**TRƯỜNG ĐẠI HỌC TRÀ VINH**

**KHOA KỸ THUẬT VÀ CÔNG NGHỆ**

Ảnh có chứa biểu tượng, vòng tròn, Phông chữ, Nhãn hiệu

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

**ĐỒ ÁN THỰC TẬP CƠ SỞ NGÀNH**

**Tên đề tài:**

**Đồ án : Thiết kế hệ thống mạng không dây cho khuôn viên trường trung học phổ thông**

Giảng viên hướng dẫn : **ThS. Dương Ngọc Vân Khanh**

Sinh viên thực hiện: **Trần Ngọc Hạnh**

Mã số sinh viên: **170123355**

Lớp **: DX23TT10**

Khoá **: 2023-2027**

**Trà Vinh, ngày 19 tháng 04 năm 2025**

# **MỤC LỤC**

[**MỤC LỤC 2**](#_Toc196771710)

[**BẢNG CÁC KÝ HIỆU, CHỮ VIẾT TẮT 6**](#_Toc196771711)

[**Lời Nói Đầu 7**](#_Toc196771712)

[**CHƯƠNG 1: TỔNG QUAN 8**](#_Toc196771713)

[**1. Giới thiệu chung 8**](#_Toc196771714)

[**2. Tiếp cận đơn vị 8**](#_Toc196771715)

[**2.1 Khảo sát thực tế trường THPT Thăng Long Hà Nội 8**](#_Toc196771716)

[**2.1.1 Sơ đồ khảo sát thực tế 8**](#_Toc196771717)

[**2.1.2 Nhận xét về hệ thống hiện tại và dự án của hệ thống mới 8**](#_Toc196771718)

[**2.1.3 Yêu cầu của hệ thống 9**](#_Toc196771719)

[**2.1.4 Sơ đồ logic 10**](#_Toc196771720)

[**2.1.5 Kế hoạch phân bố IP và VLAN 10**](#_Toc196771721)

[**2.2 Sơ đồ vật lý và đi dây( Lan) và đi dây Wlan( wifi) 11**](#_Toc196771722)

[**2.3 Dự kiến xây dựng hệ thống đường mạng 13**](#_Toc196771723)

[**2.4 Thông tin về địa chỉ IP 14**](#_Toc196771724)

[**CHƯƠNG 2: NGHIÊN CỨU LÝ THUYẾT 16**](#_Toc196771725)

[**1. Giới thiệu mạng Campus Network 16**](#_Toc196771726)

[**2. Mạng Campus truyền thống 16**](#_Toc196771727)

[**2.1. Vấn đề khả năng hoạt động của mạng và giải pháp 17**](#_Toc196771728)

[**Đụng độ (Collision) 17**](#_Toc196771729)

[**Băng thông (Bandwidth) 17**](#_Toc196771730)

[**Broadcast và multicast 17**](#_Toc196771731)

[**2.2 Luật 80/20 17**](#_Toc196771732)

[**Luật mới 20/80 17**](#_Toc196771733)

[**3. Các mô hình mạng Campus 18**](#_Toc196771734)

[**3.1. Mô hình mạng chia sẻ 18**](#_Toc196771735)

[**3.2. Mô hình phân đoạn LAN và WLAN 20**](#_Toc196771736)

[**1. Giới thiệu về phân đoạn mạng LAN và WLAN 20**](#_Toc196771737)

[**2. Phân đoạn mạng LAN 20**](#_Toc196771738)

[**3. Phân đoạn mạng WLAN 21**](#_Toc196771739)

[**4. So sánh phân đoạn LAN và WLAN 21**](#_Toc196771740)

[**5. Ứng dụng của phân đoạn mạng LAN và WLAN 21**](#_Toc196771741)

[**3.3. Mô hình lưu lượng mạng 22**](#_Toc196771742)

[**3.4. Mô hình mạng dự đoán trước 23**](#_Toc196771743)

[**4. Mô hình mạng ba lớp của Cisco 23**](#_Toc196771744)

[**4.1. Lớp truy cập (Access) 23**](#_Toc196771745)

[**4.2. Lớp phân phối (Distribution) 24**](#_Toc196771746)

[**4.3. Lớp nhân (Core) 24**](#_Toc196771747)

[**5. Mô hình Modular trong thiết kế mạng Campus 24**](#_Toc196771748)

[**5.1. Khối Switch 24**](#_Toc196771749)

[**5.2. Khối nhân (Core) 25**](#_Toc196771750)

[**Collapsed core 25**](#_Toc196771751)

[**Dual Core 25**](#_Toc196771752)

[**5.3. Các khối building khác 25**](#_Toc196771753)

[**Khối Server Farm 25**](#_Toc196771754)

[**Khối quản lý 25**](#_Toc196771755)

[**6. Mạng LAN ảo (Virtual LAN - VLAN) 26**](#_Toc196771756)

[**6.1. Các kiểu thành viên của VLAN (VLAN Membership) 26**](#_Toc196771757)

[**Static VLAN 26**](#_Toc196771758)

[**Dynamic VLAN 26**](#_Toc196771759)

[**6.2. Triển khai VLAN 26**](#_Toc196771760)

[**CHƯƠNG 3: HIỆN THỰC HÓA NGHIÊN CỨU 28**](#_Toc196771761)

[**1. Giới thiệu mạng Backup 28**](#_Toc196771762)

[**2. Tầm quan trọng của backup dữ liệu 28**](#_Toc196771763)

[**2.1. Các dữ liệu cần backup 28**](#_Toc196771764)

[**2.2. RPO và RTO - Yếu tố chính đo lường khi lên kế hoạch Backup dữ liệu 29**](#_Toc196771765)

[**3. Giải pháp backup dữ liệu 32**](#_Toc196771766)

[**3.1. Local Backup 32**](#_Toc196771767)

[**3.1.1. Ưu điểm của Local Backup 32**](#_Toc196771768)

[**3.1.2. Nhược điểm của Local Backup 32**](#_Toc196771769)

[**3.2. Online Backup (sao lưu trực tuyến) 33**](#_Toc196771770)

[**3.2.1. Ưu điểm của Online Backup 33**](#_Toc196771771)

[**3.2.2. Nhược điểm của Online Backup 34**](#_Toc196771772)

[**4. Hệ thống lưu trữ 34**](#_Toc196771773)

[**4.1. Backup dữ liệu vào USB - External HardDrive 34**](#_Toc196771774)

[**4.2. Backup dữ liệu bằng thiết bị chuyên dụng - NAS - SAN 35**](#_Toc196771775)

[**4.3. Backup dữ liệu vào Tapes ( băng từ ) 35**](#_Toc196771776)

[**CHƯƠNG 4: CÁC PHƯƠNG PHÁP BẢO MẬT HỆ THỐNG 36**](#_Toc196771777)

[**1. Thiết kế cơ sở hạ tầng theo mô hình SOA 36**](#_Toc196771778)

[**2. Phương thức thiết kế phân lớp – Hierarchical 37**](#_Toc196771779)

[**2.1. Khu vực LAN 37**](#_Toc196771780)

[**2.2. Khu vực kết nối WAN 38**](#_Toc196771781)

[**2.3. Khu vực các máy chủ public 38**](#_Toc196771782)

[**3. Mô hình triển khai dịch vụ và quản lý người dùng 38**](#_Toc196771783)

[**4. Phân hoạch VLAN (LAN ảo) 39**](#_Toc196771784)

[**5. Nhóm giải pháp về hệ thống ngăn chặn, phát hiện tấn công 40**](#_Toc196771785)

[**5.1. Hệ thống tường lửa đa tầng 40**](#_Toc196771786)

[**5.2. Hệ thống phát hiện và chống xâm nhập IDS/IPS 40**](#_Toc196771787)

[**5.3. Danh sách điều khiển truy xuất, an toàn cổng thiết bị, lọc địa chỉ mạng 41**](#_Toc196771788)

[**5.3.1.Danh sách điều khiển truy xuất 41**](#_Toc196771789)

[**5.3.2. Bảo mật cổng của thiết bị. 41**](#_Toc196771790)

[**6. Nhóm giải pháp khác 41**](#_Toc196771791)

[**6.1 Xây dựng hệ thống cập nhật, sửa lỗi tập trung 41**](#_Toc196771792)

[**6.2. Ghi nhật ký, theo dõi, giám sát hệ thống 42**](#_Toc196771793)

[**6.2.1. Ghi nhật ký 42**](#_Toc196771794)

[**6.2.2. Theo dõi, giám sát 42**](#_Toc196771795)

[**6.3. Giải pháp mã hóa dữ liệu và đường truyền 42**](#_Toc196771796)

[**6.4. Đào tạo người dùng 43**](#_Toc196771797)

[**6.5. Hệ thống chống virus 43**](#_Toc196771798)

[**CHƯƠNG 5. KẾT QUẢ NGHIÊN CỨU 44**](#_Toc196771799)

[**CHƯƠNG 6. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 48**](#_Toc196771800)

[**DANH MỤC TÀI LIỆU THAM KHẢO 51**](#_Toc196771801)

[**Phụ lục 53**](#_Toc196771802)

[**Lời cảm ơn 56**](#_Toc196771803)

# **BẢNG CÁC KÝ HIỆU, CHỮ VIẾT TẮT**

| Ký hiệu/Chữ viết tắt | Ý nghĩa |
| --- | --- |
| AP | Access Point (Điểm truy cập không dây) |
| DMZ | Demilitarized Zone (Vùng phi quân sự) |
| IDS/IPS | Intrusion Detection System/Intrusion Prevention System |
| LAN | Local Area Network (Mạng nội bộ có dây) |
| QoS | Quality of Service (Chất lượng dịch vụ) |
| RPO | Recovery Point Objective (Thời điểm phục hồi) |
| RTO | Recovery Time Objective (Thời gian phục hồi) |
| SOA | Service-Oriented Architecture (Kiến trúc định hướng dịch vụ) |
| SSID | Service Set Identifier (Định danh tập hợp dịch vụ) |
| VAP | Virtual Access Point (Điểm truy cập ảo) |
| VLAN | Virtual Local Area Network (Mạng nội bộ ảo) |
| WAN | Wide Area Network (Mạng diện rộng) |
| WLAN | Wireless Local Area Network (Mạng nội bộ không dây) |

# **Lời Nói Đầu**

Trong thời đại công nghệ thông tin phát triển vượt bậc, mạng không dây đã trở thành một phần không thể thiếu trong đời sống hiện đại, đặc biệt trong môi trường giáo dục. Việc triển khai một hệ thống mạng không dây hiệu quả không chỉ đáp ứng nhu cầu truy cập thông tin nhanh chóng mà còn tạo điều kiện thuận lợi cho việc học tập, giảng dạy và quản lý tại các cơ sở giáo dục. Với ý nghĩa đó, đồ án "Thiết kế mạng không dây cho khuôn viên trường THPT" được thực hiện nhằm nghiên cứu và đề xuất một giải pháp mạng tối ưu, đáp ứng nhu cầu thực tiễn của môi trường học đường.

Đồ án không chỉ là cơ hội để em củng cố kiến thức chuyên môn về mạng máy tính và công nghệ không dây mà còn giúp em rèn luyện kỹ năng phân tích, thiết kế và giải quyết vấn đề thực tế. Dưới sự hướng dẫn tận tình của ThS. Dương Ngọc Vân Khanh, em đã nỗ lực hoàn thiện đồ án với mong muốn mang lại một giải pháp mạng không dây hiệu quả, ổn định và phù hợp với điều kiện thực tế của khuôn viên trường THPT.

Trong quá trình thực hiện, em đã cố gắng nghiên cứu các tài liệu liên quan, áp dụng các phương pháp thiết kế hiện đại và tham khảo ý kiến từ giảng viên hướng dẫn để đảm bảo tính khoa học và thực tiễn của đồ án. Tuy nhiên, do hạn chế về kinh nghiệm và thời gian, đồ án khó tránh khỏi những thiếu sót. Em rất mong nhận được những ý kiến đóng góp quý báu từ quý thầy cô và các bạn để đồ án được hoàn thiện hơn.

Em xin chân thành cảm ơn ThS. Dương Ngọc Vân Khanh đã tận tình hướng dẫn, hỗ trợ em trong suốt quá trình thực hiện đồ án. Đồng thời, em xin gửi lời cảm ơn đến nhà trường, các thầy cô trong khoa và bạn bè đã tạo điều kiện và động viên em hoàn thành tốt nhiệm vụ này.

Em hy vọng rằng đồ án sẽ đóng góp một phần nhỏ vào việc nâng cao chất lượng ứng dụng công nghệ thông tin trong giáo dục, đồng thời là nền tảng để em tiếp tục học hỏi và phát triển trong lĩnh vực mạng máy tính.

Trân trọng,

Trần Ngọc Hạnh

# **CHƯƠNG 1: TỔNG QUAN**

1. **Giới thiệu chung**

Đồ án nghiên cứu và đề xuất giải pháp thiết kế mạng không dây (WLAN) cho trường THPT Thăng Long Hà Nội, nhằm đáp ứng nhu cầu truy cập thông tin, hỗ trợ học tập, giảng dạy và quản lý hiệu quả. Vấn đề được tiếp cận thông qua khảo sát hiện trạng, phân tích yêu cầu, và thiết kế hệ thống mạng theo mô hình Client-Server, sử dụng mô hình ba lớp của Cisco (Access,Distribution, Core)

Tên gọi: Trường THPT Thăng Long Hà Nội

Địa chỉ: Số 44 - Tạ Quang Bửu - Hai Bà Trưng, Hanoi, Vietnam

Điện thoại: 024 3868 2655

## **2. Tiếp cận đơn vị**

## **2.1 Khảo sát thực tế trường THPT Thăng Long Hà Nội**

## **2.1.1 Sơ đồ khảo sát thực tế**

Ảnh có chứa văn bản, biểu đồ, ảnh chụp màn hình, Hình chữ nhật

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

Sơ đồ khảo sát thực tế

## **2.1.2 Nhận xét về hệ thống hiện tại và dự án của hệ thống mới**

Ưu điểm

Hiện tại, trường THPT Thăng Long Hà Nội đã có hệ thống mạng LAN tương đối ổn định, phục vụ khá tốt cho các hoạt động cần thiết của các phòng ban.

Nhược điểm của hệ thống hiện tại

Chưa đáp ứng tối đa yêu cầu sử dụng tài nguyên của các phòng ban, chưa tận dụng tối đa tài nguyên vốn có của trường học.

Phương hướng giải quyết

Dự án của hệ thống mới là xây dựng được 1 mô hình mạng WLAN có thể đáp ứng đầy đủ yêu cầu sử dụng mạng của các phòng ban hoạt động trường học.

Sử dụng tối đa tài nguyên sẵn có trong trường học một cách hợp lý mà không tốn kém cho phí lắp đặt lại có thể mở rộng thêm khi hệ thống cần

## **2.1.3 Yêu cầu của hệ thống**

Yêu cầu các phòng được lắp đặt hệ thống mạng:

- Thực hành tin: 20 máy tính nối mạng.

- VP Công đoàn: 1 máy tính nối mạng.

- Thư viện: 1 máy tính nối mạng.

- Kế toán: 1 máy tính nối mạng và 1 máy in.

- Phó hiệu trưởng: 1 máy tính nối mạng.

- Phó hiệu trưởng: 1 máy tính nối mạng.

- Hiệu trưởng: 1 máy tính nối mạng

- Bảo Vệ: 1 máy tính nối mạng

- Hội Đồng: 1 máy tính nối mạng

- Thiết kế hệ thống mạng theo mô hình Client-Server.

- Tất cả các máy tính trong hệ thống mạng đều có thể giao tiếp được với nhau.

- Tất cả các máy tính có cấu hình mạnh.

- Monitor: Samsung 20inch.

## **2.1.4 Sơ đồ logic**

Ảnh có chứa văn bản, ảnh chụp màn hình

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

Sơ đồ logic

## **2.1.5 Kế hoạch phân bố IP và VLAN**

Bảng Thông tin về Vlan

|  |  |  |
| --- | --- | --- |
| Vlan\_ID | Tên Vlan | Ghi chú |
| 1 | Vlan 1 | Không dùng |
| 10 | Vlan 10 | Phòng thực hành tin |
| 20 | Vlan 20 | Văn phòng công đoà |
| 30 | Vlan 30 | P. Thư viện |
| 40 | Vlan 40 | P. Kế toán |
| 50 | Vlan 50 | P. Phó hiệu trưởng |
| 60 | Vlan 60 | P. Phó hiệu trưởng |
| 70 | Vlan 70 | P. Hiệu trưởng |
| 80 | Vlan 80 | P. Bảo vệ |
| 90 | Vlan 90 | P. Hôi đồng |
| 100 | Vlan 100 | Giảng đường A |
| 110 | Vlan 110 | Giảng đường B |
| 120 | Vlan 120 | Giảng đường C |

## **2.2 Sơ đồ vật lý và đi dây( Lan) và đi dây Wlan( wifi)**

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

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

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

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

Khu nhà Hiệu Bộ

Ảnh có chứa biểu đồ, Bản vẽ kỹ thuật, bản phác thảo, Kế hoạch

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

Giảng đường A

Ảnh có chứa biểu đồ, Bản vẽ kỹ thuật, Kế hoạch, sơ đồ

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

Giảng đường B

Ảnh có chứa biểu đồ, Bản vẽ kỹ thuật, Kế hoạch, sơ đồ

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

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

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

Giảng đường C

## **2.3 Dự kiến xây dựng hệ thống đường mạng**

Bảng Hệ thống đường mạng

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Tên phòng | Số nút mạng | Số PC | Số mét dây |
| 1 | Thực hành tin | 02 | 20 | 120m |
| 2 | VP. Công Đoàn | 02 | 02 | 25m |
| 3 | Thư viện | 02 | 01 | 20m |
| 4 | Kế toán | 02 | 01 | 20m |
| 5 | Phó hiệu trưởng | 02 | 01 | 30m |
| 6 | Phó hiệu trưởng | 02 | 01 | 25m |
| 7 | Hiệu trưởng | 02 | 01 | 20m |
| 8 | Bảo vệ | 02 | 01 | 10m |
| 9 | Hội đồng | 02 | 01 | 35m |
| 10 | Giảng đường A | 12 | 01 | 60m |
| 12 | Giảng đường B | 20 | 01 | 100m |
| 13 | Giảng đường C | 16 | 01 | 80m |

| **STT** | **Tên phòng** | **Số nút mạng** | **Số PC** | **Số mét dây** | **WLAN (Có/Không)** |
| --- | --- | --- | --- | --- | --- |
| 1 | Thực hành tin | 02 | 20 | 120m | Có |
| 2 | VP. Công Đoàn | 02 | 02 | 25m | Có |
| 3 | Thư viện | 02 | 01 | 20m | Có |
| 4 | Kế toán | 02 | 01 | 20m | Không |
| 5 | Phó hiệu trưởng | 02 | 01 | 30m | Không |
| 6 | Phó hiệu trưởng | 02 | 01 | 25m | Không |
| 7 | Hiệu trưởng | 02 | 01 | 20m | Không |
| 8 | Bảo vệ | 02 | 01 | 10m | Không |
| 9 | Hội đồng | 02 | 01 | 35m | Không |
| 10 | Giảng đường A | 12 | 01 | 60m | Có |
| 11 | Giảng đường B | 20 | 01 | 100m | Có |
| 12 | Giảng đường C | 16 | 01 | 80m | Có |

## **2.4 Thông tin về địa chỉ IP**

Bảng Thông tin IP

| **VLAN ID** | **Tên VLAN** | **Dải địa chỉ IP** |
| --- | --- | --- |
| 1 | VLAN 1 | 192.168.1.2 – 192.168.1.254 |
| 10 | VLAN 10 | 192.168.10.2 – 192.168.10.254 |
| 20 | VLAN 20 | 192.168.20.2 – 192.168.20.254 |
| 30 | VLAN 30 | 192.168.30.2 – 192.168.30.254 |
| 40 | VLAN 40 | 192.168.40.2 – 192.168.40.254 |
| 50 | VLAN 50 | 192.168.50.2 – 192.168.50.254 |
| 60 | VLAN 60 | 192.168.60.2 – 192.168.60.254 |
| 70 | VLAN 70 | 192.168.70.2 – 192.168.70.254 |
| 80 | VLAN 80 | 192.168.80.2 – 192.168.80.254 |
| 90 | VLAN 90 | 192.168.90.2 – 192.168.90.254 |
| 100 | VLAN 100 | 192.168.100.2 – 192.168.100.254 |
| 110 | VLAN 110 | 192.168.110.2 – 192.168.110.254 |
| 120 | VLAN 120 | 192.168.120.2 – 192.168.120.254 |

| **VLAN ID** | **Tên VLAN** | **Dải địa chỉ IP (có dây)** | **Dải địa chỉ IP (không dây WLAN)** |
| --- | --- | --- | --- |
| 1 | VLAN 1 | 192.168.1.2 – 192.168.1.254 | 192.168.1.100 – 192.168.1.200 |
| 10 | VLAN 10 | 192.168.10.2 – 192.168.10.254 | 192.168.10.100 – 192.168.10.200 |
| 20 | VLAN 20 | 192.168.20.2 – 192.168.20.254 | 192.168.20.100 – 192.168.20.200 |
| 30 | VLAN 30 | 192.168.30.2 – 192.168.30.254 | 192.168.30.100 – 192.168.30.200 |
| 40 | VLAN 40 | 192.168.40.2 – 192.168.40.254 | 192.168.40.100 – 192.168.40.200 |
| 50 | VLAN 50 | 192.168.50.2 – 192.168.50.254 | 192.168.50.100 – 192.168.50.200 |
| 60 | VLAN 60 | 192.168.60.2 – 192.168.60.254 | 192.168.60.100 – 192.168.60.200 |
| 70 | VLAN 70 | 192.168.70.2 – 192.168.70.254 | 192.168.70.100 – 192.168.70.200 |
| 80 | VLAN 80 | 192.168.80.2 – 192.168.80.254 | 192.168.80.100 – 192.168.80.200 |
| 90 | VLAN 90 | 192.168.90.2 – 192.168.90.254 | 192.168.90.100 – 192.168.90.200 |
| 100 | VLAN 100 | 192.168.100.2 – 192.168.100.254 | 192.168.100.100 – 192.168.100.200 |
| 110 | VLAN 110 | 192.168.110.2 – 192.168.110.254 | 192.168.110.100 – 192.168.110.200 |
| 120 | VLAN 120 | 192.168.120.2 – 192.168.120.254 | 192.168.120.100 – 192.168.120.200 |

# **CHƯƠNG 2: NGHIÊN CỨU LÝ THUYẾT**

## **1. Giới thiệu mạng Campus Network**

- Internet đã thay đổi cuộc sống chúng ta, với sự gia tăng số lượng của các dịch vụ giao dịch trực tuyến, giáo dục, và giải trí,… điều này thúc đẩy chúng ta tìm ra nhiều phương pháp để truyền thông với nhau. Liên mạng (internetworing) là sự truyền thông giữa một hay nhiều mạng, gồm có nhiều máy tính kết nối lại với nhau. Liên mạng máy tính ngày càng lớn mạnh để hỗ trợ cho các nhu cầu truyền thông khác nhau của hệ thống đầu cuối. Một liên mạng đòi hỏi nhiều giao thức và tính năng để cho phép sự mở rộng. Các liên mạng lớn gồm có 3 thành phần như sau:

• Mạng Campus: gồm có các user kết nối cục bộ trong một hay một nhóm

các tòa nhà.

• Mạng WAN: kết nối các mạng Campus lại với nhau.

• Kết nối từ xa: liên kết các nhánh và các user đơn lẻ tới mạng Campus

hay Internet.

- Thiết kế một liên mạng là một công việc thử thách năng lực đối với

người thiết kế. Để thiết kế một liên mạng có độ tin cậy và có tính mở rộng, thì

người thiết kế phải hiểu rõ về ba thành phần quan trọng của một liên mạng với những đòi hỏi thiết kế khác nhau

Ảnh có chứa biểu đồ, Kế hoạch, Bản vẽ kỹ thuật, hàng

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

Hình 1.1 ví dụ về internetworing

## **2. Mạng Campus truyền thống**

- Trong các năm 1990, mạng Campus truyền thống bắt đầu là một mạng LAN và lớn dần. Tuy nhiên, các LAN không thể lớn dần mãi mãi, mà đến một độ lớn nào đó, chúng ta cần phải cần phân đoạn mạng (chia mạng thành các khu vực hay miền cho dễ quản lý) để duy trì khả năng hoạt động của mạng sao cho: thời gian đáp ứng (trả lời) cần được đảm bảo với các chức năng của mạng. Thêm nữa, phần lớn các ứng dụng phải được lưu trữ và chuyển tiếp có một điều cần thiết nữa là chất lượng các dịch vụ tùy

### 2.1. Vấn đề khả năng hoạt động của mạng và giải pháp

- Tính sẵn sàng và khả năng hoạt động là hai vấn đề chính đối với mạng Campus truyền thống. Tính sẵn sàng bị ảnh hưởng bởi số lượng user cố gắng truy cập mạng ở cùng một thời điểm, cộng với độ tin cậy của chính mạng đó. Khả năng hoạt động trong mạng Campus truyền thống bao gồm các vấn đề như: đụng độ, băng thông, broadcast, multicast.

### **Đụng độ (Collision)**

- Đụng độ là: hiện tượng các tín hiệu phát từ hai máy gây nhiễu lẫn nhau. Hai tín hiệu gây nhiễu lẫn nhau còn gọi là xung đột. Miền đụng độ(Collision Domain): đây là một vùng có khả năng bị đụng độ do hai hay nhiều máy tính cùng gởi tín hiệu lên môi trường truyền thông. Miền quảng bá (Broadcast Domain): đây là một vùng mà gói tin phát tán hay quảng bá (gói tin broadcast) có thể đi qua được. Trong miền quảng bá có thể bao gồm nhiều miền đụng độ.

### **Băng thông (Bandwidth)**

• Độ rộng.

• Khoảng cách.

### **Broadcast và multicast**

- VLAN cũng là một giải pháp, nhưng VLAN chỉ là miền broadcast với đường biên ảo. Một VLAN là một nhóm các thiết bị trên các phân đoạn mạng khác nhau, đó là một miền broadcast bởi người quản trị mạng. Lợi ích của VLAN là vị trí vật lý không còn là nhân tố xác định cổng (port) mà ta sẽ thêm vào một thiết bị trong mạng. Ta có thể thêm một thiết bị vào bất kỳ port nào của switch và người quản trị mạng sẽ gán port cho VLAN. Lưu ý là chỉ có router hoặc switch lớp 3 mới có thể truyền thông giữa các VLAN khác nhau

## **2.2 Luật 80/20**

Luật 80/20 có nghĩa là 80% lưu lượng của user là trên đoạn mạng cục bộ (các phân đoạn mạng), còn lại 20% hoặc ít hơn là qua router hoặc bridge đến các đoạn mạng khác. Nếu nhiều hơn 20% lưu lượng qua thiết bị phân đoạn mạng, thì phát sinh vấn đề về khả năng hoạt động của mạng. Hình 1.2 sau biểu diễn một mạng 80/20 truyền thống. Bởi vì người quản trị mạng chịu trách nhiệm thiết kế và thực hiện, nên họ cải tiến khả năng hoạt động của mạng trong mạng 80/20 bằng cách chắc chắn rằng tất cả các tài nguyên mạng cho user được chứa bên trong đoạn mạng cục bộ. Tài nguyên bao gồm máy chủ, máy in, thư mục dùng chung, phần mềm, và các ứng dụng .

### **Luật mới 20/80**

Ngày nay, thay vì phân tán các máy chủ, chúng được tập trung lại tạo thành “trang trại” máy chủ (server farm) để kiểm soát dịch vụ mạng có tính bảo mật, giảm chi phí và dễ quản trị, nên luật 80/20 đã trở nên lỗi thời và không còn làm việc trong môi trường này nữa. Trong môi trường như vậy, tất cả lưu lượng phải qua backbone (đường trục) của Campus, nghĩa là ta có luật mới 20/80, trong đó 20% là lưu lượng trên đoạn mạng cục bộ và 80% là lưu lượng qua đoạn mạng để lấy các dịch vụ mạng. Hình 1.3 biểu diễn mạng 20/80 mới.

VLAN (Virtual LAN)

Với luật 20/80 có nhiều user hơn cần truyền qua miền broadcast, và điều này gây thêm gánh nặng cho việc định tuyến hoặc chuyển mạch lớp 3. Bằng cách sử dụng VLAN, bên trong mô hình mạng Campus, ta có thể điều khiển được lưu lượng và user truy cập dễ dàng hơn trong mạng Campus truyền thống. VLAN làm giảm miền broadcast bằng cách sử dụng router hoặc switch để thực hiện các chức năng lớp 3.

## 3. Các mô hình mạng Campus

- Một mạng Campus gồm có nhiều LAN trong một hoặc nhiều tòa nhà, tất cả các kết nối nằm trong cùng một khu vực địa lý. Thông thường các mạng Campus gồm có Ethernet, Wireless LAN, Fast Ethernet, Fast EtherChannel, Gigabit Ethernet và FDDI. Sau đây là các mô hình mạng được dùng để phân loại và thiết kế mạng Campus:

♣ Mô hình mạng chia sẻ (Shared Network Model).

♣ Mô hình phân đoạn LAN (LAN Segmentation Model).

♣ Mô hình lưu lượng mạng (Network Traffic Model).

♣ Mô hình mạng dự đoán trước (Predictable Network Model).

### **3.1. Mô hình mạng chia sẻ**

Mô hình **mạng chia sẻ** (hay còn gọi là **Shared Network Model**) là một cách tổ chức và phân bổ các tài nguyên mạng giữa các thiết bị trong mạng. Trong mô hình này, nhiều thiết bị có thể chia sẻ cùng một kết nối mạng, giúp tiết kiệm chi phí và đơn giản hóa việc triển khai mạng. Mạng chia sẻ thường được sử dụng trong các môi trường như trường học, văn phòng, và các khu vực có nhu cầu chia sẻ tài nguyên một cách đồng bộ.

Mô hình mạng chia sẻ có thể bao gồm các loại hình kết nối mạng có dây (Ethernet) hoặc không dây (Wi-Fi), với việc các thiết bị chia sẻ băng thông và tài nguyên mạng như một phần của một cấu trúc chung.

**Các thành phần chính trong mô hình mạng chia sẻ:**

1. **Thiết bị chia sẻ tài nguyên**:
   * **Máy chủ (Server)**: Là các thiết bị lưu trữ và quản lý tài nguyên mạng như tệp, dữ liệu, máy in và các ứng dụng.
   * **Switches và Routers**: Các thiết bị mạng (như công tắc và bộ định tuyến) đảm bảo rằng dữ liệu có thể được truyền từ thiết bị này sang thiết bị khác trong mạng chia sẻ. Switch giúp kết nối các thiết bị trong cùng một mạng LAN, trong khi Router điều hướng dữ liệu giữa các mạng khác nhau.
2. **Điểm truy cập không dây (Access Points - APs)**: Các điểm truy cập Wi-Fi cho phép các thiết bị di động kết nối với mạng chia sẻ mà không cần sử dụng dây cáp.
3. **Thiết bị cuối (End Devices)**: Là các thiết bị mà người dùng sử dụng để kết nối với mạng, bao gồm máy tính, điện thoại, máy in, máy quét, và các thiết bị ngoại vi khác.

**Các loại mô hình mạng chia sẻ:**

1. **Mạng chia sẻ có dây (Wired Shared Network)**:
   * Trong mô hình này, các thiết bị kết nối với nhau qua các dây cáp vật lý, thường là cáp Ethernet.
   * Tất cả các thiết bị trong mạng đều chia sẻ một kết nối cáp duy nhất đến Switch hoặc Router.
   * Ví dụ: Trong một văn phòng hoặc khuôn viên trường học, các máy tính và thiết bị ngoại vi như máy in có thể được kết nối với nhau qua hệ thống cáp Ethernet và chia sẻ một đường truyền mạng chung.
2. **Mạng chia sẻ không dây (Wireless Shared Network)**:
   * Các thiết bị kết nối qua sóng vô tuyến (Wi-Fi) mà không cần dây cáp.
   * Điểm truy cập không dây (APs) được sử dụng để cung cấp kết nối Wi-Fi cho các thiết bị trong mạng.
   * Ví dụ: Một khuôn viên trường học có thể sử dụng các AP để cung cấp Wi-Fi cho học sinh và giáo viên, giúp họ kết nối với các tài nguyên mạng như máy tính, máy in, và các ứng dụng trực tuyến.

**Ưu điểm của mô hình mạng chia sẻ:**

1. **Tiết kiệm chi phí**: Việc chia sẻ tài nguyên giúp giảm bớt chi phí đầu tư vào phần cứng mạng (như router, switch), vì các thiết bị có thể sử dụng chung một kết nối mạng.
2. **Đơn giản hóa việc quản lý**: Mô hình mạng chia sẻ giúp giảm bớt sự phức tạp trong việc thiết lập và duy trì mạng, đặc biệt là trong các môi trường có nhiều thiết bị.
3. **Dễ dàng mở rộng**: Nếu cần mở rộng mạng, bạn chỉ cần thêm các thiết bị mới vào mạng mà không cần thay đổi cấu trúc mạng chính.
4. **Tăng tính linh hoạt**: Các thiết bị di động có thể kết nối với mạng chia sẻ không dây mà không cần cắm cáp, tạo sự thuận tiện trong việc truy cập tài nguyên mạng.

**Nhược điểm của mô hình mạng chia sẻ:**

1. **Khả năng tắc nghẽn băng thông**: Khi nhiều thiết bị chia sẻ một kết nối mạng duy nhất, băng thông có thể bị tắc nghẽn nếu nhiều thiết bị cùng truy cập mạng cùng một lúc.
2. **Bảo mật**: Mạng chia sẻ có thể dễ bị tấn công nếu không được bảo vệ đúng cách, vì tất cả các thiết bị trong mạng đều có thể truy cập chung tài nguyên.
3. **Hiệu suất mạng**: Nếu mạng không được quản lý đúng cách, hiệu suất có thể bị ảnh hưởng, đặc biệt khi có quá nhiều thiết bị kết nối hoặc khi tài nguyên mạng bị sử dụng quá mức.

**Ví dụ về mô hình mạng chia sẻ:**

1. **Trường học**:
   * Trong một trường học, học sinh và giáo viên có thể sử dụng cùng một mạng chia sẻ để truy cập Internet, tài liệu học tập, và máy in. Hệ thống Wi-Fi được cài đặt tại các lớp học, thư viện và các khu vực công cộng để hỗ trợ kết nối không dây.
2. **Văn phòng**:
   * Trong một văn phòng, các máy tính và thiết bị ngoại vi có thể được kết nối với nhau qua một hệ thống mạng chia sẻ có dây hoặc không dây. Nhân viên có thể chia sẻ dữ liệu, máy in, và các tài nguyên khác một cách hiệu quả.

## **3.2. Mô hình phân đoạn LAN và WLAN**

### **1. Giới thiệu về phân đoạn mạng LAN và WLAN**

**Phân đoạn mạng** là một kỹ thuật sử dụng để chia mạng thành các phần nhỏ hơn, giúp tối ưu hóa hiệu suất, nâng cao bảo mật và dễ dàng quản lý. Trong một hệ thống mạng lớn, việc phân đoạn giúp giảm bớt tắc nghẽn, cải thiện khả năng xử lý và bảo vệ dữ liệu khỏi các nguy cơ bị xâm nhập.

**Mạng LAN (Local Area Network)** và **WLAN (Wireless Local Area Network)** đều có thể được phân đoạn, tuy nhiên, phương thức và các yếu tố triển khai sẽ có sự khác biệt tùy theo công nghệ (có dây hay không dây).

* **LAN (Mạng nội bộ có dây)**: Là mạng kết nối các thiết bị trong một khu vực hạn chế như trong một tòa nhà hoặc khuôn viên nhỏ. Thường sử dụng các công nghệ như Ethernet và cáp đồng trục để kết nối các thiết bị mạng.
* **WLAN (Mạng nội bộ không dây)**: Là mạng kết nối các thiết bị không sử dụng dây cáp mà sử dụng sóng vô tuyến (Wi-Fi) để truyền dữ liệu giữa các thiết bị.

### **2. Phân đoạn mạng LAN**

**Phân đoạn mạng LAN** là quá trình chia mạng có dây thành các phần nhỏ hơn, giúp cải thiện hiệu suất và bảo mật cho mạng. Điều này có thể được thực hiện thông qua việc sử dụng **VLAN (Virtual Local Area Network)**.

**VLAN** là một phương pháp phân đoạn mạng LAN, cho phép nhóm các thiết bị có thể ở bất kỳ đâu trong mạng LAN, nhưng vẫn có thể chia sẻ một mạng con chung.

**Cách thức hoạt động của VLAN**:

* **VLAN** chia mạng LAN thành các nhóm nhỏ hơn, mỗi nhóm hoạt động như một mạng riêng biệt.
* Các thiết bị trong mỗi VLAN có thể giao tiếp với nhau mà không cần đi qua các VLAN khác, giúp giảm lưu lượng mạng và bảo mật tốt hơn.
* **Switch Layer 3** có thể được sử dụng để kết nối các VLAN và định tuyến lưu lượng giữa các VLAN.

**Ưu điểm của VLAN**:

* **Tăng cường bảo mật**: Mỗi VLAN có thể được phân quyền truy cập riêng biệt, giúp hạn chế quyền truy cập vào các thiết bị trong các VLAN khác.
* **Quản lý đơn giản**: Mạng LAN có thể dễ dàng mở rộng và quản lý, đặc biệt khi cần nhóm các thiết bị theo chức năng hoặc vị trí.
* **Tối ưu hóa hiệu suất mạng**: Phân đoạn giúp giảm lưu lượng mạng và tránh tình trạng tắc nghẽn.

### **3. Phân đoạn mạng WLAN**

**Phân đoạn WLAN** có thể thực hiện bằng cách sử dụng **Virtual Access Points (VAPs)** hoặc **SSID (Service Set Identifier)** để tạo ra các phân đoạn mạng không dây.

**Cách thức hoạt động của WLAN phân đoạn**:

* **SSID** là một tên mạng được sử dụng để phân biệt các mạng WLAN trong một khu vực.
* **VAP (Virtual Access Point)** cho phép một điểm truy cập không dây (Access Point - AP) phục vụ nhiều SSID khác nhau, tương tự như việc phân đoạn mạng LAN với VLAN.
* Các thiết bị kết nối với các SSID khác nhau sẽ được phân đoạn thành các nhóm riêng biệt và có thể được cấu hình để có các quyền truy cập khác nhau.

**Ưu điểm của phân đoạn WLAN**:

* **Tăng cường bảo mật**: Các SSID riêng biệt có thể cấu hình với các chính sách bảo mật khác nhau, giúp kiểm soát tốt hơn việc truy cập vào mạng.
* **Quản lý dễ dàng hơn**: Mỗi SSID có thể được gán cho các nhóm người dùng khác nhau (như học sinh, giáo viên, nhân viên) để hạn chế việc truy cập tài nguyên.
* **Tối ưu băng thông**: Phân đoạn giúp tránh tình trạng tắc nghẽn mạng khi nhiều thiết bị đồng thời kết nối vào cùng một SSID.

### **4. So sánh phân đoạn LAN và WLAN**

| **Tiêu chí** | **LAN (Mạng có dây)** | **WLAN (Mạng không dây)** |
| --- | --- | --- |
| **Công nghệ sử dụng** | Ethernet, cáp đồng trục, cáp quang | Wi-Fi, sóng vô tuyến |
| **Phân đoạn** | VLAN (Virtual LAN) | SSID, VAP (Virtual Access Point) |
| **Bảo mật** | Phân quyền dựa trên VLAN | Phân quyền dựa trên SSID, WPA/WPA2 |
| **Quản lý** | Dễ dàng thông qua switch và router | Dễ dàng thông qua cấu hình AP và SSID |
| **Khả năng mở rộng** | Cần cáp vật lý, giới hạn theo phạm vi cáp | Không cần cáp, có thể mở rộng dễ dàng, nhưng phụ thuộc vào phạm vi sóng AP |
| **Chi phí** | Chi phí cài đặt cao hơn (cáp, switch, router) | Chi phí cài đặt thấp hơn (AP, router) |

### **5. Ứng dụng của phân đoạn mạng LAN và WLAN**

* **Mạng LAN**:
  + **Doanh nghiệp**: Phân chia các bộ phận của công ty thành các VLAN khác nhau để bảo mật và dễ dàng quản lý mạng.
  + **Trường học**: Các phòng học có thể được kết nối trong cùng một VLAN, nhưng các phòng chức năng như thư viện, phòng giáo viên có thể được phân thành các VLAN riêng biệt.
* **Mạng WLAN**:
  + **Trường học**: Các SSID có thể được phân bổ cho các nhóm học sinh, giáo viên, và nhân viên, giúp kiểm soát việc truy cập vào mạng Wi-Fi.
  + **Văn phòng**: Phân đoạn mạng không dây giúp giảm tắc nghẽn và cung cấp dịch vụ Wi-Fi cho từng bộ phận hoặc nhóm người dùng khác nhau trong văn phòng.

## **3.3. Mô hình lưu lượng mạng**

**1. Giới thiệu về lưu lượng mạng trong thiết kế Campus Network**

Trong thiết kế và xây dựng mạng **Campus Network**, việc hiểu và kiểm soát **lưu lượng mạng** là một yếu tố cực kỳ quan trọng để đảm bảo hiệu suất tối ưu và tính sẵn sàng của hệ thống. Mạng Campus sẽ phục vụ một số lượng lớn người dùng và các thiết bị, do đó cần phải đảm bảo rằng mọi thiết bị, người dùng, và ứng dụng trong mạng đều có thể truyền tải dữ liệu hiệu quả và không gặp phải các vấn đề về tắc nghẽn hay gián đoạn.

Lưu lượng mạng không phải chỉ đơn giản là việc truyền tải dữ liệu từ thiết bị này đến thiết bị khác, mà còn liên quan đến các kiểu dữ liệu khác nhau tùy thuộc vào từng ứng dụng. Các ứng dụng như email, duyệt web, và in ấn sẽ có lưu lượng đơn giản, ít biến động, trong khi các ứng dụng như video streaming, VoIP, hay truyền hình trực tuyến (TV) có lưu lượng phức tạp và khó đoán trước.

**2. Các kiểu lưu lượng mạng**

Lưu lượng mạng có thể được phân loại thành các nhóm chính sau:

* **Lưu lượng văn bản (Text-based traffic)**: Bao gồm các ứng dụng như email, duyệt web, và các ứng dụng văn phòng (Word, Excel…). Lưu lượng này chủ yếu mang dữ liệu văn bản và có ít yêu cầu về băng thông.
* **Lưu lượng tệp (File transfer traffic)**: Lưu lượng này liên quan đến việc truyền tải các tệp giữa các máy tính. Các ứng dụng này yêu cầu băng thông cao hơn và có thể gây ra tắc nghẽn mạng nếu không được kiểm soát tốt.
* **Lưu lượng thoại (Voice traffic)**: Lưu lượng này đến từ các ứng dụng VoIP, yêu cầu độ trễ thấp và không bị gián đoạn trong suốt quá trình truyền tải. Đây là một loại lưu lượng có tính thời gian thực (real-time traffic).
* **Lưu lượng video (Video traffic)**: Các ứng dụng video trực tuyến như video conference, video streaming (YouTube, Zoom, TV) yêu cầu băng thông cao và khả năng xử lý lưu lượng lớn.

**3. Phân đoạn và tối ưu hóa lưu lượng mạng**

Để tối ưu hóa lưu lượng và đảm bảo mạng hoạt động hiệu quả, có thể thực hiện các chiến lược phân đoạn mạng, đưa ra các kỹ thuật kiểm soát lưu lượng và đảm bảo tài nguyên mạng được phân bổ hợp lý. Các bước cần thực hiện bao gồm:

* **Gán lại tài nguyên sẵn có**: Khi các máy chủ và người dùng trong mạng trở nên quá tải hoặc không gần nhau về mặt vật lý, có thể điều chỉnh lại các tài nguyên mạng để đưa các người dùng và các server lại gần nhau hơn. Việc này giúp giảm độ trễ và cải thiện hiệu suất mạng.
* **Chuyển các ứng dụng và các tệp đến các server khác nhau**: Các tệp hoặc ứng dụng có thể được chuyển đến các máy chủ khác nhau trong mạng để tránh tắc nghẽn tại các điểm cụ thể. Các server có thể được phân bổ theo các nhóm ứng dụng để tối ưu hóa hiệu suất và sử dụng tài nguyên mạng.
* **Chuyển các user gần với nhóm của họ**: Người dùng có thể được chuyển logic (dựa trên VLAN) hoặc vật lý đến các vị trí gần các nhóm hoặc các ứng dụng mà họ sử dụng nhiều nhất. Điều này giúp giảm thời gian truy cập và giảm tải trên mạng.
* **Thêm nhiều server và tài nguyên**: Để phục vụ nhu cầu sử dụng dữ liệu ngày càng tăng, việc thêm các server mới hoặc tăng cường tài nguyên là cần thiết. Các server này sẽ giúp đưa tài nguyên lại gần các nhóm người dùng hơn, giảm độ trễ và cải thiện hiệu suất.

**4. Xử lý lưu lượng mạng trong môi trường Campus**

* **VLAN (Virtual LAN)**: Phân chia mạng thành các VLAN khác nhau để tách biệt lưu lượng của các nhóm người dùng khác nhau. Ví dụ, có thể có một VLAN dành cho phòng học, một VLAN dành cho các phòng ban quản lý, và một VLAN dành cho các dịch vụ như in ấn hay server. Điều này giúp giảm bớt lưu lượng không cần thiết và tăng hiệu suất mạng.
* **QoS (Quality of Service)**: Đảm bảo rằng các ứng dụng quan trọng (như VoIP và video) được ưu tiên khi có sự cạnh tranh về tài nguyên mạng. QoS giúp phân loại lưu lượng và cung cấp các ưu tiên khác nhau đối với từng loại ứng dụng, đảm bảo chất lượng dịch vụ cho các ứng dụng yêu cầu thời gian thực.
* **Cân bằng tải (Load balancing)**: Việc sử dụng các kỹ thuật cân bằng tải giúp phân phối đều lưu lượng đến các server khác nhau, tránh việc tập trung tải quá nhiều vào một server. Điều này cũng giúp tăng khả năng chịu lỗi và đảm bảo tính sẵn sàng cho mạng.

## **3.4. Mô hình mạng dự đoán trước**

- Luồng lưu lượng trong mạng Campus có thể phân thành ba loại, dựa vịtrí các dịch vụ mạng liên quan đến người dùng đầu cuối. Bảng 1.1 cho biết danhsách các kiểu lưu lượng này, cùng với phạm vi của nó.

- Lớp Access, Distribution và Core là ba lớp của mô hình thiết mạng balớp của Cisco mà ta sẽ tìm hiểu trong phần tiếp theo

## **4. Mô hình mạng ba lớp của Cisco**

- Ta có thể thiết kế mạng Campus để mỗi lớp hỗ trợ các luồng lưu lượng hoặc dịch vụ như đã đề cập trong bảng 1.1. Cisco đưa ra mô hình thiết kế mạng cho phép người thiết kế tạo một mạng luận lý bằng cách định nghĩa và sử dụng các lớp của thiết bị mang lại tính hiệu quả, tính thông minh, tính mở rộng và quản lý dễ dàng. --Mô hình này gồm có ba lớp: Access, Distribution, và Core.Mỗi lớp có các thuộc tính riêng để cung cấp cả chức năng vật lý lẫn luận lý ở mỗi điểm thích hợp trong mạng Campus. Việc hiểu rõ mỗi lớp và chức năng cũng như hạn chế của nó là điều quan trọng để ứng dụng các lớp đúng cách quá trính thiết kế.

## **4.1. Lớp truy cập (Access)**

- Lớp truy cập xuất hiện ở người dùng đầu cuối được kết nối vào mạng.

Các thiết bị trong lớp này thường được gọi là các switch truy cập, và có các đặc điểm sau:

• Chi phí trên mỗi port của switch thấp

• Mật độ port cao.

• Mở rộng các uplink đến các lớp cao hơn.

• Chức năng truy cập của người dùng như là thành viên VLAN, lọc lưu

lượng và giao thức, và QoS.

• Tính co dãn thông qua nhiều uplink.

## **4.2. Lớp phân phối (Distribution)**

- Lớp phân phối cung cấp kết nối bên trong giữa lớp truy cập và lớp nhân

của mạng Campus. Thiết bị lớp này được gọi là các switch phân phát, và có các đặc điểm như sau:

• Thông lượng lớp ba cao đối với việc xử lý gói.

• Chức năng bảo mật và kết nối dựa trên chính sách qua danh sách truy

cập hoặc lọc gói.

• Tính năng QoS.

• Tính co dãn và các liên kết tốc độ cao đến lớp Core và lớp Access.

## **4.3. Lớp nhân (Core)**

- Lớp nhân của mạng Campus cung cấp các kết nối của tất cả các thiết bị lớp phân phối. Lớp nhân thường xuất hiện ở phần xương sống (backbone) của mạng, và phải có khả năng chuyển mạch lưu lượng một cách hiệu quả. Các thiết bị lớp nhân thường được gọi là các backbone switch, và có những thuộc tính sau:

• Thông lượng ở lớp 2 hoặc lớp 3 rất cao.

• Chi phí cao

• Có khả năng dự phòng và tính co dãn cao.

• Chức năng QoS.

## **5. Mô hình Modular trong thiết kế mạng Campus**

-Ta có thể chia mạng Campus thành các phần cơ bản sau:

• Khối chuyển mạch (switch): là một nhóm các switch thuộc lớp Access

và lớp Distribution.

• Khối lõi (core): là backbone của mạng Campus.

- Các khối liên quan khác có thể tồn tại mặc dù nó không góp phần vào toàn bộ chức năng của mạng Campus, nhưng nó được thiết kế tách biệt và thêm vào thiết kế mạng. Các khối này gồm có:

• Khối Server Farm

• Khối quản lý (Management)

• Khối Enterprise biên (Enterprise Edge):

• Khối nhà cung cấp dịch vụ biên (Service Provider Edge):

## **5.1. Khối Switch**

• Kiểu lưu lượng.

• Tổng dung lượng chuyển mạch lớp 3 tại lớp Distribution.

• Số người được kết nối đến switch của lớp Access.

• Ranh giới địa lý của mạng con hoặc VLAN.

• Kích thước của miền Spanning Tree.

- Việc thiết kế một khối Switch chỉ dựa vào số người dùng hoặc số trạm

chứa trong khối thường không đúng lắm. Thông thường không quá 2000 user được đặt bên trong một khối Switch. Tuy nhiên việc ước lượng kích thước ban đầu cũng đem lại nhiều lợi ích vì vậy ta phải dựa vào các yếu tố sau:

• Loại lưu lượng và hoạt động của nó.

• Kích thước và số lượng của các nhóm làm việc (workgroup).

## **5.2. Khối nhân (Core)**

- Một khối core được yêu cầu để kết nối 2 hoặc nhiều hơn các khối switch trong mạng Campus. Bởi vì lưu lượng từ tất cả các khối Switch, các khối Server Farm, và khối Enterprise biên phải đi qua khối nhân, nên khối nhân phải có khả năng và tính đàn hồi chấp nhận được. Nhân là khái niệm cơ bản trong mạng Campus, và nó mang nhiều lưu lượng hơn các khối khác.

### **Collapsed core**

- Khối Collapsed Core là sự phân lớp của lớp nhân, được che lấp trong lớp phân phối. Ở đây, các chức năng của cả lớp phân phối và nhân đều được cung cấp trong cùng các thiết bị switch. Điều này thường thấy trong mạng Campus nhỏ hơn mà không xác nhận sự tách rời của lớp nhân.

### **Dual Core**

- Một Dual Core kết nối hai hay nhiều khối Switch để dự phòng, nhưng

khối Core không thể có tính mở rộng khi có nhiều khối Switch được thêm vào. Hình 1.10 minh họa khối Dual Core. Chú ý rằng khối Core này xuất hiện như là một module độc lập và không được ghép vào trong bất kỳ khối hoặc lớp nào.

## **5.3. Các khối building khác**

- Để có được những điều cần thiết trên, ta có thể nhóm các tài nguyên vào

các khối building giống như là mô hình khối switch. Các khối này cũng có

switch của lớp Distribution và có các kết nối dự phòng nối trực tiếp vào lớp

Core, nó cũng chứa các tài nguyên của Enterprise. Hầu hết các khối building đều có trong mạng Campus vừa và lớn

### **Khối Server Farm**

- Các máy chủ riêng có các kết nối mạng đơn đến một trong các switch

của lớp phân phối. Nếu một máy chủ dự phòng được sử dụng, thì nó nên kết nối đến switch luân phiên của phân phối.

### **Khối quản lý**

- Khối Switch quản lý mạng thường có lớp phân phối kết nối vào các

switch của khối nhân. Vì các công cụ này được dùng để phát hiện lỗi xảy ra tại thiết bị và các kết nối, nên lợi ích của nó rất quan trọng. Các kết nối dự phòng và

switch dự phòng đều được sử dụng.

**Khối Enterprise biên**

**Khối nhà cung cấp dịch vụ biên**

## **6. Mạng LAN ảo (Virtual LAN - VLAN)**

• Vấn đề về băng thông: trong một số trường hợp một mạng Campus ở

lớp 2 có thể mở rộng thêm một số building nữa, hay số user tăng lên thì nhu cầu sử dụng băng thông cũng tăng, do đó băng thông cũng như khả năng thực thi của

mạng sẽ giảm.

• Vấn đề về bảo mật: bởi vì user nào cũng có thể thấy các user khác

trong cùng một flat network, do đó rất khó để bảo mật.

• Vấn đề về cân bằng tải: trong flat network ta không thể thực hiện

truyền trên nhiều đường đi, vì lúc đó mạng rất dễ bị lặp, tạo nên “broadcast

storm” ảnh hưởng đến băng thông của đường truyền. Do đó không thể chia tải (còn gọi là cân bằng tải).

## **6.1. Các kiểu thành viên của VLAN (VLAN Membership)**

- Khi VLAN được cung cấp ở switch lớp Access, thì các đầu cuối người dùng phải có một vài phương pháp để lấy các thành viên đến nó. Có 2 kiểu tồn tại trên Cisco Catalyst Switch đó là:

• Static VLAN.

• Dynamic VLAN.

### **Static VLAN**

- Kiểu thành viên Static VLAN thường được quản lý trong phần cứng với mạch tích hợp ứng dụng đặc biệt ASIC (Application Specific Intergrated Circuit) trong switch. Kiểu này cung cấp khả năng hoạt động tốt vì tất cả việc ánh xạ các port được làm ở mức phần cứng vì vậy không cần có bảng truy tìm phức tạp.

### **Dynamic VLAN**

- Dynamic VLAN cung cấp thành viên dựa trên địa chỉ MAC của thiết bị người dùng đầu cuối. Khi một thiết bị kết nối đến một port của switch, switch phải truy vấn đến cơ sở dữ liệu để thiết lập thành viên VLAN. Người quản trị mạng phải gán địa chỉ MAC của user vào một VLAN trong cơ sở dữ liệu của VMPS (VLAN Membership Policy Server). Hình 1.12 biểu diễn Dynamic VLAN với bảng địa chỉ MAC

## **6.2. Triển khai VLAN**

- Để thực thi VLAN, ta phải xem xét số thành viên của VLAN, thông thường số VLAN sẽ phụ thuộc vào kiểu lưu lượng, kiểu ứng dụng, phân đoạn các nhóm làm viện phổ biến và các yêu cầu quản trị mạng.

• **End-to-end VLAN**

Do tính chất của công việc, một nhóm các thành viên trong cùng một dự án nhưng có vị trí địa lý khác nhau, hoặc thành viên thường xuyên thay đổi vị trí địa lý nhưng yêu cầu vẫn giữ nguyên VLAN. Khi đó VLAN triển khai sẽ là End-to-end VLAN, tất cả các thành viên trong một VLAN nên có cùng kiểu truyền dữ liệu 80/20 (80% băng thông cho VLAN hiện thời/ 20% băng thông cho các truy cập từ xa).

• **Local VLAN**

Trong một số mô hình mạng, các thành viên trong cùng một nhóm hay phòng ban có chung vị trí địa lý, họ không có nhu cầu di chuyển do mục đích tập trung tài nguyên. Khi đó người ta sử dụng Local VLAN, trong mô hình này, tất cả các thành viên trong một VLAN nên có cùng kiểu truyền dữ liệu 20/80 (20% băng thông cho VLAN hiện thời/80% băng thông cho các truy cập từ xa).

# **CHƯƠNG 3: HIỆN THỰC HÓA NGHIÊN CỨU**

## **1. Giới thiệu mạng Backup**

Sao lưu (backup) là quá trình tạo bản copy dữ liệu hoặc hệ thống mà bạn cần sử dụng để khôi phục dữ liệu trong trường hợp dữ liệu gốc bị mất hoặc hỏng. Các Doanh nghiệp (DN) cũng có thể sử dụng bản backup để khôi phục các bản sao của các tệp cũ hơn trong trường hợp dữ liệu bị thất thoát hoặc mất.

## **2. Tầm quan trọng của backup dữ liệu**

- Trong thời đại CNTT 4.0 ngày nay, dữ liệu là vô cùng quan trọng đối với các doanh nghiệp nhỏ và lớn. Dữ liệu bao gồm : thông tin khách hàng, hợp đồng , các thiết kế - bản vẽ hoặc các dữ liệu liên quan đến hệ thống như Mail Server , Database , CRM , ERP.. vv

- Khi doanh nghiệp bị thất thoát hoặc mất dữ liệu có thể dẫn đến thiệt hại vô cùng lớn về mặt tiền bạc cũng như tổn hại đến uy tín của Công Ty. Theo số liệu thống kê 40% doanh nghiệp không thể phục hồi sau khi mất dữ liệu.

- Đa phần các công ty cần có nhân viên IT để quản lý toàn bộ chiến lược backup, bao gồm các giải pháp và công cụ backup; phạm vi dự phòng; lịch trình và cơ sở hạ tầng; mạng và lưu trữ; thời gian phục hồi (RTO), thời điểm phục hồi (RPO),…

## **2.1. Các dữ liệu cần backup**

- Nhiệm vụ đầu tiên của backup là phải hiểu, xác định dữ liệu nào cần backup và quản lý, bảo vệ dữ liệu. Để giảm nguy cơ mất dữ liệu, bạn không chỉ backup các file và dữ liệu, mà bạn còn phải backup toàn bộ hệ thống, các ứng dụng, các cấu hình.

- Trong trường hợp Doanh nghiệp sử dụng hệ thống ảo hóa, không chỉ backup các VMs mà còn bao gồm backup cả host và setting management.

- Đối với các DN sử dụng Cloud Server cũng cần đưa hệ thống này vào danh sách đối tượng cần được tiến backup. Cuối cùng, đừng quên backup dữ liệu trên các thiết bị di động, máy tính bảng…của các thành viên quan trọng của DN. Ví dụ như các CEO thường lưu trữ dữ liệu quan trọng lên tablet cá nhân và các dữ liệu này vô cùng quan trọng.

- Mỗi doanh nghiệp khi chọn một giải pháp backup, hãy chắc chắn rằng nó có thể bảo vệ được tất cả hệ thống và dữ liệu của doanh nghiệp.

## **2.2. RPO và RTO - Yếu tố chính đo lường khi lên kế hoạch Backup dữ liệu**

- Khi đã quyết định được phạm vi backup của mình, thì quyết định quan trọng tiếp theo là tần suất cần backup và xác định lịch để backup dữ liệu. Có 2 yếu tố chính để quyết định việc này là RTO và RPO.

- RPO - Thời điểm phục hồi. Thời điểm ở đây là thời điểm cụ thể, ví dụ như 1 giờ trước, 1 ngày trước hoặc 1 tuần trước. Đại khái là 1 thời điểm đã xảy ra và Doanh nghiệp muốn dữ liệu được phục hồi vào đúng thời điểm mà họ mong muốn.

- RPO càng nhỏ có nghĩa là mất ít dữ liệu hơn, những nó đòi hỏi nhiều bản backup hơn, dung lượng lưu trữ lớn hơn, nhiều tài nguyên mạng và máy tính hơn để thực hiện việc backup.

- Nhiều công ty vừa và nhỏ thường xác định RPO được tính theo giờ. Ví dụ RPO là 24 giờ, điều đó có nghĩa là doanh nghiệp cần phải thực hiện backup hàng ngày. Chúng ta cũng có thể phân chia RPO tùy theo đánh giá rủi ro của doanh nghiệp – RPO ngắn hơn cho các hệ thống quan trọng và RPO dài hơn cho các hệ thống thứ cấp.

- Việc tính toán RPO cần dựa trên tiêu chí là lượng dữ liệu thất thoát có thể quy ra bao nhiêu tiền, và đầu tư vào giải pháp backup có mang lại giá trị

tương xứng hay không.

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

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

- Một biến quan trọng khác là Recovery Time Objective (RTO) - Thời gian phục hồi - Ví dụ như phòng nhân sự mất file tính lương và họ yêu cầu DN trong vòng 1 tiếng phải phục hồi cho họ ngay, như vậy RTO = 1 giờ. RTO càng nhỏ thì chi phí càng cao.

- Khi hệ thống ngừng hoạt động, công ty của bạn sẽ bị tổn thất và cần phục hồi nhanh để giảm thiểu tổn thất đó. Tuy nhiên, như với RPO, RTO ngắn hơn đòi hỏi hệ thống mạng, hạ tầng và công nghệ để lưu trữ nhanh hơn – vì vậy nó đắt hơn. Đối với 1 số doanh nghiệp đòi hỏi RTO = 0, điển hình là các ngân hàng, các công ty cung cấp service IT cho khách hàng với cam kết on time 24/24 kể cả động đất sóng thần. Với các doanh nghiệp loại này, thay vì họ chỉ tốn 1 triệu $ đầu tư cho hệ thống production chạy thì giờ họ sẽ tốn thêm 2, 3 triệu $ thậm chí nhiều hơn để đầu tư những site tương tự ở vị trí khác nhau và hệ thống backup chạy real time cùng production vận hành liên tục..

Các dạng backup dữ liệu

Tùy vào mức độ lưu trữ và thao tác lưu trữ, backup được chia thành 3

dạng:

**Full Backup**

Full backup là sao lưu toàn bộ dữ liệu đang có.

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

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

Ưu điểm của full backup:

- Lưu trữ toàn bộ dữ liệu của ngày thực hiện backup

- Tính an toàn cao cho dữ liệu

Nhược điểm của full backup:

- Thời gian backup lâu hơn

- Tốn dung lượng dự trữ

- Chi phí đầu tư thiết bị lưu trữ lớn

**Differential Backup là gì?**

Differential backup cho phép sao lưu những phần dữ liệu thay đổi so với lần full backup gần nhất.

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

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

Ưu điểm của differential backup

- Thời gian sao lưu nhanh hơn full backup

- Tiết kiệm dung lượng lưu trữ hơn so với full backup

- Tốc độ phục hồi dữ liệu nhanh hơn so với Incremental backup

Nhược điểm của differential backup

- Khi khôi phục dữ liệu cần hai bản backup: 1 từ file full backup gần nhất và 1 từ file differential backup ở thời điểm cần khôi phục

**Incremental Backup là gì?**

Với Incremental backup, hệ thống thực hiện sao lưu những dữ liệu mới so với lần incremental backup gần nhất.

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

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

Ưu điểm của Incremental backup

- So với hai dạng trên thì incremental backup có thời gian thực hiện nhanh

nhất

Cần dung lượng backup ít nhất

Nhược điểm của Incremental backup

- Khi muốn khôi phục dữ liệu, bạn cần phải có: 1 file full backup gần

nhất, tất cả các file incremental backup kể từ thời điểm full backup cần khôi

phục

- Thời gian thực hiện lâu nhất

Có thể hiểu như sau, nếu cần backup dữ liệu của ngày thứ 4 thì bạn phải

có file full backup của ngày chủ nhật và 3 file incremental backup của ngày thứ

2, thứ 3, thứ 4 kế tiếp.

Các nhà quản trị mạng cũng lưu ý cần thực hiện backup theo lộ trình như sau:

- Full backup hàng tháng

- Differential backup hàng tuần

- Incremental backup hàng ngày

## **3. Giải pháp backup dữ liệu**

Nếu chúng ta thu hẹp các phương tiện lưu trữ dữ liệu hiện nay, thì có hai loại cơ bản. Đầu tiên là lưu trữ dữ liệu cục bộ - LOCAL BACKUP và thứ hai là lưu trữ dữ liệu trực tuyến - ONLINE BACKUP thông qua các nhà cung cấp dịch vụ đám mây. Các doanh nghiệp có thể lựa chọn giải pháp giúp đảm bảo backup và phục hồi dữ liệu an toàn và hiệu quả nhất.

## **3.1. Local Backup**

Local Backup là khi bạn sử dụng các bộ nhớ cục bộ, chẳng hạn như ổ cứng, đĩa, flash drive, type hoặc ổ cứng ngoài để lưu trữ các file trên máy tính.

Local Backup là phương pháp lưu trữ dữ liệu sử dụng các thiết bị lưu trữ

cục bộ. Một số thiết bị thường được sử dụng : USB, Ổ cứng ngoài, Băng từ

( Tape ) cho đến các thiết bị chuyên dụng như NAS , SAN.

## **3.1.1. Ưu điểm của Local Backup**

➣ Tốc độ

Việc Backup và khôi phục thực hiện qua hệ thống mạng LAN do dữ liệu được lưu trữ cục bộ tại công ty nên tốc độ có phần nhỉnh hơn so với Cloud

Backup.

➣ Bảo mật

Dữ liệu được đặt tại công ty nên tương đối an toàn về bảo mật. Tuy nhiên việc bảo mật trong phương pháp này phụ thuộc khá nhiều vào quy trình thiết lập và trình độ kỹ thuật của công ty trong việc lưu trữ và bảo vệ dữ liệu.

## **3.1.2. Nhược điểm của Local Backup**

✔ Khả năng mở rộng

Một vấn đề phức tạp của giải pháp Local Backup về việc mở rộng dung lượng lưu trữ cho dữ liệu Backup. Ví dụ: doanh nghiệp lưu trữ dữ liệu trong ổ cứng với dung lượng 5TB. Sau này, nếu kích thước tổng thể của dữ liệu vượt quá giới hạn này, thì người dùng sẽ không có lựa chọn nào khác ngoài việc mua thêm một ổ cứng khác hoặc xóa đi các dữ liệu cũ.

Trong trường hợp doanh nghiệp sử dụng các thiết bị chuyên dụng như NAS / SAN, việc mở rộng trên các thiết bị này tùy thuộc vào độ tương thích của

thiết bị.

✔ Chi phí

Chi phí xây dựng cho một giải pháp backup đáp ứng các chỉ tiêu về nhu cầu và bảo mật cũng như phần mềm backup rất tốn kém bao gồm việc đầu tư hạ tầng mạng cho đến các thiết bị lưu trữ. Bên cạnh đó, hệ thống lưu trữ cần được kiểm tra và bảo trì định kỳ. Các tài nguyên khác xung quanh yêu cầu đáp ứng tiêu chí HVAC để đảm bảo an toàn phần cứng cũng rất tốn kém.

✔ Khả năng phục hồi sau thảm họa

Việc đặt dữ liệu tại công ty cũng dẫn đến rủi ro về mặt an toàn. Nếu

doanh nghiệp xảy ra các sự cố chập điện cháy nổ ảnh hưởng đến thiết bị lưu trữ thì các dữ liệu sẽ không có khả năng phục hồi.

## **3.2. Online Backup (sao lưu trực tuyến)**

Giải pháp Online Backup (Còn được hiểu theo nhiều cách gọi như Remote backup, Cloud Backup hoặc BaaS). Hoạt động trên mô hình đơn vị cung cấp giải pháp cho doanh nghiệp theo dạng dịch vụ - bao gồm phần mềm Backup (có thể hiểu theo SaaS) và nơi lưu trữ (Cloud Storage) . Hiện nay mô hình dịch vụ backup dữ liệu này đang rất phát triển vì những tiện ích và chi phí hợp lý mà nó đem lại vì doanh nghiệp không cần phải đầu tư hạ tầng cho các tác vụ backup.

## 3.2.1. Ưu điểm của Online Backup

➠ Tiện lợi

Giải pháp Online Backup không yêu cầu doanh nghiệp phải triển khai hạ

tầng backup phức tạp. Tất cả các thao tác thực hiện được thông qua 1 giao diện web duy nhất giúp việc thiết lập các kế hoạch backup trở nên dễ dàng hơn bao giờ hết. Người dùng không còn cần phải thực hiện việc lên lịch thay tape hay lên lịch chạy backup mỗi ngày với cơ chế tự động backup mà giải pháp này đem lại.

➠ An toàn

Vì dữ liệu của doanh nghiệp được lưu trữ trên cloud, chính vì thế bạn

không cần phải lo lắng về các mối đe dọa như hỏa hoạn, lũ lụt hoặc trộm cắp.

Thực tế, đối với các đơn vị cung cấp dịch vụ uy tín, các dữ liệu được đặt tại nơi

đặc biệt như trung tâm dữ liệu đáp ứng tiêu chuẩn quốc tế.

Một số giải pháp online backup với công nghệ hiện đại thực hiện mã hóa

dữ liệu các backup item theo các tiêu chuẩn mã hóa cao cấp như AES-256 hạn

chế được rủi ro truy cập trái phép vào dữ liệu.

➠ Phục hồi dữ liệu nhanh chóng

Nếu dữ liệu bị mất hoặc bị xóa, điều này có thể xảy ra thông qua lỗi người

dùng; tuy nhiên các bản sao lưu luôn có sẵn và dễ dàng tìm thấy. Online Backup có nhiều cấp độ dự phòng giúp doanh nghiệp lưu trữ nhiều bản sao dữ liệu ở các vị trí độc lập với nhau. Chính vì thế, doanh nghiệp lưu trữ nhiều cấp độ thì càng tốt, mỗi cấp sẽ đảm bảo dữ liệu của doanh nghiệp được bảo vệ tốt hơn và cho phép người sử dụng truy cập phiên bản sao lưu khi dữ liệu biến mất.

➠ Dễ dàng tiếp cận

Truy cập từ xa cũng là một lợi ích đơn giản và khả thi để thực hiện Online

Backup.

➠ Chi phí hợp lý

Khi sử dụng dịch vụ này, các chi phí được chuyển đổi từ Capex sang

Opex. Đối với một vài đơn vị cung cấp dịch vụ, có thể hiểu theo hình thức Pay

As You Go.

Với hình thức dịch vụ này, doanh nghiệp sẽ tận dụng được tối đa chi phí

đầu tư cho việc backup dữ liệu / hệ thống mà không cần lo lắng tài nguyên sử

dụng đã tố ưu hay chưa.

## **3.2.2. Nhược điểm của Online Backup**

Tuy nhiên giải pháp Online Backup vẫn có những khó khăn vì dữ liệu

được sao lưu trực tuyến, dẫn đến tốc độ kết nối internet rất quan trọng. Trong

quá trình backup, nếu kích thước của dữ liệu được tải lên lớn, thì có thể mất

nhiều thời gian hơn để backup toàn bộ dữ liệu lên cloud storage.

Tuy vậy, điều này có thể dễ dàng khắc phục bằng cách tạo lập tự động các

kế hoạch backup vận hành vào thời điểm công ty ít hoạt động ( giữa trưa hoặc

vào ban đêm tùy theo DN )

## **4. Hệ thống lưu trữ**

Dữ liệu backup được đặt tại hệ thống lưu trữ dữ liệu. Vì vậy các DN phải

lựa chọn giải pháp, đảm bảo kết nối và dễ điều khiển trong việc backup và phục hồi dữ liệu.

## **4.1. Backup dữ liệu vào USB - External HardDrive**

Cách backup này rất nhanh, tiện lợi và không cần mạng.

Nhưng nhược điểm của thiết bị này là chúng dễ dàng bị hư hỏng bởi nhiều

yếu tố như mất trộm, vô nước hay cháy nổ, các bản backup của DN cũng bị mất

theo nếu chỉ được lưu ở đây.

Ảnh có chứa máy tính, máy tính xách tay, Thiết bị đầu ra, Thiết bị điện

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

## **4.2. Backup dữ liệu bằng thiết bị chuyên dụng - NAS - SAN**

Đây là một trong những lựa chọn lưu trữ phổ biến nhất, tuy nhiên chi phí đầu tư cho thiết bị này cũng khá lớn đặc biệt là SAN. Với NAS (Network Attached Storage), SAN (Storage Area Network) , DN có thể lưu trữ nhiều hoặc tất cả các bản backup của công ty tại thiết bị này và khôi phục dữ liệu hoặc hệ thống trong trường hợp mất dữ liệu hoặc hệ thống bị tấn công.

Tuy nhiên, giải pháp này không đáp ứng được nhu cầu Disaster Recovery trong trường hợp Doanh nghiệp xảy ra cháy nổ hoặc thảm họa tự nhiên.

## 4.3. Backup dữ liệu vào Tapes ( băng từ )

Giải pháp này thường được sử dụng để giải quyết cho các doanh nghiệp trong trường hợp thảm hóa tự nhiên xảy ra, dữ liệu cần được lưu trữ một bản copy ở vị trí thật xa, ít nhất là cách 100 dặm tính từ vị trí doanh nghiệp của bạn. Một trong những cách truyền thống để làm điều đó là lưu trữ các bản sao dữ liệu của DN trên các thiết bị tape và vận chuyển tape từ đến một địa điểm ở xa. Các công nghệ tape hiện đại, như LTO-7, cho phép bạn lưu trữ tới 2,5TB dữ liệu nén trên một tape duy nhất, chúng khá hiệu quả nếu bạn cần bảo vệ một lượng lớn dữ liệu.

# **CHƯƠNG 4: CÁC PHƯƠNG PHÁP BẢO MẬT HỆ THỐNG**

- Thiết kế, quy hoạch một hệ thống mạng lớn không đơn thuần là phát triển thêm các thiết bị hỗ trợ người dùng mà phải dựa trên mô hình chuẩn đã và đang áp dụng cho các hệ thống mạng tiên tiến tại các cơ quan, doanh nghiệp phát triển trên thế giới, đó chính là mô hình mạng Định hướng Kiến trúc Dịch vụ (Service-Oriented Architecture – SOA).

## **1. Thiết kế cơ sở hạ tầng theo mô hình SOA**

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

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

Kiến trúc SOA gồm có 3 lớp:

**Lớp cơ sở hạ tầng mạng** (networked infrasstructure layer): là lớp mạng liên kết các khối chức năng theo kiến trúc phân tầng, có trật tự.

**Lớp dịch vụ tương tác** (Interactive services layer): bao gồm sự kết hợp một số kiến trúc mạng đầy đủ với nhau tạo thành các chức năng cho phép nhiều ứng dụng có thể sử dụng trên mạng.

**Lớp ứng dụng** (Application layer): Bao gồm các loại ứng dụng cộng tác và nghiệp vụ. Các ứng dụng này kết hợp với các dịch vụ tương tác cung cấp ở lớp dưới sẽ giúp triển khai nhanh và hiệu quả

Trong phần này, tôi xin giới thiệu sơ lược về các phương thức thiết kế mạng và bảo mật được sử dụng trong việc thiết kế các hệ thống mạng lớn và hiện đại của các tổ chức và doanh nghiệp lớn. Tương ứng với kiến trúc SOA là thuộc lớp Cơ sở hạ tầng mạng.

## **2. Phương thức thiết kế phân lớp – Hierarchical**

Hierarchical là Một mạng là gồm nhiều mạng LAN trong một hoặc nhiều toà nhà, tất cả các kết nối thường nằm trong một khu vực địa lý. Thông thường các Campus gồm có Ethernet, Wireless LAN, Gigabit Ethernet, FDDI (Fiber Distributed Data Interface). Được thiết kế theo các tầng, khu vực khác nhau; trên mỗi tầng, mỗi khu vực được triển khai các thiết bị, các chính sách mạng tương ứng.

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

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

Sơ đồ thiết kế hệ thống mạng SOA theo các khu vực, tầng

### **2.1. Khu vực LAN**

Từ mô hình trên ta cũng thấy được rằng khu vực này được thiết kế theo tầng. Tầng lõi, tầng phân tán, tầng truy xuất vừa đảm bảo tính dự phòng đường truyền, lưu lượng mạng được phân bố đều, toàn mạng được chia thành nhiều phân đoạn để dễ dàng kiểm soát và bảo mật.

### **2.2. Khu vực kết nối WAN**

Đây là vùng cung cấp các kết nối ra môi trường Internet và các cơ quan thành viên, đối tác. Tại đây phải đảm bảo tính sẵn sàng cao và tính dự phòng đường truyền. Vì vậy hệ thống cân bằng tải và dự phòng đường truyền WAN cần được triển khai.

### **2.3. Khu vực các máy chủ public**

Khu vực này thường được biết đến với tên là vùng phi quân sự (DMZ- demilitarized zone) có nghĩa rằng tại khu vực này được hệ thống tường lửa kiểm soát vào ra các máy chủ rất chặt chẽ nhằm ngăn chặn các cuộc tấn công của Hacker, người dùng trong LAN…

+ Ưu điểm: dự phòng, dễ phát triển, hiệu năng cao, dễ khắc phục sự cố, thích hợp với môi trường đào tạo và nghiên cứu ở các trường đại học và cao đẳng, doanh nghiệp lớn.

+ Khó khăn khi xây dựng mạng theo phân lớp là chi phí khá cao, cần đội ngũ quản trị hệ thống chuyên nghiệp

## **3. Mô hình triển khai dịch vụ và quản lý người dùng**

Mô hình này được triển khai trên cơ sở hạ tầng đã thiết kế là yếu tố quyết định đến hiệu năng hoạt động và cách thức quản lý hệ thống. Thực tế một số cơ quan, doanh nghiệp hiện nay đang triển khai hệ thống mạng theo mô hình mạng ngang hàng. Mô hình này chỉ triển khai cho các tổ chức có quy mô nhỏ hẹp. Khi quy mô hệ thống có trên hàng trăm máy tính, nhiều phòng ban, chức năng thì việc quản lý theo mô hình ngang hàng không còn phù hợp nữa. Giải pháp triển khai dịch vụ và quản lý người dùng theo mô hình chủ-khách là giải pháp tối ưu, hiệu quả nhất. Hệ thống này có nhiều thuận

lợi và tính năng tối ưu như:

– Phần quyền truy nhập vào các tài nguyên dùng chung trên mạng.

– Triển khai cấu hình các phần mềm, dịch vụ tự động cho các máy khách, người dùng nhanh chóng.

– Triển khai một chính sách bảo mật cho toàn đơn vị một cách dễ dàng, thống nhất, tập trung, ví dụ: Khi người dùng không sử dụng trong thời gian nhất định, hệ thống sẽ tự lock, luôn yêu cầu người dùng đặt mật khẩu cho hệ điều hành ở chế độ phức tạp, thường xuyên thay đổi mật khẩu…nhằm tránh các hacker dùng các phần mềm giải mã mật khẩu.

– Dễ dàng giám sát an ninh, bảo mật, logging v.v

## 4. Phân hoạch VLAN (LAN ảo)

Thực trạng hệ thống mạng ở một số doanh nghiệp hiện nay được phân chia thành các khu vực, chưa kiểm soát được lưu lượng download và upload cũng như băng thông truy xuất Internet của người dùng. Mô hình mạng như vậy là một miền quảng bá, mỗi gói tin kiểu quảng bá thì ở bất kỳ máy nào cũng có thể tới được tất cả các máy tính khác trong mạng nên có những vấn đề sau:

– Về băng thông: Toàn doanh nghiệp là một vùng quảng bá rất lớn, số máy tính, số người dùng sẽ tăng lên khi đơn vị phát triển thêm các khu vực khác. Do vậy băng thông, hiệu năng của toàn mạng sẽ giảm, thậm chí thường gây tắc nghẽn.

– Về bảo mật: Việc kiểm soát bảo mật gặp rất nhiều khó khăn khi hệ thống trải rộng khắp toàn cơ quan, doanh nghiệp. Để giải quyết các vấn đề trên, chúng ta đưa ra giải pháp chia mạng thành nhiều mạng LAN ảo. VLAN được định nghĩa là một nhóm logic các thiết bị mạng, và được thiết lập dựa trên các yếu tố chức năng, bộ phận, ứng dụng của tổ chức. Việc chia VLAN thành các phân hệ khác nhau giúp khả năng bảo mật, quản lý và hiệu năng đạt kết quả cao nhất.

Ảnh có chứa biểu đồ, hàng, ảnh chụp màn hình, Phông chữ

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

Minh họa về nhiều VLAN khác nhau ở một trường học

Ví dụ: Tất cả các máy tính thuộc các phòng thực hành, thí nghiệm trong toàn trường thì thuộc vlan01; các phòng ban thuộc vlan02, các wireless thuộc vlan03 v.v. Các VLAN đó mặc định sẽ không liên lạc được với nhau. Khi muốn có sự liên lạc giữa các VLAN với nhau ta tiến hành cấu hình trên thiết bị định tuyến router và kiểm soát băng thông giữa các Vlan. (hình 2)

## **5. Nhóm giải pháp về hệ thống ngăn chặn, phát hiện tấn công**

### **5.1. Hệ thống tường lửa đa tầng**

Hệ thống tường lửa là hệ thống kiểm soát truy nhập giữa mạng Internet và mạng nội bộ. Tường lửa có 2 loại: phần cứng và phần mềm. Mỗi loại có các ưu điểm khác nhau. Phần cứng có hiệu năng ổn định, không phụ thuộc vào hệ điều hành, virus, mã độc, ngăn chặn tốt giao thức ở tầng mạng trong mô hình tham chiếu TCP/IP. Phần mềm rất linh hoạt trong những cấu hình ở giao thức tầng ứng dụng trong mô hình TCP/IP.

Ví dụ, tường lửa tầng thứ nhất (thường là phần cứng) đã loại bỏ hầu hết các kiểu tấn công trực diện vào hệ thống máy chủ web, máy chủ mail như kiểu tấn công phân tán (DDOS), tức hacker dùng các công cụ tạo các yêu cầu truy xuất tới máy chủ từ nhiều máy tính khác trên mạng với tần suất cao để nhằm làm cho máy chủ quá tải và dẫn tới ngừng phục vụ.

Nhưng hacker cũng không dừng tại đó, chúng có thể vượt qua hệ thống tường lửa tầng thứ nhất với những gói tin hợp lệ để vào hệ thống mạng LAN. Bằng các giao thức tầng ứng dụng chúng có thể lại đạt được mục đích. Chính vì thế triển khai hệ thống tường lửa phần mềm sẽ hỗ trợ và làm gia tăng tính bảo mật cho toàn mạng. Trong trường hợp, một hệ thống tường lửa gặp sự cố thì hệ thống còn lại vẫn kiểm soát được. Sau đây là giải pháp thiết kế hệ thống tường lửa thường đa tầng, nó bao

gồm ít nhất 2 tầng chính sau: tường lửa trước và tường lửa sau.

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

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

Hệ thống tường lửa với 2 tầng trước và sau

### **5.2. Hệ thống phát hiện và chống xâm nhập IDS/IPS**

Hiện nay các hình thức tấn công của người có ý đồ xấu ngày càng nhiềuvà tinh vi. Ví dụ: Trong đơn vị có thể tự cài đặt các công cụ (Ethereal, Cain & abel…) trên máy tính làm việc hoặc máy tính xách tay để tiến hành nghe lén hay quét trực tiếp lên các máy chủ, từ đó có thể lấy các tài khoản email, Web, FTP, SQL server nhằm thay đổi điểm thi, tiền học phí đã nộp, thay đổi lịch công tác… các hình thức tấn công kiểu này, hệ thống tường lửa không thể phát hiện.

Giải pháp hữu hiệu cho thực trạng này là xây dựng hệ thống IDS/IPS (Intrusion Detection System/Intrusion Prevention System). IDS/IPS là hệ thống bảo mật vô cùng quan trọng, nó có khả năng phát hiện ra các cuộc tấn công dựa vào các dấu hiệu thiết lập sẵn hoặc các đoạn mã độc hại, bất thường trên giao thông mạng; đồng thời có thể loại bỏ chúng trước khi có thể gây hại cho hệ thống.

## **5.3. Danh sách điều khiển truy xuất, an toàn cổng thiết bị, lọc địa chỉ mạng**

### **5.3.1.Danh sách điều khiển truy xuất**

Tình trạng các phòng ban, …đang tự triển khai mạng wireless và mở rộng mạng LAN, nhất là tại các phòng có nhiều thiết bị di động, laptop dẫn tới số kết nối vào mạng nội bộ tăng, băng thông toàn mạng giảm và khó kiểm soát bảo mật.  
Danh sách truy nhập là gồm các luật cho phép hay ngăn chặn các gói tin sau khi tham chiếu vào thông tin trong tiêu đề của gói tin để giới hạn các người dùng có thể truy xuất vào các hệ thống máy chủ nội bộ v.v.

### **5.3.2. Bảo mật cổng của thiết bị, lọc địa chỉ vật lý của thiết bị mạng** Ở các điểm truy nhập mạng công cộng, việc mở rộng LAN của người dùng; việc truy xuất vào các máy chủ nội bộ cần được kiểm soát. Các giải pháp như cấu hình bảo mật cổng của thiết bị, quản lý địa chỉ vật lý là giải pháp cực kỳ an ninh và hiệu quả trong trường hợp này. – Cấu hình bảo mật cổng của thiết bị trên các switch nhằm đảm bảo không thể mở rộng LAN khi chưa có sự đồng ý của người quản trị hệ thống, nếu vi phạm điều đó, port trên switch đó sẽ chuyển về trạng thái cấm hoặc trạng thái ngừng hoạt động. – Địa chỉ vật lý là địa chỉ được cài đặt sẵn từ nhà sản xuất. Về nguyên tắc tất cả các máy tính trên mạng sẽ không trùng nhau về địa chỉ này. Sự kiểm soát theo địa chỉ này là rất cụ thể tới từng máy tính trong mạng, trừ khi người dùng có quyền cài đặt phần mềm và làm giả địa chỉ này ở máy tính đó, hoặc là mở máy tính rồi thay thế card giao tiếp mạng mới. – Các thiết bị mạng hiện nay đều được trang bị chức năng ngăn theo địa chỉ vật lý này giúp quản trị mạng kiểm soát được người dùng sử dụng mạng, nhất là muốn triển khai trên hệ thống wireless.

## **6. Nhóm giải pháp khác**

### **6.1 Xây dựng hệ thống cập nhật, sửa lỗi tập trung**

Công đoạn đầu tiên của hacker khi tiến hành tấn công là khảo sát hệ thống đích để tìm ra các lỗi của hệ điều hành, của các dịch vụ, của các ứng dụng khi... chúng chưa được cập nhật trên website của nhà cung cấp.

Thực trạng ở các cơ quan, doanh nghiệp cho thấy việc sử dụng các sản phẩm phần mềm hầu như ít cập nhật các bản vá lỗi, có chăng cũng đang riêng lẻ trên các máy tính cá nhân, đó chính là cơ hội cho hacker dùng các công để khai thác lỗ hổng bảo mật. Để cập nhật bản vá lỗi cho tất cả các máy khách trong toàn bộ hệ thống qua Internet mất thời gian và tốn nhiều băng thông đường truyền và không thống nhất.

Giải pháp xây dựng hệ thống tự động cập nhật từ nhà cung cấp trên Internet về máy chủ rồi từ máy chủ này, triển khai cho tất cả các máy khách trong toàn mạng.

Hệ thống WSUS (Windows Server Update Services) của Microsoft không những cập nhập bản vá lỗi cho hệ điều hành Windows mà còn cập nhật bản vá lỗi cho tất cả các sản phẩm khác của hãng bao gồm Internet Explorer, SQL server, Office, Mail, máy chủ Web v.v

## **6.2. Ghi nhật ký, theo dõi, giám sát hệ thống**

### **6.2.1. Ghi nhật ký**

Giải pháp ghi lại các phiên kết nối, các phiên đăng nhập của người dùng, các tiến trình hoạt động sẽ giúp quản trị mạng có thể tìm lại dấu vết của người dùng, hacker và các lỗi có thể gây ra cho hệ thống trước đó. Các máy chủ Web , máy chủ Email và máy chủ ứng dụng khác cần được kích hoạt tính năng ghi nhật ký, việc quản lý lưu trữ các thông tin này là rất cần thiết. Hacker chuyên nghiệp khi đã xâm nhập thành công vào hệ thống, việc không thể bỏ qua chính là việc xóa dấu vết đã được ghi. Chính vì thế triển khai hệ thống ghi nhật ký tập trung tại một máy chủ chuyên dụng khác là rất hiệu quả. Các phần mềm mã nguồn mở như: Syslog-ng: (<http://www.balabit.com>); SyslogAgent: (http://syslogserver.com) là giải pháp tốt. Hệ thống sẽ giúp chúng ta ghi các cảnh báo, thông báo từ các thiết bị phần cứng như: tường lửa, router, switch, từ các máy chủ Web, Database, và các hệ thống khác.

### **6.2.2. Theo dõi, giám sát**

Theo dõi, giám sát là công việc thường xuyên và quan trọng của nhà quản trị mạng chuyên nghiệp, đó chính là công việc phòng chống hiệu quả trước khi sự cố xuất hiện. Theo dõi, giám sát có thể:

– Phát hiện trên hệ thống mạng có nhiều virus phát tán.

– Giám sát các máy tính trong mạng LAN và trên môi trường Internet.

– Theo dõi hiệu năng hoạt động các phần cứng của máy chủ để tiến hành

nâng cấp, bảo trì, bảo dưỡng.

– Phát hiện hacker đang dùng các công cụ nghe lén mật khẩu, quét các lỗi

của hệ thống và các ứng dụng.

– Thống kê số lượng các kết nối, các session cũng như những lưu lượng

bất thường trên hệ thống mạng v.v

### **6.3. Giải pháp mã hóa dữ liệu và đường truyền**

Dữ liệu trên máy chủ, máy tính cá nhân của các cơ quan, doanh nghiệp hiện chưa an toàn vì không được mã hóa nội dung và kể cả khi đi trên đường truyền. Dữ liệu ấy có thể được đọc bởi:

– Người dùng đăng nhập thành công vào máy tính

– Hacker dùng các phần mềm capture (bắt) thông tin trên đường truyền

– Tại các máy chủ và máy tính có lưu trữ dữ liệu nhạy cảm, có dữ liệu cần

chia sẽ; tại các thiết bị lưu trữ cần thiết phải tiến hành mã hóa nội dung, điều đó đảm bảo rằng nếu có mất thiết bị lưu trữ, máy tính, người tấn công cũng không thể giải mã được dữ liệu.

Giải pháp Ipsec sẽ được triển khai tại các hệ thống máy chủ và máy người dùng cũng như các thiết bị mạng phải được cấu hình.

### **6.4. Đào tạo người dùng**

Theo các thống kê về an ninh mạng của CERT (Computer Emergency Response Team-http://www.cert.org/) cho thấy, có khoảng 70% số trường hợp bị thất thoát thông tin có liên quan tới yếu tố con người bên trong các hệ thống còn 30% là xuất phát từ bên ngoài mạng nội bộ của các tổ chức thông qua các hành vi truy nhập trái phép hệ thống của hacker.

Theo chuẩn quản lý an ninh thông tin (Information Security Management) ISO 17799/BS-7799, trong đó có tiêu chí về “An ninh về nhân sự (Personnel Security)” mô tả trách nhiệm của nhân viên, vai trò của các cá nhân trong an ninh thông tin, nhằm giảm thiểu các sai sót do lỗi của con người, do ăn cắp hoặc lạm dụng tài sản công.

Do vậy việc đào tạo người dùng để họ tự bảo vệ các tài nguyên cho máy tính họ và cho cả tổ chức là nhiệm vụ hết sức quan trọng.

Đào tạo người dùng biết cách phòng chống các thủ đoạn của hacker như lừa đảo qua email. Ví dụ: hacker thường lợi dụng tính tò mò của người dùng khi tham gia Internet để lấy thông tin khi yêu cầu người dùng nhập vào.

Đào tạo người dùng sử dụng các công cụ, phần mềm đúng trình tự, khi cần thiết phải kịp thời báo cáo với người quản trị hệ thống.v.v.

Đào tạo người dùng phải tuân thủ nguyên tắc bảo mật và an toàn thông tin của tổ chức, kể cả khi họ không tham gia làm việc tại cơ quan.

### **6.5. Hệ thống chống virus**

Để cải thiện tốc độ xử lý của tường lửa, thông thường quản trị mạng không cấu hình kích hoạt tính năng lọc cao cấp của tường lửa (tường lửa ở các

vị trí phải xử lý lưu lượng lớn). Khi đó các chương trình quét virus được cài đặt nhằm phát hiện và ngăn chặn các đoạn mã độc, các chương trình gián điệp, các

email có tệp tin virus đính kèm.v.v. Nhưng trên thực tế để đầu tư một khối lượng lớn các chương trình virus cho tất cả các máy tính toàn cơ quan thì kinh phí đầu

tư khá cao.

Để giảm chi phí bản quyền, giải pháp là triển khai mô hình chống virus

chủ – khách. Hiện nay có nhiều hãng nỗi tiếng như Norton, Kaspersky, Trend

micro .v.v có thể triển khai theo mô hình này. Lợi ích khi triển khai hệ thống là:

– Chi phí giảm hơn nhiều so với cài đặt trên từng máy khách

– Việc cập nhật phiên bản mới của các máy khách dễ dàng, nhanh

chóng và hiệu quả cao.

# **CHƯƠNG 5. KẾT QUẢ NGHIÊN CỨU**

**KẾT QUẢ NGHIÊN CỨU**

Đồ án đã nghiên cứu và đề xuất một giải pháp thiết kế mạng không dây (WLAN) cho khuôn viên trường THPT Thăng Long Hà Nội, nhằm đáp ứng nhu cầu truy cập thông tin, hỗ trợ học tập, giảng dạy và quản lý hiệu quả. Kết quả nghiên cứu được tổng hợp như sau:

**1. Khảo sát và phân tích hiện trạng**

* **Hiện trạng hệ thống mạng hiện tại**:
  + Trường THPT Thăng Long Hà Nội đã có hệ thống mạng LAN tương đối ổn định, phục vụ tốt cho các hoạt động cơ bản của các phòng ban.
  + **Ưu điểm**: Hệ thống LAN hiện tại đáp ứng được một số nhu cầu cơ bản.
  + **Nhược điểm**: Chưa tối ưu hóa tài nguyên, chưa đáp ứng đầy đủ yêu cầu sử dụng mạng của các phòng ban, đặc biệt là nhu cầu truy cập không dây. Hệ thống chưa khai thác hết tiềm năng tài nguyên sẵn có, dẫn đến hạn chế về hiệu suất và khả năng mở rộng.
* **Yêu cầu của hệ thống mới**:
  + Thiết kế mạng WLAN theo mô hình Client-Server, đảm bảo tất cả máy tính trong hệ thống có thể giao tiếp với nhau.
  + Các phòng ban được trang bị mạng có dây và không dây (WLAN) với số lượng thiết bị cụ thể:
    - Phòng Thực hành tin: 20 máy tính nối mạng.
    - Văn phòng Công đoàn, Thư viện, Kế toán, Hiệu trưởng, Phó hiệu trưởng, Bảo vệ, Hội đồng: Mỗi phòng 1 máy tính nối mạng (Kế toán có thêm 1 máy in).
    - Giảng đường A, B, C: Mỗi giảng đường có 1 máy tính nối mạng và hỗ trợ WLAN.
  + Yêu cầu cấu hình máy tính mạnh, màn hình Samsung 20 inch.
  + Hệ thống cần ổn định, dễ mở rộng, tiết kiệm chi phí và tận dụng tối đa tài nguyên sẵn có.

**2. Thiết kế hệ thống mạng**

* **Sơ đồ khảo sát và thiết kế**:
  + Sơ đồ vật lý và logic được xây dựng, bao gồm sơ đồ tổng quan, sơ đồ khu nhà Hiệu bộ và các giảng đường A, B, C.
  + Sơ đồ đi dây LAN và WLAN được thiết kế chi tiết, đảm bảo kết nối hiệu quả giữa các khu vực.
* **Phân bổ VLAN và địa chỉ IP**:
  + **VLAN**: Hệ thống được chia thành 12 VLAN để quản lý lưu lượng và tăng cường bảo mật:
    - VLAN 1: Không sử dụng.
    - VLAN 10–120: Gán cho các phòng ban và giảng đường (Thực hành tin, Công đoàn, Thư viện, Kế toán, Hiệu trưởng, Phó hiệu trưởng, Bảo vệ, Hội đồng, Giảng đường A, B, C).
  + **Địa chỉ IP**:
    - Mỗi VLAN được gán dải địa chỉ IP riêng, ví dụ:
      * VLAN 10 (Thực hành tin): 192.168.10.2 – 192.168.10.254 (có dây), 192.168.10.100 – 192.168.10.200 (WLAN).
      * Tương tự cho các VLAN khác, đảm bảo phân biệt rõ ràng giữa mạng có dây và không dây.
  + Phân bổ này giúp quản lý lưu lượng mạng hiệu quả, giảm tắc nghẽn và tăng cường bảo mật.
* **Hệ thống đường mạng**:
  + Tổng cộng 12 phòng/khu vực được trang bị mạng, với số nút mạng, số PC và số mét dây được tính toán chi tiết:
    - Ví dụ: Phòng Thực hành tin có 2 nút mạng, 20 PC, 120m dây, hỗ trợ WLAN.
    - Giảng đường B có 20 nút mạng, 1 PC, 100m dây, hỗ trợ WLAN.
  + Một số phòng (Kế toán, Hiệu trưởng, Phó hiệu trưởng, Bảo vệ, Hội đồng) không triển khai WLAN do nhu cầu sử dụng thấp hoặc yêu cầu bảo mật cao.

**3. Nghiên cứu lý thuyết**

* **Mô hình mạng Campus**:
  + Đồ án áp dụng mô hình mạng Campus, gồm các thành phần: Mạng Campus, WAN và kết nối từ xa.
  + Mô hình mạng Campus được thiết kế theo mô hình ba lớp của Cisco (Access, Distribution, Core), đảm bảo tính mở rộng, hiệu quả và dễ quản lý:
    - **Lớp Access**: Kết nối người dùng cuối với chi phí thấp, mật độ cổng cao, hỗ trợ VLAN và QoS.
    - **Lớp Distribution**: Kết nối giữa Access và Core, cung cấp thông lượng cao, bảo mật và QoS.
    - **Lớp Core**: Xương sống của mạng, đảm bảo thông lượng cao, dự phòng và hiệu suất tối ưu.
  + Các mô hình mạng được phân tích:
    - **Mô hình mạng chia sẻ**: Tiết kiệm chi phí, đơn giản hóa quản lý, nhưng dễ tắc nghẽn băng thông và có rủi ro bảo mật.
    - **Mô hình phân đoạn LAN/WLAN**: Sử dụng VLAN và SSID để phân đoạn mạng, tăng bảo mật, tối ưu băng thông và dễ quản lý.
    - **Mô hình lưu lượng mạng**: Phân tích các loại lưu lượng (văn bản, tệp, thoại, video) để tối ưu hóa tài nguyên và đảm bảo QoS.
    - **Mô hình dự đoán trước**: Dự đoán luồng lưu lượng để thiết kế mạng hiệu quả.
* **VLAN**:
  + Sử dụng VLAN để phân đoạn mạng, giảm miền quảng bá, tăng bảo mật và hiệu suất.
  + Hai kiểu VLAN được đề xuất:
    - **Static VLAN**: Quản lý bằng phần cứng, hiệu suất cao.
    - **Dynamic VLAN**: Dựa trên địa chỉ MAC, linh hoạt nhưng cần cơ sở dữ liệu VMPS.
  + Áp dụng VLAN End-to-end cho các nhóm phân tán địa lý và Local VLAN cho các nhóm cố định.

**4. Giải pháp sao lưu (Backup)**

* **Tầm quan trọng**:
  + Dữ liệu (thông tin khách hàng, hợp đồng, thiết kế, hệ thống Mail Server, Database, CRM, ERP) là tài sản quan trọng, mất dữ liệu có thể gây thiệt hại lớn về tài chính và uy tín.
  + 40% doanh nghiệp không thể phục hồi sau mất dữ liệu, do đó backup là yếu tố thiết yếu.
* **Dữ liệu cần backup**:
  + File, ứng dụng, cấu hình hệ thống, máy chủ ảo (VMs), host, thiết bị di động của các nhân sự quan trọng (CEO).
  + Cloud Server cũng cần được đưa vào kế hoạch backup.
* **RPO và RTO**:
  + **RPO (Recovery Point Objective)**: Thời điểm phục hồi, xác định lượng dữ liệu có thể mất. Ví dụ, RPO 24 giờ yêu cầu backup hàng ngày.
  + **RTO (Recovery Time Objective)**: Thời gian phục hồi, ví dụ, RTO 1 giờ cho các hệ thống quan trọng như phòng nhân sự.
  + RPO và RTO ngắn hơn đòi hỏi đầu tư lớn vào hạ tầng và công nghệ.
* **Các dạng backup**:
  + **Full Backup**: Sao lưu toàn bộ dữ liệu, an toàn nhưng tốn thời gian và dung lượng.
  + **Differential Backup**: Sao lưu dữ liệu thay đổi so với full backup gần nhất, tiết kiệm dung lượng, phục hồi cần cả full và differential backup.
  + **Incremental Backup**: Sao lưu dữ liệu mới so với lần backup trước, nhanh và tiết kiệm dung lượng, nhưng phục hồi phức tạp.
  + **Lộ trình đề xuất**: Full backup hàng tháng, differential hàng tuần, incremental hàng ngày.
* **Giải pháp lưu trữ**:
  + **Local Backup** (USB, ổ cứng ngoài, NAS, SAN):
    - **Ưu điểm**: Tốc độ nhanh, bảo mật tương đối cao (tùy quy trình).
    - **Nhược điểm**: Khó mở rộng, chi phí cao, rủi ro do thảm họa (cháy nổ, mất trộm).
  + **Online Backup (Cloud Backup)**:
    - **Ưu điểm**: Tiện lợi, an toàn (mã hóa AES-256, lưu trữ tại trung tâm dữ liệu chuẩn quốc tế), chi phí hợp lý (Pay As You Go), dễ phục hồi.
    - **Nhược điểm**: Phụ thuộc vào tốc độ Internet, thời gian backup lớn với dữ liệu lớn.
  + **Backup bằng Tapes**: Phù hợp cho lưu trữ dữ liệu ở vị trí xa (Disaster Recovery), ví dụ LTO-7 lưu trữ 2,5TB dữ liệu nén.

**5. Phương pháp bảo mật hệ thống**

* **Mô hình SOA (Service-Oriented Architecture)**:
  + Thiết kế mạng theo ba lớp: Cơ sở hạ tầng mạng, Dịch vụ tương tác, Ứng dụng.
  + Lớp cơ sở hạ tầng mạng sử dụng mô hình phân lớp (Hierarchical) với các khu vực:
    - **LAN**: Phân tầng (Core, Distribution, Access) để đảm bảo dự phòng, phân bố lưu lượng, bảo mật.
    - **WAN**: Kết nối Internet và đối tác, triển khai cân bằng tải và dự phòng.
    - **DMZ**: Vùng phi quân sự, kiểm soát chặt chẽ máy chủ công cộng bằng tường lửa.
* **Phân hoạch VLAN**:
  + Chia mạng thành nhiều VLAN (ví dụ, VLAN 01 cho phòng thực hành, VLAN 02 cho phòng ban, VLAN 03 cho wireless) để giảm miền quảng bá, tăng bảo mật và hiệu suất.
  + Kiểm soát băng thông và liên lạc giữa các VLAN qua router.
* **Giải pháp bảo mật**:
  + **Tường lửa đa tầng**:
    - Tường lửa phần cứng (tầng 1) ngăn chặn tấn công DDOS.
    - Tường lửa phần mềm (tầng 2) xử lý tấn công tầng ứng dụng.
  + **IDS/IPS**: Phát hiện và ngăn chặn xâm nhập dựa trên dấu hiệu hoặc mã độc.
  + **Danh sách điều khiển truy xuất (ACL)**: Giới hạn truy cập vào máy chủ nội bộ.
  + **Bảo mật cổng và lọc địa chỉ MAC**: Ngăn mở rộng LAN trái phép, kiểm soát thiết bị bằng địa chỉ vật lý.
  + **Hệ thống cập nhật tập trung (WSUS)**: Tự động cập nhật bản vá lỗi cho hệ điều hành và ứng dụng.
  + **Ghi nhật ký và giám sát**: Ghi lại phiên kết nối, phát hiện virus, giám sát hiệu năng và lưu lượng bất thường.
  + **Mã hóa dữ liệu và đường truyền (IPsec)**: Bảo vệ dữ liệu trên máy chủ, thiết bị lưu trữ và đường truyền.
  + **Đào tạo người dùng**: Nâng cao nhận thức về an ninh mạng, phòng chống lừa đảo qua email, tuân thủ quy định bảo mật.
  + **Hệ thống chống virus (mô hình chủ-khách)**: Triển khai phần mềm chống virus (Norton, Kaspersky) để giảm chi phí và tăng hiệu quả.

# **CHƯƠNG 6. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**

Đồ án "Thiết kế mạng không dây cho khuôn viên trường THPT" đã được thực hiện với mục tiêu xây dựng một hệ thống mạng không dây (WLAN) hiệu quả, ổn định và đáp ứng nhu cầu học tập, giảng dạy và quản lý tại trường THPT Thăng Long Hà Nội. Qua quá trình nghiên cứu, khảo sát và thiết kế, đồ án đã đạt được những kết quả đáng ghi nhận như sau:

1. **Phân tích và khảo sát hiện trạng**:
   * Đã đánh giá được hệ thống mạng LAN hiện tại của trường, nhận diện các ưu điểm (ổn định cơ bản) và nhược điểm (chưa tối ưu tài nguyên, thiếu mạng không dây toàn diện).
   * Xác định rõ yêu cầu của hệ thống mới, bao gồm số lượng thiết bị, cấu hình, và các khu vực cần triển khai mạng (phòng thực hành, văn phòng, giảng đường).
2. **Thiết kế hệ thống mạng**:
   * Đề xuất mô hình mạng WLAN theo chuẩn Client-Server, sử dụng mô hình mạng Campus với ba lớp (Access, Distribution, Core) của Cisco, đảm bảo tính mở rộng, hiệu suất cao và dễ quản lý.
   * Phân hoạch VLAN chi tiết (12 VLAN) và gán dải địa chỉ IP riêng cho từng khu vực, giúp quản lý lưu lượng mạng, tăng cường bảo mật và giảm tắc nghẽn.
   * Thiết kế sơ đồ vật lý, logic và đi dây (LAN/WLAN) cho các khu vực như khu nhà Hiệu bộ, giảng đường A, B, C, đảm bảo kết nối ổn định và tối ưu tài nguyên.
3. **Nghiên cứu lý thuyết**:
   * Áp dụng các mô hình mạng tiên tiến như mô hình chia sẻ, phân đoạn LAN/WLAN, lưu lượng mạng và dự đoán trước để tối ưu hóa hiệu suất.
   * Sử dụng VLAN (Static và Dynamic) để phân đoạn mạng, giảm miền quảng bá, tăng bảo mật và quản lý hiệu quả hơn.
   * Phân tích các giải pháp sao lưu (Full, Differential, Incremental) và lưu trữ (Local, Online, Tapes), nhấn mạnh tầm quan trọng của backup trong việc bảo vệ dữ liệu.
4. **Bảo mật hệ thống**:
   * Đề xuất mô hình SOA (Service-Oriented Architecture) với thiết kế phân lớp (Hierarchical), bao gồm các khu vực LAN, WAN và DMZ.
   * Triển khai các giải pháp bảo mật toàn diện như tường lửa đa tầng, IDS/IPS, ACL, bảo mật cổng, mã hóa dữ liệu (IPsec), hệ thống cập nhật tập trung (WSUS), ghi nhật ký, giám sát, và đào tạo người dùng.
   * Đảm bảo hệ thống mạng an toàn trước các mối đe dọa như tấn công DDOS, nghe lén, hoặc truy cập trái phép.
5. **Ý nghĩa thực tiễn**:
   * Giải pháp mạng không dây được đề xuất đáp ứng đầy đủ nhu cầu sử dụng mạng của các phòng ban và giảng đường, đồng thời tận dụng tối đa tài nguyên sẵn có của trường.
   * Hệ thống mạng góp phần nâng cao chất lượng giảng dạy, học tập và quản lý thông qua việc cung cấp kết nối nhanh chóng, ổn định và an toàn.
   * Đồ án là nền tảng để áp dụng công nghệ thông tin vào môi trường giáo dục, đồng thời cung cấp tài liệu tham khảo cho các dự án tương tự trong tương lai.

Mặc dù đã nỗ lực hoàn thiện, đồ án không tránh khỏi những hạn chế do giới hạn về kinh nghiệm, thời gian và nguồn lực. Tuy nhiên, với sự hướng dẫn tận tình của ThS. Dương Ngọc Vân Khanh và sự hỗ trợ từ nhà trường, đồ án đã đạt được mục tiêu đề ra và mang lại giá trị thực tiễn.

**5.2. Hướng phát triển**

Để nâng cao tính hiệu quả và khả năng ứng dụng của hệ thống mạng không dây trong tương lai, đồ án đề xuất các hướng phát triển sau:

1. **Thử nghiệm và triển khai thực tế**:
   * Tiến hành thử nghiệm hệ thống mạng trong môi trường thực tế tại trường THPT Thăng Long Hà Nội để đánh giá hiệu suất, khả năng chịu tải và độ ổn định của WLAN, đặc biệt trong điều kiện đông người dùng (ví dụ, giờ học cao điểm).
   * Thu thập phản hồi từ giáo viên, học sinh và nhân viên để điều chỉnh và tối ưu hóa hệ thống.
2. **Nâng cấp công nghệ**:
   * Tích hợp các công nghệ Wi-Fi tiên tiến như Wi-Fi 6 hoặc Wi-Fi 6E để tăng tốc độ truyền dữ liệu, giảm độ trễ và hỗ trợ số lượng thiết bị kết nối lớn hơn.
   * Xem xét triển khai các thiết bị mạng hỗ trợ IPv6 để chuẩn bị cho xu hướng phát triển mạng trong tương lai.
3. **Tối ưu chi phí và tài nguyên**:
   * Xây dựng kế hoạch chi tiết về chi phí triển khai, bao gồm chi phí thiết bị (router, switch, access point), phần mềm, và bảo trì, nhằm đảm bảo tính khả thi trong môi trường trường học với ngân sách hạn chế.
   * Tìm kiếm các giải pháp mã nguồn mở hoặc thiết bị giá rẻ nhưng vẫn đảm bảo chất lượng để giảm chi phí đầu tư.
4. **Tăng cường bảo mật**:
   * Triển khai các công cụ giám sát mạng thời gian thực (real-time monitoring) để phát hiện và xử lý nhanh các mối đe dọa bảo mật.
   * Nâng cấp hệ thống IDS/IPS với các thuật toán AI để cải thiện khả năng phát hiện các cuộc tấn công tinh vi.
   * Tăng cường đào tạo người dùng (giáo viên, học sinh, nhân viên) về an ninh mạng, đặc biệt là cách phòng chống lừa đảo qua email và sử dụng mật khẩu an toàn.
5. **Mở rộng hệ thống**:
   * Thiết kế hệ thống cho phép dễ dàng mở rộng khi trường có thêm khu vực mới hoặc tăng số lượng người dùng.
   * Tích hợp các dịch vụ đám mây (cloud services) để hỗ trợ lưu trữ tài liệu học tập, quản lý dữ liệu và sao lưu từ xa, giảm phụ thuộc vào hạ tầng cục bộ.
6. **Nghiên cứu sâu hơn**:
   * Tiếp tục nghiên cứu các giải pháp quản lý lưu lượng mạng (traffic management) và QoS để ưu tiên băng thông cho các ứng dụng quan trọng (ví dụ, video học trực tuyến, VoIP).
   * Khám phá các công nghệ mới như SD-WAN (Software-Defined Wide Area Network) để cải thiện kết nối giữa các khu vực trong trường và với Internet.
7. **Hợp tác và chuyển giao**:
   * Hợp tác với các công ty công nghệ hoặc chuyên gia mạng để triển khai và bảo trì hệ thống, đảm bảo tính chuyên nghiệp và bền vững.
   * Chuyển giao tài liệu và hướng dẫn vận hành cho đội ngũ quản trị mạng của trường để họ có thể tự quản lý và bảo trì hệ thống.

# **DANH MỤC TÀI LIỆU THAM KHẢO**

Sách và giáo trình

* Cisco Systems. (2014). *CCNA Routing and Switching Study Guide*. Indianapolis: Sybex.  
  *(Tài liệu tham khảo về thiết kế mạng, VLAN, và mô hình ba lớp của Cisco).*
* Kurose, J. F., & Ross, K. W. (2020). *Computer Networking: A Top-Down Approach* (8th ed.). Boston: Pearson.  
  *(Cung cấp kiến thức nền tảng về mạng máy tính, giao thức, và mạng không dây).*
* Stallings, W. (2017). *Data and Computer Communications* (10th ed.). Boston: Pearson.  
  *(Nguồn tham khảo về mạng LAN, WLAN, và các vấn đề bảo mật mạng).*
* Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer Networks* (6th ed.). Boston: Pearson.  
  *(Tài liệu về mạng Campus, phân đoạn mạng, và quản lý lưu lượng).*

Bài báo và tài liệu học thuật

* Cisco Systems. (2009). *Campus Network for High Availability Design Guide*. Cisco Press.  
  *(Hướng dẫn thiết kế mạng Campus với các lớp Access, Distribution, Core).*
* IEEE Standards Association. (2011). *IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.  
  *(Tiêu chuẩn kỹ thuật về mạng không dây Wi-Fi).*
* Peterson, L. L., & Davie, B. S. (2011). *Wireless Networking in the Enterprise: A Case Study*. IEEE Communications Magazine, 49(3), 78-84.  
  *(Nghiên cứu về triển khai mạng không dây trong môi trường doanh nghiệp và giáo dục).*

Tài liệu trực tuyến

* Cisco Systems. (2023). *Cisco Networking Academy: Introduction to VLANs*. Truy cập từ: <https://www.netacad.com>.  
  *(Hướng dẫn về VLAN và phân đoạn mạng).*
* Microsoft. (2023). *Windows Server Update Services (WSUS) Documentation*. Truy cập từ: <https://docs.microsoft.com>.  
  *(Tài liệu về hệ thống cập nhật tập trung WSUS).*
* Balabit. (2023). *Syslog-ng: Open Source Log Management*. Truy cập từ: <http://www.balabit.com>.  
  *(Nguồn tham khảo về ghi nhật ký hệ thống, được trích dẫn trong tài liệu).*
* SyslogAgent. (2023). *SyslogAgent: Free Syslog Server for Windows*. Truy cập từ: <http://syslogserver.com>.  
  *(Tài liệu về giải pháp ghi nhật ký và giám sát mạng, được trích dẫn trong tài liệu).*
* CERT. (2023). *Computer Emergency Response Team: Security Best Practices*. Truy cập từ: <http://www.cert.org>.  
  *(Nguồn về an ninh mạng và đào tạo người dùng, được trích dẫn trong tài liệu).*

Tài liệu nội bộ

* Dương Ngọc Vân Khanh. (2023). *Giáo trình Mạng máy tính*. Trường Đại học Trà Vinh.  
  *(Tài liệu hướng dẫn của giảng viên về mạng máy tính và mạng không dây).*
* Khoa Kỹ thuật và Công nghệ. (2023). *Hướng dẫn thực hiện đồ án thực tập cơ sở ngành*. Trường Đại học Trà Vinh.  
  *(Tài liệu hướng dẫn cấu trúc và yêu cầu đồ án).*

Tài liệu khác

* Veeam Software. (2022). *Backup and Recovery Best Practices*. Truy cập từ: <https://www.veeam.com>.  
  *(Hướng dẫn về các phương pháp sao lưu Full, Differential, Incremental).*
* ISO/IEC. (2005). *ISO 17799/BS-7799: Information Security Management*.  
  *(Tiêu chuẩn về quản lý an ninh thông tin, được trích dẫn trong tài liệu).*
* Ruckus Networks. (2020). *Designing Wi-Fi for Schools: A Practical Guide*. Truy cập từ: <https://www.ruckusnetworks.com>.  
  *(Hướng dẫn thiết kế mạng không dây cho môi trường giáo dục).*

# **Phụ lục**

**Phụ lục 1: Sơ đồ khảo sát thực tế**

* **Hình 1**: Sơ đồ khảo sát thực tế khuôn viên trường THPT Thăng Long Hà Nội.  
  *(Hình ảnh từ tài liệu gốc, media/image2.png, mô tả bố trí các khu vực trong trường để lập kế hoạch triển khai mạng).*

**Phụ lục 2: Sơ đồ logic**

* **Hình 2**: Sơ đồ logic của hệ thống mạng được thiết kế.  
  *(Hình ảnh từ tài liệu gốc, media/image3.png, thể hiện cấu trúc logic của mạng Client-Server và kết nối giữa các VLAN).*

**Phụ lục 3: Sơ đồ vật lý và đi dây**

* **Hình 3**: Sơ đồ vật lý và đi dây LAN/WLAN tổng quan.  
  (Hình ảnh từ tài liệu gốc, media/image4.png, mô tả bố trí thiết bị và dây cáp trong toàn khuôn viên trường).
* **Hình 4**: Sơ đồ đi dây khu nhà Hiệu bộ.  
  (Hình ảnh từ tài liệu gốc, media/image5.png, chi tiết hóa kết nối mạng trong khu vực Hiệu bộ).
* **Hình 5**: Sơ đồ đi dây giảng đường A.  
  (Hình ảnh từ tài liệu gốc, media/image6.png, mô tả bố trí mạng tại giảng đường A).
* **Hình 6**: Sơ đồ đi dây giảng đường B.  
  (Hình ảnh từ tài liệu gốc, media/image7.png, mô tả bố trí mạng tại giảng đường B).
* **Hình 7**: Sơ đồ đi dây giảng đường C.  
  (Hình ảnh từ tài liệu gốc, media/image9.png, mô tả bố trí mạng tại giảng đường C).

**Phụ lục 4: Bảng thông tin VLAN**

* **Bảng 1**: Thông tin chi tiết về VLAN được thiết kế.  
  *(Trích từ tài liệu gốc, chương 1, mục 2.1.5).*

| **VLAN\_ID** | **Tên VLAN** | **Ghi chú** |
| --- | --- | --- |
| 1 | VLAN 1 | Không dùng |
| 10 | VLAN 10 | Phòng thực hành tin |
| 20 | VLAN 20 | Văn phòng công đoàn |
| 30 | VLAN 30 | Phòng thư viện |
| 40 | VLAN 40 | Phòng kế toán |
| 50 | VLAN 50 | Phòng phó hiệu trưởng |
| 60 | VLAN 60 | Phòng phó hiệu trưởng |
| 70 | VLAN 70 | Phòng hiệu trưởng |
| 80 | VLAN 80 | Phòng bảo vệ |
| 90 | VLAN 90 | Phòng hội đồng |
| 100 | VLAN 100 | Giảng đường A |
| 110 | VLAN 110 | Giảng đường B |
| 120 | VLAN 120 | Giảng đường C |

**Phụ lục 5: Bảng phân bổ địa chỉ IP**

* **Bảng 2**: Thông tin dải địa chỉ IP cho các VLAN.  
  *(Trích từ tài liệu gốc, chương 1, mục 2.4).*

| **VLAN ID** | **Tên VLAN** | **Dải địa chỉ IP (có dây)** | **Dải địa chỉ IP (không dây WLAN)** |
| --- | --- | --- | --- |
| 1 | VLAN 1 | medi/image20.png 192.168.1.2 – 192.168.1.254 | 192.168.1.100 – 192.168.1.200 |
| 10 | VLAN 10 | 192.168.10.2 – 192.168.10.254 | 192.168.10.100 – 192.168.10.200 |
| 20 | VLAN 20 | 192.168.20.2 – 192.168.20.254 | 192.168.20.100 – 192.168.20.200 |
| 30 | VLAN 30 | 192.168.30.2 – 192.168.30.254 | 192.168.30.100 – 192.168.30.200 |
| 40 | VLAN 40 | 192.168.40.2 – 192.168.40.254 | 192.168.40.100 – 192.168.40.200 |
| 50 | VLAN 50 | 192.168.50.2 – 192.168.50.254 | 192.168.50.100 – 192.168.50.200 |
| 60 | VLAN 60 | 192.168.60.2 – 192.168.60.254 | 192.168.60.100 – 192.168.60.200 |
| 70 | VLAN 70 | 192.168.70.2 – 192.168.70.254 | 192.168.70.100 – 192.168.70.200 |
| 80 | VLAN 80 | 192.168.80.2 – 192.168.80.254 | 192.168.80.100 – 192.168.80.200 |
| 90 | VLAN 90 | 192.168.90.2 – 192.168.90.254 | 192.168.90.100 – 192.168.90.200 |
| 100 | VLAN 100 | 192.168.100.2 – 192.168.100.254 | 192.168.100.100 – 192.168.100.200 |
| 110 | VLAN 110 | 192.168.110.2 – 192.168.110.254 | 192.168.110.100 – 192.168.110.200 |
| 120 | VLAN 120 | 192.168.120.2 – 192.168.120.254 | 192.168.120.100 – 192.168.120.200 |

**Phụ lục 6: Bảng hệ thống đường mạng**

* **Bảng 3**: Thông tin chi tiết về hệ thống đường mạng.  
  *(Trích từ tài liệu gốc, chương 1, mục 2.3).*

| **STT** | **Tên phòng** | **Số nút mạng** | **Số PC** | **Số mét dây** | **WLAN (Có/Không)** |
| --- | --- | --- | --- | --- | --- |
| 1 | Thực hành tin | 2 | 20 | 120m | Có |
| 2 | VP. Công Đoàn | 2 | 2 | 25m | Có |
| 3 | Thư viện | 2 | 1 | 20m | Có |
| 4 | Kế toán | 2 | 1 | 20m | Không |
| 5 | Phó hiệu trưởng | 2 | 1 | 30m | Không |
| 6 | Phó hiệu trưởng | 2 | 1 | 25m | Không |
| 7 | Hiệu trưởng | 2 | 1 | 20m | Không |
| 8 | Bảo vệ | 2 | 1 | 10m | Không |
| 9 | Hội đồng | 2 | 1 | 35m | Không |
| 10 | Giảng đường A | 12 | 1 | 60m | Có |
| 11 | Giảng đường B | 20 | 1 | 100m | Có |
| 12 | Giảng đường C | 16 | 1 | 80m | Có |

**Phụ lục 7: Minh họa mô hình mạng và bảo mật**

* **Hình 8**: Ví dụ về mô hình liên mạng (Internetworking).  
  *(Hình ảnh từ tài liệu gốc, media/image10.png, chương 2, mục 1).*
* **Hình 9**: Minh họa mô hình SOA theo các khu vực, tầng.  
  *(Hình ảnh từ tài liệu gốc, media/image17.png, chương 4, mục 2).*
* **Hình 10**: Minh họa nhiều VLAN khác nhau trong trường học.  
  *(Hình ảnh từ tài liệu gốc, media/image18.png, chương 4, mục 4).*
* **Hình 11**: Hệ thống tường lửa với 2 tầng trước và sau.  
  *(Hình ảnh từ tài liệu gốc, media/image19.png, chương 4, mục 5.1).*

**Phụ lục 8: Minh họa các phương pháp sao lưu**

* **Hình 12**: Minh họa RPO và RTO.  
  *(Hình ảnh từ tài liệu gốc, media/image11.png, chương 3, mục 2.2).*
* **Hình 13**: Minh họa Full Backup.  
  *(Hình ảnh từ tài liệu gốc, media/image12.png, chương 3, mục 2.2).*
* **Hình 14**: Minh họa Differential Backup.  
  *(Hình ảnh từ tài liệu gốc, media/image13.png, chương 3, mục 2.2).*
* **Hình 15**: Minh họa Incremental Backup.  
  *(Hình ảnh từ tài liệu gốc, media/image14.png, chương 3, mục 2.2).*
* **Hình 16**: Minh họa Backup dữ liệu vào USB/External HardDrive.  
  *(Hình ảnh từ tài liệu gốc, media/image15.png, chương 3, mục 4.1).*

# Lời cảm ơn

Tôi xin chân thành cảm ơn ThS. Dương Ngọc Vân Khanh đã tận tình hướng dẫn và hỗ trợ tôi trong suốt quá trình thực hiện đồ án. Đồng thời, tôi gửi lời cảm ơn sâu sắc đến Ban Giám hiệu Trường Đại học Trà Vinh, các thầy cô trong Khoa Kỹ thuật và Công nghệ, cùng các bạn bè đã tạo điều kiện và động viên tôi hoàn thành nhiệm vụ này.

Những ý kiến đóng góp quý báu từ thầy cô và các bạn là nguồn động lực lớn để tôi hoàn thiện đồ án. Tôi rất mong tiếp tục nhận được những góp ý để đồ án được cải thiện hơn trong tương lai.

Trân trọng,  
Trần Ngọc Hạnh