TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG VIỆT - HÀN

**KHOA KỸ THUẬT MÁY TÍNH VÀ ĐIỆN TỬ**



ĐỒ ÁN MÔN HỌC

**CHUYỂN MẠCH VÀ ĐỊNH TUYẾN HỆ THỐNG MẠNG CHO CÔNG TY THỰC PHẨM ĐÔNG Á**

**Sinh viên thực hiện:** Biện Phương Vy – 23NS103

Nguyễn Quang Vương- 23NS101

Lê Thị Vy- 23NS104

Lê Đinhg Vũ- 23CE.B03

**Lớp học phần:** Chuyển mạch và định tuyến

**Giảng viên hướng dẫn:** ThS. Lê Tự Thanh

***Đà Nẵng, tháng 12 năm 2025***

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG VIỆT - HÀN

**KHOA KỸ THUẬT MÁY TÍNH VÀ ĐIỆN TỬ**



ĐỒ ÁN MÔN HỌC

**CHUYỂN MẠCH VÀ ĐỊNH TUYẾN HỆ THỐNG MẠNG CHO CÔNG TY THỰC PHẨM ĐÔNG Á**

**Sinh viên thực hiện:** Biện Phương Vy – 23NS103

Nguyễn Quang Vương- 23NS101

Lê Thị Vy- 23NS104

Lê Đinhg Vũ- 23CE.B03

Cao Bá Vương – 21...

**Lớp học phần:** Chuyển mạch và định tuyến

**Giảng viên hướng dẫn:** ThS. Lê Tự Thanh

***Đà Nẵng, tháng 12 năm 2025***

**NHẬN XÉT**

**(Của giảng viên hướng dẫn)**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

Đà Nẵng, tháng 12 năm 2025

Giảng viên hướng dẫn

ThS. Lê Tự Thanh

LỜI CẢM ƠN

Chúng em xin chân thành cảm ơn Khoa Kỹ thuật máy tính và Điện tử Trường Đại học Công nghệ Thông tin và Truyền thông Việt-Hàn cũng như là thầy/cô giảng dạy học phần Chuyển mạch và định tuyến đã tạo điều kiện cho chúng em trang bị những kiến thức, kỹ năng cơ bản cần có để hoàn thành đồ án môn học này.

Đặc biệt, em xin gửi đến giảng viên hướng dẫn thầy ThS. Lê Tự Thanh, người đã tận tình hướng dẫn, giúp đỡ chúng em trong suốt quá trình hoàn thành đồ án một lời cảm ơn sâu sắc nhất.

Tuy nhiên trong quá trình thực hiện đồ án, vì kiến thức chuyên ngành còn nhiều hạn chế nên chúng em vẫn còn nhiều thiếu sót khi tìm hiểu, đánh giá và trình bày về đề tài. Rất mong nhận được sự quan tâm, góp ý của các thầy/cô giảng viên bộ môn để đề tài của em được đầy đủ và hoàn chỉnh hơn.

Em xin chân thành cảm ơn!

*Sinh viên đại diện,*

# MỤC LỤC

Trang

[LỜI CẢM ƠN i](#_Toc12401)

[MỤC LỤC ii](#_Toc12221)

[DANH MỤC CÁC TỪ VIẾT TẮT v](#_Toc21856)

[DANH MỤC HÌNH ẢNH vii](#_Toc16655)

[DANH MỤC BẢNG ix](#_Toc21164)

[MỞ ĐẦU 1](#_Toc27835)

[A. GIỚI THIỆU 1](#_Toc27895)

[B. PHƯƠNG PHÁP NGHIÊN CỨU 3](#_Toc27469)

[C. Ý NGHĨA KHOA HỌC VÀ THỰC TIỄN 4](#_Toc10972)

[CHƯƠNG 1: CƠ SỞ LÝ THUYẾT 6](#_Toc21866)

[1.1 PHÂN MỀM MÔ PHỎNG HỆ THỐNG CISCO PACKET TRACER 6](#_Toc3901)

[1.1.1 Giới thiệu Cisco Packet Tracer 6](#_Toc5564)

[1.1.2 Tính năng của Cisco Packet Tracer 6](#_Toc1287)

[1.1.3 Ứng dụng của Cisco Packet Tracer 10](#_Toc4799)

[1.1.4 Ưu điểm và hạn chế 10](#_Toc27394)

[1.2 CÔNG NGHỆ CHUYỂN MẠCH 11](#_Toc24938)

[1.2.1 Chuyển mạch (Switching) 11](#_Toc13899)

[1.2.2 Thiết bị chuyển mạch (Switch) 11](#_Toc11849)

[1.2.3 Nguyên lý hoạt đông: 12](#_Toc17824)

[1.2.4 Chức năng của Switch: 13](#_Toc6163)

[1.2.5 Phân loại các thiết bị : 14](#_Toc21509)

[1.2.6 Ưu điểm và hạn chế của Switch: 14](#_Toc20545)

[1.3 CÔNG NGHỆ ĐỊNH TUYẾN 15](#_Toc11654)

[1.3.1 Định tuyến (Routing) 15](#_Toc14656)

[1.3.2 Các giao thức định tuyến 15](#_Toc7974)

[1.3.3 Thiết bị định tuyến (Router) 16](#_Toc14116)

[1.3.4 Chức năng của Router 17](#_Toc9027)

[1.3.5 Kiến trúc của Router 21](#_Toc20239)

[1.3.6 Phân loại Router 22](#_Toc5605)

[1.3.7 Ưu điểm và nhược điểm của Router 24](#_Toc21154)

[1.4 Thiết bị bảo mật 24](#_Toc22752)

[1.4.1 Vai trò của Firewall 25](#_Toc54)

[1.4.2 Chức năng của Firewall 25](#_Toc19889)

[1.4.3 Ứng dụng thực tế của Firewall: 26](#_Toc1463)

[1.5 VLAN 28](#_Toc31603)

[1.5.1 Khái niệm VLAN 28](#_Toc838)

[1.5.2 Chức năng của VLAN 28](#_Toc10602)

[1.5.3 Ưu điểm và hạn chế 29](#_Toc21528)

[CHƯƠNG 2: PHÂN TÍCH THIẾT KẾ HỆ THỐNG MẠNG CHO CÔNG TY THỰC PHẨM ĐÔNG Á 30](#_Toc15089)

[2.1 TỔNG QUAN VỀ CÔNG TY THỰC PHẨM ĐÔNG á 30](#_Toc22317)

[2.1.1 Giới thiệu chung 30](#_Toc16336)

[2.1.2 Cấu trúc Campus của Công ty Thực phẩm Đông Á 30](#_Toc32464)

[2.1.3 Cấu trúc tổ chức phòng ban 32](#_Toc1092)

[2.1.4 Khảo sát và thu thập thông tin 33](#_Toc25855)

[2.2 Thiết kế và xây dựng hệ thống 35](#_Toc1596)

[2.2.1 Lý thuyết về thiết kế và xây dựng hệ thống mạng 35](#_Toc21547)

[2.2.2 Yêu cầu về giám sát hệ thống 36](#_Toc8605)

[2.2.3 Thiết kế mạng logic 36](#_Toc28406)

[2.2.4 Thiết kế mạng vật lý 37](#_Toc5006)

[2.2.5 Thiết kế bảo mật 38](#_Toc14035)

[2.2.6 Đảm bảo dự phòng và khả năng mở rộng: 38](#_Toc13580)

[2.2.7 Kiểm thử và triển khai 39](#_Toc28855)

[2.2.8 Đánh giá và tối ưu hóa 40](#_Toc3942)

[2.3 Công nghệ và các thiết bị thích hợp cho hệ thống 40](#_Toc8249)

[2.3.1 Công nghệ cáp dẫn Cat6a 40](#_Toc16718)

[2.3.2 Công nghệ chuyển mạch 42](#_Toc21718)

[2.3.3 Công nghệ bảo mật Firepower 2110-ASA-K9: 43](#_Toc8599)

[2.4 Mô phỏng hệ thống mạng cho công ty Thực Phẩm Đông Á 44](#_Toc8758)

[2.4.1 Phân chia IP cho các vùng mạng 44](#_Toc13542)

[2.4.2 Tiến hành cấu hình mô phỏng 48](#_Toc9117)

[2.4.3 Sơ đồ vật lý 58](#_Toc30168)

[CHƯƠNG 3: KẾT QUẢ ĐẠT ĐƯỢC 59](#_Toc11251)

[3.1 TIẾN HÀNH KIỂM TRA ĐƯỜNG TRUYỀN TRONG HỆ THỐNG MẠNG 59](#_Toc11119)

[a. DHCP tự động cấp phát IP 59](#_Toc3849)

[b. Ping trong hệ thống LAN 59](#_Toc10173)

[c. Ngăn chặn tin tặc 60](#_Toc5638)

[d. Kiểm tra đường dự phòng 61](#_Toc22832)

[KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 62](#_Toc22)

[KẾT LUẬN 62](#_Toc10982)

[PHƯƠNG HƯỚNG PHÁT TRIỂN 62](#_Toc14813)

# DANH MỤC CÁC TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **STT** | **Viết tắt** | **Cụm từ tiếng Anh đầy đủ** |
| 1 | LAN | Local Area Network – Mạng cục bộ |
| 2 | WAN | Wide Area Network – Mạng diện rộng |
| 3 | VLAN | Virtual Local Area Netwwork – Mạng LAN ảo |
| 4 | MAC | Media Access Control – Địa chỉ điều khiển truy cập môi trường. |
| 5 | TCP | Transmission Control Protocol |
| 6 | UDP | User Datagram Protocol |
| 7 | RIP | Routing Information Protocol |
| 8 | OSPF | Open Shortest Path First |
| 9 | EIGRP | Enhance Interior Gateway Routing Protocol |
| 10 | BGP | Border Gateway Protocol |
| 11 | ACL | Access Control List |
| 12 | STP | Spanning Tree Protocol |
| 13 | QoS | Quality of Service |
| 14 | DHCP | Dynamic Host Configuration Protocol |
| 15 | VPN | Virtual Private Network |
| 16 | QC | Quality Control |
| 17 | R&D | Research and Development |

# DANH MỤC HÌNH ẢNH

***[Hình 1.1 Phần mềm Cisco Packet Tracer 1](#_Toc216995744)***

***[Hình 1.2 Mô phỏng cho một hệ thống mạng đơn giản 2](#_Toc216995745)***

***[Hình 1.3 Mạng LAN và cấu hình các dịch vụ Server 3](#_Toc216995746)***

***[Hình 1.4 Hỗ trợ cấu hình giả lập thực tế bằng CLI 4](#_Toc216995747)***

***[Hình 1.5 Thiết bị Switch tại Layer 2 7](#_Toc216995748)***

***[Hình 1.6 Switch giúp chia nhỏ và kết nối các thiết bị khác 8](#_Toc216995749)***

***[Hình 1.7 Thiết bị định tuyến Router 12](#_Toc216995750)***

***[Hình 1.8 Giao thức định tuyến tĩnh 12](#_Toc216995751)***

***[Hình 1.9 Giao thức định tuyến động OSPF 13](#_Toc216995752)***

***[Hình 1.10 Giao thức định tuyến động BGP trên Router Edge 13](#_Toc216995753)***

***[Hình 1.11 Phân chia Subnetting 14](#_Toc216995754)***

***[Hình 1.12 Sử dụng firewall ngăn chặn tấn công DDOS 15](#_Toc216995755)***

***[Hình 1.13 Router Core cho một hệ thống mạng nhỏ 17](#_Toc216995756)***

***[Hình 1.14 Router Edge 18](#_Toc216995757)***

***[Hình 1.15 Router Wireless 18](#_Toc216995758)***

***[Hình 1.16 Thiết bị firewall 20](#_Toc216995759)***

***[Hình 1.17 Mô phỏng bảo mật ngăn chặn tấn công IPS 21](#_Toc216995760)***

***[Hình 1.18 Mô phỏng quản lý lưu lượng QoS thông qua Firewall (ASA) 22](#_Toc216995761)***

***[Hình 1.19 Mô tả VLAN 23](#_Toc216995762)***

***[Hình 2.1 Tòa nhà Công ty Thực phẩm Đông Á 25](#_Toc216995763)***

***[Hình 2.2 Cấu trúc tổ chức phòng ban 27](#_Toc216995764)***

***[Hình 2.3 Ví dụ mô hình mạng hoàn chỉnh 30](#_Toc216995765)***

***[Hình 2.4 Thiết kế mạng logic theo mô hình 3 lớp 31](#_Toc216995766)***

***[Hình 2.5 Thiết kế mô hình mạng vật lý 32](#_Toc216995767)***

***[Hình 2.6 Mô tả một vài tính năng bảo mật và phân luồng 33](#_Toc216995768)***

***[Hình 2.7 Mô hình dự phòng tại các Dis 34](#_Toc216995769)***

***[Hình 2.8 Ảnh vật lý CAT6A 35](#_Toc216995770)***

***[Hình 2.9 Ảnh vật lý Router Cisco ISR 4331/K9 36](#_Toc216995771)***

***[Hình 2.10 Ảnh vật lý Switch Cisco Catalyst 1000 37](#_Toc216995772)***

***[Hình 2.11 Ảnh vật lý Switch Cisco 3650-24PS-L 38](#_Toc216995773)***

***[Hình 2.12 Ảnh vật lý của Firepower - ASA - K9 38](#_Toc216995774)***

***[Hình 2.13 Lệnh chia vlan 43](#_Toc216995775)***

***[Hình 2.14 Cấu hình địa chỉ IP cho các liên kết Core 44](#_Toc216995776)***

***[Hình 2.15 Cấu hình định tyến 44](#_Toc216995777)***

***[Hình 3.1 Kiểm tra tự động cấp phát IP tại DHCP 46](#_Toc216995778)***

***[Hình 3.2 Ping từ VLAN 10- VLAN 80 46](#_Toc216995779)***

# DANH MỤC BẢNG

***[Bảng 2.1 Quy mô chi nhánh Đà Nẵng](#_Toc216995723)*** *[26](#_Toc216995723)*

***[Bảng 2.2 Bảng mô tả cấu trúc tổ chức phòng ban](#_Toc216995724)*** *[27](#_Toc216995724)*

***[Bảng 2.3 Quy mô nhân sự](#_Toc216995725)*** *[28](#_Toc216995725)*

***[Bảng 2.4 Bảng chia IP cho người dùng cuối](#_Toc216995726)*** *[39](#_Toc216995726)*

***[Bảng 2.5 Bảng chia IP cho vùng Server Farm](#_Toc216995727)*** *[41](#_Toc216995727)*

***[Bảng 2.6 Bảng chia IP cho các mạng Peer-to-Peer](#_Toc216995728)*** *[42](#_Toc216995728)*

# MỞ ĐẦU

## A. GIỚI THIỆU

**1. Lý do chọn đề tài**

Trong bối cảnh hiện đại, công nghệ thông tin đã trở thành một phần không thể thiếu trong hoạt động của các tổ chức tài chính, đặc biệt là trong việc quản lý và vận hành hệ thống giao dịch. Với sự phát triển nhanh chóng của các dịch vụ tài chính trực tuyến, nhu cầu về một hệ thống mạng ổn định, bảo mật và hiệu quả trở nên ngày càng cấp thiết. Đối với Công ty Thực phẩm Đông Á, việc xây dựng một hệ thống mạng mạnh mẽ không chỉ đảm bảo các giao dịch diễn ra thông suốt mà còn hỗ trợ công ty mở rộng quy mô, phục vụ tốt hơn nhu cầu của khách hàng, và đáp ứng các tiêu chuẩn bảo mật tài chính nghiêm ngặt.

Hơn nữa, thiết kế hệ thống mạng phù hợp sẽ giúp công ty giảm thiểu các rủi ro từ tấn công mạng và các sự cố bất ngờ, bảo vệ an toàn cho các dữ liệu quan trọng như thông tin khách hàng, giao dịch, v.v. Đồng thời, việc phân tích và thiết kế mạng hợp lý sẽ giúp công ty xây dựng nền tảng vững chắc cho các ứng dụng và dịch vụ trong tương lai, như giao dịch trực tuyến, phân tích dữ liệu lớn, và các dịch vụ dựa trên điện toán đám mây.

Chính vì vậy, nhóm chúng em chọn đề tài "Thiết kế hệ thống mạng cho Công ty Thực phẩm Đông Á" nhằm đưa ra giải pháp mạng tối ưu, đáp ứng được các nhu cầu về hiệu suất, bảo mật và khả năng mở rộng.

**2. Mục đích nghiên cứu**

Mục tiêu chính của đề tài là phân tích và thiết kế một hệ thống mạng hoàn chỉnh cho Công ty Thực phẩm Đông Á đảm bảo đáp ứng các yêu cầu về hiệu suất, bảo mật, và khả năng mở rộng. Trong bối cảnh ngành tài chính ngày càng phụ thuộc vào công nghệ thông tin và mạng internet, việc xây dựng một hệ thống mạng đáng tin cậy, bảo mật và linh hoạt sẽ hỗ trợ tối ưu hóa các hoạt động giao dịch, bảo vệ dữ liệu và tạo điều kiện cho công ty phát triển trong tương lai.

Các mục tiêu cụ thể của đề tài bao gồm:

**Đảm bảo hiệu suất cao cho hệ thống mạng**: Thiết kế mạng có khả năng đáp ứng lưu lượng truy cập lớn, đặc biệt trong các giờ cao điểm của giao dịch tài chính, đồng thời đảm bảo độ trễ thấp để hỗ trợ các ứng dụng thời gian thực như giao dịch trực tuyến.

**Tăng cường bảo mật**: Đề xuất các giải pháp bảo mật như firewall, VPN, IPS/IDS nhằm bảo vệ dữ liệu nhạy cảm của công ty và ngăn chặn các cuộc tấn công từ bên ngoài, đảm bảo tuân thủ các quy định bảo mật trong ngành tài chính.

**Khả năng mở rộng và linh hoạt**: Thiết kế hệ thống mạng linh hoạt và dễ mở rộng, sẵn sàng cho các nhu cầu tăng trưởng trong tương lai, khi công ty mở rộng quy hoặc triển khai các dịch vụ tài chính mới.

**Tối ưu hóa chi phí vận hành**: Lựa chọn các giải pháp mạng phù hợp, giúp công ty tối ưu hóa chi phí mà vẫn đảm bảo hiệu quả, đặc biệt khi kết hợp các loại kết nối như leased line và SD-WAN.

Với các mục tiêu đã đề cập, hy vọng đề tài sẽ cung cấp được một giải pháp mạng phù hợp, giúp công ty cải thiện chất lượng dịch vụ, đảm bảo tính an toàn và sẵn sàng cho các cơ hội phát triển trong thời đại số.

**3. Đối tượng và phạm vi nghiên cứu**

**Đối tượng nghiên cứu :**

Các kỹ thuật chuyển mạch và định tuyến được ứng dụng trong việc xây dựng, quản lý và vận hành hệ thống mạng của Công ty Thực phẩm Đông Á. Cụ thể, đề tài tập trung vào cơ chế hoạt động của các thiết bị chuyển mạch Layer 2, Layer 3, các giao thức định tuyến động và tĩnh đang được sử dụng trong hệ thống mạng doanh nghiệp hiện nay. Bên cạnh đó, đề tài cũng xem xét cách thức các thiết bị mạng phối hợp với nhau để đảm bảo truyền tải dữ liệu hiệu quả, phân đoạn mạng bằng VLAN, định tuyến giữa các mạng con và tối ưu hóa luồng dữ liệu trong toàn bộ hệ thống.

**Phạm vi ngiên cứu :**

Đề tài tập trung vào cấu trúc mạng nội bộ (LAN) và mạng diện rộng (WAN) của Công ty Thực phẩm Đông Á, bao gồm mô hình phân lớp, thiết kế hệ thống chuyển mạch, thiết kế và triển khai các giao thức định tuyến như RIP, OSPF hoặc EIGRP tùy theo yêu cầu của mô hình. Đề tài không đi sâu vào các vấn đề an ninh mạng nâng cao, hệ thống giám sát hiệu năng hoặc các giải pháp ảo hóa mạng phức tạp, mà chỉ tập trung mô tả và phân tích các kỹ thuật liên quan trực tiếp đến hoạt động chuyển mạch và định tuyến nhằm đảm bảo hệ thống hoạt động ổn định, hiệu quả và đáp ứng nhu cầu truyền tải dữ liệu của tổ chức.

## B. PHƯƠNG PHÁP NGHIÊN CỨU

**1. Phương pháp nghiên cứu lý thuyết**

Phương pháp này được sử dụng để thu thập và tổng hợp các kiến thức liên quan đến chuyển mạch, định tuyến, mô hình phân lớp mạng và những giao thức phổ biến như VLAN, STP, OSPF, EIGRP hay RIP. Các tài liệu học thuật, giáo trình chuyên ngành và tiêu chuẩn của Cisco được phân tích nhằm xây dựng nền tảng hiểu biết vững chắc về nguyên lý hoạt động của hệ thống mạng doanh nghiệp.

**2. Phương pháp khảo sát yêu cầu**

Áp dụng để thu thập thông tin về quy mô tổ chức, số lượng người dùng, loại dịch vụ cần cung cấp và nhu cầu băng thông. Việc khảo sát giúp xác định những ràng buộc về thiết bị, chi phí và khả năng mở rộng, từ đó định hướng cho chiến lược thiết kế mạng phù hợp. Trong trường hợp đề tài không dựa trên một mô hình thực tế sẵn có, phương pháp phân tích yêu cầu được sử dụng để xác định rõ các tiêu chí về hiệu năng, độ tin cậy, khả năng quản lý và an toàn thông tin.

**3. Phương pháo mô hình hóa**

Áp dụng để biểu diễn cấu trúc mạng dưới dạng sơ đồ logic và sơ đồ vật lý. Mô hình hóa giúp đánh giá vị trí lắp đặt thiết bị, phân vùng mạng bằng VLAN, bố trí đường kết nối và xác định vai trò cụ thể của từng thiết bị trong mô hình. Các mô hình này là cơ sở cho việc triển khai mô phỏng và kiểm thử.

**4. Phương pháp mô phỏng và thực ngiệm**

Các phần mềm như Cisco Packet Tracer, EVE-NG hoặc GNS3 được sử dụng để mô phỏng hoạt động của thiết bị chuyển mạch và router, kiểm tra khả năng định tuyến, đo độ ổn định của mạng, kiểm tra khả năng dự phòng và xử lý các tình huống lỗi. Dữ liệu thu được từ mô phỏng được dùng để phân tích mức độ phù hợp của thiết kế, từ đó đưa ra điều chỉnh cần thiết.

**5. Phương pháp đánh giá và so sánh**

Phương pháp này được sử dụng để lựa chọn cấu hình tối ưu giữa nhiều phương án, dựa trên tiêu chí về hiệu năng, chi phí, khả năng mở rộng và tính an toàn. Phương pháp này giúp đảm bảo rằng giải pháp được đề xuất không chỉ đáp ứng đúng yêu cầu mà còn mang tính thực tiễn cao và có thể triển khai trong môi trường doanh nghiệp.

## C. Ý NGHĨA KHOA HỌC VÀ THỰC TIỄN

**1. Ý nghĩa khoa học**

Đề tài tập trung đề xuất các giải pháp thiết kế mạng tối ưu cho Công ty Thực phẩm Đông Á, đáp ứng yêu cầu về quản lý, sản xuất và kinh doanh trong môi trường doanh nghiệp hiện đại. Nghiên cứu này góp phần làm rõ khả năng ứng dụng các công nghệ mạng tiên tiến như Policy-Based Routing (PBR), VLAN Trunking và HSRP trong mô hình mạng doanh nghiệp ngành thực phẩm, nơi đòi hỏi tính ổn định, bảo mật và khả năng mở rộng cao.

Bên cạnh đó, đề tài góp phần nâng cao nhận thức về vai trò và tầm quan trọng của hạ tầng mạng trong hoạt động quản trị, sản xuất và phân phối của doanh nghiệp thực phẩm. Kết quả nghiên cứu có thể làm nền tảng cho các hướng nghiên cứu chuyên sâu hơn, chẳng hạn như tối ưu hóa lưu lượng mạng trong các nhà máy sản xuất lớn hoặc ứng dụng trí tuệ nhân tạo (AI) trong giám sát, quản trị và tối ưu hệ thống mạng doanh nghiệp.

**2. Ý nghĩa thực tiễn**

Hệ thống mạng được thiết kế giúp Công ty Thực phẩm Đông Á tối ưu hóa công tác quản lý nội bộ, nâng cao hiệu quả vận hành trong các bộ phận như sản xuất, kho vận, kế toán và kinh doanh. Mô hình mạng có khả năng tích hợp linh hoạt các công nghệ hiện đại như kết nối từ xa thông qua VPN, lưu trữ và chia sẻ dữ liệu trên nền tảng đám mây (Cloud Storage), đáp ứng nhu cầu làm việc linh hoạt và mở rộng trong tương lai.

Ngoài ra, mô hình mạng được xây dựng theo hướng tối ưu chi phí đầu tư nhưng vẫn đảm bảo hiệu suất và độ tin cậy cao, phù hợp để triển khai thực tế tại các doanh nghiệp thực phẩm quy mô vừa và nhỏ. Hệ thống cũng góp phần tăng cường bảo mật thông tin doanh nghiệp, hạn chế rủi ro từ các mối đe dọa như tấn công mạng, mã độc hoặc đánh cắp dữ liệu, từ đó đảm bảo an toàn cho dữ liệu sản xuất, kinh doanh và thông tin khách hàng.

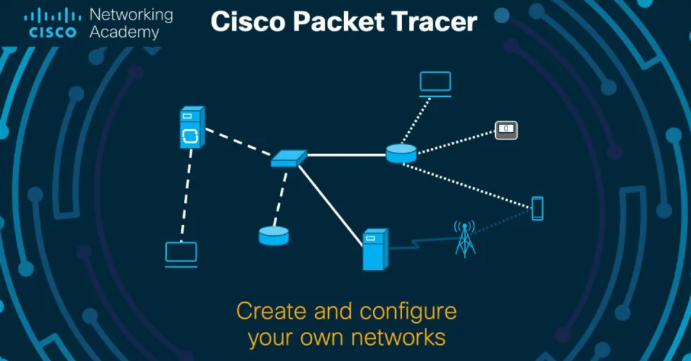
# CƠ SỞ LÝ THUYẾT

## PHÂN MỀM MÔ PHỎNG HỆ THỐNG CISCO PACKET TRACER

### Giới thiệu Cisco Packet Tracer

Cisco Packet Tracer là một công cụ mô phỏng mạng mạnh mẽ do Cisco phát triển, được sử dụng chủ yếu để thiết kế, mô phỏng, và kiểm tra các mạng máy tính. Nó hỗ trợ việc học tập và thực hành các kỹ năng về mạng, đặc biệt là trong các chương trình học của Cisco Networking Academy.

Cisco Packet Tracer giúp người dùng xây dựng và kiểm tra các mạng từ đơn giản đến phức tạp mà không cần phải sử dụng phần cứng thực tế, giúp tiết kiệm chi phí và thời gian.

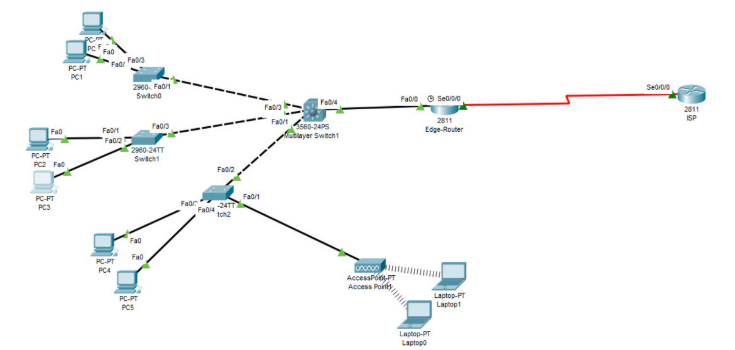


**Hình 1.1 Phần mềm Cisco Packet Tracer**

### Tính năng của Cisco Packet Tracer

**Mô phỏng mạng:**

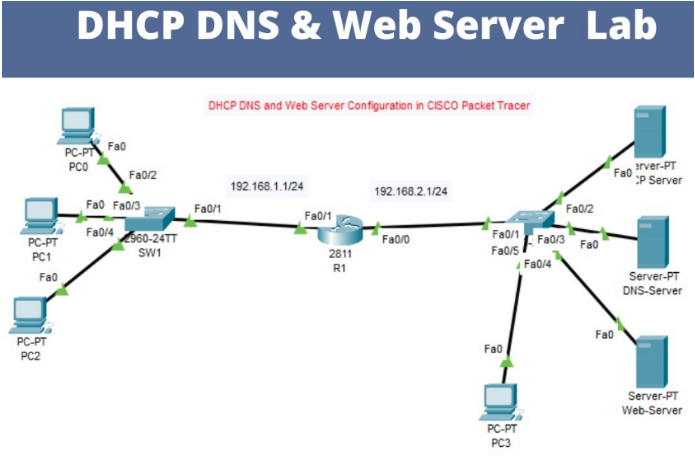
* Cisco Packet Tracer cho phép người dùng tạo và mô phỏng các mạng LAN, WAN và các mô hình mạng phức tạp khác mà không cần phải sử dụng phần cứng thực tế.
* Người dùng có thể mô phỏng nhiều thiết bị mạng như Router, Switch, Access Point, Máy tính, Server, và các thiết bị mạng khác.
* Công cụ này hỗ trợ mô phỏng cả mạng có dây và mạng không dây (Wi-Fi), giúp người dùng dễ dàng thử nghiệm các cài đặt và giao thức mạng khác nhau trong môi trường ảo.



**Hình 1.2 Mô phỏng cho một hệ thống mạng đơn giản**

**Tạo mạng ảo ( Virtual Network):**

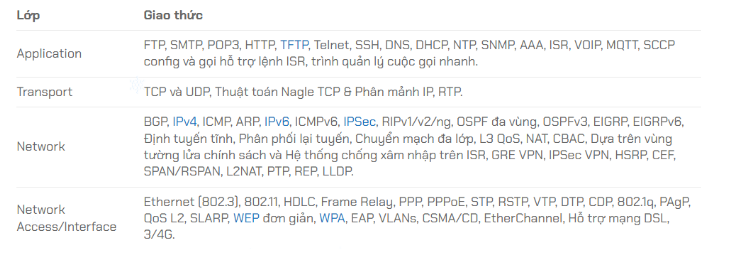
* Người dùng có thể tạo các mạng LAN, WAN, và các mô hình mạng phức tạp với các cấu hình định tuyến, chuyển mạch, và các giao thức như OSPF, EIGRP, RIP, v.v.
* Hỗ trợ nhiều giao thức mạng, bao gồm TCP/IP, DHCP, DNS, HTTP, v.v.



**Hình 1.3 Mạng LAN và cấu hình các dịch vụ Server**

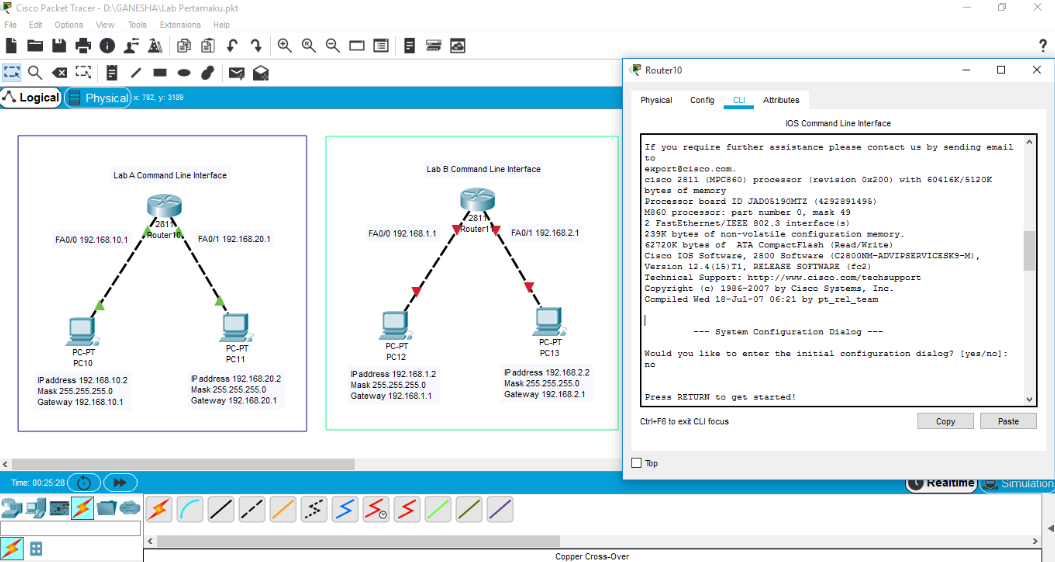
**Hỗ trợ các giao thức mạng:**

* Packet Tracer hỗ trợ hầu hết các giao thức của Cisco, giúp mô phỏng các tình huống mạng thực tế và các cấu hình nâng cao.
* Các giao thức như VLAN, STP (Spanning Tree Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First) có thể được cấu hình và mô phỏng trong môi trường ảo.



**Khả năng giả lập thiết bị thực tế:**

* Mô phỏng các thiết bị Cisco thực tế như **Router**, **Switch**, **Firewall**, và **Access Points**. Người dùng có thể cấu hình thiết bị theo cách giống như trên thiết bị thực tế.
* Dễ dàng thực hiện các thao tác cấu hình như trong CLI (Command Line Interface) của các thiết bị Cisco.



**Hình 1.4 Hỗ trợ cấu hình giả lập thực tế bằng CLI**

**Giao diện trực quan và dễ sử dụng:**

* Cisco Packet Tracer ‘có giao diện đồ họa người dùng (GUI) đơn giản và dễ sử dụng, cho phép người dùng kéo và thả thiết bị vào mô hình mạng.
* Hỗ trợ cả giao diện CLI và GUI để cấu hình các thiết bị, giúp học viên và kỹ sư có thể làm quen với cả hai phương thức.

**Hỗ trợ học tập và giảng dạy:**

* Cisco Packet Tracer là một công cụ tuyệt vời cho việc học và giảng dạy về mạng, giúp người học thực hành và xây dựng các mô hình mạng mà không cần đến thiết bị phần cứng đắt tiền.
* Tích hợp các bài học và bài tập thực hành từ **Cisco Networking Academy**, giúp người học luyện tập các kỹ năng và kiến thức về mạng.

**Quản lý giám sát:**

* Hệ thống mô phỏng có thể giám sát lưu lượng mạng, giúp người dùng theo dõi hoạt động của các gói tin, phân tích mạng, và kiểm tra kết nối giữa các thiết bị.
* Cho phép người dùng kiểm tra trạng thái của thiết bị trong mạng, chẳng hạn như router, switch, và máy tính.

### Ứng dụng của Cisco Packet Tracer

* **Mô hình hóa mạng**: Packet Tracer là công cụ lý tưởng để thiết kế và mô hình hóa các mạng trước khi triển khai thực tế, giúp đảm bảo rằng mạng được thiết kế sẽ hoạt động như dự kiến.
* **Tìm hiểu và thử nghiệm các giao thức**: Packet Tracer hỗ trợ một loạt các giao thức mạng, cho phép bạn thử nghiệm và hiểu rõ cách chúng hoạt động, đặc biệt hữu ích khi bạn muốn nghiên cứu về các giao thức mạng cụ thể.
* **Nghiên cứu và phát triển dự án**: Công cụ này là lựa chọn hàng đầu để thực hiện nghiên cứu và phát triển các dự án mạng. Bạn có thể tạo các mô hình mạng phức tạp để thử nghiệm các ý tưởng và giải pháp mạng.
* **Hỗ trợ giảng dạy từ xa**: Trong bối cảnh học tập từ xa, Packet Tracer là công cụ không thể thiếu để tạo bài giảng và hoạt động học trực tuyến trong môi trường giảng dạy từ xa.
* **Tạo môi trường thử nghiệm IoT**: Packet Tracer cung cấp khả năng tích hợp các thiết bị IoT, giúp bạn tạo và thử nghiệm các ứng dụng và kịch bản IoT một cách dễ dàng.
* **Tích hợp phát triển ứng dụng**: Bạn có thể sử dụng Packet Tracer để tích hợp mã Python và tự động hóa mạng, từ đó phát triển các ứng dụng và kịch bản tùy chỉnh một cách hiệu quả.

### Ưu điểm và hạn chế

**Ưu điểm :**

* Miễn phí (với tài khoản Cisco Networking Academy).
* Dễ sử dụng với giao diện thân thiện và trực quan.
* Mô phỏng thiết bị thực tế giúp học viên làm quen với các thiết bị mạng của Cisco.
* Giáo dục và đào tạo rất hiệu quả trong môi trường học.
* Kiểm tra mạng và lỗi: Packet Tracer cho phép bạn dễ dàng kiểm tra mạng và phát hiện các vấn đề cũng như lỗi trong mạng. Điều này giúp bạn phát triển kỹ năng sửa lỗi và tối ưu hóa mạng của mình.
* Thực hành trong môi trường an toàn: Packet Tracer cung cấp một môi trường an toàn và ảo để bạn thực hành và thử nghiệm các kỹ thuật mạng. Hỗ trợ mô phỏng mạng phức tạp với nhiều tính năng.

**Hạn chế :**

* Không mô phỏng hoàn toàn: Một số tính năng hoặc thiết bị mới của Cisco không được mô phỏng hoàn toàn trong Packet Tracer.
* Chỉ hỗ trợ thiết bị Cisco: Cisco Packet Tracer chủ yếu hỗ trợ các thiết bị của Cisco, do đó không thể mô phỏng các thiết bị của các nhà cung cấp khác như Juniper, HP, v.v.
* Giới hạn trong môi trường phức tạp: Mặc dù rất mạnh mẽ, nhưng Packet Tracer có thể không mô phỏng được tất cả các tình huống và cấu hình phức tạp mà có thể xảy ra trong môi trường thực tế.

## CÔNG NGHỆ CHUYỂN MẠCH

### Chuyển mạch (Switching)

Chuyển mạch (Switching) là quá trình tiếp nhận và chuyển tiếp khung dữ liệu (frame) trong phạm vi mạng cục bộ (LAN) dựa trên địa chỉ MAC. Thiết bị thực hiện chủ yếu là Switch, có nhiệm vụ học địa chỉ MAC của các thiết bị kết nối vào từng cổng và lưu thông tin này vào bảng MAC (MAC Address Table). Khi một frame đi vào switch, switch sẽ kiểm tra MAC đích và quyết định chuyển frame ra đúng cổng tương ứng; trường hợp chưa biết MAC đích, switch sẽ phát tán (flooding) ra các cổng còn lại trong cùng VLAN để tìm thiết bị đích. Nhờ cơ chế này, switching giúp tăng hiệu suất truyền dữ liệu trong LAN, giảm xung đột và tối ưu băng thông so với thiết bị hub truyền thống.

### Thiết bị chuyển mạch (Switch)

Switch (bộ chuyển mạch) là một thiết bị mạng dùng đểkết nối các thiết bị khác nhau trong cùng một mạng, chẳng hạn như máy tính, máy in, và [máy chủ](https://vinahost.vn/server-la-gi/), tạo thành một hệ thống mạng nội bộ ([LAN – Local Area Network](https://vinahost.vn/mang-lan-la-gi/)).

Switch hoạt động ở tầng liên kết dữ liệu (Layer 2) của mô hình OSI, giúp chuyển tiếp dữ liệu giữa các thiết bị bằng cách kiểm tra và định tuyến các gói dữ liệu đến đúng địa chỉ MAC (Media Access Control) của thiết bị đích.



**Hình 1.5 Thiết bị Switch tại Layer 2**

Switch còn là một phần quan trọng của hạ tầng [mạng](https://vinahost.vn/network-la-gi/), vì nó giúp các thiết bị trong mạng giao tiếp với nhau một cách hiệu quả, tăng băng thông và cải thiện hiệu suất.

Các Switch cao cấp hơn còn có thể hoạt động ở tầng mạng (Layer 3), cung cấp thêm các chức năng định tuyến và quản lý mạng linh hoạt.

### Nguyên lý hoạt đông:

Switch hoạt động dựa trên bảng MAC (MAC Address Table) và cơ chế học hỏi động (Dynamic Learning.

* **Học địa chỉ MAC:** Switch đọc địa chỉ MAC nguồn từ gói tin nhận được và lưu vào bảng MAC với cổng kết nối tương ứng.
* **Chuyển tiếp gói tin:** Dựa trên địa chỉ MAC của thiết bị đích, switch quyết định chuyển gói tin tới cổng nào.
* **Flooding:** Nếu địa chỉ MAC đích chưa được biết, switch gửi gói tin tới tất cả các cổng (trừ cổng nguồn).
* **Xử lý Broadcast và Multicast:** Gói tin Broadcast được gửi tới tất cả các thiết bị trong mạng. Gói tin Multicast được gửi tới các thiết bị tham gia vào nhóm Multicast cụ thể.
* **Kiểm soát lưu lượng và giảm xung đột**: Mỗi cổng trên bộ chuyển mạch hoạt động như một miền va chạm (collision domain) riêng biệt.
* **Cải thiện hiệu suất mạng**: Với việc chuyển tiếp dữ liệu chính xác và nhanh chóng, Switch giúp tăng băng thông mạng và tối ưu hóa hiệu suất.

### Chức năng của Switch:

**Chuyển các khung dữ liệu:** Switch được sử dụng để chuyển các khung dữ liệu giữa các thiết bị được kết nối với nhau. Chúng sẽ đóng vai trò giống như một người cảnh sát giao thông phân luồng dữ liệu trong mạng cục bộ. Từ đó, giúp các loại dữ liệu sẽ được chuyển đến đúng nơi mà chúng phải đến, không làm tắc nghẽn hay gián đoạn.

**Chia nhỏ hệ thống mạng LAN thành các segment nhỏ hơn:** Thông qua các cổng kết nối của Switch, nhiều segment được nối lại với nhau một cách dễ dàng hơn. Chức năng ngày của Switch sẽ giúp tạo ra các miền đụng độ nhỏ hơn về cung cấp băng thông lớn cho người dùng.



Hình 1.6 Switch giúp chia nhỏ và kết nối các thiết bị khác

**Kết nối được nhiều segment:** Khi hai máy tính liên kết với nhau, công dụng của Switch đó chính là nhận biết xem máy nào đang kết nối vào cổng của nó. Sau đấy, chúng sẽ thực hiện thiết lập mạng ảo giữa 2 cổng với nhau một cách tương thích nhất mà không làm ảnh hưởng đến việc lưu thông của các cổng khác.

**Xây dựng bảng và cung cấp thông tin:** Có liên quan đến các gói và gửi chúng đến đúng địa chỉ theo yêu cầu. Tức là Switch sẽ nhận dữ liệu từ các máy tính trong hệ thống và phân tích, tạo bảng sau đó gửi đi.

### Phân loại các thiết bị :

**Bảng 1.1 Phân loại các Switch**

|  |  |  |
| --- | --- | --- |
| **Tiêu chí** | **Nhóm thiết bị** | **Đặc trưng chính** |
| Khả năng quản trị | Unmanaged / Smart / Managed | Unmanaged cắm là chạy; Smart quản lý cơ bản; Managed hỗ trợ đầy đủ VLAN, STP, giám sát, bảo mật, cấu hình từ xa |
| Theo chức năng | Layer 2 / Layer 3 | L2 chuyển tiếp theo MAC; L3 vừa switching vừa routing theo IP (SVI), phục vụ inter-VLAN routing |
| Vai trò triển khai | Access / Distribution / Core | Access kết nối người dùng; Distribution tổng hợp và áp chính sách; Core chuyển mạch tốc độ cao, ưu tiên dự phòng và hiệu năng |

### Ưu điểm và hạn chế của Switch:

* **Ưu điểm:**
* Tăng hiệu suất mạng: Chuyển mạch thông minh giúp giảm va chạm dữ liệu.
* Dễ dàng mở rộng: Kết nối nhiều thiết bị mà không ảnh hưởng đến hiệu suất.
* Bảo mật: Hỗ trợ VLAN và ACL để kiểm soát truy cập.
* Quản lý linh hoạt: Switch Managed cung cấp khả năng quản lý từ xa.
* **Hạn chế:**
* Chi phí: Switch Managed hoặc Layer 3 có giá thành cao.
* Yêu cầu chuyên môn: Cần kỹ năng cấu hình và quản lý.
* Không thay thế hoàn toàn Router: Layer 3 Switch có định tuyến hạn chế so với Router chuyên dụng.

## CÔNG NGHỆ ĐỊNH TUYẾN

### Định tuyến (Routing)

Định tuyến (Routing) là quá trình xác định đường đi và chuyển tiếp gói tin (packet) giữa các mạng khác nhau dựa trên địa chỉ IP. Thiết bị thực hiện định tuyến có thể là router hoặc switch Layer 3. Khi nhận gói tin, thiết bị định tuyến tra cứu bảng định tuyến(routing table) để tìm tuyến phù hợp, quyết định next-hop hoặc giao diện ra, sau đó đóng gói dữ liệu về lớp liên kết dữ liệu tương ứng để chuyển tiếp sang chặng kế tiếp. Định tuyến là nền tảng để các mạng con (subnet/VLAN) liên lạc với nhau trong hệ thống nội bộ và là cơ chế bắt buộc để kết nối mạng LAN ra WAN/Internet.

### Các giao thức định tuyến

Bảng định tuyến có thể được hình thành theo hai hướng chính là định tuyến tĩnh (Static Routing) và định tuyến động (Dynamic Routing). Định tuyến tĩnh (Static Routing) do quản trị viên cấu hình thủ công, phù hợp cho mạng nhỏ, các tuyến cố định hoặc tuyến mặc định ra Internet; ưu điểm là kiểm soát chặt và ít tiêu tốn tài nguyên, nhưng kém linh hoạt khi topology thay đổi. Định tuyến động sử dụng các giao thức để các router trao đổi thông tin và tự cập nhật tuyến, phù hợp mạng vừa và lớn vì có khả năng thích nghi khi có sự cố hoặc mở rộng hệ thống.

**Bảng 1.2 Các giao thức định tuyến**

|  |  |  |
| --- | --- | --- |
| **Nhóm giao thức** | **Giao thức tiêu biểu** | **Đặc trưng và phạm vi sử dụng** |
| Static | Static Route, Default Route | Cấu hình thủ công; đơn giản, dễ kiểm soát; phù hợp tuyến cố định hoặc tuyến mặc định |
| Distance Vector | RIP | Dựa trên số hop; cấu hình đơn giản; hạn chế quy mô và hội tụ chậm hơn |
| Link State | OSPF | Dựa trên trạng thái liên kết; hội tụ nhanh, mở rộng tốt; phổ biến trong mạng campus/doanh nghiệp |
| Advanced Distance Vector | EIGRP (Cisco) | Hội tụ nhanh, linh hoạt trong môi trường Cisco; phù hợp triển khai nội bộ |
| Inter-domain | BGP | Định tuyến liên miền, dùng cho ISP/kết nối Internet; thường học ở mức tổng quan |

Trong phạm vi bài thực hành/mô phỏng, nội dung thường tập trung vào việc hiểu cơ chế bảng định tuyến, cấu hình tuyến tĩnh, triển khai OSPF cơ bản và kiểm tra đường đi bằng các công cụ như ping, traceroute và các lệnh show.

### Thiết bị định tuyến (Router)

 Router (thiết bị định tuyến) là một thiết bị mạng chuyên dụng dùng để kết nối các mạng khác nhau và định tuyến lưu lượng dữ liệu giữa chúng.

Router hoạt động ở tầng 3 (Network Layer) của mô hình OSI, sử dụng địa chỉ IP để định tuyến và truyền tải dữ liệu giữa các mạng.

Router phục vụ hai chức năng chính: Quản lý lưu lượng giữa các mạng này bằng cách chuyển tiếp gói dữ liệu đến địa chỉ IP dự định của chúng và cho phép nhiều thiết bị sử dụng cùng một kết nối Internet.



Hình 1.7 Thiết bị định tuyến Router

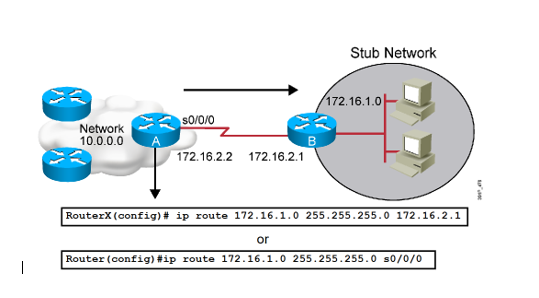
### Chức năng của Router

**Định tuyến (Routing):**

**Router** xác định đường đi tốt nhất để truyền dữ liệu từ nguồn đến đích thông qua bảng định tuyến (Routing Table).Bảng này chứa các mạng đích, thông tin về đường đi tốt nhất và giao diện (interface) sử dụng.

Router cập nhật thông tin bảng qua các giao thức định tuyến như:

* **Static**: Định tuyến tĩnh chuyển gói dữ liệu dựa trên địa chỉ IP của thiết bị đích.



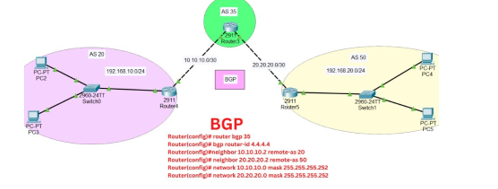
**Hình 1.8 Giao thức định tuyến tĩnh**

* **RIP (Routing Information Protocol)**: Định tuyến động dựa trên số lượng bước nhảy (hops).
* **OSPF (Open Shortest Path First)**: Định tuyến động xây dựng đường đi ngắn nhất dựa trên thuật toán Dijkstra.



**Hình 1.9 Giao thức định tuyến động OSPF**

* **BGP – Border Gateway Protocol** sử dụng các thông tin của Router Edge để quản lý cách các gói tin được định tuyến trên Internet. Điều này cung cấp sự ổn định mạng và đảm bảo sự thích ứng kịp thời của các Router trong quá trình gửi gói trên đường dẫn mạng lỗi.



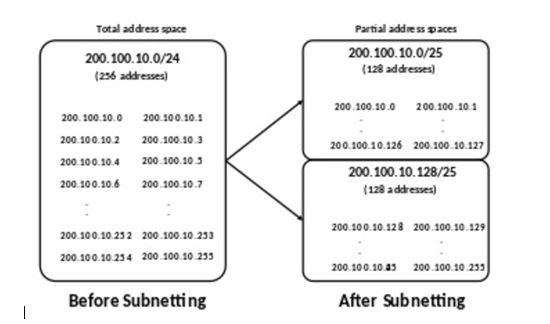
**Hình 1.10 Giao thức định tuyến động BGP trên Router Edge**

**- IGRP – Interior Gateway Routing Protocol** giúp xác định thông tin định tuyến giữa các cổng. Sau đó, các giao thức mạng khác sẽ sử dụng thông tin định tuyến đó để chỉ định cách thức truyền tải được định tuyến.

**Phân tách mạng con (Subnetting):**

**Tách một mạng lớn thành các subnet nhỏ:** Giảm tắc nghẽn lưu lượng và tăng hiệu suất truyền tải. Ví dụ từ mạng /24 có thể tách thành mạng nhỏ hơn như /26, /27.

**Cung cấp tính năng DHCP Relay:** Cho phép máy tính trong các subnet khác nhau nhận địa chỉ IP từ một máy chủ DHCP tập trung.



**Hình 1.11 Phân chia Subnetting**

**Kết nối các mạng khác nhau:**

**Mạng nội bộ và mạng bên ngoài:** Kết nối mạng LAN nội bộ với mạng WAN hoặc Internet. Chuyển đổi dữ liệu giữa các giao thức khác nhau (IP, IPv6).

**Các giao thức và tầng mạng khác nhau:** Ví dụ: Router có thể liên kết một mạng Ethernet với một mạng Frame Relay hoặc MPLS.

Định tuyến qua VPN (Virtual Private Network): Đảm bảo kết nối an toàn giữa các mạng qua môi trường công cộng.

**Chuyển đổi và chuyển tiếp gói tin:**

**Phân tích gói tin:** Router đọc địa chỉ IP nguồn và đích trong header của gói tin. So sánh địa chỉ đích với bảng định tuyến để tìm đường đi phù hợp.

**Chuyển tiếp qua Next-Hop:** Gói tin được gửi tới router hoặc thiết bị tiếp theo trên đường đến đích. Đảm bảo rằng dữ liệu được gửi chính xác qua tuyến đường tối ưu.

**Đảm bảo Bảo mật mạng:**

**Access Control Lists (ACLs)**: Lọc lưu lượng truy cập dựa trên các tiêu chí như: địa chỉ IP (nguồn, đích), các giao thức (TCP, UDP, ICMP), các cổng Server (HTTP, FTP, v.v.). Bên cạnh đó là ngăn chặn lưu lượng trái phép hoặc nguy hiểm.

**Firewall tích hợp**: Một số router hiện đại có khả năng hoạt động như một firewall, bảo vệ mạng khỏi các cuộc tấn công DDoS, brute-force, và các mối đe dọa khác.



**Hình 1.12 Sử dụng firewall ngăn chặn tấn công DDOS**

**VPN Security**: Router hỗ trợ mã hóa dữ liệu qua VPN để bảo mật kết nối từ xa.

**Các tính năng hỗ trợ thêm sau:**

Ưu tiên các loại dữ liệu quan trọng, giảm độ trễ (latency) bằng cách cân bằng tải hoặc gán băng thông cố định cho các ứng dụng cần thiết.

Định tuyến tại các Layer 2 và Layer 3.

Cung cấp nhiều công cụ quản lý như: SNMP (Simple Network Management Protocol) giám sát hiệu suất và trạng thái của mạng, **Syslog g**hi nhận và phân tích lỗi hoặc các sự kiện mạng, Remote Managementcho phép quản trị viên cấu hình từ xa qua SSH, Telnet, hoặc giao diện web.

### Kiến trúc của Router

**Phần cứng:**

**CPU (Central Processing Unit)** là "bộ não" của router, được tối ưu hóa để xử lý đồng thời nhiều luồng dữ liệu, thực hiện các tác vụ như :

* Xử lý bảng định tuyến: Đọc và quyết định tuyến đường cho dữ liệu.
* Chạy giao thức định tuyến: Như OSPF, BGP, hoặc EIGRP.
* Quản lý các dịch vụ: NAT, ACL, VPN.

**RAM (Random Access Memory):**

* Lưu trữ bảng định tuyến (Routing Table), bảng ARP, và các dữ liệu tạm thời khác. Giữ cấu hình hoạt động (Running Configuration) khi router hoạt động.
* Nội dung bị xóa khi router khởi động lại. Dung lượng RAM quyết định khả năng lưu trữ dữ liệu định tuyến và hỗ trợ các tính năng nâng cao.
* **NVRAM (Non-Volatile RAM):** Lưu lại các cấu hình khởi động (Startup Configuration). Không bị mất dữ liệu khi tắt nguồn và dữ liệu trong NVRAM sẽ được nạp vào RAM khi router khởi động.

**Flash Memory:**

* Lưu trữ Cisco IOS (Internetwork Operating System) – hệ điều hành của router. Lưu các file như hình ảnh IOS, file cấu hình dự phòng, hoặc file nhật ký.
* Nội dung không bị mất khi tắt nguồn. Hỗ trợ nâng cấp hệ điều hành bằng cách sao chép phiên bản IOS mới vào Flash.
* **Giao diện (Interfaces):** Các cổng kết nối mạng như Fast Ethernet, Gigabit Ethernet, Serial, hoặc Fiber.
* **Power Supply (Bộ nguồn):** Cung cấp năng lượng cho toàn bộ hoạt động của router. Có thể là nguồn **AC (220V)** hoặc nguồn dự phòng **DC** cho các hệ thống quan trọng. Một số dòng hỗ trợ **dual power supply** để đảm bảo dự phòng.

**Phần mềm:**

* **Cisco IOS (Internetwork Operating System):** Hệ điều hành quản lý toàn bộ hoạt động của router.
* **Giao diện dòng lệnh (CLI):** Công cụ chính để cấu hình và quản lý.
* **Module mở rộng:** Hỗ trợ thêm giao diện và chức năng, ví dụ như VPN, Voice, hoặc Wireless.

### Phân loại Router

**Router Core** được ISP nằm ở trung tâm của Internet và có khả năng chuyển tiếp thông tin theo dọc đường trục chính của cáp quang. Ngoài ra, Router Core còn được liên kết với các Router doanh nghiệp.



**Hình 1.13 Router Core cho một hệ thống mạng nhỏ**

**Router Edge** là một thiết bị vật lý có dung lượng nhỏ được kết nối với Internet công cộng, mạng WAN riêng hoặc mạng LAN bên ngoài. Chẳng hạn như Router Edge được sử dụng trong phạm vi gia đình hoặc văn phòng nhỏ.



**Hình 1.14 Router Edge**

**Router Branch** cung cấp một số tính năng khác như quản lý mạng LAN không dây và tăng tốc ứng dụng WAN.

**Router Logic** là một bộ định tuyến được sử dụng để sao chép chức năng của phần cứng, tạo ra các miền định tuyến hay triển khai một tập hợp các tác vụ được xử lý bởi Router.

**Router Wireless** là bộ định tuyến không dây có tính di động cao với đặc điểm kỹ thuật 801.11g, một tiêu chuẩn cung cấp khả năng truyền trong khoảng cách ngắn.



**Hình 1.15 Router Wireless**

### Ưu điểm và nhược điểm của Router

**Ưu điểm:**

* Router có khả năng đưa ra quyết định thông minh về cách thức dữ liệu sẽ được chuyển tiếp, giúp tối ưu hóa đường đi và tăng hiệu suất mạng.
* Nền tảng có thể kết nối nhiều thiết bị mạng với nhau, cho phép chúng giao tiếp và chia sẻ tài nguyên mạng.
* Hệ thống cung cấp các tính năng bảo mật như tường lửa và mã hóa dữ liệu để bảo vệ mạng khỏi các mối đe dọa từ Internet.
* Router có khả năng chuyển đổi giữa các giao thức mạng khác nhau, giúp các mạng có thể giao tiếp với nhau. Nền tảng phân phối các địa chỉ IP cho các thiết bị trong mạng nội bộ.

**Nhược điểm:**

* Giải pháp cấu hình và quản lý một Router khá phức tạp. Để thực hiện điều này đòi hỏi người lập trình cần có kiến thức kỹ thuật cao và thật sự tập trung trong toàn bộ quá trình giám sát.
* Một số Router có chi phí đầu tư ban đầu cao và có thể đòi hỏi chi phí duy trì.
* Công cụ yêu cầu người dùng bảo trì định kỳ và cập nhật phần mềm để đảm bảo tính ổn định và an toàn của hệ thống.

## Thiết bị bảo mật

[Thiết bị tường lửa (Firewall)](https://enootech.com/shop/000019fg100fbdl95012-firewall-fortinet-fortigate-100f-fg-100f-bdl-950-12-thiet-bi-tuong-lua-cho-van-phong-doanh-nghiep-150-nguoi-dung-4598?category=886) là một hệ thống bảo mật mạng phức tạp, được thiết kế với mục đích chính là ngăn chặn các truy cập không được phép từ bên ngoài mạng.

Firewall hoạt động như một lớp bảo vệ giữa mạng nội bộ (INSIDE) và mạng bên ngoài (OUTSIDE), chẳng hạn như Internet. Ngoài ra còn có DMZ (Demilitarized Zone) khu vực trung gian cho các dịch vụ công khai.



**Hình 1.16 Thiết bị firewall**

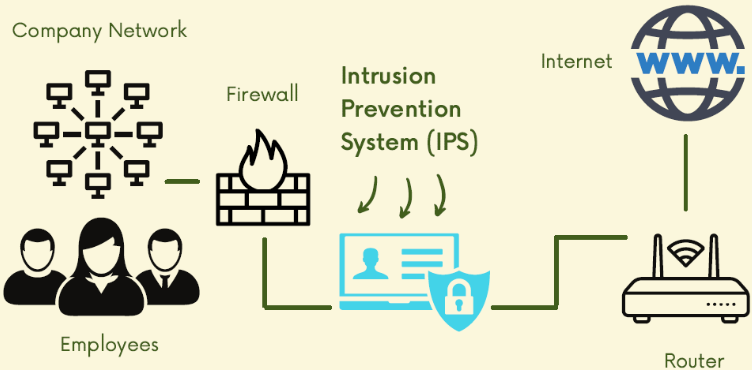
Khi dữ liệu cố gắng đi vào mạng từ internet, Firewall sẽ kiểm tra tất cả thông tin này dựa trên một tập hợp các quy tắc và tiêu chí an ninh mà nó đã được cài đặt mới quyết định cho phép truy cập hay không.

### Vai trò của Firewall

* **Bảo vệ tài nguyên mạng nội bộ:** Ngăn chặn truy cập trái phép từ bên ngoài.
* **Giám sát lưu lượng mạng:** Phân tích dữ liệu vào và ra, đảm bảo tuân thủ chính sách bảo mật.
* **Quản lý và kiểm soát truy cập:** Cho phép hoặc từ chối lưu lượng dựa trên địa chỉ IP, cổng, giao thức, hoặc ứng dụng.

### Chức năng của Firewall

* **Lọc gói tin (Packet Filtering):** Xác định lưu lượng được phép qua mạng dựa trên thông tin tiêu đề như địa chỉ IP, cổng nguồn và đích.
* **Kiểm tra trạng thái (Stateful Inspection):** Theo dõi trạng thái của các kết nối mạng, chỉ cho phép lưu lượng liên quan đến kết nối hợp lệ.
* **Bảo mật ứng dụng (Application Layer Security):** Tích hợp khả năng phát hiện và chặn lưu lượng dựa trên nội dung (DPI - Deep Packet Inspection).
* **VPN Gateway:** Hỗ trợ kết nối an toàn giữa các mạng thông qua VPN.
* **Ngăn chặn tấn công (Intrusion Prevention System - IPS):** Phát hiện và ngăn chặn các hành vi tấn công mạng.



**Hình 1.17 Mô phỏng bảo mật ngăn chặn tấn công IPS**

### Ứng dụng thực tế của Firewall:

**Trong doanh nghiệp:**

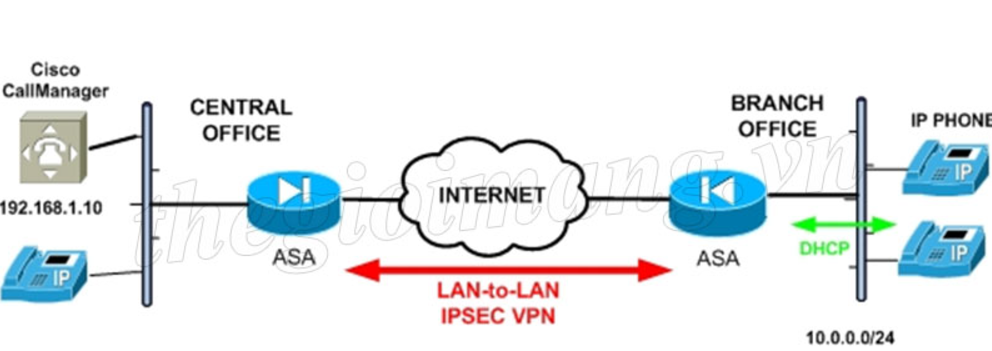
* **Ngăn chặn xâm nhập:** Firewall là lớp bảo vệ đầu tiên chống lại các cuộc tấn công từ hacker như brute force, tấn công DDoS hoặc khai thác lỗ hổng.
* **Bảo vệ thông tin nhạy cảm:** Firewall chặn các truy cập trái phép tới các cơ sở dữ liệu chứa thông tin tài chính, nhân sự hoặc chiến lược kinh doanh.
* Hạn chế truy cập và phân chia mạng nội bộ từ bên trong.
* Firewall tích hợp VPN Gateway cho phép nhân viên làm việc từ xa truy cập tài nguyên nội bộ qua kết nối an toàn.

**Trong gia đình:**

* **Bảo vệ thiết bị IoT:** Firewall bảo vệ các thiết bị IoT (smart TV, camera an ninh, loa thông minh) khỏi bị khai thác.
* **Kiểm soát truy cập Internet:** Firewall cho phép thiết lập giới hạn thời gian hoặc chặn các trang web không phù hợp (parental controls).
* Sử dụng firewall để chặn lưu lượng từ các trang web hoặc dịch vụ phân phối phần mềm độc hại và quảng cáo phiền phức.

**Trong trung tâm dữ liệu (Data Center):**

* Firewall chia các hệ thống máy chủ thành nhiều vùng bảo mật dựa trên chức năng.
* Khi một máy chủ bị tấn công, firewall ngăn chặn hacker di chuyển sang các hệ thống khác trong cùng trung tâm dữ liệu.
* **Tính năng QoS (Quality of Service):** Firewall quản lý băng thông, đảm bảo dịch vụ quan trọng như email và ứng dụng ERP không bị gián đoạn bởi lưu lượng không cần thiết.



**Hình 1.18 Mô phỏng quản lý lưu lượng QoS thông qua Firewall (ASA)**

* Firewall thế hệ mới (NGFW) tích hợp tính năng Intrusion Detection and Prevention System (IDS/IPS), phát hiện và ngăn chặn các hành vi bất thường.

**1.3.4 Ưu điểm và nhược điểm của Firewall**

**Ưu điểm:**

* Ngăn chặn truy cập trái phép và tấn công mạng.
* Dễ dàng quản lý và mở rộng với các chính sách linh hoạt.
* Bảo mật toàn diện với các tính năng nâng cao (IPS, DPI, VPN).

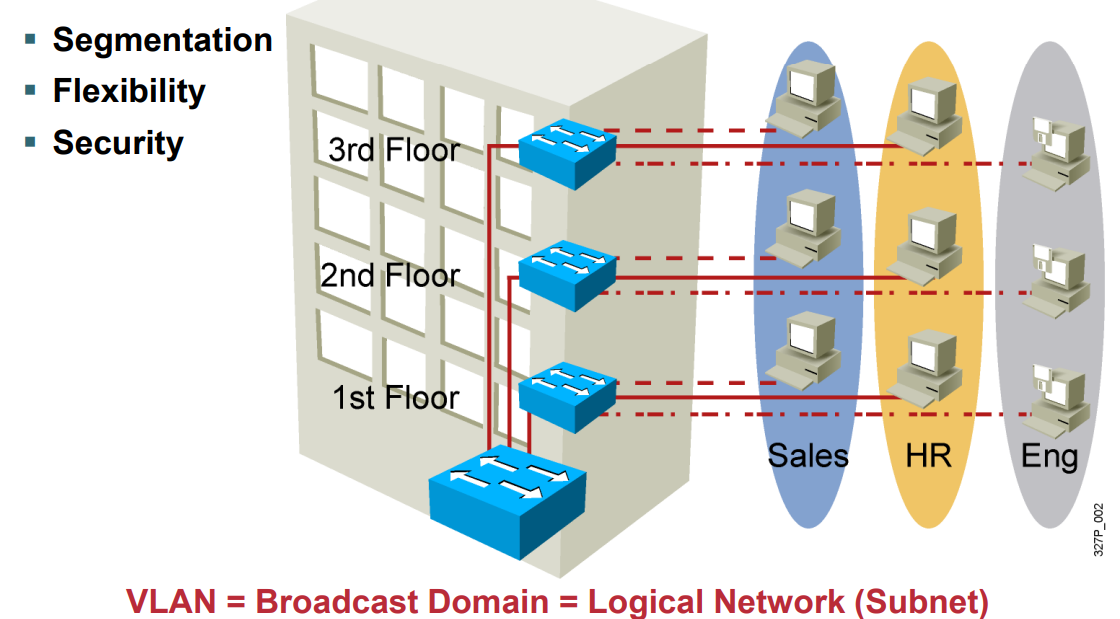
**Nhược điểm:**

* Chi phí cao đối với Firewall phần cứng cao cấp.
* Yêu cầu kiến thức chuyên môn để triển khai và quản lý.
* Firewall không bảo vệ hoàn toàn trước các mối đe dọa từ bên trong (insider threats).

## VLAN

### Khái niệm VLAN

VLAN (Virtual Local Area Network) là kỹ thuật chia một mạng LAN vật lý thành nhiều mạng LAN logic (mạng ảo) trên cùng hạ tầng switch. Mỗi VLAN tương ứng với một miền quảng bá (broadcast domain) riêng, do đó các thiết bị thuộc các VLAN khác nhau sẽ được tách biệt về mặt quảng bá và thường không thể liên lạc trực tiếp nếu không có cơ chế định tuyến giữa các VLAN (inter-VLAN routing) bằng router hoặc switch Layer 3.



**Hình 1.19 Mô tả VLAN**

### Chức năng của VLAN

VLAN có chức năng chính là phân đoạn mạng theo nhóm người dùng hoặc nhóm dịch vụ để tổ chức hệ thống mạng khoa học hơn. Nhờ tách broadcast domain, VLAN giúp giảm lưu lượng broadcast, hạn chế ảnh hưởng lan truyền khi mạng có nhiều thiết bị. Đồng thời, VLAN hỗ trợ tăng cường bảo mật và kiểm soát truy cập bằng cách cô lập các nhóm (ví dụ: sinh viên, quản trị, camera, server) và kết hợp với các cơ chế như ACL để quy định luồng truy cập giữa các VLAN. Ngoài ra, VLAN giúp dễ quản trị và mở rộng, vì việc thay đổi phân nhóm có thể thực hiện bằng cấu hình logic trên switch thay vì phải thay đổi toàn bộ hạ tầng vật lý.

### Ưu điểm và hạn chế

* **Ưu điểm**

- Phân đoạn mạng (Segmentation), giúp thu hẹp miền quảng bá, giảm tải lưu lượng broadcast và hạn chế phạm vi ảnh hưởng khi xảy ra sự cố mạng.

- Tính linh hoạt (flexibility), cho phép tổ chức mạng dựa trên phòng ban, chức năng hoặc loại dịch vụ thay vì phụ thuộc vào vị trí vật lý của người dùng.

- Nâng cao bảo mật (security), do các VLAN cách ly lưu lượng giữa các nhóm người dùng, hạn chế truy cập trái phép và hỗ trợ áp dụng các chính sách kiểm soát truy cập hiệu quả hơn

* **Hạn chế**

- Thiết kế cấu hình đòi hỏi kiến thức kỹ thuật, đặc biệt ở các phần như: Trunk 802.1Q, VLAN database, STP và định tuyến liên VLAN.

- Có thể gây lỗi kết nối diện rộng hoặc rò rỉ VLAN (VLAN hopping) nếu cấu hình sai.

- Khi các VLAN liên lạc với nhau bắt buộc phải có thiết bị Layer 3 và chính sách kiểm soát phù hợp, làm tăng yêu cầu về thiết bị và công tác quản trị.

# PHÂN TÍCH THIẾT KẾ HỆ THỐNG MẠNG CHO CÔNG TY THỰC PHẨM ĐÔNG Á

## TỔNG QUAN VỀ CÔNG TY THỰC PHẨM ĐÔNG á

### Giới thiệu chung

Công ty Thực Phẩm Đông Á là doanh nghiệp chuyên sản xuất và phân phối các nhóm sản phẩm thực phẩm đóng gói, thực phẩm tươi sống và đồ uống. Hiện nay, công ty mở rộng phạm vi kinh doanh sang các chuỗi siêu thị, nhà hàng và xuất khẩu ra thị trường quốc tế. Quy mô nhân sự của công ty tăng nhanh, kèm theo hệ thống quản lý kho, bán hàng và truyền thông nội bộ đều phụ thuộc vào hạ tầng mạng.

Việc xây dựng hệ thống chuyển mạch và định tuyến ổn định, an toàn và có khả năng mở rộng trở thành một yêu cầu cấp thiết. Hạ tầng mạng không chỉ phục vụ trao đổi dữ liệu nội bộ, mà còn cần tương thích với hệ thống ERP, máy chủ quản lý xuất nhập kho, hệ thống camera giám sát và dịch vụ email doanh nghiệp. Do đó, dự án triển khai mạng cho Công ty Thực Phẩm Đông Á tập trung vào tính ổn định – bảo mật – hiệu quả quản lý – dễ mở rộng.



**Hình 2.1 Tòa nhà Công ty Thực phẩm Đông Á**

### Cấu trúc Campus của Công ty Thực phẩm Đông Á

Công ty Thực Phẩm Đông Á hiện hoạt động với mô hình quản lý tập trung tại trụ sở chính và các văn phòng vệ tinh đặt tại các thành phố lớn trong nước. Việc phân bố chi nhánh tại nhiều khu vực tạo điều kiện thuận lợi trong việc mở rộng thị trường, tối ưu logistics và đảm bảo chuỗi cung ứng nhanh chóng giữa nhà máy, kho vận và hệ thống phân phối.

Ba chi nhánh chính hiện được đặt tại Đà Nẵng, TP. Hồ Chí Minh và Hà Nội – đây là các khu vực trung tâm về kinh tế, giao thương và hạ tầng logistics. Mỗi chi nhánh có quy mô nhân sự từ 500 đến 700 người tùy theo chức năng như vận hành kho, sản xuất, xử lý đơn hàng, phân phối và làm việc hành chính.

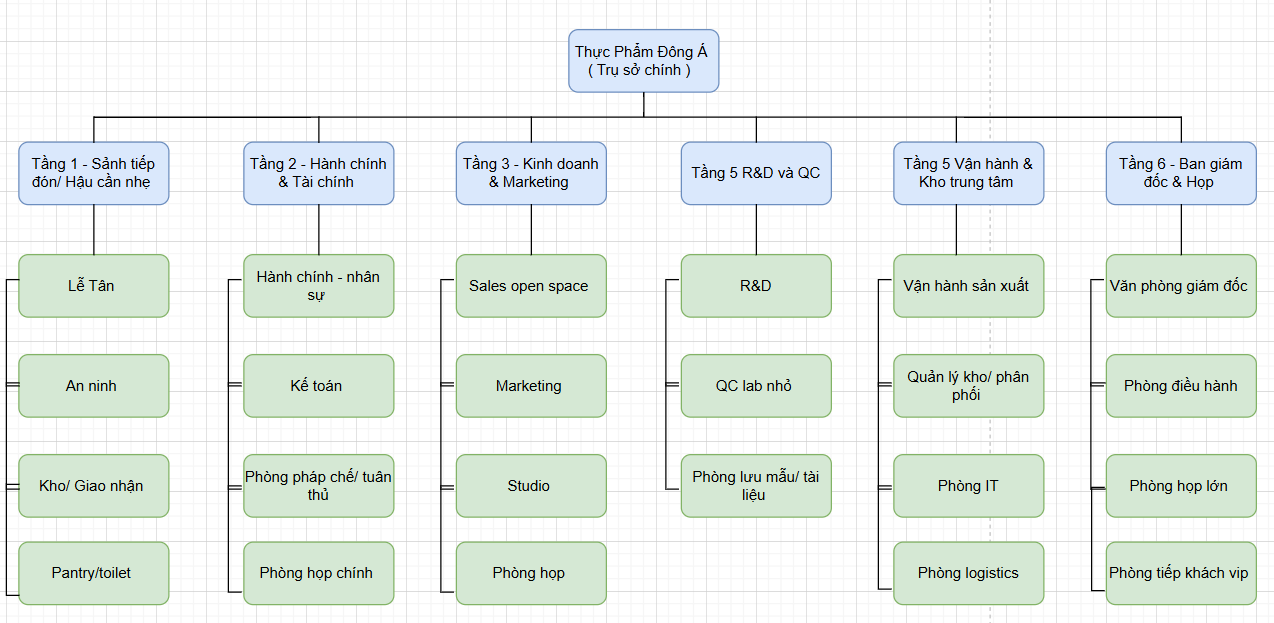
Quy mô chi nhánh Đà Nẵng:

***Quy mô chi nhánh Đà Nẵng:***

**Bảng 2.1 Quy mô chi nhánh Đà Nẵng**

|  |  |  |
| --- | --- | --- |
| Tầng | Khu vực chức năng | Mô tả ngắn gọn |
| Tầng 1 | Sảnh tiếp đón & Hậu cần nhẹ | Lễ tân, an ninh, kho – giao nhận nhỏ, pantry/toilet; tiếp xúc khách hàng và hỗ trợ luân chuyển hàng hóa cơ bản |
| Tầng 2 | Hành chính & Tài chính | Nhân sự, kế toán, pháp chế – tuân thủ, phòng họp chính; xử lý nghiệp vụ quản trị nội bộ |
| Tầng 3 | Kinh doanh & Marketing | Sales open space, marketing, studio truyền thông, phòng họp khách hàng |
| Tầng 4 | R&D & QC | Nghiên cứu phát triển sản phẩm, phòng QC nhỏ, lưu mẫu; yêu cầu bảo mật và kiểm soát truy cập cao |
| Tầng 5 | Vận hành & Kho trung tâm | Vận hành sản xuất, quản lý kho – phân phối, logistics, phòng IT |
| Tầng 6 | Ban Giám đốc & Họp | Văn phòng lãnh đạo, phòng điều hành, phòng họp lớn, tiếp khách VIP |

### Cấu trúc tổ chức phòng ban



**Hình 2.2 Cấu trúc tổ chức phòng ban**

**Bảng 2.2 Bảng mô tả cấu trúc tổ chức phòng ban**

|  |  |  |
| --- | --- | --- |
| **Tầng** | **Chức năng chính** | **Các bộ phận** |
| **Tầng 1 – Sảnh tiếp đón & Hậu cần nhẹ** | Tiếp khách, hỗ trợ vận hành ban đầu. | Lễ tân; An ninh; Kho/Giao nhận; Pantry/Toilet. |
| **Tầng 2 – Hành chính & Tài chính** | Quản trị nội bộ, tài chính, pháp lý. | Hành chính – Nhân sự; Kế toán; Phòng pháp chế – tuân thủ; Phòng họp chính. |
| **Tầng 3 – Kinh doanh & Marketing** | Phát triển thị trường, truyền thông. | Sales open space; Marketing; Studio; Phòng họp |
| **Tầng 5 – R&D & QC** | Nghiên cứu phát triển, kiểm soát chất lượng. | R&D; QC lab nhỏ; Phòng lưu mẫu/tài liệu. |
| **Tầng 5 – Vận hành & Kho trung tâm** | Sản xuất, lưu kho, phân phối. | Vận hành sản xuất; Quản lý kho/phân phối; Phòng IT; Phòng logistics |
| **Tầng 6 – Ban giám đốc & Họp** | Điều hành chiến lược, đối ngoại. | Văn phòng giám đốc; Phòng điều hành; Phòng họp lớn; Phòng tiếp khách VIP. |

### Khảo sát và thu thập thông tin

***Quy mô nhân sự***

**Bảng 2.3 Quy mô nhân sự**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tầng** | **Số phòng** | **Loại phòng** | **Số người dùng từng phòng** | **Tổng số người dùng / tầng** |
| Tầng 1  Sảnh & Hậu cần nhẹ | 4 | Lễ tân | 15 | 45 |
| An ninh | 10 |
| Kho/Giao nhận | 20 |
| Pantry / Toilet | 0 |
| Tầng 2  Hành chính & Tài chính | 4 | Hành chính – Nhân sự | 35 | 95 |
| Kế toán- Tài chính | 30 |
| Pháp chế/ Tuân thủ | 15 |
| Phòng họp chính | 15 (luân phiên) |
| Tầng 3  Kinh doanh & Marketing | 4 | Sales open space | 120 | 165 |
|  | Marketing | 25 |  |
| Studio | 10 |
| Phòng họp | 10 (luân phiên) |
| Tầng 4  R&D & QC | 3 | R&D | 40 | 70 |
| QC lab nhỏ | 20 |
| Phòng lưu mẫu / tài liệu | 10 |
| Tầng 5   Vận hành & Kho trung tâm | 4 | Vận hành sản xuất | 45 | 80 |
| Quản lý kho / phân phối | 20 |
| Phòng IT | 10 |
| Phòng logistics | 5 |
| Tầng 6   Ban giám đốc & Họp | 4 | Văn phòng giám đốc | 8 | 54 |
| Phòng điều hành | 10 |
| Phòng họp lớn | 30 (theo phiên họp) |
| **Phòng tiếp khách VIP** | **6** |

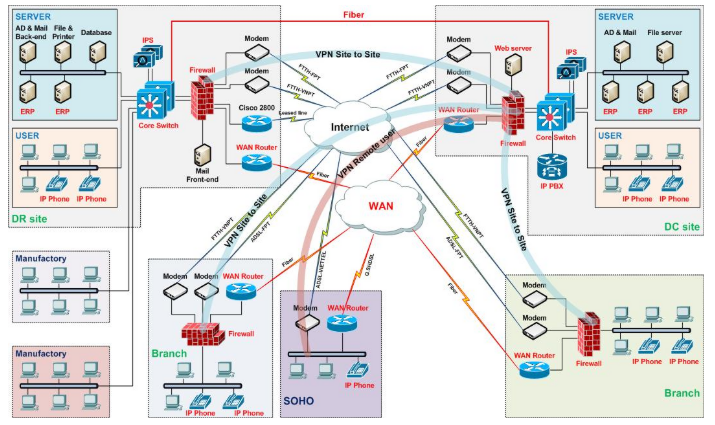
**Tổng nhân sự toàn chi nhánh :** ~ 450

## Thiết kế và xây dựng hệ thống

### Lý thuyết về thiết kế và xây dựng hệ thống mạng

Thiết kế và xây dựng hệ thống mạng là quá trình bắt đầu từ việc phân tích yêu cầu khách hàng sau đó tạo ra một cấu trúc kết nối các thiết bị, máy tính và các thành phần khác trong một tổ chức để chia sẻ dữ liệu, tài nguyên và hỗ trợ các hoạt động kinh doanh một cách hiệu quả.

Yêu cầu sự phối hợp giữa các nhóm chuyên môn, bao gồm kỹ sư mạng, quản trị viên hệ thống và chuyên gia bảo mật, nhằm xây dựng một hệ thống mạng có tính linh hoạt, khả năng mở rộng và độ tin cậy cao.



**Hình 2.3 Ví dụ mô hình mạng hoàn chỉnh**

### Yêu cầu về giám sát hệ thống

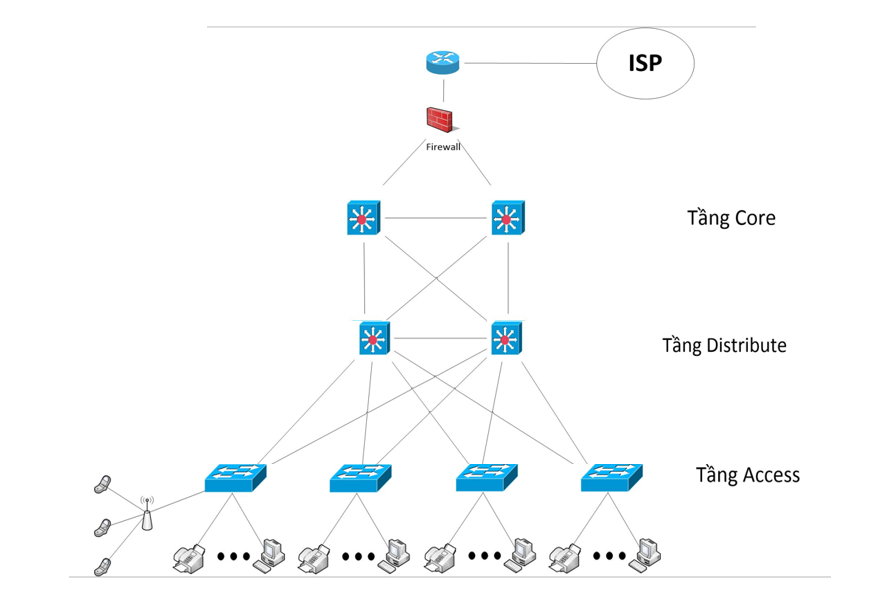
**Xác định các yêu cầu kinh doanh và kỹ thuật**: Phân tích xem mạng sẽ hỗ trợ những hoạt động nào của tổ chức như giao tiếp nội bộ, trao đổi dữ liệu, quản lý bán hàng, kiểm kê kho, và giám sát hoạt động. Yêu cầu kỹ thuật như băng thông, tốc độ kết nối, tính ổn định cũng sẽ được xem xét.

**Xác định yêu cầu phi chức năng**: Ngoài các yêu cầu chức năng như khả năng truyền thông và quản lý tài nguyên, cần xem xét các yếu tố khác như hiệu suất, khả năng phục hồi khi có sự cố, tính bảo mật, và khả năng mở rộng.

**Xác định mục tiêu dịch vụ**: Các yếu tố như thời gian hoạt động, độ trễ, và băng thông cần được định rõ nhằm đảm bảo hệ thống mạng có thể hỗ trợ các dịch vụ mà tổ chức yêu cầu.

### Thiết kế mạng logic

**Phân cấp mạng:** Mạng thường được chia thành các lớp khác nhau như lớp truy cập (Access Layer), lớp phân phối (Distribution Layer), và lớp lõi (Core Layer). Thiết kế theo phân cấp này giúp tối ưu hóa luồng dữ liệu và tăng tính khả dụng.



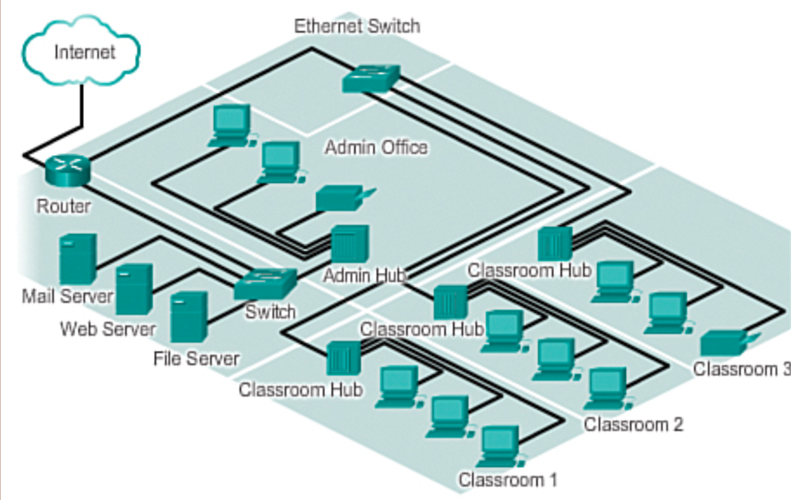
**Hình 2.4 Thiết kế mạng logic theo mô hình 3 lớp**

**Xác định VLAN và chia phân đoạn mạng:** Để tăng tính bảo mật và tối ưu hóa băng thông, các VLAN có thể được thiết lập cho từng phòng ban, hoặc từng nhóm người dùng cụ thể. Điều này giúp cô lập lưu lượng dữ liệu giữa các bộ phận khác nhau và giảm khả năng bị tấn công từ bên trong.

**Xác định giao thức định tuyến:** Việc lựa chọn giao thức định tuyến như OSPF, EIGRP, hay BGP cần dựa trên kích thước và nhu cầu của mạng. Cấu trúc định tuyến cần được thiết kế để tối ưu hóa việc truyền tải dữ liệu và đảm bảo tính sẵn sàng.

### Thiết kế mạng vật lý

**Lựa chọn thiết bị:** Xác định các thiết bị cần thiết như router, switch, firewall, access points (APs), và các thiết bị bảo mật khác. Tùy thuộc vào mục tiêu của tổ chức, các thiết bị có thể được chọn dựa trên hiệu năng, khả năng mở rộng và tính năng bảo mật.



**Hình 2.5 Thiết kế mô hình mạng vật lý**

**Cấu trúc kết nối và cáp mạng:** Để đảm bảo tốc độ và độ tin cậy của mạng, cần xác định loại cáp (cáp quang, cáp xoắn đôi) và tiêu chuẩn kết nối (như Ethernet, Wi-Fi) phù hợp. Các tiêu chuẩn cáp và kết nối cần phải đảm bảo hiệu suất và độ ổn định cho mạng lưới.

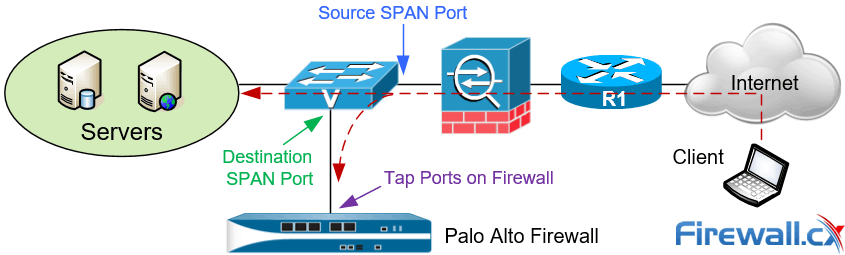
**Sắp xếp và bố trí thiết bị:** Xác định vị trí lắp đặt các thiết bị tại các vị trí như phòng máy chủ, tủ mạng và các điểm truy cập. Việc sắp xếp hợp lý sẽ giúp dễ dàng bảo trì và tối ưu hóa việc lưu thông không khí để làm mát các thiết bị.

### Thiết kế bảo mật

**Tầng bảo mật vật lý và logic**: Bảo mật vật lý bao gồm việc kiểm soát truy cập vào phòng máy chủ và khu vực thiết bị mạng. Bảo mật logic có thể bao gồm tường lửa (firewall), hệ thống phát hiện xâm nhập (IDS), và các chính sách kiểm soát truy cập (ACL).

**Chính sách bảo mật và kiểm soát truy cập**: Xây dựng các chính sách bảo mật rõ ràng về việc cấp quyền và kiểm soát truy cập đối với nhân viên và các thiết bị mạng, đảm bảo chỉ người dùng được ủy quyền mới có thể truy cập vào các tài nguyên quan trọng.

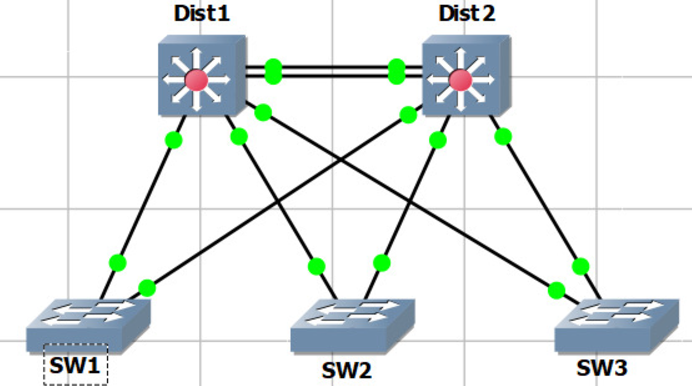
**Bảo mật mạng nội bộ và lớp 2**: Các tính năng bảo mật Layer 2 như Port Security, DHCP Snooping và Dynamic ARP Inspection (DAI) giúp ngăn chặn các tấn công phổ biến như giả mạo ARP, giả mạo DHCP, và tấn công DoS ở cấp độ mạng nội bộ.



**Hình 2.6 Mô tả một vài tính năng bảo mật và phân luồng**

### Đảm bảo dự phòng và khả năng mở rộng:

**Thiết kế dự phòng:** Các giao thức như HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol), và GLBP (Gateway Load Balancing Protocol) cho phép thiết lập các thiết bị dự phòng nhằm đảm bảo mạng vẫn hoạt động nếu một thiết bị gặp sự cố.



**Hình 2.7 Mô hình dự phòng tại các Dis**

**Cân bằng tải:** Bằng cách áp dụng các cơ chế Load Balancing, lưu lượng dữ liệu có thể được phân phối đồng đều qua các thiết bị hoặc các kết nối mạng khác nhau để giảm tải cho từng thiết bị và tránh tình trạng tắc nghẽn.

**Khả năng mở rộng:** Thiết kế mạng linh hoạt, có thể dễ dàng bổ sung thêm thiết bị và tài nguyên mà không làm ảnh hưởng đến hiệu suất hoặc độ ổn định của mạng.

### Kiểm thử và triển khai

**Kiểm thử:** Sử dụng các công cụ như Cisco Packet Tracer để mô phỏng và kiểm thử thiết kế trước khi triển khai thực tế. Điều này giúp phát hiện và sửa chữa các lỗi tiềm ẩn trước khi mạng được đưa vào hoạt động.

**Triển khai thực tế:** Thực hiện việc lắp đặt thiết bị, cài đặt cấu hình và

**Giám sát và bảo trì:** Sau khi triển khai, cần thiết lập hệ thống giám sát để theo dõi hiệu suất mạng, phát hiện các vấn đề kịp thời và tối ưu hóa hệ thống. Các công cụ giám sát như SNMP, NetFlow, và Syslog có thể cung cấp các thông tin hữu ích về hoạt động của mạng.

### Đánh giá và tối ưu hóa

**Đánh giá hiệu suất định kỳ:** Thực hiện kiểm tra định kỳ để đánh giá hiệu suất mạng, từ đó xác định các yếu tố cần cải tiến.

**Cập nhật bảo mật và phần cứng:** Đảm bảo hệ thống mạng luôn được cập nhật các bản vá bảo mật và phần cứng phù hợp để duy trì tính bảo mật và ổn định.

**Tối ưu hóa tài nguyên và chi phí:** Đánh giá cách sử dụng tài nguyên để đảm bảo hệ thống mạng vận hành hiệu quả, giúp tổ chức tiết kiệm chi phí và tài nguyên.

## Công nghệ và các thiết bị thích hợp cho hệ thống

### Công nghệ cáp dẫn Cat6a

**Ưu điểm và lý do chọn**

* Cải tiến hơn với tốc độ 10 Gbps ở khoảng cách 100m, đáp ứng tốt các ứng dụng yêu cầu băng thông cao như máy chủ, camera giám sát độ phân giải cao hoặc dịch vụ truyền phát video 4K/8K.
* Băng thông lên đến 500 MHz, hỗ trợ các ứng dụng phức tạp và kết nối trong tương lai.
* Độ bền cao, khả năng giảm nhiễu tốt, tương thích ngược và có thể hỗ trợ tương lai.
* Kết nối tại trung tâm quản lý hoặc giữa các thiết bị quan trọng như router, switch, bên cạnh đó là đáp ứng tốt cho các thiết bị đầu cuối như PC, máy in và các thiết bị không dây.



**Hình 2.8 Ảnh vật lý CAT6A**

\* Giá tiền: sử dụng loại Cat6a có bọc giáp chóng nhiễu với giá thành từ 15k - 20k VNĐ/m.

**2.3.2. Công nghệ định tuyến Cisco ISR 4331/K9**

**Ưu điểm và lý do lựa chọn:**

* Tốc độ cao,, hiệu suất mạnh mẽ với tốc độ truyền 100Mbps và cao nhất là 1Gbps, CPU 2 core tốc độ 2.4GHz, 4G DRAM và flash.
* Có khe cắm mở rộng giúp dễ dàng nâng cấp, khả năng bảo mật tốt với các tính năng như VPN, IPS và firewall, kết hợp với các tiêu chuẩn bảo mật tiên tiến.
* Linh hoạt, dễ dàng quản lý mang lại tính ổn định và độ tin cạnh cao. Bên cạnh việc tiết kiệm được nhiều chi phí, dễ dàng triển khai khi có độ tương thích cao.



**Hình 2.9 Ảnh vật lý Router Cisco ISR 4331/K9**

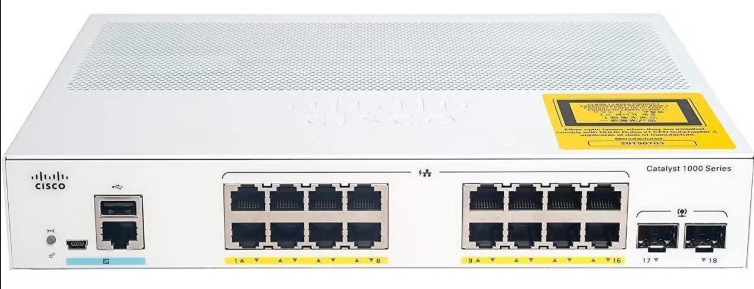
* Giá tiền tham khảo: có giá thành khá tốt từ 18 - 25 triệu cho 1 thiết bị.

### Công nghệ chuyển mạch

**Switch Cisco Catalyst 1000-16P-2G-L (Layer 2 hay tầng Access):**

**Ưu điểm nổi bật và lý do lựa chọn:**

* Có giá thành không quá cạnh tranh, hiệu quả mang lại rất tốt so với giá tiền.
* Tích hợp đầy đủ cá c tính năng của Layer 2, lại được nâng cấp nên tương thích tốt với nhiều sản phẩm cisco khác.
* Hỗ trợ PoE trên tất cả các cổng 10/100/1000 Mbps, với công suất lên đến 370W (tùy thuộc vào mô hình và yêu cầu tải)
* Băng thông chuyển mạch tối đa lên đến 32 Gbps



**Hình 2.10 Ảnh vật lý Switch Cisco Catalyst 1000**

* Giá tiền tham khảo: có giá thành từ 10 - 15 triệu VNĐ cho từng thiết bị.

**Switch Cisco Catalyst 3650-24PS-L (Layer 3 hay tầng Distribution):**

* Cisco C3650-24PS-L hỗ trợ tính năng định tuyến Layer 3, cho phép chuyển tiếp dữ liệu giữa các VLAN mà không cần sử dụng một router riêng biệt, phù hợp với yêu cầu phân vùng mạng tại các tòa nhà của bệnh viện.
* **Tốc độ**: Hỗ trợ **10 Gbps** với các module nâng cấp và có sẵn các cổng **1 Gbps**.
* Với 24 cổng PoE, switch này có thể cung cấp nguồn điện cho các thiết bị như điện thoại IP, camera giám sát, và các điểm truy cập Wi-Fi mà không cần nguồn điện riêng.
* **Quản lý và bảo mật nâng cao**: Các tính năng như Access Control Lists (ACL), Port Security, và DHCP Snooping giúp bảo vệ mạng khỏi các tấn công và truy cập trái phép, bảo vệ thông tin quan trọng của WinMart.
* Tính tương thích tốt với môi trường Cisco, chi phí hợp lý khi sử dụng tại một bệnh viên nhỏ.



**Hình 2.11 Ảnh vật lý Switch Cisco 3650-24PS-L**

* Giá tiền tham khảo: có giá thành từ 23 - 24 triệu VNĐ cho từng thiết bị.

### Công nghệ bảo mật Firepower 2110-ASA-K9:

* **Tăng cường bảo mật**: Firepower 2110 cung cấp khả năng bảo vệ mạng mạnh mẽ với tính năng **Advanced Malware Protection (AMP), ISP.**
* Với khả năng mã hóa và giải mã SSL, Firepower 2110 giúp bảo vệ dữ liệu khi truyền qua mạng, đảm bảo tính riêng tư và an toàn cho dữ liệu quan trọng.
* 8 cổng Gigabit Ethernet (10/100/1000) với khả năng sử dụng như LAN hoặc WAN. Thông lượng lên đến 4 Gbps (Firewall Throughput), 2.5Gbps IPsec VPN.
* Có sẵn cổng SFP cho kết nối quang học nếu cần.



**Hình 2.12 Ảnh vật lý của Firepower - ASA - K9**

* Giá tiền tham khảo: có giá tiền từ 60 - 75 tiệu VNĐ, khá tốt cho hệ thống của trung tâm quản lý.

## Mô phỏng hệ thống mạng cho công ty Thực Phẩm Đông Á

### Phân chia IP cho các vùng mạng

Ta sẽ phân chia dãy mạng 10.0.0.0/8 với subnet mask 255.0.0.0

**Vùng IP cho các người dùng cuối:**

**Bảng 2.4 Bảng chia IP cho người dùng cuối**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Phòng ban** | **Network ID** | **Subnet mask** | **Host Range** | **Broadcast IP** |
| VLAN11-letan | 10.43.16.0/24 | 255.255.255.0 | 10.43.16.1 - 10.43.16.250 | 10.43.16.255 |
| VLAN12-anninh | 10.43.17.0/24 | 255.255.255.0 | 10.43.17.1 - 10.43.17.250 | 10.43.17.255 |
| VLAN13-kho | 10.43.18.0/24 | 255.255.255.0 | 10.43.18.1 - 10.43.18.250 | 10.43.18.255 |
| VLAN21-hanhchinh | 10.43.24.0/24 | 255.255.255.0 | 10.43.24.1 - 10.43.24.250 | 10.43.24.255 |
| VLAN22-ketoan | 10.43.25.0/24 | 255.255.255.0 | 10.43.25.1 - 10.43.25.250 | 10.43.25.255 |
| VLAN23-phapche | 10.43.26.0/24 | 255.255.255.0 | 10.43.26.1 - 10.43.26.250 | 10.43.26.255 |
| VLAN31-sales | 10.43.32.0/24 | 255.255.255.0 | 10.43.32.1 - 10.43.32.250 | 10.43.32.255 |
| VLAN32-mkt | 10.43.33.0/24 | 255.255.255.0 | 10.43.33.1 - 10.43.33.250 | 10.43.33.255 |
| VLAN33-studio | 10.43.34.0/24 | 255.255.255.0 | 10.43.34.1 - 10.43.34.250 | 10.43.34.255 |
| VLAN41-r&d | 10.43.48.0/24 | 255.255.255.0 | 10.43.48.1 - 10.43.48.250 | 10.43.48.255 |
| VLAN42-qc | 10.43.49.0/24 | 255.255.255.0 | 10.43.49.1 - 10.43.49.250 | 10.43.49.255 |
| VLAN43-tailieu | 10.43.50.0/24 | 255.255.255.0 | 10.43.50.1 - 10.43.50.250 | 10.43.50.255 |
| VLAN51-sanxuat | 10.43.56.0/24 | 255.255.255.0 | 10.43.56.1 - 10.43.56.250 | 10.43.56.255 |
| VLAN52-kho | 10.43.57.0/24 | 255.255.255.0 | 10.43.57.1 - 10.43.57.250 | 10.43.57.255 |
| VLAN53-it | 10.43.58.0/24 | 255.255.255.0 | 10.43.57.1 - 10.43.57.250 | 10.43.58.255 |
| VLAN61-giamdoc | 10.43.64.0/24 | 255.255.255.0 | 10.43.64.1 - 10.43.64.250 | 10.43.64.255 |
| VLAN62-dieuhanh | 10.43.65.0/24 | 255.255.255.0 | 10.43.65.1 - 10.43.65.250 | 10.43.65.255 |
| VLAN63-vip | 10.43.66.0/24 | 255.255.255.0 | 10.43.66.1 - 10.43.66.250 | 10.43.66.255 |

**Bảng 5: Bảng phân chia IP cho người dùng cuối**

**Vùng IP cho vùng Server Farm:**

**Bảng 2.5 Bảng chia IP cho vùng Server Farm**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **MÁY CHỦ** | **Network ID** | **Subnet mask** | **Host Range** | **Broadcast IP** |
| DHCP Server | 10.43.150.0/24 | 255.255.255.0 | 10.43.150.1 -  10.43.150.250 | 10.43.150.255 |
| HTTP Server | 10.43.151.0/24 | 255.255.255.0 | 10.43.151.1 -  10.43.151.250 | 10.43.151.255 |
| Email Server | 10.43.152.0/24 | 255.255.255.0 | 10.43.152.1 -  10.43.152.250 | 10.43.152.255 |
| DHCPv6 Server | 10.43.153.0/24 | 255.255.255.0 | 10.43.153.1 -  10.43.153.250 | 10.43.153.255 |
| DNS | 10.43.154.0/24 | 255.255.255.0 | 10.43.154.1 -  10.43.154.250 | 10.43.154.255 |
| FTP Server | 10.43.155.0/24 | 255.255.255.0 | 10.43.155.1 -  10.43.155.250 | 10.43.155.255 |

**Bảng 6: Phân chia IP cho vùng Data Center**

**Vùng IP cho các mạng Peer-to-Peer**

**Bảng 2.6 Bảng chia IP cho các mạng Peer-to-Peer**

|  |  |  |  |
| --- | --- | --- | --- |
| **MÁY CHỦ** | **Network ID** | **Subnet mask** | **Host Range** |
| DIS 1 - CORE 1 | 10.43.201.252/30 | 255.255.255.252 | 10.43.201.253 -> 10.43.201.254 |
| DIS 2 - CORE 1 | 10.43.203.252/30 | 255.255.255.252 | 10.43.203.253 -> 10.43.203.254 |
| DIS 3 - CORE 1 | 10.43.205.252/30 | 255.255.255.252 | 10.43.205.253 -> 10.43.205.254 |
| DIS 4 - CORE 1 | 10.43.207.252/30 | 255.255.255.252 | 10.43.207.253 -> 10.43.207.254 |
| DIS 5 - CORE 1 | 10.43.209.252/30 | 255.255.255.252 | 10.43.209.253 -> 10.43.209.254 |
| DIS 6 - CORE 1 | 10.43.211.252/30 | 255.255.255.252 | 10.43.211.253 -> 10.43.211.254 |
| DIS 1 - CORE 2 | 10.43.202.252/30 | 255.255.255.252 | 10.43.202.253 -> 10.43.202.254 |
| DIS 2 - CORE 2 | 10.43.204.252/30 | 255.255.255.252 | 10.43.204.253 -> 10.43.204.254 |
| DIS 3 - CORE 2 | 10.43.206.252/30 | 255.255.255.252 | 10.43.206.253 -> 10.43.206.254 |
| DIS 4 - CORE 2 | 10.43.208.252/30 | 255.255.255.252 | 10.43.208.253 -> 10.43.208.254 |
| DIS 5 - CORE 2 | 10.43.210.252/30 | 255.255.255.252 | 10.43.210.253 -> 10.43.210.254 |
| DIS 6 - CORE 2 | 10.43.212.252/30 | 255.255.255.252 | 10.43.212.253 -> 10.43.212.254 |

**Bảng 7: Phân chia IP cho vùng Data Center**

### Tiến hành cấu hình mô phỏng

#### 2.4.2.1 Cấu hình thiết bị Switch Layer 2 ở lớp Access

Với lớp Access ta sẽ cấu hình VLAN cho switch layer 2 giúp cô lập lưu lượng giữa các phòng ban, giảm nguy cơ xung đột và tăng cường an toàn cho hệ thống mạng nội bộ, vừa thiết lập kết nối cho các thiết bị và đường đi trunking cho các gói tin ở các VLAN khác nhau. switch cho một tầng sẽ được chia VLAN và cấu hình tương tự như sau:

! ======== switch tang 1 : ======== !

en

conf t

vlan 11

name VLAN11-letan

vlan 12

name VLAN12-anninh

vlan 13

name VLAN13-kho

interface range fa0/4-8

switchport port-security

switchport port-security maximum 2

switchport port-security violation shutdown

!pc + Access point + printer

interface range fa0/4-6

switchport mode access

switchport access vlan 11

no shutdown

!pc 2

interface fa0/7

switchport mode access

switchport access vlan 12

no shutdown

!pc 3

interface fa0/8

switchport mode access

switchport access vlan 13

no shutdown

interface range fa0/1-3

!interface fa0/1

switchport mode trunk

switchport trunk allowed vlan 11,12,13

no shutdown

#### 2.4.1.2 Cấu hình thiết bị Switch Layer 3 ở lớp Distribution

Lớp Distribution đóng vai trò tổng hợp lưu lượng, định tuyến giữa các VLAN và áp dụng các chính sách bảo mật. Việc cấu hình thường bao gồm thiết lập VLAN giữa các switch và các đường trunking, định tuyến giữa các tầng bằng giao thức định tuyến động OSPF kèm thiết lập dự phòng với giao thức HSRP cho lớp Access tăng tính sẵn sàng cho các đường mạng. Bên cạnh đó sẽ thiết lập các mạng Point-to-Point lên lớp Core phục vụ cho việc định tuyến gói tin tới các địa chỉ ở bên ngoài. Các Distribute sẽ có cấu hình giống nhau và khác nhau chủ yếu ở định tuyến mạng :

!swl3-1

en

conf t

hostname DIS-6

enable secret DIS-6

ip routing

vlan 41

name VLAN41-letan

vlan 42

name VLAN42-anninh

vlan 43

name VLAN43-kho

vlan 51

name VLAN51-hanhchinh

vlan 52

name VLAN52-ketoan

vlan 53

name VLAN53-phapche

vlan 61

name VLAN61-sales

vlan 62

name VLAN62-mkt

vlan 63

name VLAN61-studio

interface vlan 41

ip address 10.43.48.1 255.255.255.0

no shutdown

interface vlan 42

ip address 10.43.49.1 255.255.255.0

no shutdown

interface vlan 43

ip address 10.43.50.1 255.255.255.0

no shutdown

interface vlan 51

ip address 10.43.56.1 255.255.255.0

no shutdown

interface vlan 52

ip address 10.43.57.1 255.255.255.0

no shutdown

interface vlan 53

ip address 10.43.58.1 255.255.255.0

no shutdown

interface vlan 61

ip address 10.43.64.1 255.255.255.0

no shutdown

interface vlan 62

ip address 10.43.65.1 255.255.255.0

no shutdown

interface vlan 63

ip address 10.43.66.1 255.255.255.0

no shutdown

!trunk

interface fa0/3

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 41,42,43

no shutdown

!trunk

interface fa0/4

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 51,52,53

no shutdown

!trunk

interface fa0/5

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 61,62,63

no shutdown

!routing

interface fa0/1

no switchport

ip address 10.43.211.253 255.255.255.252

no shutdown

!routing

ip routing

interface fa0/2

no switchport

ip address 10.43.212.253 255.255.255.252

no shutdown

!trunk

interface fa0/3

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 41,42,43

no shutdown

!trunk

interface fa0/4

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 51,52,53

no shutdown

!trunk

interface fa0/5

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 61,62,63

no shutdown

router ospf 1

router-id 6.6.6.6

network 10.43.211.252 0.0.0.3 area 0

network 10.43.212.252 0.0.0.3 area 0

network 10.43.48.0 0.0.3.255 area 0

network 10.43.56.0 0.0.3.255 area 0

network 10.43.64.0 0.0.3.255 area 0

! gui ra mang internet

ip route 0.0.0.0 0.0.0.0 10.43.212.254 1

ip route 0.0.0.0 0.0.0.0 10.43.211.254 10

! DHCP - ip helper for DHCP(10.43.150.2)

interface vlan 41

ip helper-address 10.43.150.2

interface vlan 42

ip helper-address 10.43.150.2

interface vlan 43

ip helper-address 10.43.150.2

interface vlan 51

ip helper-address 10.43.150.2

interface vlan 52

ip helper-address 10.43.150.2

interface vlan 53

ip helper-address 10.43.150.2

interface vlan 61

ip helper-address 10.43.150.2

interface vlan 62

ip helper-address 10.43.150.2

interface vlan 63

ip helper-address 10.43.150.2

! ==== HSRP - DIS 6 ==== !

! = TANG 4 = !

interface vlan 41

standby 11 ip 10.43.48.254

standby 11 priority 100

standby 11 preempt

interface vlan 42

standby 11 ip 10.43.49.254

standby 11 priority 100

standby 11 preempt

interface vlan 43

standby 11 ip 10.43.50.254

standby 11 priority 100

standby 11 preempt

! = TANG 5 = !

interface vlan 51

standby 11 ip 10.43.56.254

standby 11 priority 110

standby 11 preempt

interface vlan 52

standby 11 ip 10.43.57.254

standby 11 priority 110

standby 11 preempt

interface vlan 53

standby 11 ip 10.43.58.254

standby 11 priority 110

standby 11 preempt

! = TANG 6 = !

interface vlan 61

standby 11 ip 10.43.64.254

standby 11 priority 120

standby 11 preempt

interface vlan 62

standby 11 ip 10.43.65.254

standby 11 priority 120

standby 11 preempt

interface vlan 63

standby 11 ip 10.43.66.254

standby 11 priority 120

standby 11 preempt

! == SSH == !

ip domain-name vku.domain

username admin password 123

crypto key generate rsa

1024

line vty 0 4

login local

transport input ssh

end

wr mem

#### 2.4.1.3 Cấu hình thiết bị Switch Layer 3 ở lớp Core

Tại lớp Core, với chức năng chính là định tuyến thì ta sẽ cấu hình VLAN để quản lí vùng Data Center, kèm theo đó là chức năng định tuyến để các gói tin có thể ra bên ngoài bằng cách sử dụng giao thức định tuyến động OSPF, kèm theo đó là các đường dự phòng được cấu hình định tuyến tĩnh lên lớp Firewall, vừa đáp ứng được các đường dự phòng và gánh vác khối lượng mạng với nhau.

! =========== CORE 1 ===========:

en

conf t

host name CORE-1

enable secret CORE-1

! === IP FOR INTERFACE === !

interface range fa0/1-9

no switchport

! = CORE -> FW = !

interface fa0/1

ip address 10.43.221.253 255.255.255.252

no shutdown

interface fa0/2

ip address 10.43.222.253 255.255.255.252

no shutdown

! = CORE -> DIS = !

interface fa0/4

ip address 10.43.201.254 255.255.255.252

no shutdown

interface fa0/5

ip address 10.43.203.254 255.255.255.252

no shutdown

interface fa0/6

ip address 10.43.205.254 255.255.255.252

no shutdown

interface fa0/7

ip address 10.43.207.254 255.255.255.252

no shutdown

interface fa0/8

ip address 10.43.209.254 255.255.255.252

no shutdown

interface fa0/9

ip address 10.43.211.254 255.255.255.252

no shutdown

! === ROUTING === !

router ospf 1

router-id 10.10.10.11

network 10.43.201.252 0.0.0.3 area 0

network 10.43.203.252 0.0.0.3 area 0

network 10.43.205.252 0.0.0.3 area 0

network 10.43.207.252 0.0.0.3 area 0

network 10.43.209.252 0.0.0.3 area 0

network 10.43.211.252 0.0.0.3 area 0

network 10.43.150.0 0.0.0.255 area 0

network 10.43.151.0 0.0.0.255 area 0

network 10.43.152.0 0.0.0.255 area 0

network 10.43.153.0 0.0.0.255 area 0

network 10.43.154.0 0.0.0.255 area 0

network 10.43.155.0 0.0.0.255 area 0

ip routing

!tmp ip ra fw. chua co HSRP

ip route 0.0.0.0 0.0.0.0 10.43.221.254 1

ip route 0.0.0.0 0.0.0.0 10.43.222.254 10

! === DATA CENTER === !

vlan 150

name DHCP-150

interface vlan 150

ip address 10.43.150.1 255.255.255.0

no shutdown

vlan 151

name HTTP-151

interface vlan 151

ip address 10.43.151.1 255.255.255.0

no shutdown

vlan 152

name EMAIL-152

interface vlan 152

ip address 10.43.152.1 255.255.255.0

no shutdown

vlan 153

name DHCPv6-153

interface vlan 153

ip address 10.43.153.1 255.255.255.0

no shutdown

vlan 154

name DNS-154

interface vlan 154

ip address 10.43.154.1 255.255.255.0

no shutdown

vlan 155

name HTTP-155

interface vlan 155

ip address 10.43.155.1 255.255.255.0

no shutdown

!trunk

interface fa0/10

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 150,151,152

no shutdown

!trunk

interface fa0/11

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 153,154,155

no shutdown

! === TRUNK FOR DATA CENTER === !

!trunk

interface fa0/10

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 150,151,152

no shutdown

!trunk

interface fa0/11

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 153,154,155

no shutdown

ip domain-name vku.domain

username admin password 123

crypto key generate rsa

1024

line vty 0 4

login local

transport input ssh

end

wr mem

#### 2.4.1.4 Cấu hình thiết bị ASA ở lớp Firewall

Tại đây với chức năng chính là bảo mật mạng, với mô hình được dựng lên với một địa chỉ của tin tặc, ta sẽ cấu hình Access-list để ngăn chặn IP đó truy cập tài nguyên của khu vực, đồng thời mở kết nối từ trong ra ngoài và hướng lên Router biên. Song song với đó ta cũng cấu hình hai đường định tuyến tĩnh lên hai Router biên để chia sẻ vận tải.

! ======== ASA 1 ======== !

en

conf t

hostname ASA-1

enable password ASA-1

!

interface GigabitEthernet1/1

nameif outside1

security-level 100

ip address 10.43.231.253 255.255.255.252

no shutdown

!

interface GigabitEthernet1/2

nameif outside2

security-level 100

ip address 10.43.232.253 255.255.255.252

no shutdown

interface GigabitEthernet1/3

nameif inside1

security-level 100

ip address 10.43.221.254 255.255.255.252

no shutdown

!

interface GigabitEthernet1/4

nameif inside2

security-level 100

ip address 10.43.223.254 255.255.255.252

no shutdown

! muon 2 interface inside1/2 muon di toi mang dich 10.0.0.0/8 thi di qua 1 trong 2 mang nay

route inside1 10.0.0.0 255.0.0.0 10.43.221.253 1

route inside2 10.0.0.0 255.0.0.0 10.43.223.253 10

route outside1 0.0.0.0 0.0.0.0 10.43.231.254 1

route outside2 0.0.0.0 0.0.0.0 10.43.232.254 10

! ACL

access-list BLOCK-HACKER extended deny ip host 9.9.9.9 any

access-list BLOCK-HACKER extended permit ip any any

access-group BLOCK-HACKER in interface outside1

access-group BLOCK-HACKER in interface outside2

end

wr mem

#### 2.4.1.5 Cấu hình thiết bị Router biên

Chức năng chính của Router biên đó là đưa các địa chỉ nội bộ ra ngoài internet bằng giao thức NAT, kết nối lên thiết bị ISP của nhà mạng và kết nối với thế giới bên ngoài. Cũng như các thiết bị khác, ở đây ta sẽ có hai Router biên mô phỏng hai nhà mạng khác nhau phục vụ cho việc dự phòng:

! ======== ASA 1 ======== !

en

conf t

hostname ASA-1

enable password ASA-1

!

interface GigabitEthernet1/1

nameif outside1

security-level 100

ip address 10.43.231.253 255.255.255.252

no shutdown

!

interface GigabitEthernet1/2

nameif outside2

security-level 100

ip address 10.43.232.253 255.255.255.252

no shutdown

interface GigabitEthernet1/3

nameif inside1

security-level 100

ip address 10.43.221.254 255.255.255.252

no shutdown

!

interface GigabitEthernet1/4

nameif inside2

security-level 100

ip address 10.43.223.254 255.255.255.252

no shutdown

! muon 2 interface inside1/2 muon di toi mang dich 10.0.0.0/8 thi di qua 1 trong 2 mang nay

route inside1 10.0.0.0 255.0.0.0 10.43.221.253 1

route inside2 10.0.0.0 255.0.0.0 10.43.223.253 10

route outside1 0.0.0.0 0.0.0.0 10.43.231.254 1

route outside2 0.0.0.0 0.0.0.0 10.43.232.254 10

! ACL

access-list BLOCK-HACKER extended deny ip host 9.9.9.9 any

access-list BLOCK-HACKER extended permit ip any any

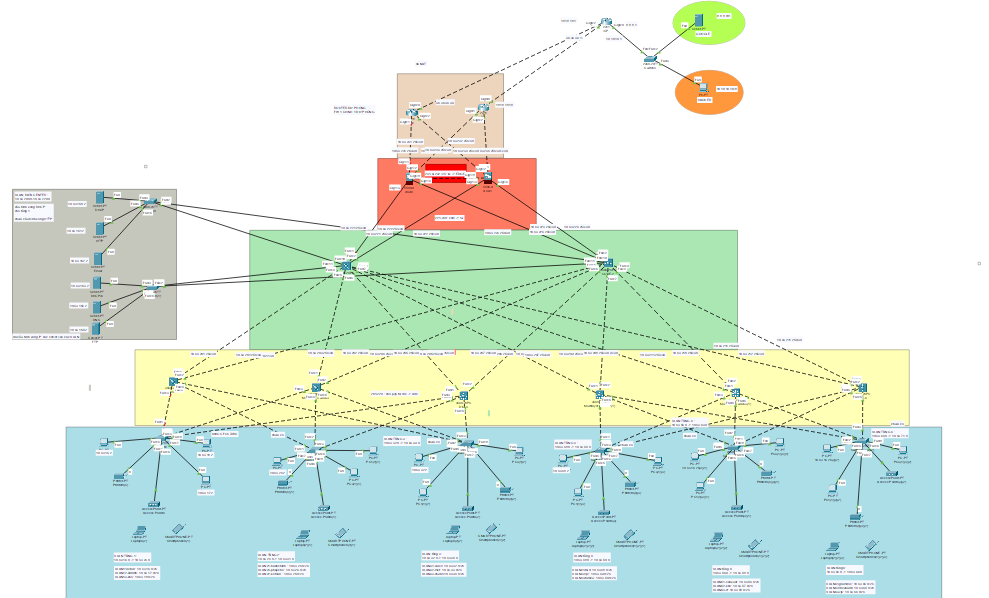
access-group BLOCK-HACKER in interface outside1

access-group BLOCK-HACKER in interface outside2

end

wr mem

### Sơ đồ vật lý

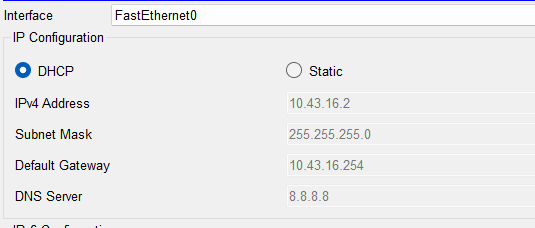


# KẾT QUẢ ĐẠT ĐƯỢC

## TIẾN HÀNH KIỂM TRA ĐƯỜNG TRUYỀN TRONG HỆ THỐNG MẠNG

### a. DHCP tự động cấp phát IP

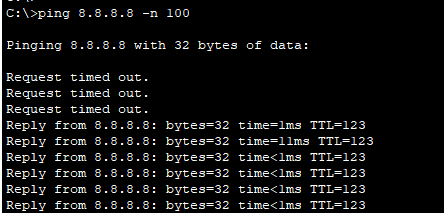
- PC tại VLan 10 được tự động cấp IP từ máy chủ DHCP từ VLan 70.



**Hình 3.1 Kiểm tra tự động cấp phát IP tại DHCP**

### b. Ping trong hệ thống LAN

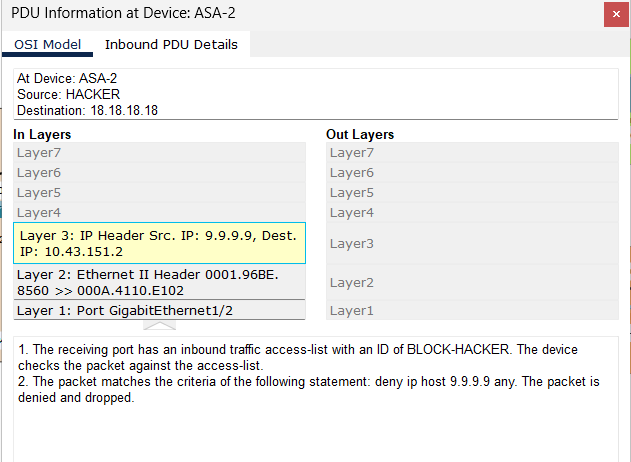
- Tiến hành Ping từ Laptop tại VLan 10 - VLan 80 và sau đó là ping ngược lại để kiểm tra đường truyền trong LAN.



**Hình 3.2 Ping từ VLAN 10- VLAN 80**

### c. Ngăn chặn tin tặc

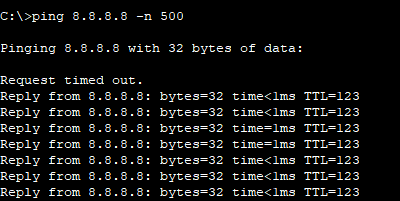
Từ máy chủ của tin tặc đã được cấu hình, truy cập trang web thông qua đường dẫn <http://18.18.18.18> để truy cập trang web của bệnh viện. Hành động này sẽ bị chặn bởi Firewall ASA bằng Access-list



***Hình 3.3 Tin tặc bị tường lửa ngăn chặn truy cập***

### d. Kiểm tra đường dự phòng

Lần lượt tắt các kết nối từ Distribute của tầng 1 lên Core, từ Core lên ASA và ASA lên Router biên 1, ta sẽ thấy gói tin sẽ bắt đầu định tuyến đường đi dự phòng và thành công đi tới đích.



***Hình 3.4 Thiết lập đường dự phòng thành công***

# KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

## KẾT LUẬN

Từ những kiến thức đã học và tìm hiểu từ các nguồn, nhóm chúng em đã phân tích và thiết kế được các mô hình hệ thống mạng theo mô hình phân cấp, thiết kế mô hình mạng WAN, mô hình DMZ và mô hình mạng không dây, tìm hiểu các hãng thiết bị cần sử dụng khi thiết kế hệ thống mạng. Ngoài ra trong đề tài lần này chúng em đã thực hiện được những vấn đề như chia VLAN cho mạng, sử dụng kỹ thuật VTP, STP, Các kết nối đều xây dựng Backup (dự phòng). Không chỉ vậy chúng em đã xây dựng thành công các giao thức định tuyến tĩnh và định tuyến động với máy chủ Web Server, FTP Server, DNS Server, DHCP và triển khai chính sách Access-list. Qua những thông tin này, chúng em hiểu rõ hơn về thiết kế hệ thống mạng, chuyển mạch và định tuyến và chi phí khi triển khai.

## PHƯƠNG HƯỚNG PHÁT TRIỂN

Tuy chúng em đã vận dụng những kiến thức đã học nhưng bài báo cáo của nhóm em vẫn chưa được hoàn thiện một cách chỉnh chu nhất. Vì vậy mà nhóm chúng em dự định làm thêm là sẽ vẽ được các mô hình chi tiết cụ thể nhất và áp dụng triển khai thực nghiệm ngoài đời thực nếu có cơ hội trong tương lai.

**DANH MỤC TÀI LIẸU THAM KHẢO**

**Tiếng Việt**

[1] Wikipedia (2024). VirusTotal. Truy cập tại: <https://vi.wikipedia.org/wiki/VirusTotal> (Ngày truy cập: 20 tháng 3 năm 2025).

[2] nTrust (2024). Phần mềm chống lừa đảo. Truy cập tại: <https://ntrust.vn> (Ngày truy cập: 10 tháng 4 năm 2025).

**Tiếng Anh**

[3] GeeksforGeeks (n.d.). *Kotlin Tutorial*. Available at: <https://www.geeksforgeeks.org/kotlin-programming-language/> (Accessed: April 11, 2025).

[4] Android Developers (n.d.). *Jetpack Compose UI App Development Toolkit*. Available at:<https://developer.android.com/courses/pathways/compose> (Accessed: April 12, 2025).

[5] Cloudinary (2025). Cloudinary CLI Tutorials. Available at: <https://cloudinary.com/documentation/cloudinary_cli_tutorials> (Accessed: April 15, 2025

**BẢNG ĐÁNH GIÁ ĐIỂM :**

|  |  |
| --- | --- |
| **Thành viên** | **Đánh giá điểm cá nhân** |
| Lê Đình Vũ | **9.0** |
| Biện Phương Vy | **8.0** |
| Nguyễn Quang Vương | **8.2** |
| Lê Thị Vy | **8.0** |
| **Điểm cả nhóm** | **9.0** |