**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

Logo, company name

Description automatically generated

**BÀI TẬP LỚN**

**TÊN HỌC PHẦN: MẠNG MÁY TÍNH**

**ĐỀ TÀI: Tìm hiểu công nghệ IPv6 và chuyển đổi từ IPv4**

**Giáo viên hướng dẫn: Th.S Lê Văn Phong**

**Th.S Nguyễn Văn Nhân**

**Sinh viên thực hiện:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Mã sv** | **Họ và tên** | **Lớp** |
| **1** | **1771020534** | **Đào Đức Phong** | **CNTT 17-02** |

**Hà Nội, năm 2025**

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

Logo, company name

Description automatically generated

**BÀI TẬP LỚN**

**TÊN HỌC PHẦN: MẠNG MÁY TÍNH**

**ĐỀ TÀI : Tìm hiểu công nghệ IPv6 và chuyển đổi từ IPv4**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Mã Sinh Viên** | **Họ và Tên** | **Ngày Sinh** | **Điểm** | |
| **Bằng Số** | **Bằng Chữ** |
| **1** | **1771020534** | **Đào Đức Phong** | **05/11/2005** |  |  |

**CÁN BỘ CHẤM THI 1 CÁN BỘ CHẤM THI 2**

**Hà Nội, năm 2025**

# LỜI NÓI ĐẦU

Trong thời đại công nghệ 4.0, mạng Internet đã trở thành một hạ tầng thiết yếu, gắn liền với mọi hoạt động của con người, tổ chức và doanh nghiệp. Tuy nhiên, sự bùng nổ của các thiết bị kết nối mạng đã dẫn đến những thách thức lớn về khả năng mở rộng và đáp ứng nhu cầu sử dụng địa chỉ IP. Trước bối cảnh đó, công nghệ IPv6 đã ra đời như một giải pháp tất yếu để thay thế và khắc phục các hạn chế của IPv4, mở ra hướng phát triển bền vững cho mạng lưới toàn cầu.

IPv6 không chỉ mang đến không gian địa chỉ gần như vô hạn mà còn tích hợp nhiều tính năng vượt trội như hiệu suất cao, bảo mật tốt hơn và khả năng tối ưu hoá hoạt động mạng. Việc chuyển đổi từ IPv4 sang IPv6 là một bước đi quan trọng và cần thiết, nhưng cũng đặt ra nhiều thách thức từ góc độ kỹ thuật, quản lý và chi phí.

Báo cáo này được thực hiện với mục tiêu tìm hiểu sâu về công nghệ IPv6, từ lý thuyết đến các khía cạnh thực tiễn của quá trình chuyển đổi từ IPv4. Qua đó, tôi mong muốn không chỉ làm sáng tỏ vai trò của IPv6 trong việc thúc đẩy sự phát triển của Internet mà còn đóng góp một góc nhìn hữu ích vào việc xây dựng lộ trình chuyển đổi hiệu quả cho các tổ chức và doanh nghiệp.

Tôi xin gửi lời cảm ơn chân thành đến giảng viên bộ môn Mạng Máy tính đã tận tình hướng dẫn, cùng sự hỗ trợ từ các tài liệu tham khảo đáng tin cậy. Hy vọng rằng bài báo cáo sẽ mang lại những thông tin thiết thực và hữu ích đến quý thầy cô và bạn đọc.

# MỤC LỤC

[LỜI NÓI ĐẦU 3](#_Toc190383237)

[MỤC LỤC 4](#_Toc190383238)

[MỤC LỤC HÌNH ẢNH 7](#_Toc190383239)

[MỤC LỤC BẢNG 8](#_Toc190383240)

[CHƯƠNG 1 : KIẾN THỨC CƠ SỞ 9](#_Toc190383241)

[1.1. Tổng quan về bảo mật dữ liệu trong mạng 9](#_Toc190383242)

[1.1.1 Định nghĩa và vai trò của mạng máy tính 9](#_Toc190383243)

[1.1.2 Phân loại mạng máy tính (LAN, WAN, MAN, Internet) 9](#_Toc190383244)

[1.1.3 Các thành phần cơ bản trong mạng máy tính 10](#_Toc190383245)

[1.2. Tầng ứng dụng 11](#_Toc190383246)

[1.2.1 Chức năng của tầng ứng dụng 11](#_Toc190383247)

[1.2.2 Các giao thức phổ biến trong tầng ứng dụng (HTTP, FTP, SMTP, DNS) 11](#_Toc190383248)

[1.2.3 Ứng dụng tầng ứng dụng trong đời sống 12](#_Toc190383249)

[1.3. Tầng giao vận 13](#_Toc190383250)

[1.3.1 Vai trò của tầng giao vận 13](#_Toc190383251)

[1.3.2 Giao thức TCP và UDP 13](#_Toc190383252)

[1.3.3 So sánh TCP và UDP 15](#_Toc190383253)

[1.4. Tầng mạng 15](#_Toc190383254)

[1.4.1 Chức năng của tầng mạng 15](#_Toc190383255)

[1.4.2 Giao thức IP (IPv4 và IPv6) 16](#_Toc190383256)

[1.5. Tầng liên kết dữ liệu và mạng cục bộ (LAN) 17](#_Toc190383257)

[1.5.1 Chức năng của tầng liên kết dữ liệu 17](#_Toc190383258)

[1.5.2 Công nghệ Ethernet và các giao thức liên quan 18](#_Toc190383259)

[1.5.3 Mạng cục bộ (LAN) và ứng dụng thực tiễn 18](#_Toc190383260)

[CHƯƠNG 2 : PHÂN THÍCH ĐỀ TÀI VÀ GIẢI QUYẾT ĐỀ TÀI 20](#_Toc190383261)

[2.1. Tổng quan về công nghệ Ipv6 20](#_Toc190383262)

[2.1.1 Khái niệm Ipv6 20](#_Toc190383263)

[2.1.2 Vai trò của Ipv6 trong Internet và mạng LAN 20](#_Toc190383264)

[2.1.3 Các nguy cơ và thách thức đối với Ipv6 21](#_Toc190383265)

[2.2. Các loại địa chỉ Ipv6 21](#_Toc190383266)

[2.3. Cách hoạt động của IPv6. 22](#_Toc190383267)

[2.3.1 Tự động cấu hình địa chỉ (Stateless Address Autoconfiguration - SLAAC) 22](#_Toc190383268)

[*2.3.1 Giao thức Neighbor Discovery Protocol (NDP)* 22](#_Toc190383269)

[2.3.3. Giao thức ICMPv6 22](#_Toc190383270)

[2.4. Ưu điểm và nhược điểm của Ipv6 so với Ipv4. 23](#_Toc190383271)

[2.4.1 Ưu điểm của IPv6 23](#_Toc190383272)

[2.4.2. Nhược điểm của Ipv6. 23](#_Toc190383273)

[2.4.3. Bảng so sánh IPv4 và IPv6 24](#_Toc190383274)

[2.5. Thực hành trên Cisco packet tracer. 24](#_Toc190383275)

[2.5.1. Mô hình Ipv6 và Ipv4 sử dụng công nghệ dualstack. 24](#_Toc190383276)

[2.5.2. Kết quả 25](#_Toc190383277)

[CHƯƠNG 3 : Công Cụ Hỗ Trợ Chuyển Đổi và Triển Khai IPv6 26](#_Toc190383278)

[3.1. Vai trò của công cụ và công nghệ trong quá trình chuyển đổi IPv6 26](#_Toc190383279)

[3.2. Công cụ giám sát và phân tích dữ liệu mạng 26](#_Toc190383280)

[3.2.1. Wireshark 26](#_Toc190383281)

[3.2.2. PRTG Network Monitor 27](#_Toc190383282)

[3.2.3. Microsoft Network Monitor 27](#_Toc190383283)

[3.3. Công cụ cấu hình và triển khai hạ tầng IPv6 28](#_Toc190383284)

[*3.3.1.* *OpenWRT* 28](#_Toc190383285)

[*3.3.2.* *FreeBSD* 28](#_Toc190383286)

[*3.3.3.*  *NAT64* 29](#_Toc190383287)

[3.4. Công cụ bảo mật và kiểm tra tính an toàn 29](#_Toc190383288)

[*3.4.1. IPv6 Compatibility Test* 29](#_Toc190383289)

[*3.4.2. Cisco Security Solutions* 30](#_Toc190383290)

[*3.4.3. Huawei IPv6 Transition Toolkit* 30](#_Toc190383291)

[KẾT LUẬN 31](#_Toc190383292)

[DANH MỤC TÀI LIỆU THAM KHẢO 32](#_Toc190383293)

# MỤC LỤC HÌNH ẢNH

[Hình ảnh 1 : Sử dụng môi trường mô phỏng để thấy sự khác biệt rõ ràng 32](#_Toc187700544)

[Hình ảnh 2 :Kết quả so sánh 35](#_Toc187700545)

# MỤC LỤC BẢNG

[Table 1 : So sánh TCP và UDP lập bảng 14](#_Toc187700562)

[Table 2 : So sán giao thức IP (IPv4 và IPv6) 16](#_Toc187700563)

[Table 3 : Phân loại mã hoá đối xứng và bất đối xứng 22](#_Toc187700564)

[Table 4 : Nhược điểm của Ipv6 và mô tả 27](#_Toc187700565)

[Table 5: Sự khác biệt giữa Ipv6 và Ipv4 32](#_Toc187700566)

# CHƯƠNG 1 : KIẾN THỨC CƠ SỞ

## Tổng quan về bảo mật dữ liệu trong mạng

### Định nghĩa và vai trò của mạng máy tính

#### Định nghĩa

Mạng máy tính là hệ thống kết nối các thiết bị (máy tính, điện thoại, máy in, v.v.) để chia sẻ dữ liệu, tài nguyên và dịch vụ thông qua các giao thức truyền thông.

#### Vai trò

Chia sẻ tài nguyên: Giúp sử dụng chung các thiết bị như máy in, ổ cứng, máy chủ, v.v.

Trao đổi thông tin: Cung cấp khả năng gửi, nhận dữ liệu giữa các thiết bị nhanh chóng và hiệu quả.

Tăng cường hiệu suất làm việc: Hỗ trợ làm việc nhóm, quản lý dữ liệu tập trung.

Ứng dụng đa dạng: Hỗ trợ các hoạt động như thương mại điện tử, giáo dục trực tuyến, quản lý doanh nghiệp, v.v.

Kết nối toàn cầu: Giúp các thiết bị truy cập và chia sẻ thông tin trên Internet.

### Phân loại mạng máy tính (LAN, WAN, MAN, Internet)

#### **LAN (Local Area Network)**:

Phạm vi: Hẹp, thường trong một tòa nhà, văn phòng, trường học.

Tốc độ: Cao, kết nối nội bộ nhanh.

Mục đích: Chia sẻ tài nguyên, dữ liệu trong phạm vi nhỏ.

#### **WAN (Wide Area Network)**:

Phạm vi: Rộng, kết nối các thành phố, quốc gia.

Tốc độ: Thấp hơn LAN, phụ thuộc vào hạ tầng mạng.

Mục đích: Kết nối mạng LAN ở các địa điểm khác nhau.

#### MAN (Metropolitan Area Network):

Phạm vi: Trung bình, trong một thành phố hoặc khu vực đô thị.

Tốc độ: Trung bình, cao hơn WAN nhưng thấp hơn LAN.

Mục đích: Kết nối các mạng trong một thành phố, ví dụ giữa các trường đại học hoặc chi nhánh công ty.

#### Internet:

Phạm vi: Toàn cầu.

Tốc độ: Đa dạng, phụ thuộc vào hạ tầng và nhà cung cấp.

Mục đích: Kết nối hàng tỷ thiết bị trên toàn thế giới để trao đổi thông tin.

### Các thành phần cơ bản trong mạng máy tính

#### Thiết bị đầu cuối:

Bao gồm máy tính, điện thoại, máy in, máy chủ,... đóng vai trò gửi/nhận dữ liệu trong mạng.

#### Thiết bị kết nối mạng:

Switch: Kết nối các thiết bị trong cùng một mạng nội bộ (LAN).

Router: Kết nối các mạng khác nhau, định tuyến dữ liệu qua mạng Internet.

Access Point (AP): Kết nối không dây các thiết bị vào mạng.

#### Môi trường truyền dẫn:

Cáp mạng: Dây đồng (cáp xoắn đôi, cáp đồng trục) hoặc cáp quang.

Kết nối không dây: Wi-Fi, Bluetooth, sóng radio.

#### Giao thức mạng:

Quy định cách thức giao tiếp giữa các thiết bị, ví dụ: TCP/IP, HTTP, FTP.

#### Dịch vụ mạng:

Hỗ trợ các chức năng như truyền tệp, duyệt web, email, dịch vụ DNS.

#### Hệ điều hành mạng (NOS):

Phần mềm quản lý hoạt động của các thiết bị trong mạng, như Windows Server, Linux.

Các thành phần này phối hợp để tạo thành một hệ thống mạng hoàn chỉnh, đảm bảo truyền tải và xử lý thông tin hiệu quả.

## Tầng ứng dụng

### Chức năng của tầng ứng dụng

Giao tiếp với người dùng: Cung cấp các giao thức và dịch vụ để người dùng tương tác với mạng (HTTP, FTP, SMTP, DNS, v.v.).

Truy cập và xử lý dữ liệu: Hỗ trợ ứng dụng truy xuất, gửi và nhận dữ liệu qua mạng.

Đảm bảo định dạng dữ liệu: Định dạng dữ liệu phù hợp giữa các hệ thống, bao gồm mã hóa và chuyển đổi định dạng.

Quản lý phiên làm việc: Thiết lập, duy trì và đồng bộ hóa các phiên làm việc giữa các thiết bị hoặc ứng dụng.

### Các giao thức phổ biến trong tầng ứng dụng (HTTP, FTP, SMTP, DNS)

#### HTTP (Hypertext Transfer Protocol)

Chức năng: Giao thức truyền tải siêu văn bản, được sử dụng để trao đổi dữ liệu giữa máy khách và máy chủ web.

Đặc điểm: Hoạt động theo mô hình yêu cầu-đáp ứng, sử dụng cổng 80 (HTTP) và 443 (HTTPS).

#### FTP (File Transfer Protocol)

Chức năng: Giao thức truyền tệp, cho phép người dùng tải lên và tải xuống tệp giữa máy tính và máy chủ.

Đặc điểm: Hoạt động trên cổng 21, hỗ trợ chế độ kết nối chủ động và bị động.

#### SMTP (Simple Mail Transfer Protocol)

Chức năng: Giao thức truyền email, sử dụng để gửi thư từ máy khách đến máy chủ hoặc giữa các máy chủ email.

Đặc điểm: Hoạt động trên cổng 25 (mặc định) hoặc 587 (bảo mật).

#### DNS (Domain Name System)

Chức năng: Giao thức chuyển đổi tên miền (domain name) thành địa chỉ IP và ngược lại.

Đặc điểm: Hoạt động trên cổng 53, sử dụng cơ chế phân tán để lưu trữ thông tin.

### Ứng dụng tầng ứng dụng trong đời sống

#### Truy cập website (HTTP/HTTPS)

Người dùng truy cập các trang web để tra cứu thông tin, mua sắm, học tập, giải trí.

#### Chuyển tệp (FTP)

Sử dụng để tải tệp dữ liệu từ máy chủ (như phần mềm, tài liệu) hoặc lưu trữ dữ liệu trực tuyến.

#### Gửi và nhận email (SMTP, IMAP, POP3)

Gửi thư điện tử qua các nền tảng như Gmail, Outlook, phục vụ liên lạc cá nhân và công việc.

#### Tra cứu thông tin mạng (DNS)

Dịch tên miền thành địa chỉ IP để truy cập các dịch vụ trực tuyến một cách dễ dàng.

#### Hội nghị trực tuyến (HTTP, WebSocket)

Ứng dụng trong các nền tảng như Zoom, Microsoft Teams để học tập và làm việc từ xa.

#### Mạng xã hội (HTTP/HTTPS)

Kết nối và chia sẻ thông tin qua Facebook, Instagram, TikTok.

## Tầng giao vận

### Vai trò của tầng giao vận

#### Chuyển dữ liệu giữa thiết bị

Đảm bảo dữ liệu được truyền từ thiết bị nguồn đến thiết bị đích đúng thứ tự và không mất mát.

#### Kiểm soát luồng dữ liệu

Quản lý tốc độ truyền để tránh tình trạng quá tải giữa các thiết bị.

#### Đảm bảo độ tin cậy

Sử dụng cơ chế xác nhận (ACK) và gửi lại dữ liệu khi phát hiện lỗi, đảm bảo truyền tải chính xác (TCP).

#### Định danh ứng dụng

Sử dụng số cổng (port) để phân biệt các ứng dụng khác nhau trên cùng một thiết bị.

#### Hỗ trợ truyền dữ liệu không kết nối

Với giao thức UDP, tầng này cung cấp khả năng truyền dữ liệu nhanh mà không cần thiết lập kết nối trước.

### Giao thức TCP và UDP

#### TCP (Transmission Control Protocol)

Đặc điểm:

Kết nối, đáng tin cậy, đảm bảo dữ liệu truyền đầy đủ và đúng thứ tự.

Có cơ chế kiểm tra lỗi, xác nhận và gửi lại dữ liệu khi bị mất.

Ứng dụng:

Truyền email (SMTP), duyệt web (HTTP/HTTPS), truyền tệp (FTP).

#### UDP (User Datagram Protocol)

Đặc điểm:

Không kết nối, không đảm bảo độ tin cậy hoặc thứ tự dữ liệu.

Truyền nhanh, không có cơ chế kiểm tra lỗi hay gửi lại.

Ứng dụng:

Truyền phát video, âm thanh (streaming), trò chơi trực tuyến, DNS.

### So sánh TCP và UDP

|  |  |  |
| --- | --- | --- |
| Tiêu chí | TCP (Transmission Control Protocol) | UDP (User Datagram Protocol) |
| Kết nối | Có kết nối (Connection-oriented). | Không kết nối(Connectionless). |
| Độ tin cậy | Đảm bảo truyền dữ liệu chính xác, không mất gói. | Không đảm bảo độ tin cậy, có thể mất gói. |
| Thứ tự dữ liệu | Đảm bảo dữ liệu đến đúng thứ tự. | Không đảm bảo dữ liệu đến đúng thứ tự. |
| Kiểm tra lỗi | Có cơ chế kiểm tra lỗi, xác nhận (ACK), và gửi lại. | Chỉ kiểm tra lỗi cơ bản, không có gửi lại gói. |
| Tốc độ | Chậm hơn do kiểm tra và xác nhận. | Nhanh hơn do không kiểm tra và xác nhận. |
| Sử dụng tài nguyên | Tiêu tốn tài nguyên cao hơn. | Tiêu tốn tài nguyên ít hơn. |
| Ứng dụng | Email (SMTP), duyệt web (HTTP/HTTPS), truyền tệp (FTP). | Truyền phát video/âm thanh, DNS, game trực tuyến. |
| Cổng phổ biến | |  | | --- | | Cổng 80 (HTTP), 443 (HTTPS), 25 (SMTP). |  |  | | --- | |  | | Cổng 53 (DNS), 161 (SNMP). |

Table : So sánh TCP và UDP lập bảng

## Tầng mạng

### Chức năng của tầng mạng

#### Định tuyến (Routing):

Tìm đường đi tối ưu để truyền dữ liệu từ nguồn đến đích qua các mạng trung gian.

#### Đánh địa chỉ (Addressing):

Gán địa chỉ IP cho các thiết bị để định danh và truyền dữ liệu chính xác.

#### Chia nhỏ và lắp ghép gói tin:

Phân chia dữ liệu thành các gói tin nhỏ và ghép lại ở đầu nhận.

#### Kiểm soát lưu lượng:

Điều phối dữ liệu để tránh tình trạng nghẽn mạng.

#### Quản lý lỗi:

Phát hiện và xử lý lỗi trong quá trình truyền dữ liệu.

#### Hỗ trợ giao thức IP:

Cung cấp giao thức IP (IPv4, IPv6) để đảm bảo truyền tải dữ liệu qua các mạng khác nhau

### Giao thức IP (IPv4 và IPv6)

|  |  |  |
| --- | --- | --- |
| Tiêu chí | IPv4 | IPv6 |
| Độ dài địa chỉ | 32 bit (dạng xxx.xxx.xxx.xxx). | 128 bit (dạng xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx). |
| Số lượng địa chỉ | ~4,3 tỷ địa chỉ. | Rất lớn (2^128 địa chỉ). |
| Không gian địa chỉ | Hạn chế, có thể cạn kiệt. | Rất rộng, không lo cạn kiệt. |
| Cấu hình | Yêu cầu cấu hình thủ công hoặc DHCP. | Tự động cấu hình với tính năng Auto Configuration. |
| Bảo mật | Không hỗ trợ bảo mật tích hợp. | Tích hợp IPSec để tăng cường bảo mật. |
| Hiệu quả định tuyến | Ít hiệu quả hơn, sử dụng NAT để tiết kiệm địa chỉ. | Hiệu quả hơn nhờ loại bỏ NAT. |
| Hỗ trợ QoS (Chất lượng dịch vụ) | Hạn chế. | Hỗ trợ tốt hơn với trường "Flow Label". |
| Tương thích với hệ thống cũ | Rất phổ biến, hỗ trợ hầu hết thiết bị. | Chưa được hỗ trợ hoàn toàn ở một số thiết bị cũ. |
| Ứng dụng | Sử dụng phổ biến trong mạng truyền thống. | Dần thay thế IPv4, phù hợp với IoT và mạng hiện đại. |

Table : So sán giao thức IP (IPv4 và IPv6)

## Tầng liên kết dữ liệu và mạng cục bộ (LAN)

### Chức năng của tầng liên kết dữ liệu

#### Đóng gói dữ liệu:

Chuyển đổi dữ liệu thành các khung (frame) để truyền qua mạng vật lý.

#### Địa chỉ hóa:

Sử dụng địa chỉ MAC để định danh các thiết bị trong cùng một mạng cục bộ (LAN).

#### Phát hiện và sửa lỗi:

Phát hiện lỗi trong quá trình truyền và sửa lỗi cơ bản (nếu có).

#### Kiểm soát luồng:

Điều chỉnh tốc độ truyền dữ liệu giữa các thiết bị để tránh nghẽn mạng.

#### Quản lý truy cập:

Điều phối quyền truy cập vào phương tiện truyền dẫn, đảm bảo tránh xung đột khi nhiều thiết bị cùng gửi dữ liệu.

#### Hỗ trợ tầng vật lý:

Tương tác với tầng vật lý để đảm bảo dữ liệu được truyền đúng định dạng qua cáp hoặc không dây.

### Công nghệ Ethernet và các giao thức liên quan

#### Công nghệ Ethernet:

Là chuẩn mạng cục bộ (LAN) phổ biến, cho phép các thiết bị trong mạng trao đổi dữ liệu.

Sử dụng giao thức **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) để phát hiện và xử lý xung đột dữ liệu trên đường truyền.

#### Tốc độ Ethernet:

Bao gồm các phiên bản: Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), và 10 Gigabit Ethernet (10 Gbps).

#### Cấu trúc Ethernet Frame:

Gồm các thành phần: Tiêu đề (Header), Dữ liệu (Payload), và Kiểm tra lỗi (FCS).

#### Giao thức liên quan:

**ARP (Address Resolution Protocol):** Chuyển đổi địa chỉ IP thành địa chỉ MAC.

**RARP (Reverse ARP):** Chuyển đổi địa chỉ MAC thành địa chỉ IP.

**Spanning Tree Protocol (STP):** Tránh vòng lặp trong mạng Ethernet bằng cách vô hiệu hóa các liên kết dư thừa.

#### Ứng dụng:

Kết nối các thiết bị trong văn phòng, trường học, trung tâm dữ liệu với độ ổn định và tốc độ cao.

### Mạng cục bộ (LAN) và ứng dụng thực tiễn

#### Mạng cục bộ (LAN):

Là mạng kết nối các thiết bị trong một khu vực giới hạn như văn phòng, nhà ở, hoặc trường học.

Dùng công nghệ như Ethernet, Wi-Fi để truyền dữ liệu nhanh và ổn định.

#### Đặc điểm:

Tốc độ cao, độ trễ thấp.

Phạm vi nhỏ, quản lý dễ dàng.

Chi phí thiết lập thấp.

#### Ứng dụng thực tiễn:

**Văn phòng:** Kết nối máy tính, máy in, và thiết bị chia sẻ tài nguyên.

**Trường học:** Quản lý hệ thống học tập, kết nối các phòng máy tính.

**Nhà ở:** Chia sẻ Internet và dữ liệu giữa các thiết bị trong gia đình.

**Trung tâm dữ liệu:** Liên kết các máy chủ, lưu trữ và xử lý dữ liệu.

# CHƯƠNG 2 : PHÂN THÍCH ĐỀ TÀI VÀ GIẢI QUYẾT ĐỀ TÀI

## Tổng quan về công nghệ Ipv6

### Khái niệm Ipv6

**IPv6 (Internet Protocol version 6)** là phiên bản mới nhất của giao thức Internet (IP), được thiết kế để thay thế **IPv4** nhằm mở rộng không gian địa chỉ và cải thiện hiệu suất mạng. IPv6 sử dụng địa chỉ **128-bit** thay vì **32-bit** như IPv4, giúp cung cấp một số lượng địa chỉ gần như vô hạn.

### Vai trò của Ipv6 trong Internet và mạng LAN

#### Giải quyết vấn đề cạn kiệt địa chỉ IPv4:

Internet ngày càng mở rộng, đặc biệt với sự bùng nổ của IoT, nhưng IPv4 chỉ có khoảng **4,3 tỷ địa chỉ**, không đủ đáp ứng.

IPv6 với **128-bit địa chỉ** cung cấp một số lượng gần như vô hạn, giúp mọi thiết bị có thể kết nối mà không cần NAT.

#### Cải thiện định tuyến trên Internet:

IPv6 hỗ trợ **tự động cấu hình** và **định tuyến tốt hơn** nhờ thiết kế địa chỉ phân cấp, giúp các ISP quản lý mạng dễ dàng hơn.

#### Hỗ trợ bảo mật tốt hơn trên Internet:

**IPSec được tích hợp bắt buộc trong IPv6**, giúp mã hóa và bảo mật dữ liệu khi truyền tải trên mạng toàn cầu.

#### Cải thiện hiệu suất dịch vụ trực tuyến:

IPv6 loại bỏ **NAT** (Network Address Translation), giúp kết nối P2P (peer-to-peer) như **VoIP, game online, video call** hoạt động hiệu quả hơn.

#### Tự động cấu hình trong mạng LAN:

IPv6 hỗ trợ **SLAAC (Stateless Address Autoconfiguration)**, giúp thiết bị tự động nhận địa chỉ mà không cần DHCP.

Giảm tải cho **máy chủ DHCP**, phù hợp với mạng nội bộ lớn (công ty, trường học).

#### Tối ưu định tuyến trong LAN:

IPv6 cải thiện việc định tuyến nội bộ, giảm bớt các bảng định tuyến phức tạp, giúp mạng LAN hoạt động trơn tru hơn.

### Các nguy cơ và thách thức đối với Ipv6

#### Nguy cơ:

Tấn công bằng quét địa chỉ (Address Scanning Attack).

Tấn công giả mạo địa chỉ (IPv6 Spoofing).

Tấn công DoS/DdoS trên Ipv6.

Lỗ hổng từ cơ chế tự động cấu hình (SLAAC & RA Spoofing).

Bảo mật chưa đồng bộ với Ipv4.

#### Thách thức:

Chi phí triển khai cao.

Thiếu kỹ năng quản trị Ipv6.

Khả năng tương thích ngược với IPv4 kém.

Hiệu suất chưa ổn định.

Thiếu hỗ trợ từ nhà cung cấp dịch vụ (ISP).

## Các loại địa chỉ Ipv6

#### Ipv6 có ba loại địa chỉ chính:

**Unicast** (địa chỉ đơn): Chỉ định một thiết bị cụ thể trên mạng.

* + **Global Unicast**: Địa chỉ công khai trên Internet, giống IPv4 Public.
  + **Unique Local**: Giống IPv4 Private (FC00::/7).
  + **Link-Local**: Bắt buộc trên mỗi giao diện, dùng trong cùng một liên kết, luôn có tiền tố FE80::/10.
* **Multicast** (địa chỉ nhóm): Một gói tin gửi đến nhiều thiết bị cùng một lúc, thay thế **Broadcast** trong IPv4.
* **Anycast** (địa chỉ bất kỳ): Gửi đến nhiều thiết bị nhưng chỉ có một thiết bị gần nhất nhận gói tin.

## Cách hoạt động của IPv6.

### Tự động cấu hình địa chỉ (Stateless Address Autoconfiguration - SLAAC)

#### Thiết bị IPv6 có thể tự tạo địa chỉ mà không cần DHCP nhờ vào SLAAC**:**

Giao diện sẽ tạo địa chỉ **Link-Local** (FE80::/10).

Nếu nhận được tiền tố từ router, thiết bị sẽ tạo địa chỉ **Global Unicast**.

***2.3.1 Giao thức Neighbor Discovery Protocol (NDP)***

#### Pv6 không dùng ARP như IPv4, thay vào đó sử dụng **NDP (Neighbor Discovery Protocol)** để tìm địa chỉ MAC của thiết bị khác trong mạng. NDP gồm:

**Router Advertisement (RA)**: Router quảng bá thông tin mạng.

**Router Solicitation (RS)**: Host yêu cầu router gửi thông tin mạng.

**Neighbor Solicitation (NS) & Neighbor Advertisement (NA)**: Tương tự ARP Request/Reply trong IPv4.

**Redirect**: Hướng dẫn host đến router tối ưu hơn.

### 2.3.3. Giao thức ICMPv6

#### ICMPv6 (Internet Control Message Protocol for IPv6) thay thế ICMP trong IPv4, được sử dụng cho:

Ping giữa các thiết bị IPv6.

Giao thức NDP.

Phát hiện lỗi và kiểm soát lưu lượng mạng.

## 2.4. Ưu điểm và nhược điểm của Ipv6 so với Ipv4.

### Ưu điểm của IPv6



Table 3 : Ưu điểm của Ipv6 và mô tả.

### Nhược điểm của Ipv6.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Nội dung do AI tạo ra có thể không chính xác.

Table 4 : Nhược điểm của Ipv6 và mô tả.

### 2.4.3. Bảng so sánh IPv4 và IPv6



Table 5 : Sự khác biệt giữa Ipv6 và Ipv4.

## 2.5. Thực hành trên Cisco packet tracer.

### 2.5.1. Mô hình Ipv6 và Ipv4 sử dụng công nghệ dualstack.

Ảnh có chứa biểu đồ, ảnh chụp màn hình, hàng, văn bản

Nội dung do AI tạo ra có thể không chính xác.

Img1 : Sử dụng môi trường mô phỏng để có thể thấy sự khác biệt rõ ràng.

### 2.5.2. Kết quả

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Img2 : Kết quả so sánh.

# CHƯƠNG 3 : Công Cụ Hỗ Trợ Chuyển Đổi và Triển Khai IPv6

## Vai trò của công cụ và công nghệ trong quá trình chuyển đổi IPv6

Quá trình chuyển đổi từ IPv4 sang IPv6 không chỉ là một quyết định chiến lược mà còn là thử thách kỹ thuật lớn đối với mọi tổ chức, từ doanh nghiệp vừa và nhỏ cho đến các tập đoàn công nghệ lớn. Việc chuyển đổi này đòi hỏi một loạt công cụ và giải pháp nhằm giám sát, phân tích, cấu hình và tối ưu hóa hệ thống mạng. Các công cụ và công nghệ này đóng vai trò cốt lõi trong việc khắc phục lỗi, giám sát hiệu suất hoạt động, kiểm tra tính tương thích và đảm bảo bảo mật dữ liệu xuyên suốt quá trình vận hành.

Chẳng hạn, đối với các tổ chức sử dụng hạ tầng cũ, việc xác định khả năng tương thích giữa thiết bị và giao thức IPv6 cần sự hỗ trợ của các công cụ kiểm tra chuyên sâu. Đồng thời, giải pháp giám sát mạng liên tục giúp phát hiện kịp thời các sự cố liên quan đến định tuyến hoặc băng thông. Đặc biệt, bảo mật trở thành yếu tố then chốt trong bối cảnh gia tăng các cuộc tấn công vào hạ tầng mạng.

## Công cụ giám sát và phân tích dữ liệu mạng

* + 1. **Wireshark**

Wireshark là công cụ phân tích gói tin mã nguồn mở hàng đầu, được sử dụng rộng rãi trong lĩnh vực quản trị mạng và an ninh mạng. Công cụ này cho phép người dùng theo dõi và kiểm tra chi tiết các gói dữ liệu truyền qua mạng, giúp phân tích thông tin ở nhiều lớp khác nhau trong mô hình OSI. Wireshark hỗ trợ cả giao thức IPv4 và IPv6, giúp đảm bảo tính linh hoạt và khả năng thích nghi với các hệ thống mạng hiện đại.

Ưu điểm:

* Hiển thị dữ liệu trực quan, dễ hiểu.
* Hỗ trợ lọc, tìm kiếm và phân loại gói tin theo nhiều tiêu chí.
* Giám sát mạng theo thời gian thực và lưu trữ dữ liệu để phân tích sau.

Nhược điểm:

* Đòi hỏi kiến thức chuyên môn để sử dụng hiệu quả.
* Khả năng phân tích trên mạng mã hóa bị hạn chế.
  + 1. **PRTG Network Monitor**

PRTG Network Monitor là một công cụ mạnh mẽ cung cấp khả năng giám sát mạng theo thời gian thực, giúp quản trị viên dễ dàng phát hiện và xử lý các vấn đề như tắc nghẽn băng thông, lỗi kết nối hay các sự cố định tuyến nghiêm trọng trên cả IPv4 và IPv6.

Ưu điểm:

* Hiển thị dữ liệu giám sát dưới dạng dashboard trực quan.
* Tích hợp cảnh báo tự động qua email hoặc thông báo đẩy.
* Hỗ trợ báo cáo chi tiết về hiệu suất mạng.

Nhược điểm:

* Yêu cầu phần cứng mạnh để hoạt động ổn định.
* Phiên bản miễn phí bị giới hạn số lượng cảm biến giám sát.
  + 1. **Microsoft Network Monitor**

Microsoft Network Monitor hỗ trợ kiểm tra tính tương thích giữa các thiết bị mạng và dịch vụ ứng dụng với IPv6.

Ưu điểm:

* Ghi nhận và phân tích chi tiết các gói tin truyền qua mạng.
* Hỗ trợ nhiều giao thức khác nhau.
* Giao diện thân thiện với người dùng.

Nhược điểm:

* Không còn được Microsoft phát triển và cập nhật.
* Ít tính năng nâng cao so với Wireshark.

## Công cụ cấu hình và triển khai hạ tầng IPv6

* + 1. ***OpenWRT***

OpenWRT là nền tảng mã nguồn mở giúp cấu hình router hoạt động trên cả IPv4 và IPv6 thông qua mô hình Dual-Stack.

Ưu điểm:

* Linh hoạt, có thể tùy chỉnh toàn diện.
* Hỗ trợ các module mở rộng cho quản lý băng thông, bảo mật.
* Giám sát dữ liệu mạng chi tiết.

Nhược điểm:

* Yêu cầu kiến thức kỹ thuật để thiết lập.
* Có thể không tương thích với một số phần cứng cũ.
  + 1. ***FreeBSD***

FreeBSD là một nền tảng hệ điều hành mã nguồn mở được đánh giá cao về tính ổn định và hiệu suất mạnh mẽ.

Ưu điểm:

* Hỗ trợ đầy đủ các giao thức IPv4 và IPv6.
* Tối ưu hóa hiệu suất máy chủ, giảm thiểu độ trễ.

Nhược điểm:

* Yêu cầu kỹ năng chuyên sâu để quản trị.
* Cộng đồng hỗ trợ nhỏ hơn so với Linux.

***3.3.3. NAT64***

NAT64 giúp các thiết bị chỉ hỗ trợ IPv4 có thể giao tiếp với hệ thống mạng IPv6.

Ưu điểm:

* Giúp quá trình chuyển đổi diễn ra từng bước mà không gây gián đoạn.
* Giảm chi phí nâng cấp hệ thống.

Nhược điểm:

* Có thể làm giảm hiệu suất do quá trình ánh xạ địa chỉ.
* Không hỗ trợ tất cả các ứng dụng cũ.

**3.4. Công cụ bảo mật và kiểm tra tính an toàn**

***3.4.1. IPv6 Compatibility Test***

IPv6 Compatibility Test giúp kiểm tra khả năng tương thích của hệ thống mạng với IPv6.

Ưu điểm:

* Xác định các điểm yếu bảo mật và lỗi cấu hình.
* Cung cấp báo cáo chi tiết giúp tối ưu hệ thống.

Nhược điểm:

* Chỉ kiểm tra được những vấn đề phổ biến, không phát hiện được lỗ hổng chuyên sâu.

***3.4.2. Cisco Security Solutions***

Bộ giải pháp bảo mật toàn diện của Cisco giúp bảo vệ hệ thống IPv6 trước các cuộc tấn công mạng.

Ưu điểm:

* Hỗ trợ tường lửa thế hệ mới, IDS/IPS và VPN tích hợp IPv6.
* Cập nhật thường xuyên để đối phó với các mối đe dọa mới.

Nhược điểm:

* Chi phí cao.
* Cấu hình phức tạp, đòi hỏi chuyên môn cao.

***3.4.3. Huawei IPv6 Transition Toolkit***

Bộ công cụ hỗ trợ giám sát, bảo mật và tối ưu hóa hệ thống IPv6.

Ưu điểm:

* Giúp doanh nghiệp nhanh chóng thích nghi với IPv6.
* Phát hiện kịp thời các bất thường trong mạng.

Nhược điểm:

* Không hỗ trợ nhiều hệ điều hành khác nhau.
* Phụ thuộc vào hệ sinh thái của Huawei.

# KẾT LUẬN

Trong bài tập lớn này, tôi đã nghiên cứu và trình bày một cách chi tiết về quá trình chuyển đổi từ IPv4 sang IPv6 – một bước tiến mang tính chiến lược và không thể thiếu trong lĩnh vực công nghệ mạng hiện nay. Nội dung bài tập đã tập trung làm rõ các vấn đề quan trọng như thực trạng áp dụng IPv6 tại Việt Nam và thế giới, các thách thức kỹ thuật và quản lý gặp phải, cũng như những giải pháp triển khai hiệu quả nhằm hỗ trợ quá trình chuyển đổi này.

Một trong những điểm nổi bật của bài tập là đã phân tích rõ ràng về lý do cần thiết của việc chuyển đổi sang IPv6 trong bối cảnh nhu cầu kết nối và trao đổi dữ liệu ngày càng bùng nổ. Sự phát triển mạnh mẽ của các công nghệ như IoT (Internet of Things), dịch vụ đám mây, và trí tuệ nhân tạo đã làm gia tăng áp lực lên hạ tầng mạng toàn cầu vốn dựa trên IPv4. Với không gian địa chỉ gần như cạn kiệt, IPv4 không còn đủ khả năng đáp ứng nhu cầu này, dẫn đến sự ra đời và phát triển mạnh mẽ của IPv6 với không gian địa chỉ gần như vô hạn.

Bài tập cũng đã đưa ra các phương pháp và giải pháp kỹ thuật giúp doanh nghiệp, tổ chức tối ưu hóa quá trình chuyển đổi sang IPv6. Các công nghệ như Dual-Stack, Tunneling và NAT64 được giới thiệu như những công cụ quan trọng hỗ trợ kết nối đồng thời giữa IPv4 và IPv6, giảm thiểu sự gián đoạn trong quá trình vận hành hệ thống mạng. Đặc biệt, các công cụ phân tích và giám sát mạng như Wireshark, PRTG Network Monitor, OpenWRT, FreeBSD, Cisco Security Solutions và Huawei IPv6 Transition Toolkit đã được đề cập để giúp quản trị viên nhanh chóng phát hiện, xử lý sự cố và tối ưu hiệu suất hệ thống.

Tuy vậy, bài tập vẫn còn tồn tại một số hạn chế nhất định. Thứ nhất, do giới hạn về thời gian và nguồn tư liệu tham khảo, nội dung liên quan đến các phương pháp bảo mật dành riêng cho IPv6 chưa được khai thác đầy đủ. Đây là một khía cạnh quan trọng cần được nghiên cứu sâu hơn trong tương lai vì nguy cơ tấn công mạng ngày càng tinh vi khi môi trường IPv6 trở nên phổ biến hơn. Thứ hai, bài tập chủ yếu tập trung vào giải pháp kỹ thuật phổ biến mà chưa có điều kiện đi sâu vào việc nghiên cứu, phân tích tình hình triển khai thực tế tại Việt Nam, nơi quá trình chuyển đổi sang IPv6 còn gặp nhiều trở ngại về cơ sở hạ tầng và nhận thức công nghệ.

Về hướng phát triển, chủ đề chắc chắn sẽ tiếp tục là một vấn đề quan trọng trong tương lai. Với tốc độ phát triển mạnh mẽ của các công nghệ số, nhu cầu kết nối không chỉ dừng lại ở con người mà còn mở rộng đến hàng tỷ thiết bị thông minh khác. Do đó, việc triển khai IPv6 một cách toàn diện, kết hợp với nghiên cứu các giải pháp bảo mật và tối ưu hiệu suất sẽ trở thành xu hướng tất yếu để xây dựng một hạ tầng mạng bền vững, đáp ứng nhu cầu của cuộc sống số hiện đại.

# DANH MỤC TÀI LIỆU THAM KHẢO

Trong quá trình tham khảo và nghiên cứu cũng như thu thập thông tin từ các nguồn tài liệu sau đây:

1. <https://www.ods.vn/tai-lieu/>
2. <https://cystack.net/blog/>
3. <https://securitybox.vn>
4. <https://vinsep.com/>
5. <https://securitybox.vn/>
6. <https://viblo.asia/>

Link github: https://github.com/nielday/Mangmaytinhipv4toipv6