KHOA KỸ THUẬT VÀ CÔNG NGHỆ

**BỘ MÔN CÔNG NGHỆ THÔNG TIN**

****

**THỰC TẬP ĐỒ ÁN CƠ SỞ NGÀNH**

**HỌC KỲ I, NĂM HỌC 2024-2025**

**TÌM HIỂU VÀ MÔ PHỎNG QUÁ TRÌNH TRAO ĐỔI CÁC GÓI TIN TRONG GIAO THỨC ICMP**

*Sinh viên thực hiện:*

Nguyễn Nhựt Trường - 110122025

*Giáo viên hướng dẫn:*

Huỳnh Văn Thanh

***Trà Vinh, 29 tháng 12 năm 2024***

KHOA KỸ THUẬT VÀ CÔNG NGHỆ

**BỘ MÔN CÔNG NGHỆ THÔNG TIN**

****

**THỰC TẬP ĐỒ ÁN CƠ SỞ NGÀNH**

**HỌC KỲ I, NĂM HỌC 2024-2025**

**TÌM HIỂU VÀ MÔ PHỎNG QUÁ TRÌNH TRAO ĐỔI CÁC GÓI TIN TRONG GIAO THỨC ICMP**

*Sinh viên thực hiện:*

Nguyễn Nhựt Trường – 110122025

*Giáo viên hướng dẫn:*

Huỳnh Văn Thanh

***Trà Vinh, 29 tháng 12 năm 2024***

**NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN**

*Trà Vinh, ngày …… tháng …… năm ……*

**Giáo viên hướng dẫn**

*(Ký tên và ghi rõ họ tên)*

**NHẬN XÉT CỦA THÀNH VIÊN HỘI ĐỒNG**

*Trà Vinh, ngày …… tháng …… năm ……*

**Thành viên hội đồng**

*(Ký tên và ghi rõ họ tên)*

**LỜI CẢM ƠN**

Lời nói đầu, em xin gửi lời cảm ơn chân thành tới Thầy Huỳnh Văn Thanh, người đã tận tâm hướng dẫn và đồng hành cùng em trong quá trình thực hiện đề án cơ sở ngành.

Sự chỉ dẫn tận tình, những kiến thức quý báu và sự khích lệ mà thầy đã dành cho em không chỉ giúp em hoàn thành đề án mà còn mở ra nhiều góc nhìn mới, tiếp thêm động lực mà niềm đam mê trong học tập cũng như nghiên cứu.

Em thực sự biết ơn những giờ phút Thầy đã dành ra để giải đáp thắc mắc, góp ý chỉnh sửa, và truyền đạt kinh nghiệm quý giá. Thành quả em đạt được ngày hôm nay là nhờ vào sự hỗ trợ và tâm huyết của Thầy.

Một lần nữa, em xin kính chúc Thầy thật nhiều sức khỏe, niềm vui và thành công trong sự nghiệp giảng dạy. Em hy vọng sẽ tiếp tục được học hỏi từ Thầy trong những chặng đường sắp tới.

Xin chân thành cảm ơn Thầy.

TràVinh, 29 Tháng 12 năm 2024

**Nguyễn Nhựt Trường**

**MỤC LỤC**

[CHƯƠNG 1: TỔNG QUAN VỀ MẠNG MÁY TÍNH 8](#_Toc24937)

[1.1. Mạng máy tính là gì? 8](#_Toc22846)

[1.2. Phân loại mạng máy tính. 8](#_Toc14659)

[1.2.1. Diện Tích Phủ Sóng: 8](#_Toc13144)

[1.2.2. Cấu trúc kết nối: 8](#_Toc25759)

[1.2.3. Phương thức truyền tải dữ liệu: 8](#_Toc26724)

[1.3. Các thành phần cơ bản trong mạng máy tính 8](#_Toc29626)

[1.3.1. Thiết bị kết nối. 8](#_Toc13685)

[1.3.2. Thiết bị mạng. 9](#_Toc3582)

[1.3.3. Phương tiện truyền dẫn. 9](#_Toc4203)

[1.3.4. Giao thức mạng. 9](#_Toc30071)

[1.3.5. Phần mềm mạng. 9](#_Toc4103)

[1.4. Mô hình tham chiếu OSI và TCP/IP. 9](#_Toc30506)

[1.4.1. Mô Hình Tham Chiếu OSI (Open Systems Interconnection): 9](#_Toc8568)

[1.4.2. Mô hình TCP/IP 10](#_Toc14045)

[1.4.3. So Sánh OSI và TCP/IP: 10](#_Toc24436)

[CHƯƠNG 2: CÁC GIAO THỨC MẠNG PHỔ BIẾN 11](#_Toc31305)

[2.1. TCP/IP (Transmission Control Protocol/Internet Protocol) 11](#_Toc16170)

[2.1.1. Mô hình TCP/IP là gì? 11](#_Toc30427)

[2.1.2. Cách thức hoạt động của TCP/IP. 11](#_Toc10621)

[2.2. UDP (User Datagram Protocol) 11](#_Toc32357)

[2.2.1. UDP là gì? 11](#_Toc2930)

[2.2.2. Cách UDP hoạt động 12](#_Toc2672)

[2.2.3. Cấu trúc UDP Header 13](#_Toc32438)

[2.3. HTTP/HTTPS (Hypertext Transfer Protocol / Secure) 13](#_Toc25361)

[2.3.1. HTTP là gì? 13](#_Toc29605)

[2.3.2. Cách thức hoạt động của HTTP. 14](#_Toc17774)

[2.4. FTP (File Transfer Protocol) 14](#_Toc20538)

[2.4.1. FTP là gì? 14](#_Toc20304)

[2.4.2. Cách hoạt động của FTP. 14](#_Toc21455)

[2.5. DHCP (Dynamic Host Configuration Protocol) 15](#_Toc24702)

[2.5.1. DHCP là gì? 15](#_Toc19868)

[2.5.2. Cách thức hoạt động của DHCP. 15](#_Toc26546)

[2.6. SNMP (Simple Network Management Protocol) 16](#_Toc25675)

[2.6.1. SNMP là gì? 16](#_Toc100)

[2.6.2. Các thành phần của SNMP 17](#_Toc24353)

[2.6.3. Cách SNMP hoạt động 18](#_Toc12224)

[2.7. SSL/TLS (Secure Sockets Layer / Transport Layer Security) 19](#_Toc9616)

[2.7.1. Giao thức SSL/TLS là gì 19](#_Toc17028)

[2.7.2. SSL/TLS hoạt động như thế nào? 20](#_Toc6810)

[2.8. IPSec (Internet Protocol Security) 20](#_Toc15950)

[2.8.1. IPSec là gì? 20](#_Toc29349)

[2.8.2. Cơ chế hoạt động của IPSec. 21](#_Toc32249)

[CHƯƠNG 3: NỘI DUNG NGHIÊN CỨU 23](#_Toc3807)

[3.1. Quá trình đóng gói dữ liệu để truyền tải trong mạng qua mô hình tham chiếu OSI. 23](#_Toc32698)

[3.1.1. mô hình OSI. 23](#_Toc19958)

[3.1.2. Quá trình dữ liệu được đóng gói qua từng lớp trong mô hình OSI. 23](#_Toc7822)

[3.2. một số giao thức mạng phổ biến hoạt động ở mỗi lớp trong mô hình TCP/IP. 28](#_Toc25037)

[3.2.1. Giao thức mạng xếp theo lớp. 28](#_Toc1061)

[3.2.2. Tìm hiểu và phân tích giao thức ICMP. 38](#_Toc30542)

[3.2.3. So sánh ICMP với các giao thức cùng lớp để hiểu rõ hơn về vai trò của giao thức. 39](#_Toc29679)

[3.3. Nghiên cứu phần mềm phân tích mạng Wireshark 41](#_Toc3498)

[3.4. Mô phỏng và phân tích các thông tin trong các gói tin ICMP bằng Wireshark 42](#_Toc7124)

[3.4.1. Mô phỏng giao thức ICMP bằng một số phương pháp phổ biến: 44](#_Toc184)

[3.4.2. Phân tích gói tin. 45](#_Toc32658)

[CHƯƠNG 4: KẾT LUẬN 47](#_Toc10082)

[4.1. Kết quả đạt được: 47](#_Toc31756)

[4.2. Đánh giá và rút ra bài học: 47](#_Toc11823)

[4.3. Hướng phát triển tương lai: 47](#_Toc2578)

[DANH MỤC TÀI LIỆU THAM KHẢO 49](#_Toc22385)

**DANH MỤC HÌNH ẢNH**

[Hình 2.1. Mô hình giao thức TCP/IP 11](#_Toc3143)

[Hình 2.2. Nguyên lý hoạt đông của UDP 12](#_Toc3785)

[Hình 2.3. Cấu trúc UDP Header 13](#_Toc7634)

[Hình 2.4. Nguyên lý hoạt động của HTTP 14](#_Toc32570)

[Hình 2.5. Nguyên lý hoạt động của FTP 15](#_Toc30951)

[Hình 2.6. Cách thức hoạt động của DHCP 16](#_Toc5600)

[Hình 2.7. Các thành phần của SNMP 17](#_Toc13796)

[Hình 2.8. Cách SNMP hoạt động 18](#_Toc29245)

[Hình 2.9. Cấu Trúc của SSL/TLS 19](#_Toc9332)

[Hình 2.10. Cơ chế hoạt động cảu IPEec 21](#_Toc25270)

[Hình 3.1. Mô hình OSI 23](#_Toc18732)

[Hình 3.2. Mô hình OSI 24](#_Toc4684)

[Hình 3.3. Nguyên lý hoạt động của HTTP 29](#_Toc24792)

[Hình 3.4. Nguyên lý hoạt động của DNS 30](#_Toc22815)

[Hình 3.5. Nguyên lý hoạt động của TCP 31](#_Toc24443)

[Hình 3.6. Nguyên Lý Hoạt động của UDP 32](#_Toc28160)

[Hình 3.7. Ảnh minh họa giao thữc IP 33](#_Toc20501)

[Hình 3.8. Ảnh minh họa giao thức ICMP 33](#_Toc27037)

[Hình 3.9. Nguyên lý hoạt đông của Ethernet 34](#_Toc20497)

[Hình 3.10. Nguyên lý hoạt động của Wifi 35](#_Toc12497)

[Hình 3.11. Nguyên lý hoạt động của Point to Point 38](#_Toc15319)

[Hình 3.10. Cấu trúc Header của ICMP 38](#_Toc29674)

[Hình 3.11. Những card mạng đang có dữ liệu chạy qua 42](#_Toc23919)

[Hình 3.12. Nghiên cứu công cụ wireshark 43](#_Toc21521)

[Hình 3.13. Nghiên cứu công cụ wireshark 43](#_Toc23878)

[Hình 3.14. Mô phỏng giao thức ICMP 44](#_Toc9800)

[Hình 3.15. Thông báo gửi gói tin thành công 44](#_Toc22927)

[Hình 3.16. Lọc các gói tin ICMP 45](#_Toc8261)

[Hình 3.17. Kết quả lọc các gói tin 45](#_Toc18482)

[Hình 3.18. Chọn một gói tin để xem chi tiết 45](#_Toc17203)

[Hình 3.19. Chi tiết gói tin 46](#_Toc1283)

**DANH SÁCH BẢNG BIỂU**

[Bảng 3.1. Một số loại thông báo ICMP phổ biến 39](#_Toc10157)

[Bảng 3.2. so sánh định nghĩa và vai trò chính của ICMP, IP và ARP 40](#_Toc27103)

[Bảng 3.3. So sánh ICMP, IP và ARP 40](#_Toc28120)

[Bảng 3.4. So sánh ICMP, IP và ARP 41](#_Toc12270)

[Bảng 3.5. So sánh tổng quát ICMP, IP và ARP 41](#_Toc13979)

**MỞ ĐẦU**

**Lí do chọn đề tài:**

**- Tầm quan trọng của ICMP trong mạng máy tính**:

+ ICMP (Internet Control Message Protocol) là một giao thức quan trọng trong bộ giao thức TCP/IP, giúp quản lý và xử lý lỗi trong mạng. Hiểu rõ ICMP là nền tảng để đảm bảo mạng hoạt động ổn định và hiệu quả.

**- Khả năng ứng dụng thực tiễn cao**:

+ Việc nắm bắt cơ chế trao đổi gói tin ICMP giúp bạn hiểu rõ cách thức hoạt động của các công cụ phổ biến như ping và traceroute, từ đó áp dụng vào quản lý và chẩn đoán sự cố mạng.

- **Thách thức về phân tích và mô phỏng**:

+ ICMP tuy không phức tạp như TCP hay UDP, nhưng các thông điệp và cơ chế trao đổi gói tin của nó đặt ra thách thức trong việc hiểu rõ và mô phỏng chính xác, giúp nâng cao kỹ năng lập trình và tư duy phân tích.

- **Mở rộng kiến thức mạng máy tính**:

+ Nghiên cứu ICMP không chỉ cung cấp kiến thức chuyên sâu về giao thức này mà còn là cơ hội để hiểu cách các giao thức trong bộ TCP/IP tương tác và phối hợp với nhau.

- **Cơ hội cải thiện và tối ưu hóa mạng**:

+ Việc mô phỏng ICMP giúp bạn phát hiện và hiểu sâu hơn các vấn đề tiềm ẩn trong mạng, từ đó đề xuất các phương pháp cải thiện hiệu suất và bảo mật.

- Đóng góp vào bảo mật mạng:

+ ICMP thường bị khai thác trong các cuộc tấn công mạng, như ICMP flood hoặc ping of death. Nghiên cứu sâu về giao thức này giúp bạn nâng cao nhận thức về an ninh mạng và các biện pháp phòng chống.

**Mục đích chọn đề tài:**

**+** Tìm hiểu sâu về giao thức ICMP để hiểu rõ vai trò, cách thức hoạt động và ý nghĩa của nó trong hệ thống mạng.

+ Phát triển kỹ năng phân tích giao thức mạng và xây dựng các mô phỏng nhằm minh họa cách trao đổi gói tin ICMP trong môi trường thực tế.

+ Hiểu và sử dụng ICMP trong việc quản lý, giám sát và xử lý sự cố mạng, đồng thời nâng cao hiệu quả vận hành hệ thống mạng.

+ Nghiên cứu ICMP để phân tích và khắc phục các vấn đề như mất gói, lỗi định tuyến hoặc các sự cố khác trong hệ thống mạng.

+ Nhận biết các lỗ hổng có thể bị khai thác qua giao thức ICMP và nghiên cứu các biện pháp phòng chống hiệu quả.

+ Đề xuất các ý tưởng cải tiến dựa trên phân tích và mô phỏng giao thức ICMP, hỗ trợ nghiên cứu hoặc phát triển công nghệ mạng trong tương lai.

+ Hoàn thành nhiệm vụ nghiên cứu khoa học nhằm đáp ứng mục tiêu học tập và yêu cầu của môn học hoặc chương trình đào tạo.

**Đối tượng nghiên cứu:**

+ Quá trình đóng gói dữ liệu trong mô hình OSI: Nghiên cứu cách dữ liệu được đóng gói tại các lớp trong mô hình OSI, từ lớp ứng dụng đến lớp vật lý, và các quy trình liên quan đến việc truyền tải dữ liệu.

+ Các giao thức mạng trong mô hình TCP/IP: Tìm hiểu các giao thức phổ biến như HTTP, FTP, DNS (Lớp ứng dụng), TCP/UDP (Lớp vận chuyển), IP/ICMP (Lớp mạng), và Ethernet (Lớp liên kết dữ liệu) và cách chúng hỗ trợ truyền tải dữ liệu trong mạng.

+ Phần mềm Wireshark: Nghiên cứu cách sử dụng Wireshark để theo dõi, bắt và phân tích gói tin mạng, hiểu các thông tin chi tiết trong các gói tin ICMP và các giao thức khác.+ Gói tin ICMP và các loại thông điệp: Phân tích các gói tin ICMP, bao gồm các thông điệp như Echo Request, Echo Reply, và Destination Unreachable, để hiểu rõ cách thức hoạt động của chúng trong mạng.

+ Ứng dụng Wireshark trong phân tích mạng: Sử dụng Wireshark để mô phỏng và phân tích các gói tin ICMP, nghiên cứu cách công cụ này hỗ trợ trong việc chẩn đoán và xử lý sự cố mạng.

**Phạm vi nghiên cứu:**

+ Mô hình tham chiếu OSI: Nghiên cứu quá trình đóng gói và truyền tải dữ liệu qua các lớp trong mô hình OSI, từ lớp ứng dụng đến lớp vật lý.

+ Mô hình TCP/IP và các giao thức: Phân tích các giao thức mạng phổ biến như HTTP, TCP, IP, ICMP, và Ethernet, cùng cách chúng hoạt động ở từng lớp trong mô hình TCP/IP.

+ Wireshark: Sử dụng Wireshark để bắt và phân tích gói tin mạng, đặc biệt là gói tin ICMP.

+ Mô phỏng gói tin ICMP: Mô phỏng và phân tích các gói tin ICMP, như Echo Request và Echo Reply, bằng Wireshark để hiểu cấu trúc và xử lý sự cố mạng.

# TỔNG QUAN VỀ MẠNG MÁY TÍNH

## Mạng máy tính là gì?

- Mạng máy tính là một hệ thống bao gồm các máy tính được kết nối với nhau thông qua các phương tiện truyền dẫn (như dây cáp, sóng vô tuyến, hoặc quang học) để trao đổi dữ liệu và chia sẻ tài nguyên.

## Phân loại mạng máy tính.

Mạng máy tính có thể được phân loại dựa trên nhiều tiêu chí khác nhau. Dưới đây là một số cách phân loại phổ biến:

### Diện Tích Phủ Sóng:

- Mạng LAN (Local Area Network): Mạng cục bộ, phủ sóng trong một khu vực nhỏ như văn phòng, trường học.

- Mạng MAN (Metropolitan Area Network): Mạng đô thị, kết nối các mạng LAN trong một khu vực đô thị rộng lớn.

- Mạng WAN (Wide Area Network): Mạng diện rộng, kết nối các mạng LAN hoặc MAN ở các vị trí địa lý xa nhau, ví dụ như Internet.

- Mạng PAN (Personal Area Network): Mạng cá nhân, kết nối các thiết bị cá nhân trong phạm vi gần, như Bluetooth.

### Cấu trúc kết nối:

- Mạng Có Dây (Wired Network): Sử dụng cáp vật lý để kết nối các thiết bị.

- Mạng Không Dây (Wireless Network): Sử dụng sóng radio hoặc các công nghệ không dây khác để kết nối.

### Phương thức truyền tải dữ liệu:

- Mạng Điện Tử (Circuit Switching): Thiết lập kênh truyền cố định giữa các thiết bị trước khi truyền dữ liệu.

- Mạng Gói Tin (Packet Switching): Chia dữ liệu thành các gói tin và truyền qua các tuyến đường khác nhau.

## Các thành phần cơ bản trong mạng máy tính

### Thiết bị kết nối.

- Máy Tính và Thiết Bị Người Dùng: Máy tính cá nhân, điện thoại thông minh, máy in.

- Máy Chủ (Servers): Cung cấp dịch vụ như lưu trữ dữ liệu, máy chủ web, máy chủ email.

### Thiết bị mạng.

- Router: Chuyển tiếp dữ liệu giữa các mạng khác nhau.

- Switch: Kết nối nhiều thiết bị trong cùng một mạng LAN.

- Hub: Phát tín hiệu đến tất cả các cổng kết nối (ít được sử dụng hiện nay do hiệu quả thấp).

- Access Point: Kết nối các thiết bị không dây vào mạng có dây.

### Phương tiện truyền dẫn.

- Cáp Quang (Fiber Optic): Truyền dữ liệu với tốc độ cao và khoảng cách xa.

- Cáp Đồng (Copper Cable): Bao gồm cáp Ethernet, thường dùng trong mạng LAN.

- Truyền Thông Không Dây (Wireless Transmission): Wi-Fi, Bluetooth, và các công nghệ không dây khác.

### Giao thức mạng.

- TCP/IP: Bộ giao thức cơ bản cho Internet.

- HTTP/HTTPS: Dùng cho truyền tải dữ liệu web.

- FTP: Dùng để truyền tải tệp tin.

- SMTP/IMAP/POP3: Dùng cho dịch vụ email.

### Phần mềm mạng.

- Hệ Điều Hành Mạng: Quản lý và điều phối các tài nguyên mạng.

- Ứng Dụng Mạng: Dịch vụ như trình duyệt web, ứng dụng email.

## Mô hình tham chiếu OSI và TCP/IP.

### Mô Hình Tham Chiếu OSI (Open Systems Interconnection):

Mô hình OSI gồm 7 lớp, mỗi lớp thực hiện các chức năng cụ thể để đảm bảo truyền thông tin giữa các hệ thống mạng khác nhau.

- Lớp Vật Lý (Physical Layer): Chịu trách nhiệm truyền tải bit dữ liệu qua phương tiện truyền dẫn.

- Lớp Liên Kết Dữ Liệu (Data Link Layer): Đảm bảo truyền dữ liệu giữa hai thiết bị trực tiếp, xử lý lỗi truyền dẫn.

- Lớp Mạng (Network Layer): Quản lý việc định tuyến và chuyển tiếp gói tin giữa các mạng khác nhau.

- Lớp Giao Vận (Transport Layer): Đảm bảo truyền dữ liệu đáng tin cậy và kiểm soát luồng dữ liệu.

- Lớp Phiên (Session Layer): Quản lý các phiên làm việc giữa các ứng dụng.

- Lớp Trình Bày (Presentation Layer): Chuyển đổi dữ liệu giữa các định dạng khác nhau, mã hóa và giải mã.

- Lớp Ứng Dụng (Application Layer): Cung cấp giao diện cho các ứng dụng người dùng như email, web.

### Mô hình TCP/IP

Mô hình TCP/IP gồm 4 lớp, được thiết kế để hỗ trợ Internet và các mạng tương tự.

- Lớp Liên Kết (Link Layer): Kết hợp các chức năng của lớp Vật lý và lớp Liên kết Dữ liệu của mô hình OSI.

- Lớp Internet (Internet Layer): Tương đương với lớp Mạng của OSI, quản lý định tuyến và chuyển tiếp gói tin.

- Lớp Giao Vận (Transport Layer): Tương đương với lớp Giao Vận của OSI, bao gồm TCP và UDP để đảm bảo truyền dữ liệu.

- Lớp Ứng Dụng (Application Layer): Kết hợp các chức năng của các lớp Phiên, Trình Bày và Ứng dụng của OSI, bao gồm các giao thức như HTTP, FTP, SMTP.

### So Sánh OSI và TCP/IP:

- Số Lớp: OSI có 7 lớp, trong khi TCP/IP có 4 lớp.

- Mục Đích Thiết Kế: OSI được thiết kế như một mô hình lý thuyết để chuẩn hóa mạng, còn TCP/IP được thiết kế dựa trên thực tế và sự phát triển của Internet.

- Ứng Dụng Thực Tế: TCP/IP là bộ giao thức chính được sử dụng trên Internet, trong khi OSI thường được sử dụng như một công cụ học tập và tham chiếu.

# CÁC GIAO THỨC MẠNG PHỔ BIẾN

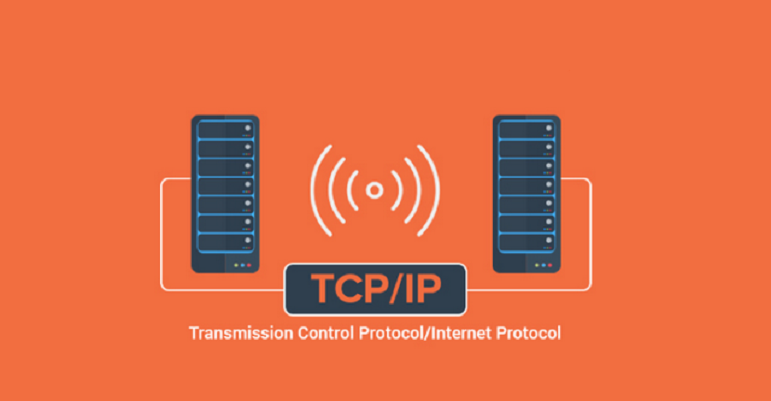
## TCP/IP (Transmission Control Protocol/Internet Protocol)

### Mô hình TCP/IP là gì?

- TCP/IP viết tắt của từ Transmission Control Protocol/Internet Protocol – Giao thức điều khiển truyền nhận/ Giao thức liên mạng. Đây là bộ các giao thức truyền thông được dùng để kết nối các thiết bị mạng trên [internet](https://vietnix.vn/internet-la-gi/" \t "https://vietnix.vn/tcp-ip-la-gi/_blank) với nhau. TCP/IP cũng có thể được dùng như một giao thức truyền thông trong [mạng máy tính](https://vietnix.vn/mang-may-tinh/" \t "https://vietnix.vn/tcp-ip-la-gi/_blank) nội bộ.

### Cách thức hoạt động của TCP/IP.

- Bộ giao thức TCP/IP áp dụng mô hình giao tiếp client-server, trong đó máy khách (client) nhận các dịch vụ (như truy cập trang web) từ một máy chủ (server) trong mạng. TCP/IP là sự kết hợp của hai giao thức như tên gọi. Trong đó, IP (Giao thức Liên mạng) chịu trách nhiệm chuyển các gói tin đến địa chỉ đích đã được xác định. Quy trình hoạt động của IP là thêm các thông tin chỉ đường vào các gói tin để chúng đến được đích quy định.



Hình 2.1. Mô hình giao thức TCP/IP

## UDP (User Datagram Protocol)

### UDP là gì?

-UDP (User Datagram Protocol) là một trong những giao thức cốt lõi của giao thức TCP/IP. Dùng UDP, chương trình trên mạng máy tính có thể gửi những dữ liệu ngắn được gọi là datagram tới máy khác. UDP không cung cấp sự tin cậy và thứ tự truyền nhận mà TCP làm; các gói dữ liệu có thể đến không đúng thứ tự hoặc bị mất mà không có thông báo. Tuy nhiên UDP nhanh và hiệu quả hơn đối với các mục tiêu như kích thước nhỏ và yêu cầu khắt khe về thời gian. Do bản chất không trạng thái của nó nên nó hữu dụng đối với việc trả lời các truy vấn nhỏ với số lượng lớn người yêu cầu.

-Những ứng dụng phổ biến sử dụng UDP như DNS (Domain Name System), ứng dụng streaming media, Voice over IP, Trivial File Transfer Protocol (TFTP), và game trực tuyến.

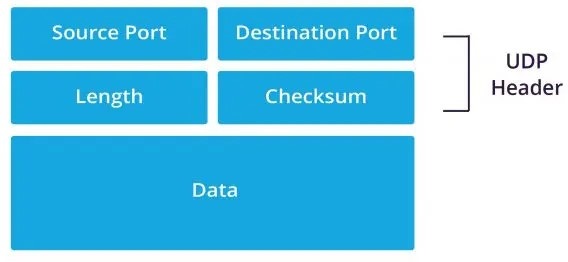
### Cách UDP hoạt động

-Giao thức UDP hoạt động tương tự như TCP, nhưng nó bỏ qua quá trình kiểm tra lỗi. Khi một ứng dụng sử dụng giao thức UDP, các gói tin được gửi cho bên nhận và bên gửi không phải chờ để đảm bảo bên nhận đã nhận được gói tin, do đó nó lại tiếp tục gửi gói tin tiếp theo. Nếu bên nhận bỏ lỡ một vài gói tin UDP, họ sẽ mất vì bên gửi không gửi lại chúng. Do đó thiết bị có thể giao tiếp nhanh hơn.



Hình 2.2. Nguyên lý hoạt đông của UDP

### Cấu trúc UDP Header



Hình 2.3. Cấu trúc UDP Header

- **Source port**: Số cổng của thiết bị gửi. Trường này có thể đặt là 0 nếu máy tính đích đến không cần trả lời người gửi.

- **Destination port**: Số cổng của thiết bị nhận.

- **Length**: Xác định chiều dài của toàn bộ datagram: phần header và dữ liệu. Chiều dài tối thiểu là 8 byte khi gói tin không có dữ liệu, chỉ có header.

**Checksum**: Kiểm tra lỗi của phần header và dữ liệu. Việc sử dụng checks.

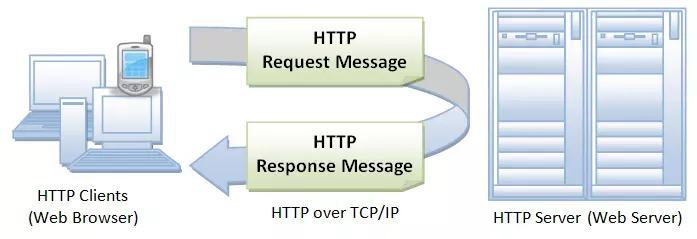
## HTTP/HTTPS (Hypertext Transfer Protocol / Secure)

### HTTP là gì?

- HTTP (HyperText Transfer Protocol - Giao thức truyền tải siêu văn bản) là một trong các giao thức chuẩn về mạng Internet, được dùng để liên hệ thông tin giữa Máy cung cấp dịch vụ (Web server) và Máy sử dụng dịch vụ (Web client), là giao thức Client/Server dùng cho World Wide Web – WWW

- HTTP là một giao thức ứng dụng của bộ giao thức TCP/IP (các giao thức nền tảng cho Internet).

### Cách thức hoạt động của HTTP.



Hình 2.4. Nguyên lý hoạt động của HTTP

- HTTP hoạt động dựa trên mô hình Client – Server. Trong mô hình này, các máy tính của người dùng sẽ đóng vai trò làm máy khách (Client). Sau một thao tác nào đó của người dùng, các máy khách sẽ gửi yêu cầu đến máy chủ (Server) và chờ đợi câu trả lời từ những máy chủ này.

- HTTP là một stateless protocol. Hay nói cách khác, request hiện tại không biết những gì đã hoàn thành trong request trước đó.

- HTTP cho phép tạo các yêu cầu gửi và nhận các kiểu dữ liệu, do đó cho phép xây dựng hệ thống độc lập với dữ liệu được truyển giao.

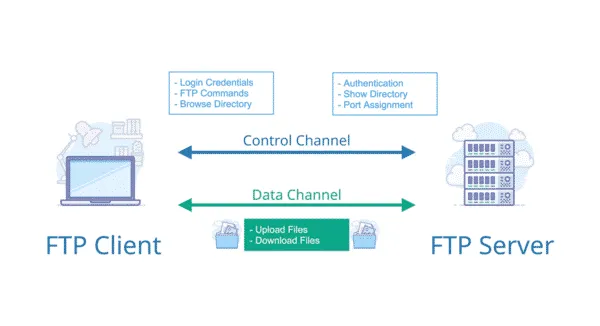
## FTP (File Transfer Protocol)

### FTP là gì?

- FTP viết tắt của từ File Transfer Protocol là giao thức truyền tải tập tin và được dùng trong việc trao đổi dữ liệu trong mạng thông qua giao thức [TCP/IP](https://vietnix.vn/tcp-ip-la-gi/" \t "https://vietnix.vn/ftp-la-gi/_blank) thường hoạt động với 2 cổng 20 và 21. Trong giao thức này, các máy client trong mạng có thể truy cập đến máy chủ FTP để gửi hoặc lấy dữ liệu. Và đặc biệt, người dùng có thể truy cập FTP để truyền và lấy dữ liệu từ xa.

### Cách hoạt động của FTP.

- FTP tồn tại như một trong những chương trình ban đầu để truy cập thông tin trên Internet rất lâu trước khi [HTTP](https://vietnix.vn/http-https-la-gi/" \t "https://vietnix.vn/ftp-la-gi/_blank) trở nên phổ biến để truy cập các trang web. Do đó, trình duyệt web trên PC của bạn, cũng như chương trình Windows Explorer hiển thị các file trên máy tính của bạn đã được sử dụng để truy cập các máy chủ FTP để lấy hoặc đặt các file từ xa.



Hình 2.5. Nguyên lý hoạt động của FTP

- **Control Connection**: Là phiên làm việc TCP logic đầu tiên được tạo ra khi quá trình truyền dữ liệu bắt đầu. Nhưng trong tiến trình này chỉ kiểm soát được các thông tin điều khiển đi qua nó. Quá trình này sẽ được duy trì trong suốt quá trình phiên làm việc diễn ra.

- **Data Connection**: Là một kết nối dữ liệu TCP được tạo ra với mục đích riêng là truyền dữ liệu giữa Client và Server. Quá trình truyền tải dữ liệu hoàn tất kết nối dữ liệu này sẽ tự động ngắt kết nối.

## DHCP (Dynamic Host Configuration Protocol)

### DHCP là gì?

- DHCP được viết tắt từ cụm từ [Dynamic Host Configuration Protocol](https://vi.wikipedia.org/wiki/DHCP) (có nghĩa là Giao thức cấu hình máy chủ). DHCP có nhiệm vụ giúp quản lý nhanh, tự động và tập trung việc phân phối địa chỉ IP bên trong một mạng. Ngoài ra DHCP còn giúp đưa thông tin đến các thiết bị hợp lý hơn cũng như việc cấu hình subnet mask hay cổng mặc định.

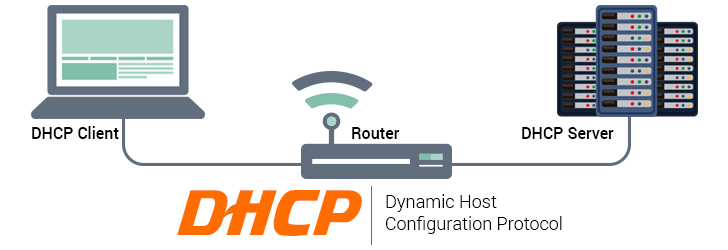
### Cách thức hoạt động của DHCP.

- Được giải thích một cách ngắn gọn nhất về cách thức hoạt động của DHCP chính là khi một thiết bị yêu cầu địa chỉ IP từ một router thì ngay sau đó router sẽ gán một địa chỉ IP khả dụng cho phép thiết bị đó có thể giao tiếp trên mạng.

- Như ở các hộ gia đình hay các doanh nghiệp nhỏ thì router sẽ hoạt động như một máy chủ DHCP nhưng ở các mạng lớn hơn thì DHCP như một máy chỉ ở vai trò là máy tính.

- Cách thức hoạt động của DHCP còn được giải thích ở một cách khác thì khi một thiết bị muốn kết nối với mạng thì nó sẽ gửi một yêu cầu tới máy chủ, yêu cầu này gọi là DHCP DISCOVER. Sau khi yêu cầu này đến máy chủ DHCP thì ngay tại đó máy chủ sẽ tìm một địa chỉ IP có thể sử dụng trên thiết bị đó tồi cung cấp cho thiết bị địa chỉ cùng với gói DHCPOFFER

- Khi nhận được IP thì thiết bị tiếp tục phản hồi lại máy chủ DHCP gói mang tên DHCPREQUEST. Lúc này là lúc chấp nhận yêu cầu thì máy chủ sẽ gửi tin báo nhận (ACK) để xác định thiết bị đó đã có IP, đồng thời xác định rõ thời gian sử dụng IP vừa cấp đến khi có địa chỉ IP mới.



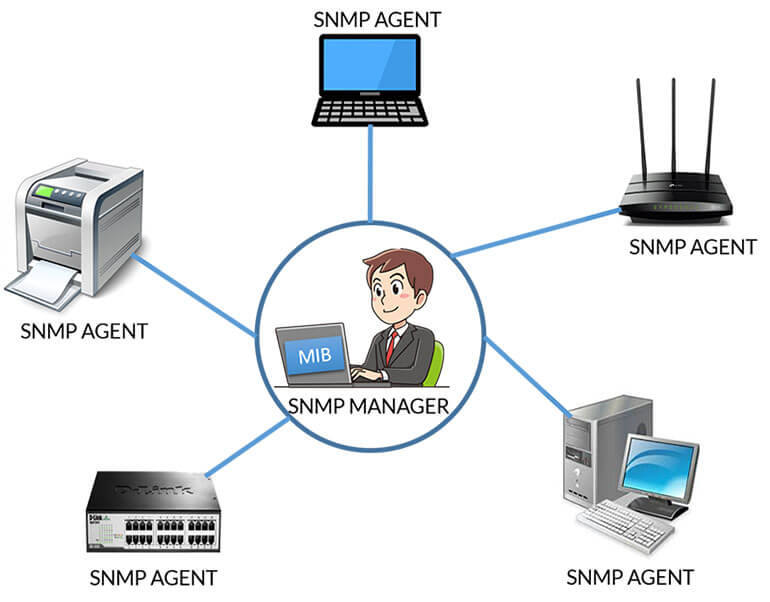
Hình 2.6. Cách thức hoạt động của DHCP

## SNMP (Simple Network Management Protocol)

### SNMP là gì?

- SNMP (Simple Network Management Protocol) là giao thức tầng ứng dụng được sử dụng để quản lý và giám sát các thiết bị mạng cũng như chức năng của chúng. SNMP cung cấp ngôn ngữ chung cho các thiết bị mạng để chuyển tiếp thông tin quản lý trong cả môi trường single-vendor và multi-vendor trong mạng cục bộ (LAN) hoặc mạng diện rộng (WAN). Phiên bản gần đây nhất của SNMP, version 3, bao gồm các cải tiến bảo mật để xác thực và mã hóa tin nhắn SNMP cũng như bảo vệ các gói trong khi truyền.

### Các thành phần của SNMP



Hình 2.7. Các thành phần của SNMP

- Có bốn thành phần chính trong mạng do SNMP quản lý:

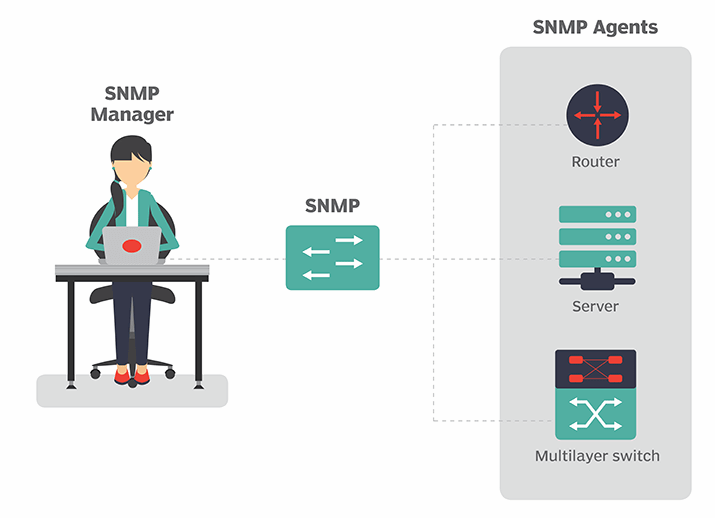
+ SNMP Agent: Chương trình này chạy trên phần cứng hoặc dịch vụ đang được giám sát, thu thập dữ liệu về các số liệu khác nhau như tình trạng sử dụng băng thông hoặc dung lượng ổ đĩa. Khi được người quản lý SNMP truy vấn, agent sẽ gửi thông tin này lại cho trình quản lý. Một agent cũng có thể chủ động thông báo cho NMS nếu xảy ra lỗi. Hầu hết các thiết bị đi kèm với một SNMP Agent được cài đặt sẵn; Thông thường nó chỉ cần được bật lên và cấu hình.

+ Các thiết bị và tài nguyên do SNMP quản lý: Đây là các node mà một agent chạy trên đó.

+ Trình quản lý SNMP (còn gọi là NMS): Nền tảng phần mềm này hoạt động như một bảng điều khiển tập trung mà các agent cung cấp thông tin. Nó sẽ chủ động yêu cầu các agent gửi thông tin cập nhật qua SNMP theo định kỳ. Những gì người quản lý mạng có thể làm với thông tin đó phụ thuộc rất nhiều vào số lượng tính năng của NMS. Có một số trình quản lý SNMP miễn phí đang được cung cấp, nhưng chúng thường bị giới hạn về khả năng hoặc số lượng node mà chúng có thể hỗ trợ. Ở mức độ cao hơn, các nền tảng cấp doanh nghiệp cung cấp các tính năng nâng cao cho các mạng phức tạp hơn, với một số sản phẩm hỗ trợ lên đến hàng chục nghìn node.

+ Cơ sở thông tin quản lý (Management information base – MIB): Cơ sở dữ liệu này là một file văn bản (.mib) phân loại và mô tả tất cả các đối tượng được sử dụng bởi một thiết bị cụ thể có thể được truy vấn hoặc kiểm soát bằng SNMP. Cơ sở dữ liệu này phải được tải vào NMS để có thể xác định và theo dõi trạng thái của các thuộc tính này. Mỗi mục MIB được gán một định danh đối tượng (OID).

### Cách SNMP hoạt động



Hình 2.8. Cách SNMP hoạt động

- NMP thực hiện vô số chức năng, dựa trên sự pha trộn giữa truyền tin push-and-pull giữa các thiết bị mạng và hệ thống quản lý. Nó có thể ra lệnh đọc hoặc ghi, chẳng hạn như đặt lại mật khẩu hoặc thay đổi cài đặt cấu hình. Nó có thể báo cáo lại mức độ sử dụng băng thông, CPU và bộ nhớ, với một số trình quản lý SNMP tự động gửi cho người quản trị một email hoặc thông báo tin nhắn văn bản nếu vượt quá ngưỡng xác định trước.

- Trong hầu hết các trường hợp, SNMP hoạt động trong một mô hình đồng bộ, với giao tiếp được khởi tạo bởi người quản lý SNMP và tác nhân gửi phản hồi. Các lệnh và thông báo này, thường được vận chuyển qua giao thức UDP hoặc TCP/IP, được gọi là đơn vị dữ liệu giao thức (PDU):

+ GET: Được tạo bởi trình quản lý SNMP và được gửi đến một agent để lấy giá trị của một biến số nào đó, được xác định bởi OID của nó, trong một MIB .

+ RESPONSE: Được gửi bởi agent cho người quản lý SNMP, được phát đi để trả lời yêu cầu GET. Chứa các giá trị của các biến được yêu cầu.

+ Được gửi bởi người quản lý SNMP đến agent để lấy các giá trị của OID tiếp theo trong hệ thống phân cấp của MIB.

+ GETBULK: Được gửi bởi người quản lý SNMP cho agent để có được các bảng dữ liệu lớn bằng cách thực hiện nhiều lệnh GETNEXT.

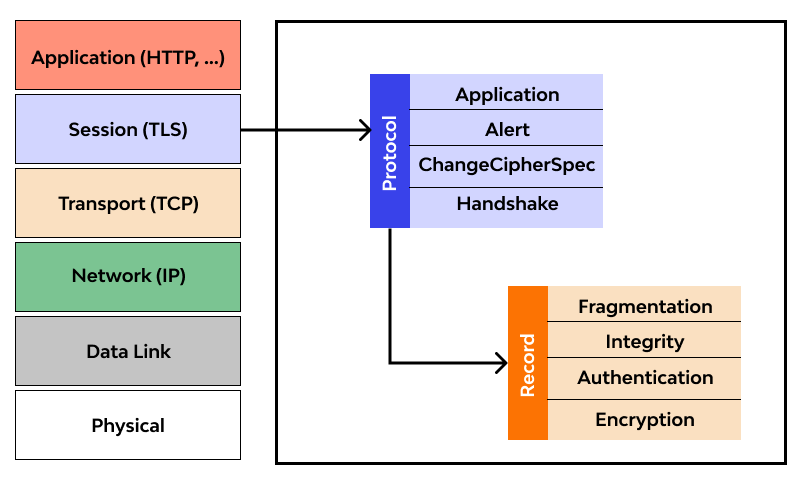
+ SET: Được gửi bởi người quản lý SNMP cho agent để đưa ra các cấu hình hoặc lệnh.

+ TRAP: Một cảnh báo không đồng bộ được gửi bởi agent đến trình quản lý SNMP để chỉ ra một sự kiện quan trọng, chẳng hạn như lỗi hoặc sự cố, đã xảy ra.

## SSL/TLS (Secure Sockets Layer / Transport Layer Security)

### **Giao thức SSL/TLS là gì**

- [Giao thức TLS](https://tenten.vn/tin-tuc/tls/) (Transport Layer Security) là một giao thức bảo mật được sử dụng để bảo vệ thông tin khi truyền qua mạng. Nó là phiên bản cải tiến, nâng cấp của giao thức SSL (Secure Sockets Layer).



Hình 2.9. Cấu Trúc của SSL/TLS

- TLS cung cấp khả năng mã hóa và xác thực dữ liệu giữa các ứng dụng, máy chủ, người dùng và hệ thống. Giao thức này được sử dụng đặc biệt trong việc tạo một kết nối an toàn thông qua giao thức HTTPS và thường được biểu thị bằng biểu tượng khóa xuất hiện trong trình duyệt web khi một phiên kết nối an toàn được thiết lập.

### **SSL/TLS hoạt động như thế nào?**

- Đoạn văn trình bày về quá trình bảo mật thông tin liên lạc bằng giao thức TLS, sử dụng cơ sở hạ tầng khóa công khai bất đối xứng để khởi tạo kết nối giữa client và server, sau đó sử dụng khóa đối xứng để mã hóa trong phần còn lại của phiên truyền dữ liệu.

- Các phương thức mã hóa bất đối xứng sử dụng hai khóa khác nhau để mã hóa thông tin liên lạc giữa hai bên, gồm khóa riêng tư và khóa công khai. Cặp khóa này có mối quan hệ được xác định bằng hàm toán học, nhưng việc tính toán ra private key từ public key gần như là bất khả thi với độ dài khóa đủ lớn.

- Sau khi trao đổi khóa chung, giao thức mã hóa đối xứng được sử dụng để trao đổi các dữ liệu lớn. Quá trình bắt tay TLS được diễn ra qua các message được gửi giữa client và server.

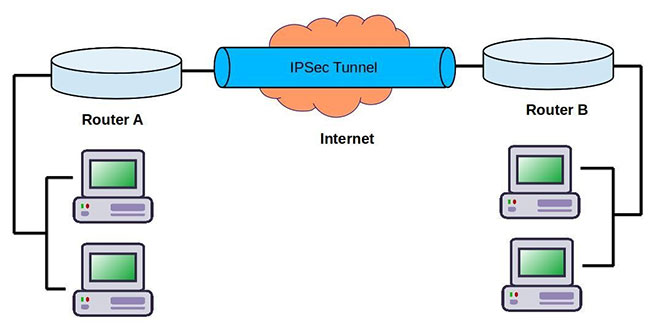
## IPSec (Internet Protocol Security)

### **IPSec là gì?**

- IPSec, viết tắt của Internet Protocol Security, là một bộ giao thức mật mã bảo vệ lưu lượng dữ liệu qua mạng Internet Protocol (IP).

- Mạng IP - bao gồm cả World Wide Web - thiếu khả năng mã hoá và bảo vệ quyền riêng tư. VPN IPSec giải quyết điểm yếu này, bằng cách cung cấp một framework cho việc giao tiếp được mã hóa và riêng tư trên web.

### **Cơ chế hoạt động của IPSec.**



Hình 2.10. Cơ chế hoạt động cảu IPEec

- Khi hai máy tính thiết lập kết nối [VPN](https://quantrimang.com/cong-nghe/ly-thuyet-vpn-la-gi-117232" \o "Lý thuyết VPN - Mạng riêng ảo là gì?), chúng phải đồng thuận về một tập hợp các giao thức bảo mật và thuật toán mã hóa, đồng thời trao đổi key mật mã để mở khóa và xem dữ liệu đã mã hóa.

- Đây là lúc IPSec phát huy vai trò. IPSec làm việc với các VPN tunnel để thiết lập kết nối hai chiều riêng tư giữa các thiết bị. IPSec không phải là một giao thức đơn lẻ; thay vào đó, đó là một bộ giao thức và tiêu chuẩn hoàn chỉnh, hoạt động cùng nhau để giúp đảm bảo tính bảo mật, toàn vẹn và xác thực của các gói dữ liệu Internet đi qua VPN tunnel.

- Đây là cách IPSec tạo một VPN tunnel bảo mật:

+ IPSec xác thực dữ liệu để đảm bảo tính toàn vẹn của gói dữ liệu trong quá trình truyền tải.

+ IPSec mã hóa lưu lượng truy cập Internet qua các VPN tunnel để không thể xem dữ liệu.

+ IPSec bảo vệ dữ liệu khỏi các cuộc tấn công Replay Attack, có thể dẫn đến việc đăng nhập trái phép.

+ IPSec cho phép trao đổi key mật mã bảo mật giữa các máy tính.

+ IPSec cung cấp hai chế độ bảo mật: Tunnel và Transport.

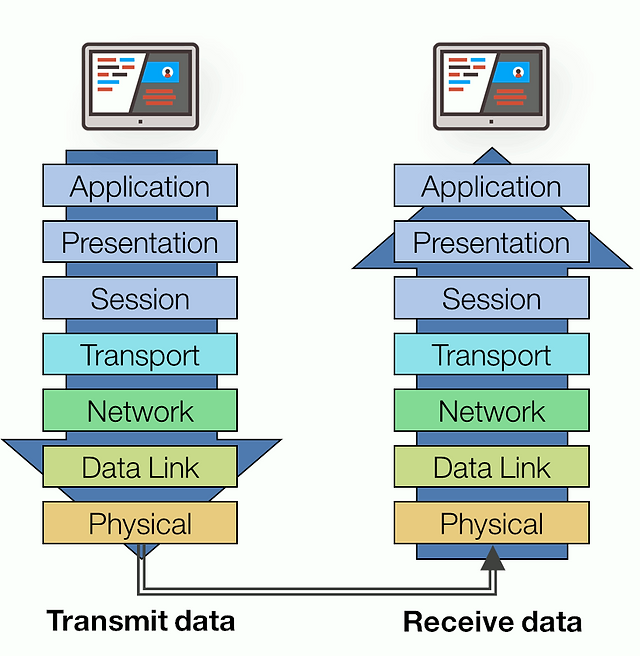
-VPN IPSec bảo vệ dữ liệu truyền từ host đến host, mạng đến mạng, host đến mạng và cổng đến gateway (được gọi là chế độ Tunnel, khi toàn bộ gói IP được mã hóa và xác thực).

# NỘI DUNG NGHIÊN CỨU

## Quá trình đóng gói dữ liệu để truyền tải trong mạng qua mô hình tham chiếu OSI.

### mô hình OSI.

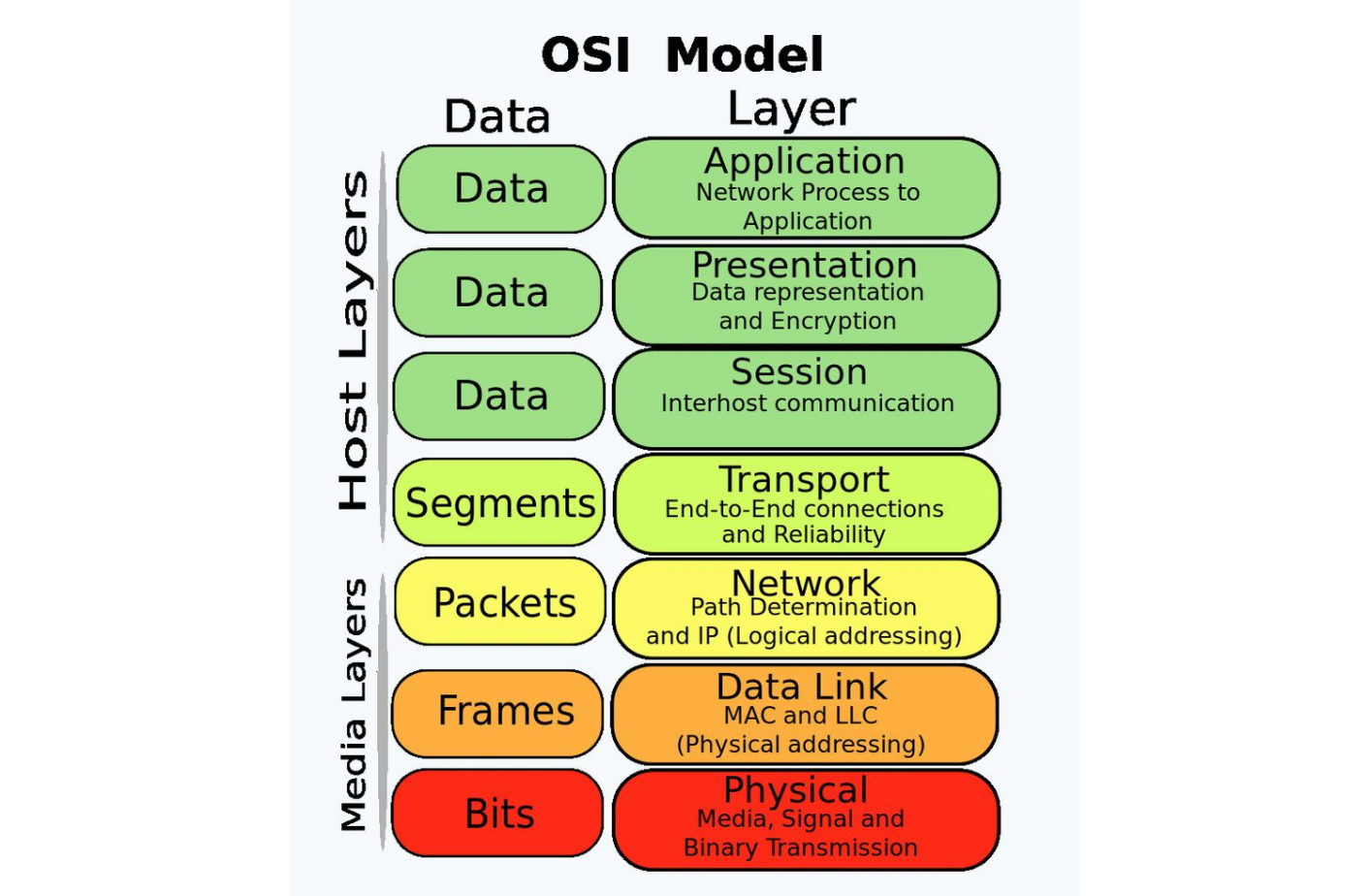
- Mô hình bao gồm 7 tầng riêng biệt nhưng chúng liên kết chặt chẽ với nhau, mỗi tầng đều có nhiệm vụ gửi/nhận dữ liệu từ tầng kề trên hoặc kề dưới nó. Tại thiết bị gửi, dữ liệu xuất phát từ tầng ứng dụng (Application layer), lần lượt được chuyển tiếp và xử lý qua mỗi tầng, cho tới tầng vật lý (Physical layer); bên nhận thu được dữ liệu từ tầng vật lý, chuyển tiếp và xử lý lần lượt qua các tầng, cho tới tầng ứng dụng, thiết bị nhận đón tiếp dữ liệu tại đây.



Hình 3.1. Mô hình OSI

### Quá trình dữ liệu được đóng gói qua từng lớp trong mô hình OSI.

- Có thể hình dung việc gửi và nhận dữ liệu dựa trên mô hình OSI giống như quá trình gửi và nhận thư: dữ liệu là nội dung thư, được ghi vào giấy, cho vào phong bì thư, đóng phong bì, dán tem, cho vào hòm thư, người đưa thư chuyển thư trong hòm tới hòm thư đích, bên nhận sẽ thực hiện ngược lại các bước này, cuối cùng đọc được nội dung thư. Mỗi bước đều lấy dữ liệu từ bước trước và xử lý thêm một thao tác, dữ liệu cũng được chuyển đổi từ hình trạng này tới hình trạng khác. Trong mô hình OSI cũng vậy, tương ứng với mỗi tầng, dữ liệu được thể hiện ở một hình thái khác nhau:



Hình 3.2. Mô hình OSI

- **Application** (tầng ứng dụng)-cung cấp giao diện, dịch vụ trực tiếp cho người dùng cuối và các ứng dụng phần mềm. Các chức năng của tầng ứng dụng:

+ Thiết bị đầu cuối ảo của mạng (Network Virtual Terminal): Cho phép các ứng dụng từ máy tính khác nhau tương tác như thể chúng đang chạy trên cùng một thiết bị. Điều này giúp người dùng có thể truy cập và sử dụng các ứng dụng hoặc dịch vụ mạng từ bất kỳ máy tính nào.

+ Quản lý, truy cập và chuyển file (FTAM- File transfer access and management): Cung cấp khả năng truyền, truy cập và quản lý các tệp tin giữa các máy tính trên mạng. Điều này bao gồm việc truyền tải tệp tin (như FTP), quản lý tệp tin từ xa, và các chức năng quản lý quyền truy cập.

+ Các dịch vụ khác như mail services, directory services: Bao gồm một loạt các ứng dụng và dịch vụ phổ biến như email (SMTP, IMAP, POP3), dịch vụ thư mục (LDAP), dịch vụ web (HTTP), và nhiều dịch vụ khác được thiết kế để hỗ trợ giao tiếp và chia sẻ thông tin trong mạng.

**- Presentation** (tầng trình bày)-mã hóa giải mã và chuyển đổi định dạng dữ liệu. Tầng trình bày còn có tên gọi khác là tầng phiên dịch (Translation layer), thực hiện một số chức năng:

+ Phiên dịch (Translation): Chuyển đổi dữ liệu giữa các định dạng mà các ứng dụng (trên tầng ứng dụng) hiểu được và định dạng mạng. Điều này bao gồm việc chuyển đổi giữa các định dạng mã hóa khác nhau, ví dụ từ ASCII sang EBCDIC.

+ Mã hóa và giải mã (Encryption and Decryption): Bảo mật thông tin bằng cách mã hóa dữ liệu trước khi chúng được gửi qua mạng và sau đó giải mã chúng khi đến nơi nhận. Điều này giúp bảo vệ dữ liệu khỏi sự truy cập không được phép.

+ Nén (Compression): Giảm kích thước của dữ liệu để tối ưu hóa việc truyền tải qua mạng. Nén có thể được thực hiện ở mức độ khác nhau tùy thuộc vào loại dữ liệu và yêu cầu cụ thể của ứng dụng.

**- Session** (tầng phiên)-quản lý và duy trì phiên giao tiếp giữa các ứng dụng. Chúng ta gọi một phiên (session) là một kết nối tạm thời giữa hai thiết bị để trao đổi dữ liệu. Tầng phiên quản lý việc thiết lập và duy trì phiên làm việc giữa các thiết bị trên mạng. Điều này giúp đảm bảo tính toàn vẹn và đáng tin cậy của phiên, đồng thời quản lý việc đồng bộ hóa dữ liệu và xác định các điểm dừng phiên (session termination). Tầng phiên chịu trách nhiệm cho:

+ Thiết lập, duy trì, chấm dứt phiên (Session establishment, maintenance, and termination): Quản lý việc bắt đầu, duy trì và kết thúc các phiên giao tiếp giữa các ứng dụng. Điều này bao gồm việc mở, duy trì và đóng cửa sổ giao tiếp giữa các người dùng hoặc các quy trình.

+ Đồng bộ hóa (Synchronization): Đảm bảo việc đồng bộ hóa dữ liệu giữa các quá trình giao tiếp. Điều này có thể bao gồm việc đánh dấu các điểm kiểm tra trong dữ liệu để cho phép phục hồi từ điểm đó nếu có lỗi hoặc sự cố xảy ra.

+ Kiểm soát hội thoại (Dialog Controller): Quản lý quyền kiểm soát giao tiếp trong một phiên. Điều này có thể bao gồm việc xác định liệu giao tiếp là một chiều (simplex), hai chiều lần lượt (half-duplex) hay hai chiều cùng lúc (full-duplex).

**- Transport** (tầng vận chuyển)-đảm bảo truyền tải dữ liệu tin cậy, kiểm soát lỗi. Thay vì chuyển tiếp các gói dữ liệu một cách độc lập như tầng mạng, tầng giao vận giúp đảm bảo các gói dữ liệu thuộc cùng một thông điệp được chuyển tiếp một cách toàn vẹn. Các chức năng của tầng vận chuyển:

+ Phân mảnh/Phân đoạn và tái hợp (Segmentation and Reassembly): Chia nhỏ dữ liệu từ tầng phiên thành các phân đoạn nhỏ hơn để truyền tải dễ dàng hơn trên mạng. Khi đến đích, những phân đoạn này được tái hợp thành dữ liệu ban đầu.

+ Kiểm soát kết nối: Thiết lập, duy trì và kết thúc các kết nối logic giữa người gửi và người nhận. Điều này bao gồm việc quản lý thiết lập kết nối, duy trì kết nối ổn định, và đóng kết nối sau khi truyền dữ liệu.

+ Kiểm soát lưu lượng: Điều chỉnh lưu lượng dữ liệu giữa người gửi và người nhận để tránh quá tải và đảm bảo truyền dữ liệu hiệu quả.

+ Kiểm soát lỗi: Phát hiện và sửa chữa lỗi có thể xảy ra trong quá trình truyền dữ liệu. Bao gồm việc kiểm tra lỗi và gửi lại dữ liệu nếu cần.

+ Định địa chỉ điểm dịch vụ (Service Point Addressing): Sử dụng cổng (port) để định địa chỉ dịch vụ tại các máy chủ, giúp xác định các ứng dụng cụ thể đang giao tiếp trên máy chủ.

**- Network** (tầng mạng)-định tuyến và quản lý địa chỉ, phân mảnh gói tin. Với sự phối hợp của hai tầng vật lý và tầng mạng, các gói dữ liệu đã có thể truyền thành công từ thiết bị này sang thiết bị khác trong cùng một môi trường truyền (cùng mạng). Tuy nhiên, trên thực tế các gói dữ liệu phần lớn được truyền thông qua hai thiết bị khác môi trường truyền, đó là lý do cần có sự tham gia của tầng mạng. Tầng mạng giúp truyền các gói dữ liệu qua các chặng trung gian, từ đó dữ liệu có thể được truyền qua nhiều mạng khác nhau. Tầng mạng có hai chức năng chính:

+ Định địa chỉ logic (Logical Addressing): Tầng mạng gán địa chỉ logic, thường là địa chỉ IP, cho mỗi thiết bị trong mạng. Điều này giúp xác định đích cuối cùng của dữ liệu trong mạng rộng lớn và đa dạng.

+ Định tuyến (Routing): Xác định lộ trình cho dữ liệu đi từ nguồn đến đích. Định tuyến dựa trên các thuật toán để chọn đường đi tối ưu nhất, giúp dữ liệu đến được đích nhanh chóng và hiệu quả. Định tuyến có thể thực hiện trong mạng nội bộ (LAN) hoặc qua các mạng khác nhau (WAN).

- **Data Link** (tần liên kết dữ liệu)-đảm bảo truyền tải chính sát và phát hiện lỗi trong dữ liệu. Ở tầng vật lý, dữ liệu được truyền qua các đường truyền vật lý (các loại cáp) nên không đảm bảo tính toàn vẹn và bảo mật. Khắc phục cho nhược điểm đó, tầng liên kết dữ liệu cung cấp các cơ chế kiểm tra lỗi, quản lý quyền truy cập và điều chỉnh việc truyền dữ liệu, giúp đảm bảo tính toàn vẹn và tin cậy của dữ liệu trên mạng. Tầng liên kết dữ liệu chịu trách nhiệm:

+ Đóng gói dữ liệu (Framing): Chia dữ liệu được nhận từ tầng mạng thành các khung (frames) nhỏ hơn để dễ dàng xử lý. Mỗi khung chứa thông tin cần thiết để kiểm soát lỗi và đồng bộ hóa.

+ Định địa chỉ vật lý (Physical addressing): Gán địa chỉ vật lý, thường là địa chỉ MAC (Media Access Control), cho mỗi thiết bị trong mạng để xác định nguồn và đích của mỗi khung dữ liệu.

+ Kiểm soát lưu lượng (Flow Control): Điều chỉnh tốc độ truyền dữ liệu giữa người gửi và người nhận để tránh quá tải dữ liệu tại người nhận. Điều này giúp đảm bảo rằng tất cả các dữ liệu được nhận một cách đầy đủ và chính xác.

+ Kiểm soát lỗi (Error control): Phát hiện và sửa chữa lỗi có thể xảy ra trong quá trình truyền dữ liệu. Điều này thường được thực hiện thông qua việc sử dụng các thuật toán kiểm tra lỗi như CRC (Cyclic Redundancy Check).

+ Kiểm soát truy cập (Access control): Xác định cách thức các thiết bị trên cùng một mạng chia sẻ kênh truyền thông. Ví dụ, trong một mạng LAN có thể sử dụng CSMA/CD (Carrier Sense Multiple Access/Collision Detection) hoặc CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) để quản lý truy cập.

**- Physical** (tầng vật lý)-truyền tín hiệu vật lý giữa các thiết bị mạng. Là tầng thấp nhất trong mô hình OSI, tầng vật lý thực hiện chức năng chuyển tiếp dữ liệu từ kênh truyền nguồn tới kênh truyền đích. Dữ liệu trong tầng vật lý được biểu diễn dưới dạng dãy bit 00 và 11. Sau khi nhận được dữ liệu từ kênh truyền khác, tầng vật lý thực hiện chuyển tiếp dữ liệu lên tầng liên kết dữ liệu. Có thể hình dung tầng vật lý chính là quá trình người đưa thư chuyển bức thư từ hòm thư này sang hòm thư khác. Quá trình này cần xem xét các yếu tố như tốc độ chuyển thư, phương tiện di chuyển, ... Tầng vật lý bao gồm các chức năng:

+ Biểu diễn bit: Chuyển đổi dữ liệu số (bit) thành tín hiệu vật lý (như tín hiệu điện, quang học, radio) để truyền trên phương tiện vật lý như cáp đồng, cáp quang, không khí.

+ Kiểm soát tốc độ dữ liệu (Bit rate control): Điều chỉnh tốc độ truyền dữ liệu, tức là số lượng bit truyền trên một kênh truyền trong một đơn vị thời gian. Điều này đảm bảo dữ liệu được truyền một cách hiệu quả và phù hợp với khả năng của phương tiện truyền dẫn.

+ Đồng bộ hóa các bit (Bit synchronization): Đảm bảo người nhận và người gửi đồng bộ về thời gian khi truyền và nhận từng bit, để tránh hiểu nhầm về dữ liệu đang được truyền.

+ Cấu hình đường truyền: Thiết lập cấu hình vật lý của đường truyền, bao gồm cài đặt các thiết bị như bộ định tuyến, switch, và hub.

+ Topo (Mô hình ghép nối) vật lý (Physical topologies): Xác định cách các thiết bị trong mạng được kết nối vật lý với nhau. Ví dụ như topo dạng sao, dạng vòng, dạng cây, ...

+ Chế độ truyền dẫn (Transmission mode): Xác định hướng truyền dữ liệu trong mạng. Có ba chế độ chính: Simplex (chỉ một hướng), Half-duplex (hai hướng nhưng không đồng thời), và Full-duplex (hai hướng đồng thời).

## một số giao thức mạng phổ biến hoạt động ở mỗi lớp trong mô hình TCP/IP.

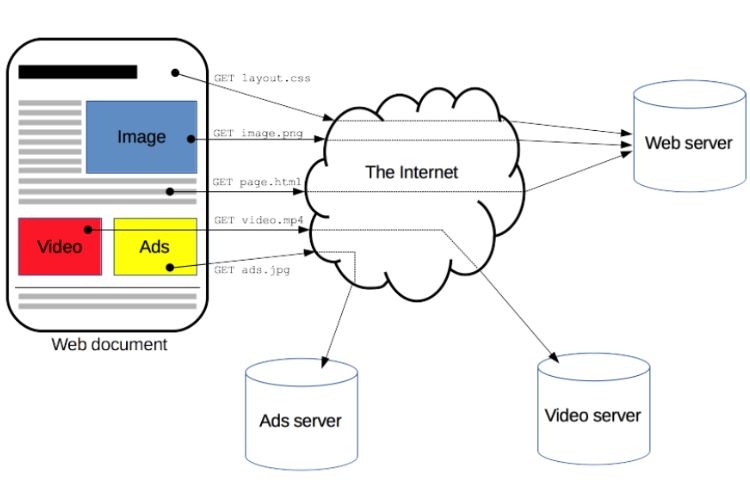
### Giao thức mạng xếp theo lớp.

1. Lớp Ứng Dụng (Application Layer)

Lớp này kết hợp các chức năng của lớp ứng dụng, lớp trình bày và lớp phiên trong mô hình OSI. Một số giao thức phổ biến:

1. HTTP/HTTPS (HyperText Transfer Protocol):

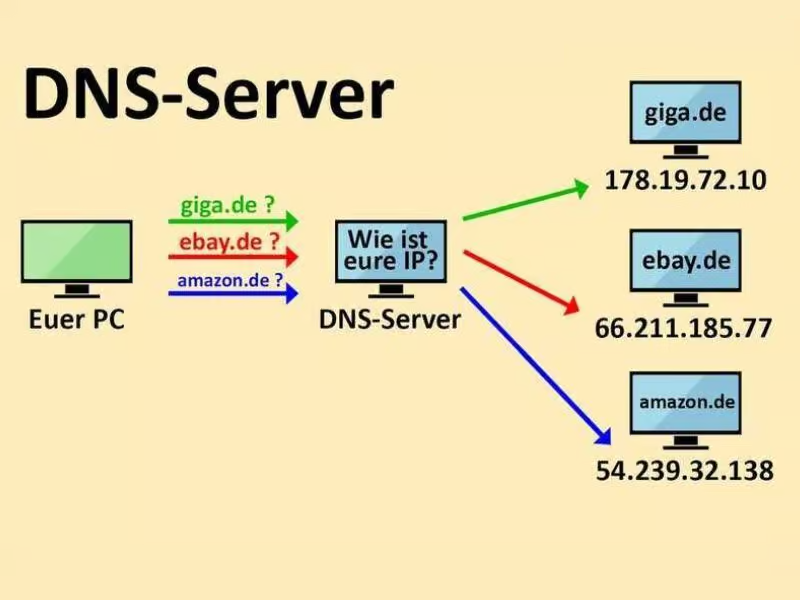
- HTTP là viết tắt của HyperText Transfer Protocol, là một giao thức truyền tải siêu văn bản, giúp cho các máy tính có thể giao tiếp với nhau qua mạng. HTTP là nền tảng của World Wide Web kết nối giữa máy chủ (server) và máy khách (client) trong cùng một hệ thống mạng. Điều này cho phép chúng ta truy cập vào các trang web, tải xuống các tệp tin, xem các hình ảnh, video…



Hình 3.3. Nguyên lý hoạt động của HTTP

1. DNS (Domain Name System):

- Hệ thống phân giải [tên miền](https://vi.wikipedia.org/wiki/T%C3%AAn_mi%E1%BB%81n" \o "Tên miền) (DNS) về căn bản là một hệ thống giúp cho việc chuyển đổi các [tên miền](https://vi.wikipedia.org/wiki/T%C3%AAn_mi%E1%BB%81n" \o "Tên miền) mà con người dễ ghi nhớ (dạng ký tự, ví dụ www.example.com) sang [địa chỉ IP](https://vi.wikipedia.org/wiki/%C4%90%E1%BB%8Ba_ch%E1%BB%89_IP" \o "Địa chỉ IP) vật lý (dạng số, ví dụ 123.11.5.19) tương ứng của tên miền đó. DNS giúp liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị trên Internet.



Hình 3.4. Nguyên lý hoạt động của DNS

- Hệ thống phân giải tên miền phân phối trách nhiệm gán tên miền và lập bản đồ những tên tới địa chỉ IP bằng cách định rõ những máy chủ có thẩm quyền cho mỗi tên miền. Những máy chủ có tên thẩm quyền được phân công chịu trách nhiệm đối với tên miền riêng của họ, và lần lượt có thể chỉ định tên máy chủ khác độc quyền của họ cho các tên miền phụ. Kỹ thuật này đã thực hiện các cơ chế phân phối DNS, chịu đựng lỗi, và giúp tránh sự cần thiết cho một trung tâm đơn lẻ để đăng ký được tư vấn và liên tục cập nhật.

1. Lớp Giao Vận (Transport Layer)

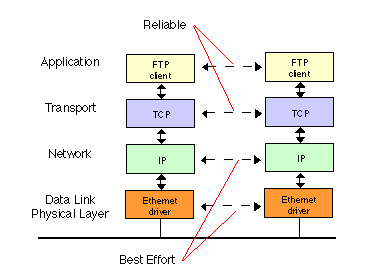
Lớp này quản lý việc truyền tải dữ liệu giữa các thiết bị:

1. TCP (Transmission Control Protocol):

- [TCP](https://bizflycloud.vn/tin-tuc/tcp-la-gi-20181022170658844.htm" \o "TCP) (Transmission Control Protocol) là một giao thức mạng quan trọng được sử dụng trong việc truyền dữ liệu qua một mạng nào đó. Một giao thức trong phạm vi mạng là một tập hợp các quy tắc và trình tự kiểm soát việc thực hiện truyền dữ liệu sao cho tất cả mọi người trên thế giới bất kể vị trí địa lý, bất kể ứng dụng, phần mềm họ đang sử dụng đều có thể thao tác theo cùng một phương thức giống nhau được gọi là TCP.

- TCP thường kết hợp với IP (Giao thức Internet) theo một cặp được gọi là TCP/IP. Bạn có thể bắt gặp cụm thuật ngữ này trong phần network setting trên máy tính, điện thoại thông minh hoặc các thiết bị cầm tay của mình. IP sẽ xử lý việc gán địa chỉ và chuyển tiếp các gói tin từ nguồn đến đích trong khi TCP kiểm soát độ tin cậy của truyền dẫn.

- Chức năng của giao thức tcp được xác định là kiểm soát mức độ tin cậy của việc truyền dữ liệu. Trên các mạng như Internet, dữ liệu được truyền theo dạng gói tin, các gói này là các cụm dữ liệu được truyền hoàn toàn độc lập trên mạng, được tập hợp lại với nhau khi chúng đến địa chỉ đích và sau đó trả về dữ liệu gốc.



Hình 3.5. Nguyên lý hoạt động của TCP

- Truyền dữ liệu trên mạng được xử lý theo các lớp, mỗi một giao thức trên một lớp sẽ thực hiện công việc bổ sung cho các lớp khác. Tập hợp các lớp này được gọi là các ngăn giao thức (protocol stack). TCP và IP làm việc liên quan chặt chẽ với nhau, lớp này trên lớp kia.

1. UDP (User Datagram Protocol):

- Giao thức UDP (User Datagram Protocol) là một giao thức cốt lõi của giao thức TCP/IP được sử dụng để thiết lập các kết nối có độ trễ thấp và giảm mất mát giữa các ứng dụng trên Internet. Giao thức UDP cung cấp hai dịch vụ không được cung cấp bởi lớp IP, đó là:

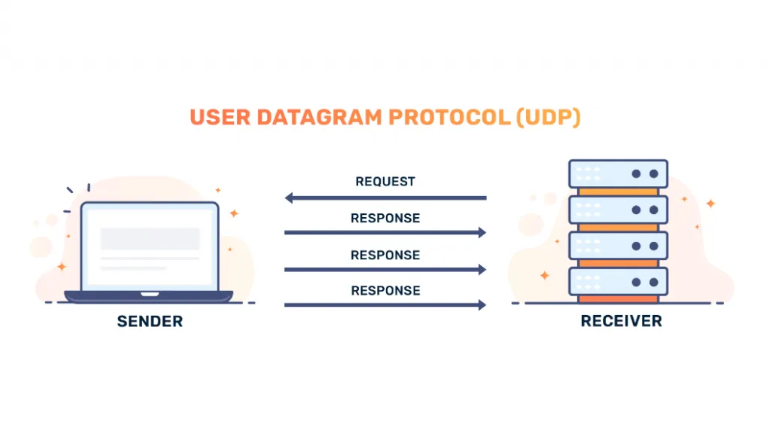
- Cung cấp các [port](https://bkhost.vn/blog/port-la-gi/) number để giúp phân biệt các yêu cầu khác nhau từ người dùng.

- Đồng thời sử dụng một thuật toán checksum để xem dữ liệu có được toàn vẹn hay không.

- UDP là một giải pháp được dùng thay cho giao thức TCP. Cả hai giao thức này đều hoạt động trên lớp IP và có lúc được gọi là UDP/IP hoặc TCP/IP. Mặc dù đều hoạt động trên giao thức IP, nhưng UDP và TCP có những khác biệt rất quan trọng. Cụ thể:

- Giao thức TCP hỗ trợ giao tiếp máy chủ tới máy chủ (host-to-host). Được coi là phương thức vận chuyển bảo mật đáng tin cậy nhưng có tốc độ truyền chậm hơn. TCP chia nhỏ các tập [dữ liệu lớn](https://bkhost.vn/blog/big-data-du-lieu-lon/) thành các gói dữ liệu riêng lẻ, đảm bảo lưu lượng và kiểm soát lỗi, thực hiện gửi lại các tập tin bị mất và gửi theo đúng thứ tự.

- Giao thức UDP cho phép giao tiếp quy trình tới quy trình (process-to-process). UDP chỉ gửi gói tin được gọi là datagram, các gói tin này được truyền đi theo các đường dẫn khác nhau giữa người gửi và người nhận. Nghĩa là UDP có khả năng làm mất dữ liệu hoặc truyền dữ liệu không theo thứ tự, tuy nhiên lại sử dụng chi phí [băng thông](https://bkhost.vn/blog/bandwidth-bang-thong/) và độ trễ thấp hơn.



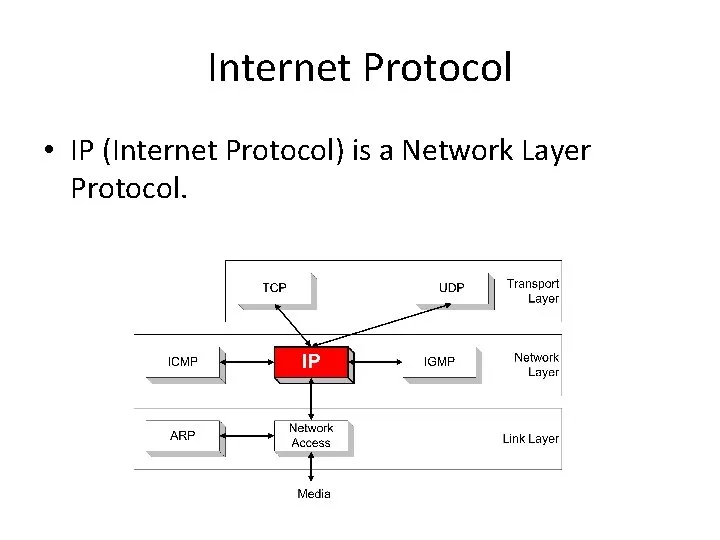
Hình 3.6. Nguyên Lý Hoạt động của UDP

1. Lớp Internet (Internet Layer)

Lớp này tương ứng với lớp mạng trong mô hình OSI, chịu trách nhiệm định tuyến và truyền tải gói tin:

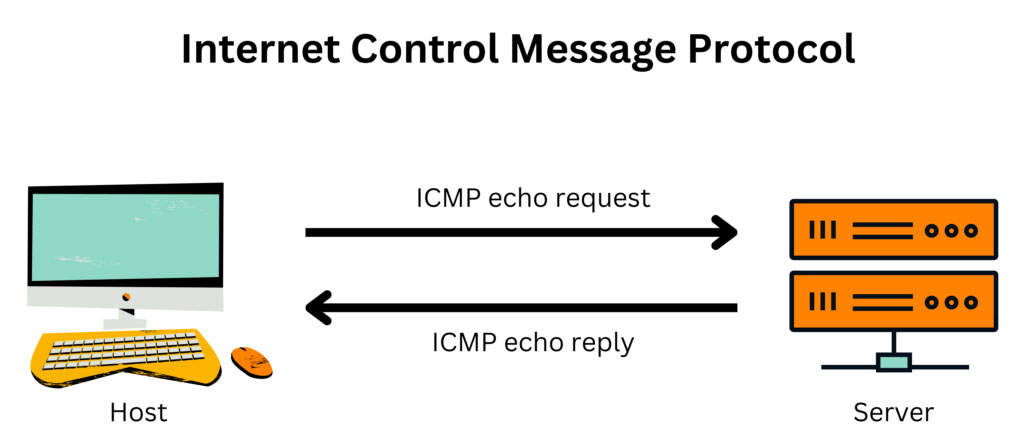
1. IP (Internet Protocol):

- Internet Protocol là - Giao thức Internet (IP) là một giao thức hoặc bộ quy tắc để định tuyến và xử lý các gói dữ liệu để chúng có thể di chuyển qua các [mạng máy tính](https://timviec365.vn/blog/mang-may-tinh-la-gi-new10173.html) và đến đích chính xác. Dữ liệu truyền qua Internet được chia thành các phần nhỏ hơn, được gọi là các gói. Thông tin IP được đính kèm vào mỗi gói và thông tin này giúp các bộ định tuyến gửi các gói đến đúng nơi. Mọi thiết bị hoặc miền kết nối với Internet đều được gán một địa chỉ IP - Internet Protocol và khi các gói được hướng đến địa chỉ IP - Internet Protocol được đính kèm với chúng, dữ liệu sẽ đến nơi cần thiết.



Hình 3.7. Ảnh minh họa giao thữc IP

1. ICMP (Internet Control Message Protocol):



Hình 3.8. Ảnh minh họa giao thức ICMP

- Giao thức ICMP là một giao thức hỗ trợ trong bộ giao thức IP với chức năng để gửi thông báo kiểm soát và thông báo lỗi giữa các thiết bị trong mạng. ICMP thường được sử dụng trong quá trình kiểm tra kết nối, chẩn đoán sự cố, và truyền tải thông báo về các vấn đề liên quan đến giao tiếp mạng.

- Một trong những trường hợp phổ biến sử dụng ICMP là khi bạn sử dụng lệnh “ping” để kiểm tra xem một thiết bị có thể truy cập được hay không, và đo đạc thời gian mà một gói tin mất đi và trở lại (round-trip time).

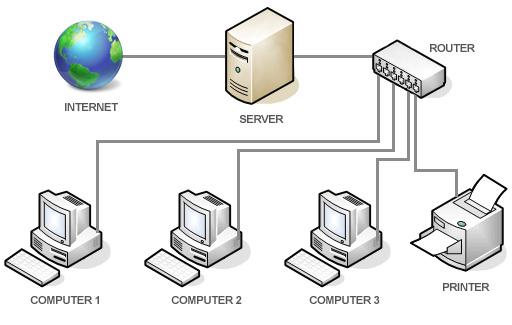
- ICMP cũng được sử dụng để thông báo lỗi khi có vấn đề xảy ra trong quá trình truyền thông mạng, như khi một đích không thể đạt được hoặc khi một dịch vụ không khả dụng.

1. Lớp Liên Kết Dữ Liệu (Link Layer)

Lớp này tương đương với hai lớp vật lý và liên kết dữ liệu trong mô hình OSI. Một số giao thức phổ biến:

1. Ethernet:

Ethernet là một giao thức mạng và một công nghệ kết nối mạng dây, được sử dụng rộng rãi trong các mạng máy tính để kết nối các thiết bị mạng với nhau. Ethernet sử dụng các chuẩn kết nối vật lý và các giao thức mạng để cho phép truyền dữ liệu giữa các thiết bị mạng như [máy tính](https://fptshop.com.vn/may-tinh-xach-tay), máy chủ, bộ định tuyến và switch.



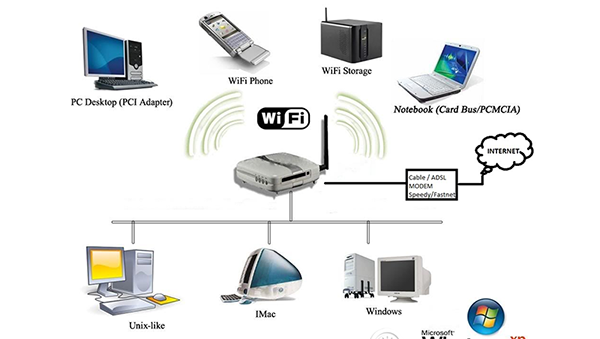
Hình 3.9. Nguyên lý hoạt đông của Ethernet

Ethernet được phát triển vào những năm 1970 bởi Xerox Corporation, Digital Equipment Corporation và Intel Corporation, và trở thành một công nghệ tiêu chuẩn cho mạng LAN (Local Area Network). Ethernet sử dụng một giao thức truyền dữ liệu thông qua cáp đồng trục hoặc cáp xoắn đôi, cho phép truyền dữ liệu với tốc độ cao và ổn định.

Hiện nay, Ethernet đã phát triển đến nhiều phiên bản và chuẩn kết nối vật lý khác nhau như Ethernet 10BASE-T, Ethernet 100BASE-TX, Ethernet 1000BASE-T, Ethernet 10GBASE-T, và Ethernet 40GBASE-T, tùy thuộc vào mục đích sử dụng và yêu cầu kết nối của các thiết bị mạng. Ethernet được sử dụng rộng rãi trong các doanh nghiệp, trường học, và các tổ chức khác để kết nối các thiết bị mạng và truyền dữ liệu giữa chúng.

1. Wi-Fi (Wireless Fidelity):

- Wifi là viết tắt của Wireless Fidelity được hiểu là sử dụng sóng vô tuyến để truyền tín hiệu. Loại sóng này có khả năng kết nối với mạng khác hay với máy tính bằng sóng vô tuyến. Nó tương tự như sóng điện thoại, truyền hình, radio. Hầu như Các thiết bị điện tử như: máy tính, laptop, [điện thoại di động](https://dienmaycholon.com/dien-thoai-di-dong" \t "https://dienmaycholon.com/kinh-nghiem-mua-sam/_blank), tablet…đều có thể truy cập wifi để truy cập mạng thỏa mãn nhu cầu của người dùng.

- Kết nối wifi hiện nay được dựa trên chuẩn liên kết IEEE 802.11 và chạy trên băng tần 54Mbps với quy mô phát tín hiệu trong vòng 30m với điều kiện không có vật cản. Nếu có vật cản, tốc độ truyền dẫn tín hiệu wifi sẽ bị kém đi nhiều.   


Hình 3.10. Nguyên lý hoạt động của Wifi

Nguyên lý hoạt động của wifi gồm có 4 thành phần:

- Đường truyền mạng: Là kết nối internet băng thông rộng. Việc kết nối này sẽ nhanh hơn so với dịch vụ kết nối quay số.

- Cổng mạng: Cổng mạng này có nhiệm vụ ngăn chặn những người truy cập vào wifi của bạn mà không được phép. Và đồng thời nó cung cấp cho bạn những công cụ trong việc quản lý như: kiểm tra mạng và các dịch vụ khác thông qua IP.

- Mạng LAN không dây: Là một hệ thống kết nối máy tính của bạn với các thiết bị khác như [Xiaomi 12T Pro 256GB](https://dienmaycholon.com/dien-thoai-di-dong/xiaomi-12t-pro-12gb-256gb) bằng sóng vô tuyến.

- Kết nối Adapter không dây: Đây là phương tiện để người khác có thể truy cập vào Wifi của bạn. Adapter không dây có thể được tích hợp sẵn, hoặc là một thiết bị rời được cắm vào máy tính.

Thông qua 4 thành phần trên, bộ phát sóng Wifi (Modem, Router) sẽ kết nối và lấy tín hiệu internet hữu tuyến qua dây cáp quang rồi chuyển tín hiệu thành vô tuyến Wifi và gửi đến các thiết bị sử dụng Wifi ([điện thoại Xiaomi](https://dienmaycholon.com/dien-thoai-di-dong-xiaomi" \t "https://dienmaycholon.com/kinh-nghiem-mua-sam/_blank), laptop, smart tivi, internet tivi).

Trên là quá trình nhận tín hiệu thông qua adapter và chuyển hóa chúng thành tín hiệu trên internet. Quá trình này có thể thực hiện ngược lại, có nghĩa là: router, modem nhận tín hiệu vô tuyến từ adapter và giải mã chúng rồi gửi qua internet.

1. PPP (Point-to-Point Protocol):

- [PPP](https://vi.wikipedia.org/wiki/PPP_(giao_th%E1%BB%A9c)" \t "https://vinahost.vn/point-to-point/_blank) không đơn thuần chỉ là một giao thức liên kết dữ liệu, mà nó còn cung cấp nhiều tính năng hữu ích như mã hoá dữ liệu khi truyền tải và xác thực kết nối.

- PPP có khả năng sử dụng trên nhiều kiểu mạng vật lý đa dạng khác nhau như dây điện thoại, mạng điện thoại, cáp tuần tự, radio và cả cáp quang giống SONET. Vậy nên PPP đã trở thành một trong những giao thức được sử dụng rộng rãi, phổ biến nhất hiện nay.

- Các nhà cung cấp dịch vụ Internet hiện nay thường lựa chọn PPP để kết nối với khách hàng, đồng thời sử dụng hai kiểu gói dữ liệu đó là PPPoE (Point-to-Point Protocol over Ethernet) và PPPoA (Point-to-Point Protocol over ATM) để có thể đảm bảo tốc độ truyền tải và chất lượng kết nối.

- Với ưu điểm nổi trội, PPP đã trở thành một công cụ đáng tin cậy trong việc thiết lập kết nối và truyền tải dữ liệu trong mạng máy tính.  
Nguyên lý hoạt động của giao thức Point to Point (PPP) được chia thành ba giai đoạn chính:

Trong giai đoạn này, hai thiết bị kết nối sẽ thực hiện các bước sau:

Giao tiếp LCP (Link Control Protocol): LCP chịu trách nhiệm thiết lập, cấu hình, kiểm tra và duy trì liên kết vật lý giữa hai thiết bị. LCP sẽ thương lượng các tham số liên kết, chẳng hạn như tốc độ dữ liệu, độ dài khung và phương thức mã hóa.

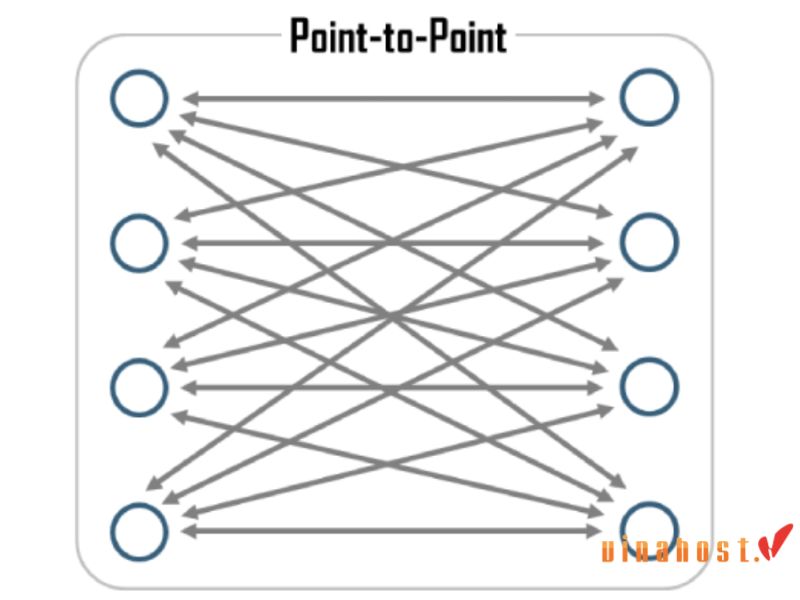
Giao tiếp AP (Authentication Protocol): AP chịu trách nhiệm xác thực các thiết bị kết nối. Các giao thức xác thực phổ biến được sử dụng với PPP bao gồm PAP (Password Authentication Protocol) và CHAP (Challenge Handshake Authentication Protocol).

Sau khi kết nối được thiết lập, dữ liệu có thể được truyền giữa hai thiết bị. Dữ liệu sẽ được đóng gói thành các khung PPP. Các khung PPP này sẽ được truyền qua liên kết vật lý.

Khi kết nối không còn cần thiết, hai thiết bị sẽ thực hiện các bước sau để kết thúc kết nối:

Thông báo LCP: Một thiết bị sẽ gửi một thông báo LCP cho thiết bị kia để thông báo rằng nó sẽ kết thúc kết nối.

Giao tiếp LCP: LCP sẽ thực hiện một cuộc kiểm tra cuối cùng để đảm bảo rằng liên kết đã được đóng đúng cách.



Hình 3.11. Nguyên lý hoạt động của Point to Point

### Tìm hiểu và phân tích giao thức ICMP.

- **ICMP**: internet control message protocol, tạm dịch là (giao thức tin nhắn điều khiển internet) là một giao thức thuộc tầng mạng trong bộ giao thức TCP/IP, được sử dụng để gửi các thông báo về lỗi, chẩn đoán, hoặc các thông tin điều khiển liên quan đến mạng. Giao thức này không được dùng để truyền dữ liệu giữa các ứng dụng mà chủ yếu hỗ trợ hoạt động của các giao thức mạng khác như IP.

Phần header của ICMP khá đơn giản, có cấu trúc như sau:



Hình 3.10. Cấu trúc Header của ICMP

Byte đầu tiên xác định **type** của ICMP message. Ví dụ: type 8 được sử dụng cho gói ICMP request và type 0 sử dụng cho gói ICMP reply, type 3 cho trường hợp thông báo lỗi “destination unreachable” – không thể truy cập được tới đích.

Byte thứ 2 được dùng để xác định loại ICMP message nào đang sử dụng. Ví dụ: “destination unreachable” có 16 code khác nhau. Khi bạn thấy code = 0 thì có nghĩa là mạng đích (destination network) không thể truy cập (unreachable), còn code = 1 thì có nghĩa là máy đích không thể truy cập (unreachable).

Trường thứ 3 gồm 2 byte dùng để checksum lại gói tin ICMP có bị lỗi hay không. Phần còn lại.

của Header phụ thuộc vào type của IMCP message mà chúng ta sử dụng.

- Các chức năng chính của ICMP:

+ báo cáo lỗi: ICMP giúp các thiết bị mạng (như router hoặc host) báo cáo các lỗi xảy ra khi xử lý các gói tin IP.

Ví dụ:

"Destination Unreachable" (Đích không thể truy cập được).

"Time Exceeded" (Hết thời gian chờ khi chuyển tiếp gói tin).

+ kiểm tra và chuẩn đoán: ICMP được sử dụng trong các công cụ chẩn đoán mạng như:

**Ping:** Kiểm tra kết nối giữa hai thiết bị mạng.

**Traceroute:** Theo dõi đường đi của gói tin qua các router.

+ Điều khiển và quản lý luồng:Thông báo "Source Quench" để yêu cầu giảm tốc độ gửi gói tin từ nguồn (hiện ít được sử dụng).

- Cách ICMP hoạt động:

+ Khi một sự kiện mạng xảy ra (ví dụ: không thể gửi gói tin), thiết bị liên quan tạo ra một thông báo ICMP.

+ Thông báo này được đóng gói trong một gói tin IP và gửi ngược lại đến nguồn hoặc một thiết bị khác để xử lý.

- Một số loại thông báo ICMP phổ biến:

|  |  |
| --- | --- |
| Mã Loại(Type) | Ý nghĩa |
| 0 | Echo Reply (phản hồi từ lệnh ping) |
| 3 | Destination Unreachable (đích không thể đến) |
| 8 | Echo Request (yêu cầu từ lệnh ping) |
| 11 | Time Exceeded (hết thời gian chờ) |

Bảng 3.1. Một số loại thông báo ICMP phổ biến

### So sánh ICMP với các giao thức cùng lớp để hiểu rõ hơn về vai trò của giao thức.

- Định nghĩa và vai trò chính:

|  |  |  |  |
| --- | --- | --- | --- |
|  | ICMP | IP | ARP |
| Tên đầy đủ | Internet Control Message Protocol | Internet Protocol | Address Resolution Protocol |
| Chức năng | Cung cấp thông báo lỗi, chẩn đoán mạng (vd: ping, traceroute) | Giao thức chính của tầng mạng, chịu trách nhiệm truyền tải dữ liệu giữa các địa chỉ IP. | Chuyển đổi địa chỉ IP thành địa chỉ MAC trong mạng nội bộ (LAN). |
| Vai trò | Hỗ trợ, kiểm tra và đảm bảo tính ổn định của giao tiếp IP. | Chuyển tiếp các gói tin từ nguồn đến đích thông qua địa chỉ IP.Chuyển tiếp các gói tin từ nguồn đến đích thông qua địa chỉ IP. | Giao tiếp giữa tầng mạng (IP) và tầng liên kết dữ liệu (MAC). |
| Thuộc tầng | Tầng mạng (Network Layer). | Tầng mạng (Network Layer). | Tầng liên kết dữ liệu (Data Link Layer), liên quan đến giao tiếp giữa thiết bị trong cùng mạng. |

Bảng 3.2. so sánh định nghĩa và vai trò chính của ICMP, IP và ARP

Cách hoạt động:

|  |  |  |  |
| --- | --- | --- | --- |
|  | ICMP | IP | ARP |
| Nguyên lý hoạt động | Gửi thông điệp phản hồi (error, thông báo) để kiểm tra mạng. | Truyền gói tin giữa các thiết bị thông qua địa chỉ IP. | Gửi yêu cầu tìm địa chỉ MAC (ARP Request) và nhận phản hồi (ARP Reply). |
| Thông điệp chính | Thông báo lỗi (Destination Unreachable, Time Exceeded), Echo Request/Reply (ping). | Gói tin dữ liệu chứa địa chỉ IP nguồn và đích. | Bảng ánh xạ IP-MAC (ARP table) để gửi gói tin đến địa chỉ MAC đích trong mạng LAN. |
| Tính liên kết | Là công cụ hỗ trợ giao thức IP, không thực hiện truyền dữ liệu. | Là giao thức chính, cung cấp giao tiếp đầu cuối. | Là giao thức bổ trợ, hoạt động trong mạng cục bộ để hỗ trợ IP. |

Bảng 3.3. So sánh ICMP, IP và ARP

-Ứng dụng và giới hạn:

|  |  |  |  |
| --- | --- | --- | --- |
|  | ICMP | IP | ARP |
| Ứng dụng chính | - Ping kiểm tra kết nối.  - Traceroute xác định đường đi của gói tin qua mạng. | - Gửi dữ liệu giữa các thiết bị trong mạng.  - Cung cấp địa chỉ logic (IP). | - Tìm địa chỉ MAC để gửi dữ liệu trong mạng LAN. |
| Ưu điểm | - Đơn giản, hiệu quả để chẩn đoán lỗi mạng. | - Cốt lõi của giao tiếp mạng, tiêu chuẩn hóa và đáng tin cậy. | - Nhanh chóng ánh xạ địa chỉ IP-MAC. |
| Hạn chế | - Không truyền dữ liệu, chỉ mang tính hỗ trợ. | - Không hoạt động trong mạng không có IP (vd: các giao thức khác ở tầng liên kết). | - Dễ bị tấn công (vd: ARP Spoofing) nếu không có biện pháp bảo vệ. |

Bảng 3.4. So sánh ICMP, IP và ARP

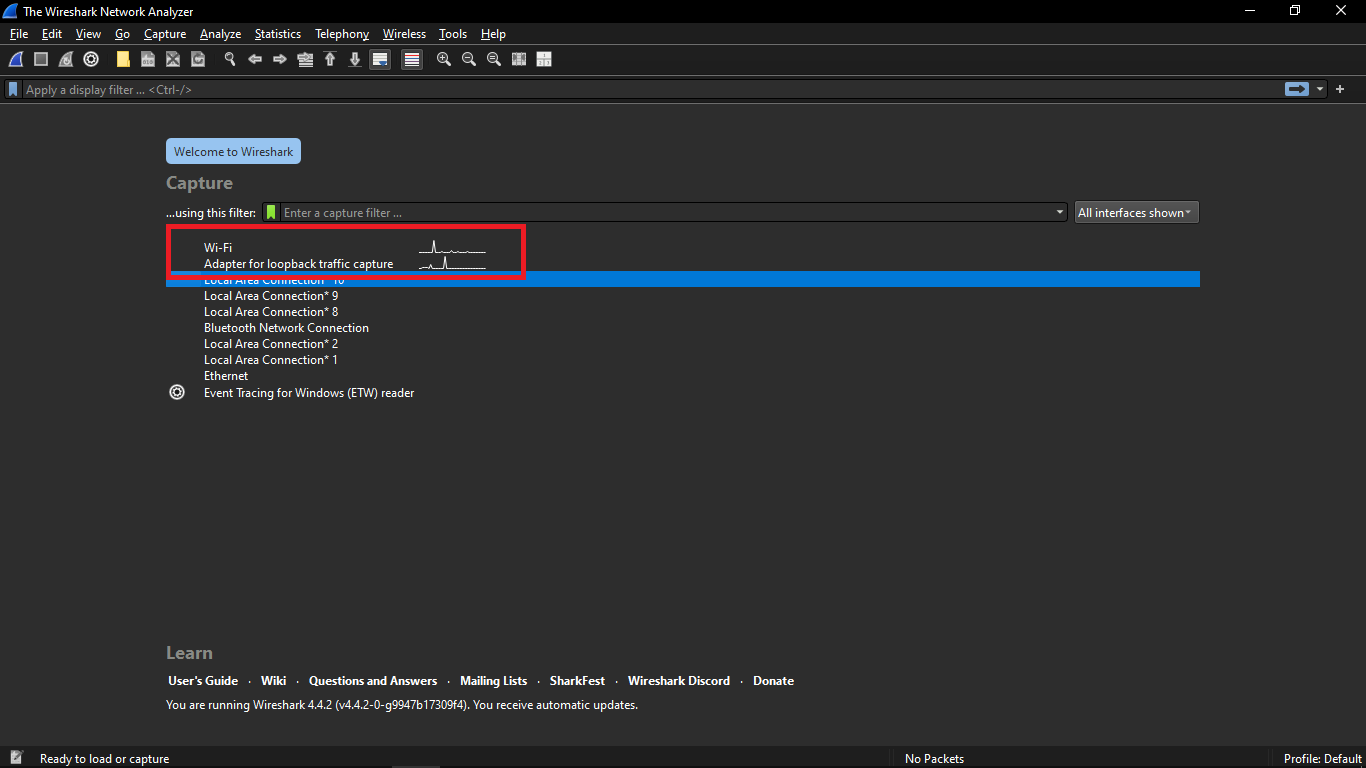
So sánh tổng quát:

|  |  |  |  |
| --- | --- | --- | --- |
|  | ICMP | IP | ARP |
| Vai trò chính | Chẩn đoán và phản hồi lỗi mạng. | Truyền tải dữ liệu. | Tìm kiếm địa chỉ MAC từ IP. |
| Dạng gói tin | ICMP Message (trong gói IP). | Gói tin IP. | Gói ARP Request/Reply. |
| Liên quan đến bảo mật | Có thể bị lạm dụng (ICMP flood). | Dễ bị tấn công nếu không mã hóa. | Dễ bị ARP Spoofing. |

Bảng 3.5. So sánh tổng quát ICMP, IP và ARP

## Nghiên cứu phần mềm phân tích mạng Wireshark

**- wireshark:** wireshark là Công dụng của ứng dụng này là dùng để bắt, phân tích và xác định các vấn đề có liên quan đến network bao gồm: kết nối chậm, rớt gói tin hoặc các truy cập bất thường. Thông qua Wireshark, quản trị viên có thể hiểu hơn về các Network Packets đang chạy trên hệ thống. Như vậy, việc xác định nguyên nhân gây ra lỗi cũng sẽ dễ dàng hơn.



Hình 3.11. Những card mạng đang có dữ liệu chạy qua

- Tính năng của wireshark:

+ Trước hết, Wireshark được Network administrators sử dụng trong việc khắc phục sự cố về mạng.

+ bên cạnh đó Wireshark còn được các kỹ sư Network security dùng để kiểm tra các vấn đề liên quan đến bảo mật.

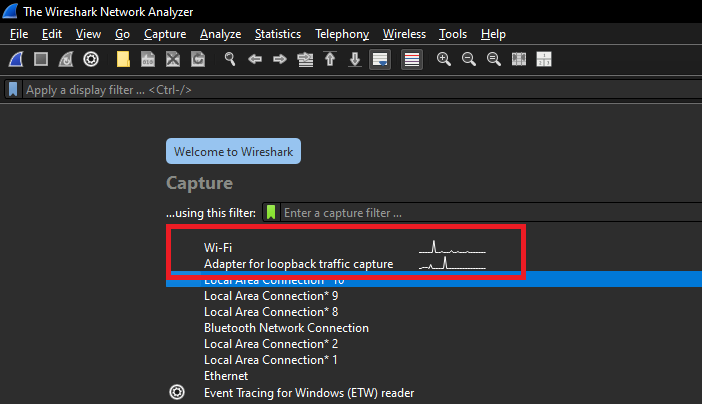
+ các developers dùng Wireshark trong việc gỡ lỗi triển khai giao thức.

+ Còn đối với người dùng mạng máy tính bình thường thì Wireshark giúp chúng ta học internals giao thức mạng.

+ Ngoài ra, Wireshark còn được sử dụng trong rất nhiều tình huống thực tế khác nữa mà chỉ những người trong giới chuyên môn mới biết câu trả lời.

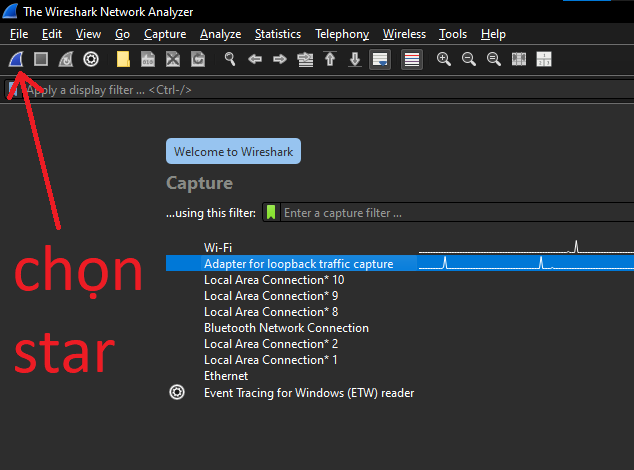
## Mô phỏng và phân tích các thông tin trong các gói tin ICMP bằng Wireshark

- mở Wireshark Trong danh sách các giao diện mạng, chọn giao diện đang hoạt động (Ethernet, Wi-Fi, v.v.). Wireshark sẽ hiển thị lưu lượng mạng theo thời gian thực:



Hình 3.12. Nghiên cứu công cụ wireshark

-Nhấn **Start** để bắt đầu thu thập gói tin.

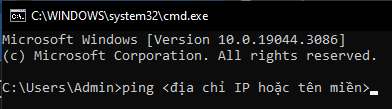


Hình 3.13. Nghiên cứu công cụ wireshark

### Mô phỏng giao thức ICMP bằng một số phương pháp phổ biến:

- sử dụng lệnh **ping:**

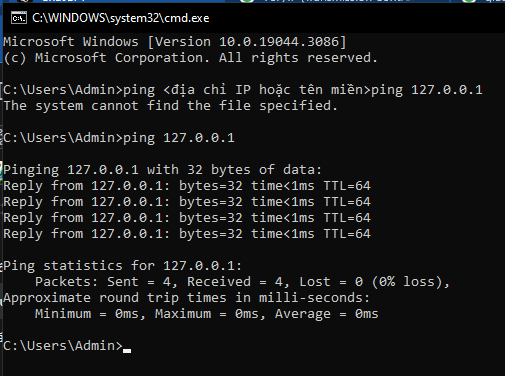
**+** Mở Command Prompt (Windows), gõ lệnh: Ping <...>



Hình 3.14. Mô phỏng giao thức ICMP

Lệnh này sẽ gửi các gói tin ICMP Echo Request tới địa chỉ và nhận ICMP Echo Reply từ máy đích.

ở đây, tôi chỉ có một máy tính nên sẽ Gửi lệnh ping đến 127.0.0.1 (loopback).



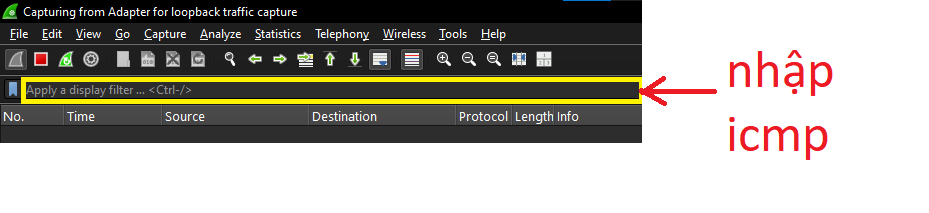
Hình 3.15. Thông báo gửi gói tin thành công

Điều này giúp kiểm tra chức năng ICMP trên máy tính mà không cần kết nối mạng thực tế.

Các thông số:

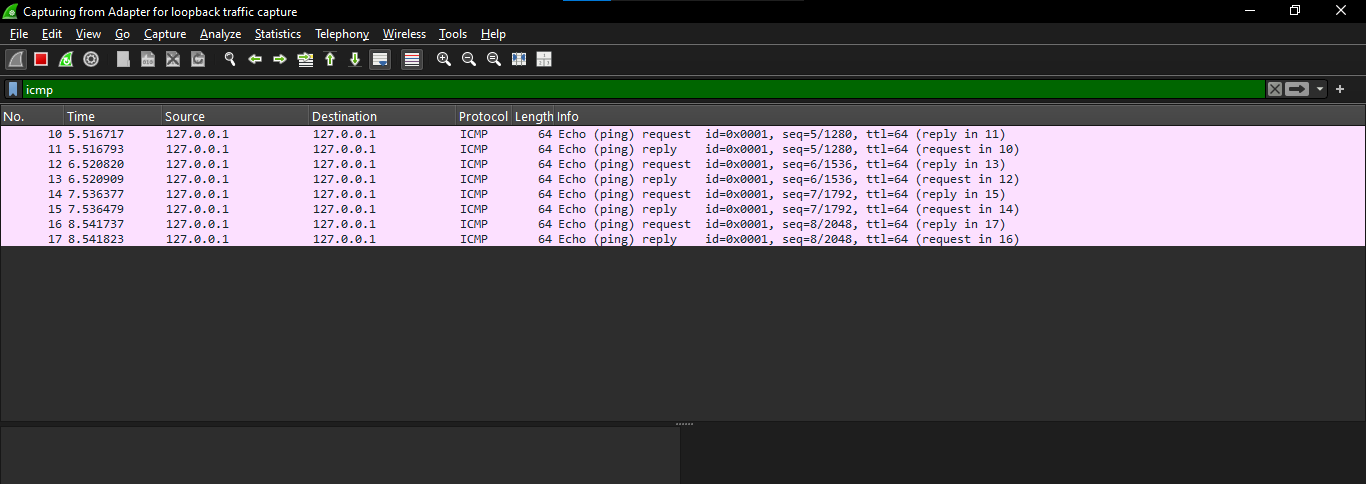
* **Reply from**: Xác nhận nhận được phản hồi từ địa chỉ đích.
* **bytes**: Kích thước gói tin.
* **time**: Thời gian phản hồi.
* **TTL**: Time-to-Live của gói tin.

+ quay lại wireshark và gõ từ khóa icmp vào trong ô Filter



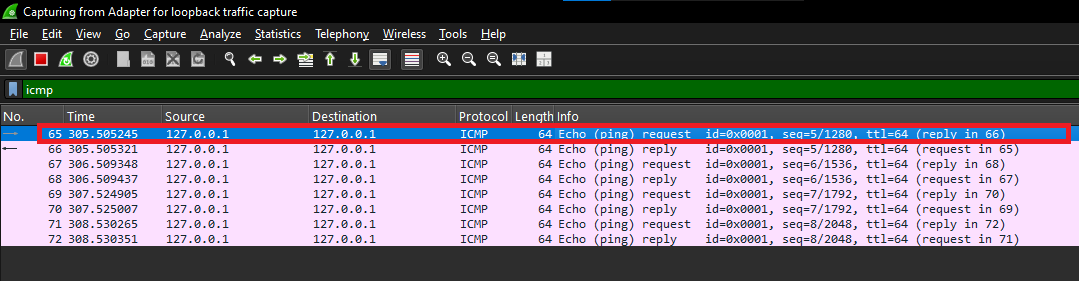
Hình 3.16. Lọc các gói tin ICMP

Kết quả :

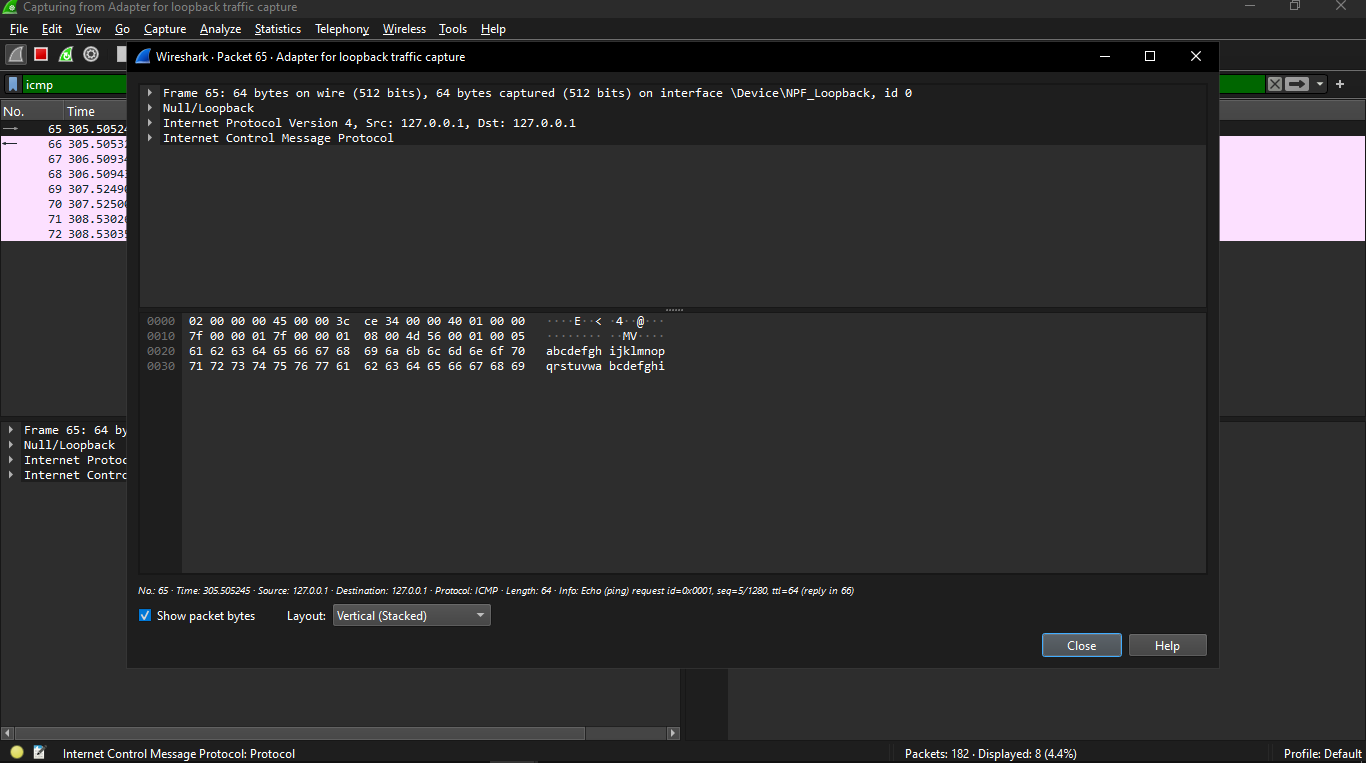


Hình 3.17. Kết quả lọc các gói tin

### Phân tích gói tin.

- Chọn một gói tin Echo Request (Type 8) hoặc Echo Reply (Type 0) để xem chi tiết.

Hình 3.18. Chọn một gói tin để xem chi tiết



Hình 3.19. Chi tiết gói tin

****-Chi tiết cơ bản của gói tin.****

* **Frame 65**: Đây là thứ tự gói tin trong danh sách thu thập.
* **64 bytes on wire (512 bits)**: Gói tin có kích thước 64 byte, tương ứng 512 bit.
* **Interface**: Gói tin được chụp trên giao diện Null/Loopback.
* **IP Source (Src)**: 127.0.0.1.
* **IP Destination (Dst)**: 127.0.0.1.

Với “**IP Source (Src)**: 127.0.0.1. “ và “ **IP Destination (Dst)**: 127.0.0.1. ” là địa chỉ loopback, cho biết gói tin được gửi và nhận bởi chính máy tính.

# KẾT LUẬN

## Kết quả đạt được:

+ Bổ xung lượng lớn kiến thức về mạng máy tính, cũng như các giao thức mạng phổ biến.

+ Hiểu thêm về khái niệm, chức năng và cách thức vận hành của các giao thức mạng phổ biến.

+ Nắm được quá trình đóng gói dữ liệu để truyền tải trong mạng qua mô hình tham chiếu OSi.

+Thành thạo sử dụng Wireshark để phân tích các giao thức mạng, tập trung vào ICMP.

+ Thành công trong việc mô phỏng các hoạt động của giao thức ICMP.

## Đánh giá và rút ra bài học:

+ Giải thích cách ICMP giúp quản lý và giám sát mạng, như kiểm tra kết nối (Ping) và xác định đường đi (Traceroute).

+ Mô tả vai trò của ICMP trong việc thông báo các lỗi mạng, giúp các thiết bị mạng và quản trị viên xử lý sự cố hiệu quả hơn.

+ Khả năng nhanh chóng phát hiện sự cố kết nối và đường truyền, đem lại Hiệu quả cao trong kiểm tra mạng.

+ Cấu trúc gói tin đơn giản giúp dễ dàng triển khai và sử dụng trong nhiều tình huống khác nhau.  
+ ICMP dễ bị khai thác trong các cuộc tấn công mạng như DDoS, Ping of Death, và ICMP tunneling.

+ Một số gói tin ICMP có thể không cung cấp đủ thông tin chi tiết để giải quyết mọi vấn đề mạng.

+ Cần triển khai các biện pháp bảo mật để hạn chế các lỗ hổng liên quan đến ICMP.

+ Đề xuất cải tiến hoặc bổ sung các tính năng mới để tăng cường hiệu quả và an toàn cho ICMP.

## Hướng phát triển tương lai:

Nghiên cứu sâu hơn về bảo mật liên quan đến ICMP:

+ Phát hiện và ngăn chặn tấn công: Nghiên cứu các phương pháp để phát hiện và ngăn chặn các cuộc tấn công sử dụng ICMP.

+ Cải thiện giao thức: Đề xuất các cải tiến trong giao thức ICMP để tăng cường bảo mật mà không ảnh hưởng đến chức năng chính.

Mở rộng mô phỏng với các giao thức khác:

+ Kết hợp ICMP với các giao thức mạng khác: Nghiên cứu cách ICMP tương tác với các giao thức khác như TCP, UDP, và HTTP trong các tình huống mạng phức tạp.

+ Mô phỏng trong môi trường thực tế lớn hơn: Thực hiện mô phỏng trên các mạng lớn và phức tạp hơn để đánh giá hiệu suất và tính ổn định của ICMP.

Ứng dụng công nghệ mới:

+ Sử dụng trí tuệ nhân tạo (AI) và học máy (Machine Learning): Áp dụng AI để phân tích và tối ưu hóa việc sử dụng ICMP trong quản lý mạng.

+ Internet vạn vật (IoT): Nghiên cứu vai trò và ứng dụng của ICMP trong các mạng IoT, nơi có nhiều thiết bị kết nối và yêu cầu quản lý hiệu quả.

Phát triển công cụ và phần mềm hỗ trợ:

+ Công cụ giám sát và phân tích ICMP: Phát triển các công cụ mới giúp giám sát, phân tích và quản lý các gói tin ICMP hiệu quả hơn.

+ Tự động hóa quá trình mô phỏng: Xây dựng các kịch bản mô phỏng tự động để dễ dàng kiểm tra và đánh giá các tình huống mạng khác nhau.

# 

# DANH MỤC TÀI LIỆU THAM KHẢO

<https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml>

<https://tenten.vn/tin-tuc/arp-la-gi/>

<https://vinahost.vn/point-to-point/#ftoc-heading-8>

<https://kb.pavietnam.vn/telnet-la-gi-1-so-dac-diem-cua-telnet.html>

<https://wiki.matbao.net/dns-la-gi-tam-quan-trong-cua-dns-trong-the-gioi-mang/>

<https://fptshop.com.vn/tin-tuc/danh-gia/http-la-gi-166491>

<https://vinahost.vn/smtp-la-gi/>

<https://tenten.vn/tin-tuc/icmp/>

<https://nhanhoa.com/tin-tuc/nat-la-gi.html>

<https://www.momo.vn/hoi-dap/cong-nghe-ssl-tls-la-gi>

<https://www.totolink.vn/article/111-dhcp-la-gi-tim-hieu-ve-dhcp.html>