạng gia đình để xác định thiết bị bằng tên thay vì địa chỉ IP.

3. Mất bao lâu từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận đối với mỗi website đã thử nghiệm. (mặc định, giá trị của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin).

Thời gian: 0.054912

4. Nội dung hiển thị trên trang web gaia.cs.umass.edu “Congratulations! You've downloaded the first Wireshark lab file!” có nằm trong các gói tin HTTP bắt được hay không? Nếu có, hãy tìm và xác định vị trí của nội dung này trong các gói tin bắt được.

Không

5. Địa chỉ IP của gaia.cs.umass.edu và website đã chọn ở bước 10 là gì? Địa chỉ IP của máy tính đang sử dụng là gì?

192.168.100.187

6. Qua ví dụ bắt gói tin trên và kết quả bắt gói tin từ Wireshark, hãy mô tả ngắn gọn diễn biến xảy ra khi bắt đầu truy cập vào một đường dẫn đến một trang web cho đến lúc xem được các nội dung trên trang web đó.

Khi truy cập một trang web, các bước diễn ra như sau (dựa trên kết quả bắt gói tin từ Wireshark):

1. Tra cứu DNS:
   * Máy tính gửi truy vấn DNS request để tìm địa chỉ IP của tên miền (ví dụ: gaia.cs.umass.edu).
   * Máy chủ DNS phản hồi với địa chỉ IP của trang web.
2. Thiết lập kết nối TCP (Three-way Handshake):
   * Máy tính gửi gói SYN đến máy chủ web.
   * Máy chủ phản hồi bằng gói SYN-ACK.
   * Máy tính gửi gói ACK, hoàn tất kết nối TCP.
3. Gửi yêu cầu HTTP/HTTPS:
   * Máy tính gửi gói HTTP GET yêu cầu nội dung trang web.
4. Máy chủ phản hồi HTTP:
   * Nếu thành công, máy chủ gửi gói HTTP 200 OK kèm theo nội dung trang web.
5. Tải và hiển thị nội dung:
   * Trình duyệt nhận dữ liệu HTML, CSS, JavaScript và các tài nguyên khác (hình ảnh, video…).
   * Nếu trang sử dụng HTTPS, quá trình TLS handshake diễn ra trước khi gửi/nhận dữ liệu.
6. Kết thúc kết nối:
   * Khi tải xong, kết nối TCP có thể được giữ hoặc đóng bằng gói FIN/ACK.