TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TP.HỒ CHÍ MINH
VIỆN CÔNG NGHỆ THÔNG TIN – ĐIỆN VÀ ĐIỆN TỬ

❁❁❁ ❁❁❁ ❁❁❁

BÁO CÁO GIỮA HỌC PHẦN THIẾT KẾ MẠNG

ĐỀ TÀI

THIẾT KẾ MẠNG CHO 3 CƠ SỞ TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TP HCM

Giảng viên hướng dẫn	**:**	**GV. Bùi Dương Thế**
Môn học	**:**	**Thiết Kế Mạng**
Mã học phần	**:**	**010112304305**
Lớp	**:**	**CN2302C**

Thành phố Hồ Chí Minh – 2025

LỜI CẢM ƠN

Chúng em xin gửi lời cảm ơn chân thành và sâu sắc đến **Thạc Sĩ Bùi Dương Thế**, người đã tận tình hướng dẫn, hỗ trợ và tạo điều kiện thuận lợi cho chúng em trong suốt quá trình học tập và thực hiện đề tài này.

Với kiến thức chuyên môn vững vàng cùng sự tận tâm trong giảng dạy, Thầy không chỉ truyền đạt cho chúng em những kiến thức quý báu mà còn định hướng tư duy khoa học và tinh thần cầu tiến, giúp chúng em hoàn thành tốt công việc của mình.

Một lần nữa, chúng em xin chân thành cảm ơn Thầy vì sự đồng hành, động viên và những góp ý quý giá trong suốt hành trình học tập và nghiên cứu vừa qua.

Trân trọng kính chúc Thầy sức khỏe, hạnh phúc và thành công trong sự nghiệp giảng dạy cũng như cuộc sống.

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

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

MỤC LỤC

MỞ ĐẦU 8

1.Giới thiệu 8

2. Mục tiêu thiết kế 8

3. Phạm vi và yêu cầu của thiết kế 9

NỘI DUNG 13

CHƯƠNG 1: TÓM LƯỢC DỰ ÁN 13

1.1 Khởi Động và Phân Tích Yêu Cầu Dự Án 13

Xác định phạm vi và mục tiêu: 13

Thu thập yêu cầu từ các bên liên quan: 13

1.2 Khảo Sát Địa Điểm và Đánh Giá Hạ Tầng 13

Thực hiện khảo sát chi tiết: 13

Đánh giá hạ tầng hiện có: 13

1.3 Lên Ý Tưởng và Xây Dựng Sơ Đồ Mạng 13

Phác thảo kiến trúc tổng thể: 13

1.4 Lập Kế Hoạch Ngân Sách và Phân Bổ Tài Nguyên 13

Định mức chi phí: 13

Phân chia giai đoạn triển khai: 13

Xác định nhân lực cần thiết: 13

1.5 Xây Dựng Chiến Lược Triển Khai và Lịch Trình 13

Lập kế hoạch triển khai chi tiết: 13

Quy hoạch việc triển khai theo khu vực: *14*

1.6 Tích Hợp Giải Pháp Bảo Mật và Tối Ưu Hóa **14**

Áp dụng các giải pháp bảo mật tiên tiến: *14*

Tối ưu hóa lưu lượng và hiệu suất: *14*

1.7 Kiểm Thử, Đào Tạo và Bàn Giao **14**

Thực hiện kiểm tra toàn diện: *14*

Đào tạo đội ngũ quản trị: *14*

Bàn giao tài liệu và hệ thống: *14*

1.8 Giám Sát Sau Triển Khai và Kế Hoạch Nâng Cấp **14**

Thiết lập hệ thống giám sát liên tục: *14*

Lập kế hoạch bảo trì và nâng cấp: *14*

CHƯƠNG 2: CÁC BƯỚC THỰC HIỆN **15**

2.1 Phân Tích Yêu Cầu **15**

2.1.1 Xác Định Nhu Cầu và Yêu Cầu Hệ Thống *15*

2.1.2. Phân Tích Cơ Sở Hạ Tầng Hiện Tại *15*

2.1.3 Tạo Sơ Đồ Mạng Chi Tiết *15*

2.1.4 Lựa Chọn Phần Cứng và Phần Mềm *16*

2.1.5. Thiết Kế Sơ Đồ Địa Chỉ IP *16*

2.1.6 Tạo Kế Hoạch Bảo Mật Mạng *16*

2.1.7 Kế Hoạch Hỗ Trợ và Bảo Trì Mạng *17*

2.1.8 Ghi Lại và Tài Liệu Hóa Hệ Thống *17*

2.1.9 Kiểm Tra và Triển Khai Thực Tế *17*

CHƯƠNG 3: PHƯƠNG ÁN THIẾT KẾ 19

3.1 Phạm Vi..... 19

3.1.1 Cơ Sở Bình Thạnh (CS1) – 2 Võ Oanh, Phường 25, Quận Bình Thạnh, TP HCM 19

3.1.2 Cơ Sở Thủ Đức (CS2) – 10 Đường số 12, Khu phố 3, Phường An Khánh, TP HCM..... 19

3.1.3 Cơ Sở Quận 12 (CS3) – 70 Tô Ký, Phường Tân Chánh Hiệp, Quận 12, TP HCM..... 20

3.2 Tổng Quan Hệ Thống Mạng..... 21

3.2.1 Cơ Sở Bình Thạnh (CS1)..... 21

3.2.2 Cơ Sở Thủ Đức (CS2)..... 21

3.2.3 Cơ Sở Quận 12 (CS3)..... 22

3.3 Tổng Hợp Toàn Hệ Thống..... 23

3.4 Mô Hình Logic 24

3.4.1 Core Layer (Tầng lõi)..... 24

3.4.2 Distribution Layer (Tầng phân phối)..... 24

3.4.3 Access Layer (Tầng truy cập) 24

3.5 Mô hình kết nối của từng cơ sở:..... 25

3.5.1 Sơ đồ mạng tổng thể cho từng cơ sở:..... 25

3.5.1.1 Cơ sở Bình Thạnh (CS1)..... 25

3.5.1.2 Cơ sở Thủ Đức (CS2) 25

3.5.1.3 Cơ sở Quận 12 (CS3)..... 25

3.5.2 Công Nghệ Sử Dụng..... 28

3.5.2.1 Mạng LAN và WAN..... 28

3.5.2.2 Cấu trúc mạng theo mô hình Star..... 28

3.5.2.3. Công nghệ không dây (Wi-Fi 6, 802.11ax)....28

3.5.2.4. Hệ thống bảo mật....28

3.5.3 Mô Hình Vật Lý....28

3.5.3.1 Thiết bị mạng....28

3.5.3.2 Cáp Kết Nối Giữa Các Thiết Bị Mạng....31

3.6 Lựa Chọn Thiết Bị 40

3.7 Triển Khai Hạ Tầng Mạng.... 40

CHƯƠNG 4: CÁC THIẾT BỊ VÀ ỨNG DỤNG DỰ KIẾN SỬ DỤNG.... 41

4.1 Các thiết bị.... 41

4.1.1 Phân tích nhu cầu sử dụng cho ba cơ sở....41

4.2 Đề xuất cấu hình chi tiết.... 42

4.2.1 Cấu hình chi tiết cụ thể cho từng thiết bị....42

4.3 Một số công nghệ được sử dụng 46

4.3.1 VLAN (Virtual Local Area Network)....46

4.3.2 VPN (Virtual Private Network) 47

4.3.3 DHCP và DNS Server....47

4.3.4 MIMO (Multiple Input Multiple Output)....47

4.4 Ứng dụng của MIMO trong mạng không dây: 48

KẾT LUẬN 49

1. Đã đạt được: 49

2. Tổng quan hệ thống mạng 49

3. Kiến trúc mạng và phân chia tài nguyên:..... 49

4. Kết nối định tuyến và quản lý hệ thống..... 50

5. Thách thức và hạn chế..... 50

6. Giá trị đạt được..... 50

TÀI LIỆU THAM KHẢO..... 51

MỞ ĐẦU

1.Giới thiệu

Xây dựng hạ tầng mạng hiện đại cho Trường Đại học Giao thông Vận tải TP. HCM

Trong kỷ nguyên số hóa, việc kết nối thông tin và truyền tải dữ liệu nhanh chóng, chính xác giữa các đơn vị trong cùng một hệ thống đóng vai trò quan trọng, đặc biệt trong lĩnh vực giáo dục. Các trường đại học cần một hạ tầng mạng vững chắc để hỗ trợ hiệu quả cho công tác giảng dạy, nghiên cứu và quản lý.

Trường Đại học Giao thông Vận tải TP. HCM, với quy mô lớn và số lượng sinh viên, giảng viên đông đảo, yêu cầu một hệ thống mạng đồng bộ, có khả năng kết nối ba cơ sở tại các địa điểm khác nhau trong thành phố. Thiết kế mạng cần đảm bảo tính ổn định, bảo mật cao và khả năng mở rộng linh hoạt, đáp ứng nhu cầu ngày càng tăng về học tập, nghiên cứu, quản lý hành chính và cung cấp các dịch vụ trực tuyến.

Việc thiết kế và triển khai một hệ thống mạng hiệu quả sẽ giúp Trường Đại học Giao thông Vận tải TP. HCM tối ưu hóa hoạt động giảng dạy, nghiên cứu và quản lý, đồng thời tạo nền tảng cho sự phát triển và mở rộng trong tương lai.

2. Mục tiêu thiết kế

Trước khi đi sâu vào các mục tiêu, chúng ta hãy lùi lại một bước và định nghĩa "**thiết kế mạng**" là gì. Nhìn chung, thiết kế mạng là tạo ra một mô hình về cách cơ sở hạ tầng CNTT của bạn sẽ được bố trí. Nó bao gồm mọi thứ từ cách bố trí vật lý của máy chủ và máy trạm của bạn đến tổ chức hợp lý của các dịch vụ mạng:

+ *Cải thiện hiệu suất và hiệu quả*
+ *Tăng cường an ninh*
+ *Giảm thời gian chết và chi phí hỗ trợ*

Khả năng mở rộng:

Khả năng của mạng lưới để phát triển và xử lý lưu lượng truy cập tăng lên được gọi là khả năng mở rộng. Khi lập kế hoạch cho khả năng mở rộng, điều cần thiết là phải xem xét sự tăng trưởng dự kiến trong tương lai của công ty và loại nhu cầu nào mà nó sẽ đặt ra cho mạng lưới. Và cũng cần phải suy nghĩ về cách chúng ta có thể thêm thiết bị hoặc người dùng mới một cách nhanh chóng và không bị gián đoạn.

Sự dư thừa:

Để mạng lưới đáng tin cậy, chúng cần có sự dự phòng. Điều đó có nghĩa là có nhiều đường dẫn để dữ liệu di chuyển và các hệ thống sao lưu tại chỗ trong trường hợp xảy ra lỗi. Sự dự phòng rất quan trọng đối với các hệ thống quan trọng như thương mại điện tử hoặc chăm sóc sức khỏe, nơi thời gian ngừng hoạt động có thể dẫn đến mất doanh thu. Điều này đạt được bằng cách sử dụng nhiều thiết bị hoặc liên kết giữa các thiết bị.

Khả năng phục hồi:

Một mạng lưới phục hồi có thể chịu được các lỗi và sự cố mất điện bất ngờ mà không bị dừng hoàn toàn. Điều này có thể đạt được thông qua dự phòng cũng như bằng cách triển khai các hệ thống thông minh có thể tự động định tuyến lại lưu lượng

truy cập hoặc khởi động lại dịch vụ. Mục tiêu là để người dùng nhận thấy khi có sự cố ngay lập tức.

Bảo mật:

Bảo mật luôn là mối quan tâm hàng đầu khi nói đến mạng. Với tin tặc ngày càng tinh vi hơn, điều quan trọng là phải có nhiều lớp bảo vệ. Có thể bao gồm tường lửa, phần mềm diệt vi-rút và hệ thống phát hiện xâm nhập. Điều quan trọng nữa là phải cập nhật hệ thống của bạn với các bản vá bảo mật mới nhất.

Hiệu suất:

Hiệu suất mạng rất quan trọng đối với các doanh nghiệp ở mọi quy mô. Mạng chậm hoặc không đáng tin cậy có thể ảnh hưởng đến năng suất của nhân viên, sự hài lòng của khách hàng và thậm chí là lợi nhuận ròng. Đó là lý do tại sao việc thiết kế mạng của bạn để đảm bảo hiệu suất tối ưu một cách cẩn thận là rất quan trọng. Điều này có thể được đảm bảo bằng cách sử dụng đúng thiết bị, tối ưu hóa lưu lượng mạng của bạn và khắc phục mọi sự cố tiềm ẩn.

Khả năng sử dụng:

Không có ích gì khi có một mạng nhanh nếu nó khó sử dụng. Hãy đảm bảo bạn thiết kế mạng của mình với tính khả dụng trong tâm trí. Nó bao gồm đảm bảo rằng người dùng có thể dễ dàng tìm thấy các tài nguyên họ cần, thiết lập các quyền người dùng phù hợp và cung cấp hướng dẫn rõ ràng về cách sử dụng mạng. Điều quan trọng cần lưu ý là không phải tất cả mọi người sử dụng mạng của bạn đều am hiểu công nghệ, vì vậy hãy đảm bảo rằng mọi người đều dễ sử dụng.

3. Phạm vi và yêu cầu của thiết kế

Thiết kế mạng cho ba cơ sở của trường Đại học Giao thông Vận tải TP. HCM việc đảm bảo ***hiệu suất bảo mật và khả năng mở rộng*** là vô cùng quan trọng, cần phải đáp ứng các yêu cầu cụ thể như sau:

Hiệu suất và Băng thông

Hiệu suất của mạng phụ thuộc vào khả năng truyền tải xử lý dữ liệu giữa các thiết bị, bao gồm máy tính, máy chủ, các thiết bị di động. Một hệ thống mạng có băng thông lớn giúp doanh nghiệp tránh được tình trạng tắc nghẽn dữ liệu đảm bảo luồng thông tin lưu thông ổn định.

Băng thông là khả năng truyền tải dữ liệu qua hệ thống mạng trong một khoảng thời gian nhất định, thường được đo bằng Mbps hoặc Gbps. Doanh nghiệp cần tính toán băng thông cần thiết dựa trên số lượng người dùng, các ứng dụng sử dụng nhiều tài nguyên (như video conferencing, truyền tải dữ liệu lớn), xu hướng phát triển trong tương lai.

Độ trễ là khoảng thời gian cần thiết để một gói dữ liệu di chuyển từ thiết bị gửi đến thiết bị nhận. Hệ thống mạng có độ trễ thấp sẽ đảm bảo phản hồi nhanh chóng cải thiện trải nghiệm người dùng, đặc biệt là trong các ứng dụng thời gian thực như video call hoặc hội nghị trực tuyến.

Chất lượng dịch vụ là cơ chế giúp ưu tiên các loại dữ liệu quan trọng hơn (như cuộc gọi VoIP, truyền phát video) so với các gói dữ liệu thông thường khác.
Khả năng bảo mật hệ thống mạng

Bảo mật mạng là một trong những yếu tố sống còn đối với bất kỳ doanh nghiệp nào, đặc biệt trong bối cảnh các cuộc tấn công mạng, vi phạm dữ liệu ngày càng tinh vi.

Tường lửa (Firewall): Tường lửa là lá chắn đầu tiên giúp ngăn chặn các cuộc tấn công từ bên ngoài. Khi thiết kế mạng, việc lựa chọn giữa tường lửa phần cứng và phần mềm hoặc kết hợp cả hai sẽ phụ thuộc vào quy mô, tính chất của doanh nghiệp. Một hệ thống tường lửa tốt sẽ giám sát lưu lượng mạng, phát hiện chặn các hành vi khả nghi.

Mã hóa (Encryption): Việc mã hóa dữ liệu, cả khi lưu trữ và truyền tải, giúp bảo vệ thông tin nhạy cảm như dữ liệu tài chính, thông tin khách hàng hoặc kế hoạch kinh doanh. Các công nghệ mã hóa phổ biến bao gồm SSL/TLS cho web, VPN cho kết nối từ xa.

Hệ thống phát hiện ngăn chặn xâm nhập (IDS/IPS): IDS phát hiện các hoạt động bất thường, giúp phát hiện sớm các mối đe dọa. IPS có khả năng ngăn chặn các cuộc tấn công ngay khi chúng xảy ra. Doanh nghiệp nên triển khai cả hai hệ thống để có sự phòng thủ nhiều lớp.

Kiểm soát truy cập (Access Control): Phân quyền kiểm soát truy cập là cách quản lý ai có quyền truy cập vào các tài nguyên mạng. 802.1X, RADIUS hoặc TACACS+ là những giải pháp kiểm soát truy cập phổ biến để đảm bảo chỉ những người dùng đã xác thực mới được phép truy cập hệ thống.

Khả năng mở rộng

Khi thiết kế mạng cho doanh nghiệp cần lưu ý, hệ thống mạng cần có khả năng mở rộng dễ dàng để hỗ trợ thêm nhiều người dùng, thiết bị và ứng dụng mới mà không làm gián đoạn hoạt động.

Mở rộng về người dùng: Hệ thống mạng phải được thiết kế dự phòng để tăng số lượng người dùng trong tương lai. Bao gồm việc tính toán đủ số cổng kết nối trên các switch, khả năng xử lý của router, các giải pháp mạng không dây có thể đáp ứng nhu cầu sử dụng cao hơn.

Mở rộng băng thông: Với nhu cầu truyền tải dữ liệu ngày càng tăng, băng thông cần được mở rộng tương ứng. Switch có khả năng Gigabit hoặc 10 Gigabit Ethernet, cáp quang là những lựa chọn giúp đáp ứng nhu cầu tăng trưởng về băng thông.

Cloud và On-premise: Hệ thống mạng hiện đại cần có khả năng tích hợp tốt với các giải pháp Cloud để lưu trữ, phân phối tài nguyên hoặc chạy ứng dụng. Đồng thời, một số hệ thống có thể phải tiếp tục sử dụng cơ sở hạ tầng on-premise. Do đó, tính linh hoạt mở rộng là rất quan trọng khi doanh nghiệp cần chuyển đổi mô hình làm việc hoặc quản lý tài nguyên.

Khả năng dự phòng và phục hồi

Mạng doanh nghiệp cần phải hoạt động liên tục không bị gián đoạn. Khả năng dự phòng giúp hệ thống mạng tránh được các rủi ro sự cố gây gián đoạn, đảm bảo tính sẵn sàng cao.

Dự phòng thiết bị: Doanh nghiệp nên thiết kế các hệ thống dự phòng, chẳng hạn như *cặp router* hoặc *switch dự phòng*, để đảm bảo khi một thiết bị gặp sự cố, thiết bị khác có thể thay thế ngay lập tức mà không làm gián đoạn hoạt động.

Kết nối đa dạng: Đối với các doanh nghiệp phụ thuộc nhiều vào Internet, việc có nhiều kết nối mạng từ các nhà cung cấp khác nhau giúp giảm thiểu rủi ro khi một kết nối gặp sự cố. *Load balancing* có thể được sử dụng để phân phối lưu lượng qua nhiều kết nối mạng.

Hệ thống sao lưu (Backup System): Việc sao lưu dữ liệu là cần thiết để đảm bảo rằng khi xảy ra sự cố, doanh nghiệp có thể khôi phục nhanh chóng. Sao lưu tự động định kỳ trên cloud hoặc local storage giúp đảm bảo tính liên tục của dữ liệu.

Khả năng quản lý giám sát

Phần mềm giám sát mạng giúp theo dõi trạng thái của các thiết bị trong hệ thống, giám sát lưu lượng, cảnh báo khi có sự cố. Các công cụ như SolarWinds, Zabbix hay Nagios có thể cung cấp thông tin chi tiết về hiệu suất của mạng và các báo cáo lỗi.

Với hệ thống lớn, doanh nghiệp có thể sử dụng ***công nghệ tự động hóa*** để quản lý, cấu hình hệ thống mạng để giảm thiểu lỗi do con người gây ra, tiết kiệm thời gian trong việc vận hành bảo trì hệ thống.

Tối ưu chi phí

Thiết kế mạng cho doanh nghiệp không chỉ cần đáp ứng các yêu cầu kỹ thuật mà còn phải cân đối chi phí để phù hợp với ngân sách của doanh nghiệp. Do đó, doanh nghiệp cần xem xét các yếu tố:

Chi phí triển khai: Việc lựa chọn phần cứng, phần mềm cần phải dựa trên nhu cầu thực tế. Ví dụ, lựa chọn giữa ***cáp đồng*** và ***cáp quang*** phụ thuộc vào băng thông, chi phí dài hạn.

Chi phí vận hành bảo trì: Hệ thống mạng cần được thiết kế sao cho dễ dàng quản lý bảo trì giúp giảm chi phí vận hành trong dài hạn. Doanh nghiệp có thể cân nhắc các giải pháp mạng ảo hoặc điện toán đám mây để tối ưu hóa chi phí phần cứng và nhân sự.

Hỗ trợ dịch vụ bảo trì

Một yếu tố quan trọng cuối cùng là khả năng hỗ trợ bảo trì hệ thống. Khi thiết kế hệ thống mạng, doanh nghiệp cần tính đến:

Hỗ trợ kỹ thuật: Việc chọn nhà cung cấp thiết bị, phần mềm uy tín với dịch vụ hỗ trợ kỹ thuật 24/7 là yếu tố giúp doanh nghiệp duy trì hoạt động mạng ổn định, nhanh chóng khắc phục các sự cố khi cần.

Bảo trì định kỳ: Doanh nghiệp cần có kế hoạch bảo trì định kỳ để kiểm tra nâng cấp hệ thống, bao gồm cả việc cập nhật phần mềm bảo mật, kiểm tra các thiết bị phần cứng điều chỉnh cấu hình hệ thống.

NỘI DUNG
CHƯƠNG 1: TÓM LƯỢC DỰ ÁN
1.1 Khởi Động và Phân Tích Yêu Cầu Dự Án
Xác định phạm vi và mục tiêu:
- Thiết lập các tiêu chí về số lượng người dùng, ứng dụng cần hỗ trợ, yêu cầu hiệu suất và bảo mật. Đồng thời, xác định mục tiêu phát triển dài hạn của hệ thống.

Thu thập yêu cầu từ các bên liên quan:
- Tổ chức các buổi họp với các phòng ban, giảng viên và sinh viên để thu thập các nhu cầu cụ thể và mong đợi từ hệ thống mạng mới.

1.2 Khảo Sát Địa Điểm và Đánh Giá Hạ Tầng
Thực hiện khảo sát chi tiết:
- Đánh giá hiện trạng cơ sở vật chất của từng cơ sở, bao gồm vị trí lắp đặt thiết bị, cấu trúc tòa nhà và các yếu tố môi trường có thể ảnh hưởng đến tín hiệu mạng.

Đánh giá hạ tầng hiện có:
- Kiểm tra và ghi nhận tình trạng của các thiết bị như switch, router, server, hệ thống cáp quang, cũng như xác định các điểm nghẽn và rủi ro bảo mật.

1.3 Lên Ý Tưởng và Xây Dựng Sơ Đồ Mạng
Phác thảo kiến trúc tổng thể:
- Xây dựng sơ đồ mạng tổng quan cho từng cơ sở với cấu trúc LAN độc lập, đồng thời thiết lập kết nối qua WAN.

Thiết kế chi tiết:
- Xác định các phân vùng mạng (VLAN) cho các nhóm người dùng khác nhau. Đề xuất sơ đồ địa chỉ IP và phân bổ tài nguyên mạng.
- Lựa chọn vị trí đặt Access Point (AP) ưu việt để tối ưu vùng phủ sóng, đặc biệt là ngoài trời.

1. 4 Lập Kế Hoạch Ngân Sách và Phân Bổ Tài Nguyên
Định mức chi phí:
- Xác định ngân sách cho phần cứng, phần mềm và nhân công.

Phân chia giai đoạn triển khai:
- Lập kế hoạch theo từng giai đoạn: khảo sát, chuẩn bị, lắp đặt, kiểm tra, bàn giao và bảo trì.

Xác định nhân lực cần thiết:
- Đánh giá yêu cầu về chuyên môn và số lượng nhân công cho từng cơ sở, đặc biệt đối với các công việc đòi hỏi kỹ năng đặc thù như thi công ngoài trời.

1.5 Xây Dựng Chiến Lược Triển Khai và Lịch Trình
Lập kế hoạch triển khai chi tiết:
- Xác định thời gian thực hiện cho từng giai đoạn (ví dụ: khảo sát 30 ngày, chuẩn bị 30 ngày, lắp đặt 15 ngày, kiểm tra 7 ngày, bàn giao 3 ngày) và bổ sung dự phòng cho các tình huống bất ngờ.

Quy hoạch việc triển khai theo khu vực:
- Thiết lập lịch trình làm việc riêng cho từng cơ sở, đảm bảo các bước được thực hiện đồng bộ và liên tục.

1.6 Tích Hợp Giải Pháp Bảo Mật và Tối Ưu Hóa

Áp dụng các giải pháp bảo mật tiên tiến:
- Triển khai firewall, IDS/IPS, và xác thực đa yếu tố (MFA) để bảo vệ hệ thống khỏi các mối đe dọa.

Tối ưu hóa lưu lượng và hiệu suất:
- Sử dụng các công cụ giám sát và điều chỉnh cấu hình mạng để đảm bảo tốc độ truy cập ổn định, đặc biệt trong giờ cao điểm.

1.7. Kiểm Thử, Đào Tạo và Bàn Giao

Thực hiện kiểm tra toàn diện:
- Kiểm thử hiệu suất, bảo mật và khả năng chịu tải của hệ thống trên từng giai đoạn, với thử nghiệm trên nhóm người dùng mẫu.

Đào tạo đội ngũ quản trị:
- Tổ chức các buổi đào tạo cho nhân viên IT và người dùng cuối về quy trình vận hành, bảo trì và xử lý sự cố.

Bàn giao tài liệu và hệ thống:
- Hoàn thiện hồ sơ thiết kế, cấu hình và tài liệu hướng dẫn để chuyển giao cho bộ phận quản trị và bảo trì.

1.8 Giám Sát Sau Triển Khai và Kế Hoạch Nâng Cấp

Thiết lập hệ thống giám sát liên tục:
- Sử dụng các công cụ giám sát tự động để theo dõi hiệu suất và an toàn của mạng, từ đó đưa ra các cảnh báo kịp thời.

Lập kế hoạch bảo trì và nâng cấp:
- Định kỳ đánh giá và bảo trì hệ thống, dự kiến nâng cấp phần cứng và phần mềm sau 3-5 năm để đảm bảo hệ thống luôn cập nhật và an toàn.

CHƯƠNG 2: CÁC BƯỚC THỰC HIỆN

2.1 Phân Tích Yêu Cầu

2.1.1 Xác Định Nhu Cầu và Yêu Cầu Hệ Thống

Thu thập thông tin người dùng:

- Đánh giá số lượng sinh viên, giảng viên và nhân viên quản lý hiện tại và dự kiến trong tương lai.
- Xác định các nhóm người dùng với các nhu cầu riêng (ví dụ: phòng lab, thư viện, văn phòng hành chính).

Định rõ mục tiêu ứng dụng:

- Liệt kê các ứng dụng giảng dạy, nghiên cứu và quản trị cần được hỗ trợ (hệ thống học trực tuyến, cơ sở dữ liệu, ứng dụng văn phòng…).

Yêu cầu bảo mật:

- Xác định các loại dữ liệu nhạy cảm cần bảo vệ (thông tin cá nhân, dữ liệu nghiên cứu).
- Đặt ra các tiêu chuẩn bảo mật bắt buộc theo quy định của nhà trường và các tiêu chuẩn ngành.

Dự báo tăng trưởng và mở rộng:

- Phân tích xu hướng tăng trưởng người dùng và thiết bị kết nối.
- Lên kế hoạch mở rộng hệ thống dựa trên các chỉ số hiện tại và dự báo trong tương lai.

2.1.2. Phân Tích Cơ Sở Hạ Tầng Hiện Tại

Đánh giá thiết bị và cấu hình mạng hiện hành:

- Kiểm tra hiệu suất của các thiết bị hiện có (router, switch, firewall, máy chủ…).
- Thu thập số liệu về băng thông, độ trễ, và hiệu quả hoạt động của hệ thống.

Thu thập phản hồi từ người dùng:

- Phỏng vấn, khảo sát người dùng về mức độ hài lòng, các vấn đề gặp phải và gợi ý cải thiện.
- Phân tích báo cáo sự cố để xác định các điểm nghẽn.

Xác định điểm mạnh và hạn chế:

- Liệt kê các ưu điểm hiện tại (ví dụ: tốc độ truy cập ổn định, khả năng kết nối nội bộ tốt).
- Ghi nhận các hạn chế (ví dụ: thiếu băng thông vào giờ cao điểm, hạn chế về bảo mật).

2.1.3 Tạo Sơ Đồ Mạng Chi Tiết

Phác thảo sơ đồ tổng thể:

- Vẽ sơ đồ hình học của hệ thống, thể hiện vị trí ba cơ sở và đường truyền dữ liệu giữa chúng.

Phân tầng mạng:

- Xác định rõ ràng các tầng:

+Mạng lõi: Hạ tầng truyền tải chính kết nối các cơ sở.

+ Mạng phân phối: Kết nối các phòng ban, khu chức năng tại mỗi cơ sở.

+Mạng truy cập: Các điểm kết nối trực tiếp với người dùng cuối.

Xác định vị trí thiết bị:

- Định vị máy chủ, router, switch, firewall và điểm truy cập Wi-Fi theo sơ đồ.
- Lên kế hoạch dự phòng đường truyền và các kịch bản phục hồi sau sự cố.

2.1.4 Lựa Chọn Phần Cứng và Phần Mềm

Nghiên cứu và so sánh thiết bị:

- Liệt kê các thương hiệu, mẫu mã router, switch, firewall, thiết bị Wi-Fi có uy tín.
- So sánh các tiêu chí: tốc độ xử lý, dung lượng, khả năng mở rộng và hỗ trợ kỹ thuật.

Lựa chọn hệ điều hành và phần mềm quản lý:

- Xác định phần mềm giám sát, quản lý mạng (Network Management System – NMS) phù hợp với quy mô và mục tiêu của hệ thống.

Xây dựng bảng tiêu chí lựa chọn:

- Đưa ra các tiêu chí kỹ thuật và kinh tế để lựa chọn giải pháp tối ưu nhất.

2.1.5. Thiết Kế Sơ Đồ Địa Chỉ IP

Đánh giá số lượng thiết bị:

- Xác định tổng số thiết bị cần cấp phát địa chỉ IP tại từng cơ sở.

Chọn loại địa chỉ IP:

- Quyết định sử dụng IPv4, IPv6 hoặc kết hợp dựa trên yêu cầu kết nối và khả năng mở rộng.

Phân chia dải IP:

- Xác định dải địa chỉ cho từng khu vực/phòng ban.

Thiết lập các subnet phù hợp, đảm bảo không gian đủ lớn cho mở rộng.

Lập sơ đồ cấp phát IP:

- Vẽ sơ đồ thể hiện các subnet, địa chỉ IP tĩnh cho các thiết bị quan trọng và địa chỉ IP động cho các thiết bị di động.

2.1.6 Tạo Kế Hoạch Bảo Mật Mạng

Xác định các rủi ro và mối đe dọa:

- Đánh giá các nguy cơ từ bên ngoài và nội bộ.
- Xác định các điểm cần bảo vệ: truy cập Internet, dữ liệu nội bộ, hệ thống lưu trữ.

Triển khai giải pháp bảo mật:

- Cấu hình firewall, thiết lập VPN cho kết nối an toàn.
- Áp dụng mã hóa dữ liệu trong quá trình truyền tải và lưu trữ.

Kiểm soát truy cập và phân quyền:

- Xây dựng hệ thống xác thực đa yếu tố và quản lý quyền truy cập theo vai trò người dùng.

Lập kế hoạch kiểm tra bảo mật:

- Thiết lập quy trình kiểm tra định kỳ (pen-testing, audit bảo mật) để kịp thời phát hiện và khắc phục lỗ hổng.

2.1.7 Kế Hoạch Hỗ Trợ và Bảo Trì Mạng

Giám sát hiệu suất liên tục:

- Cài đặt hệ thống giám sát tự động (ví dụ: sử dụng SNMP, NetFlow) để theo dõi tình trạng mạng 24/7.

Lập lịch bảo trì định kỳ:

- Xác định các khoảng thời gian bảo trì, kiểm tra định kỳ thiết bị và phần mềm.

Đào tạo nhân viên kỹ thuật:

- Tổ chức các khóa đào tạo định kỳ cho đội ngũ kỹ thuật về quy trình vận hành, xử lý sự cố và cập nhật hệ thống.

Thiết lập quy trình xử lý sự cố:

- Xác định các bước phản ứng khi hệ thống gặp sự cố, từ cảnh báo đến khắc phục và báo cáo hậu sự cố.

Cập nhật hệ thống tự động:

- Lên kế hoạch triển khai các bản cập nhật phần mềm và vá lỗi bảo mật một cách tự động hoặc theo lịch trình.

2.1.8 Ghi Lại và Tài Liệu Hóa Hệ Thống

Tạo hồ sơ thiết kế mạng:

- Ghi chép chi tiết sơ đồ mạng, cấu hình thiết bị, bảng địa chỉ IP và các chính sách bảo mật.

Lưu trữ thông số kỹ thuật:

- Lập tài liệu về thông số kỹ thuật của từng thiết bị, phần mềm được sử dụng trong hệ thống.

Quản lý tài liệu:

- Thiết lập hệ thống lưu trữ tài liệu điện tử, có thể truy cập dễ dàng cho các thành viên kỹ thuật và quản trị.

Cập nhật định kỳ:

- Đảm bảo tài liệu được cập nhật theo các thay đổi trong cấu trúc hệ thống và quy trình bảo trì.

2.1.9 Kiểm Tra và Triển Khai Thực Tế

Thực hiện kiểm thử hệ thống:

- Triển khai thử nghiệm (pilot) trên một phần nhỏ của mạng để đánh giá hiệu suất, tính ổn định và khả năng bảo mật.

Đánh giá kết quả thử nghiệm:

- Thu thập dữ liệu, phản hồi từ người dùng thử nghiệm và phân tích các chỉ số hiệu suất.

Điều chỉnh thiết kế:

- Dựa trên kết quả kiểm thử, điều chỉnh sơ đồ, cấu hình thiết bị và quy trình bảo

mật cho phù hợp.
Triển khai toàn diện:
- Sau khi hoàn thiện thử nghiệm, tiến hành triển khai hệ thống mạng trên toàn bộ ba cơ sở.
Giám sát và đánh giá sau triển khai:
- Tiếp tục theo dõi hiệu suất của hệ thống, đảm bảo các chỉ số vận hành ổn định và kịp thời khắc phục sự cố phát sinh.

Qua quá trình thực hiện các bước trên, hệ thống mạng cho ba cơ sở của Trường Đại học Giao thông Vận tải TP. HCM sẽ được xây dựng với cấu trúc hiện đại, hiệu suất cao, bảo mật nghiêm ngặt và khả năng mở rộng linh hoạt, đáp ứng đầy đủ nhu cầu giảng dạy, nghiên cứu và quản trị hành chính của nhà trường.

CHƯƠNG 3: PHƯƠNG ÁN THIẾT KẾ

3.1 Phạm Vi

Phương án này nhằm đảm bảo rằng hệ thống mạng cho ba cơ sở được thiết kế một cách khoa học, đáp ứng đủ yêu cầu hoạt động đồng thời của người dùng trong từng ca học – làm việc, từ đó giúp tối ưu hóa hiệu suất và đảm bảo trải nghiệm sử dụng ổn định cho mọi đối tượng.

3.1.1 Cơ Sở Bình Thạnh (CS1) – 2 Võ Oanh, Phường 25, Quận Bình Thạnh, TP HCM

- Số lượng người dùng dự kiến**:** 4.500 – 5.500 người
- Số người truy cập đồng thời mỗi ca học – làm việc: 2.300 – 2.800 người

Phân bổ theo khu vực:

Khu vực	Đối tượng	Số lượng (ước tính)
Phòng học	Sinh viên	700 – 1.200
Phòng giảng viên	Giảng viên	60
Phòng ban hành chính	Nhân viên nội bộ	70
Phòng lab / máy tính	Sinh viên, giảng viên	420
Khu vực khác	Bảo vệ, vệ sinh	40

3.1.2 Cơ Sở Thủ Đức (CS2) – 10 Đường số 12, Khu phố 3, Phường An Khánh, TP HCM

- Số lượng người dùng dự kiến: 3.500 – 4.500 người
- Số người truy cập đồng thời mỗi ca học – làm việc: 1.300 – 1.800 người

Phân bổ theo khu vực:

Khu vực	Đối tượng	Số lượng (ước tính)
Phòng học	Sinh viên	850 – 1.400
Phòng giảng viên	Giảng viên	45
Phòng ban hành chính	Nhân viên nội bộ	30
Phòng lab / máy tính	Sinh viên, giảng viên	250
Khu vực khác	Bảo vệ, vệ sinh	20

3.1.3 Cơ Sở Quận 12 (CS3) – 70 Tô Ký, Phường Tân Chánh Hiệp, Quận 12, TP HCM

- Số lượng người dùng dự kiến: 3.800 – 4.200 người
- Số người truy cập đồng thời mỗi ca học – làm việc: 1.700 – 2.200 người

Phân bổ theo khu vực:

Khu vực	Đối tượng	Số lượng (ước tính)
Phòng học	Sinh viên	600 – 1.100
Phòng giảng viên	Giảng viên	55
Phòng ban hành chính	Nhân viên nội bộ	40
Phòng lab / máy tính	Sinh viên, giảng viên	300
Khu vực khác	Bảo vệ, vệ sinh	25

3.2 Tổng Quan Hệ Thống Mạng

3.2.1 Cơ Sở Bình Thạnh (CS1)

- Quy mô tổng thể: 4.500 – 5.500 người dùng đăng ký
- Lưu lượng truy cập đồng thời trung bình: 2.300 – 2.800 người dùng/ca
- Dự phòng: Hệ thống có khả năng mở rộng thêm 15 – 20%, đảm bảo đáp ứng khi có sự kiện lớn hoặc tăng trưởng số lượng sinh viên

Phân vùng mạng:

Tên VLAN	Mục đích	Đối tượng sử dụng	Đặc điểm
VLAN Sinh viên	Học tập, nghiên cứu, truy cập tài liệu	Sinh viên	Kiểm soát truy cập internet, bảo vệ tài nguyên nội bộ
VLAN Giảng viên & Nhân viên	Quản lý, giảng dạy, hành chính	Giảng viên, nhân viên	Ưu tiên băng thông, bảo mật cao hơn VLAN sinh viên
VLAN Phòng Lab & Phòng máy	Tài nguyên chuyên biệt, băng thông cao	Người dùng trong phòng Lab	Kết nối với máy chủ nội bộ, yêu cầu hiệu suất cao
VLAN Dịch vụ khác	Bảo mật riêng biệt cho các bộ phận hỗ trợ	Bảo vệ, vệ sinh, khách mời	Hạn chế truy cập, cô lập với VLAN quan trọng

3.2.2 Cơ Sở Thủ Đức (CS2)

- Quy mô tổng thể: 3.500 – 4.500 người dùng đăng ký
- Lưu lượng truy cập đồng thời trung bình: 1.300 – 1.800 người dùng/ca
- Dự phòng: Hệ thống có khả năng mở rộng thêm **15 – 20%**, đảm bảo hiệu suất khi có hội thảo, sự kiện hoặc tăng số lượng sinh viên

Phân vùng mạng:

Tên VLAN	Mục đích	Đối tượng sử dụng	Đặc điểm
VLAN Sinh viên	Dành cho truy cập tài nguyên học tập	Sinh viên	Truy cập tài liệu, giới hạn băng thông
VLAN Giảng viên	Kết nối ưu tiên, dữ liệu giảng dạy	Giảng viên	Ưu tiên băng thông, bảo mật dữ liệu
VLAN Phòng Lab	Kết nối tốc độ cao, nghiên cứu khoa học	Nhà nghiên cứu, sinh viên Lab	Hiệu suất cao, truy cập máy chủ nội bộ
VLAN Hành chính & Quản lý	Cơ sở dữ liệu, bảo mật nội bộ	Nhân viên hành chính, quản lý	Bảo mật cao, hạn chế truy cập bên ngoài

3.2.3 Cơ Sở Quận 12 (CS3)

- Quy mô tổng thể: 3.800 – 4.200 người dùng đăng ký
- Lưu lượng truy cập đồng thời trung bình: 1.700 – 2.200 người dùng/ca
- Dự phòng: Hệ thống có thể mở rộng 15 – 20% để đảm bảo khả năng đáp ứng khi cần thiết

Phân vùng mạng:

Tên VLAN	Mục đích	Đối tượng sử dụng	Đặc điểm
VLAN Sinh viên & Phòng học	Đáp ứng lưu lượng lớn	Sinh viên, phòng học	Hỗ trợ số lượng lớn kết nối, tối ưu băng thông
VLAN Giảng viên	Ưu tiên truy cập dữ liệu, hệ thống nội bộ	Giảng viên	Truy cập hệ thống giảng dạy, bảo mật cao
VLAN Phòng Lab & Phòng máy	Hỗ trợ truy cập dữ liệu chuyên sâu	Nhà nghiên cứu, sinh viên Lab	Kết nối tốc độ cao, truy cập tài nguyên chuyên biệt
VLAN Dịch vụ khác	Bảo vệ, nhân viên, hệ thống camera	Bảo vệ, nhân viên kỹ thuật	Cách ly với các VLAN khác, bảo mật hệ thống

3.3 Tổng Hợp Toàn Hệ Thống

- Quy mô tổng thể: 11.800 – 14.200 người dùng đăng ký
- Lưu lượng truy cập đồng thời trung bình: 5.300 – 6.800 người dùng/ca
- Dự phòng: 15 – 20%, đảm bảo hiệu suất cao ngay cả trong giờ cao điểm hoặc khi có sự kiện

Hệ thống phân vùng mạng chung:

Tên VLAN	Mục đích	Đối tượng sử dụng	Đặc điểm
VLAN Sinh viên	Phục vụ các hoạt động học tập, truy cập tài nguyên trường	Sinh viên	Truy cập internet và hệ thống trường, kiểm soát băng thông
VLAN Giảng viên	Kết nối giảng dạy, quản lý nội dung học tập	Giảng viên	Ưu tiên truy cập dữ liệu giảng dạy, bảo mật nâng cao
VLAN Hành chính	Dữ liệu bảo mật cho bộ phận quản lý và nhân viên	Nhân viên hành chính	Bảo vệ dữ liệu nội bộ, hạn chế truy cập từ bên ngoài
VLAN Phòng Lab	Hiệu suất cao dành riêng cho nghiên cứu	Nhà nghiên cứu, sinh viên Lab	Tốc độ cao, truy cập tài nguyên nghiên cứu chuyên sâu
VLAN Dịch vụ khác	Dành cho bảo vệ, hệ thống camera, thiết bị IoT	Bảo vệ, kỹ thuật viên	Tách biệt hoàn toàn, tối ưu bảo mật hệ thống

3.4 Mô Hình Logic

Hệ thống mạng cho ba cơ sở được thiết kế theo mô hình **phân cấp 3 lớp (Three-Tier Architecture)** để đảm bảo tính hiệu quả, dễ dàng quản lý và mở rộng khi cần thiết.

Hệ thống được chia thành ba tầng chính:

3.4.1 Core Layer (Tầng lõi)

- Chứa router trung tâm tại mỗi cơ sở, đóng vai trò kết nối giữa các VLAN nội bộ với mạng WAN.
- Xử lý lưu lượng lớn, quản lý định tuyến, đảm bảo kết nối ổn định giữa các thiết bị.
- Kết nối với Firewall để bảo vệ hệ thống trước các mối đe dọa từ Internet.

3.4.2 Distribution Layer (Tầng phân phối)

- Chứa switch Layer 3 (Cisco Catalyst 9500 hoặc Aruba CX 6400), chịu trách nhiệm routing VLAN.
- Kết nối trực tiếp với tầng Core thông qua cáp quang tốc độ cao (10GbE hoặc 40GbE).
- Kiểm soát chính sách bảo mật và quản lý lưu lượng mạng giữa các VLAN.

3.4.3 Access Layer (Tầng truy cập)

- Gồm switch Layer 2 (Cisco Catalyst 9200 hoặc Aruba 2930F), kết nối đến thiết bị đầu cuối.

- Hỗ trợ kết nối có dây (Ethernet) và không dây (Wi-Fi 6).
- Access Point (AP) triển khai tại các khu vực quan trọng để cung cấp kết nối Wi-Fi ổn định.

3.5 Mô hình kết nối của từng cơ sở:

3.5.1 Sơ đồ mạng tổng thể cho từng cơ sở:

3.5.1.1 Cơ sở Bình Thạnh (CS1)

- Router kết nối Internet và mạng WAN nội bộ giữa các cơ sở.
- Switch Core Layer 3 chịu trách nhiệm routing giữa các VLAN.
- Switch Layer 2 phân phối kết nối đến phòng học, phòng lab, giảng viên.
- Hệ thống Access Point (AP) triển khai tại các vị trí chiến lược để đảm bảo phủ sóng Wi-Fi.

3.5.1.2 Cơ sở Thủ Đức (CS2)

- Kiến trúc tương tự CS1, nhưng tối ưu cho quy mô nhỏ hơn.

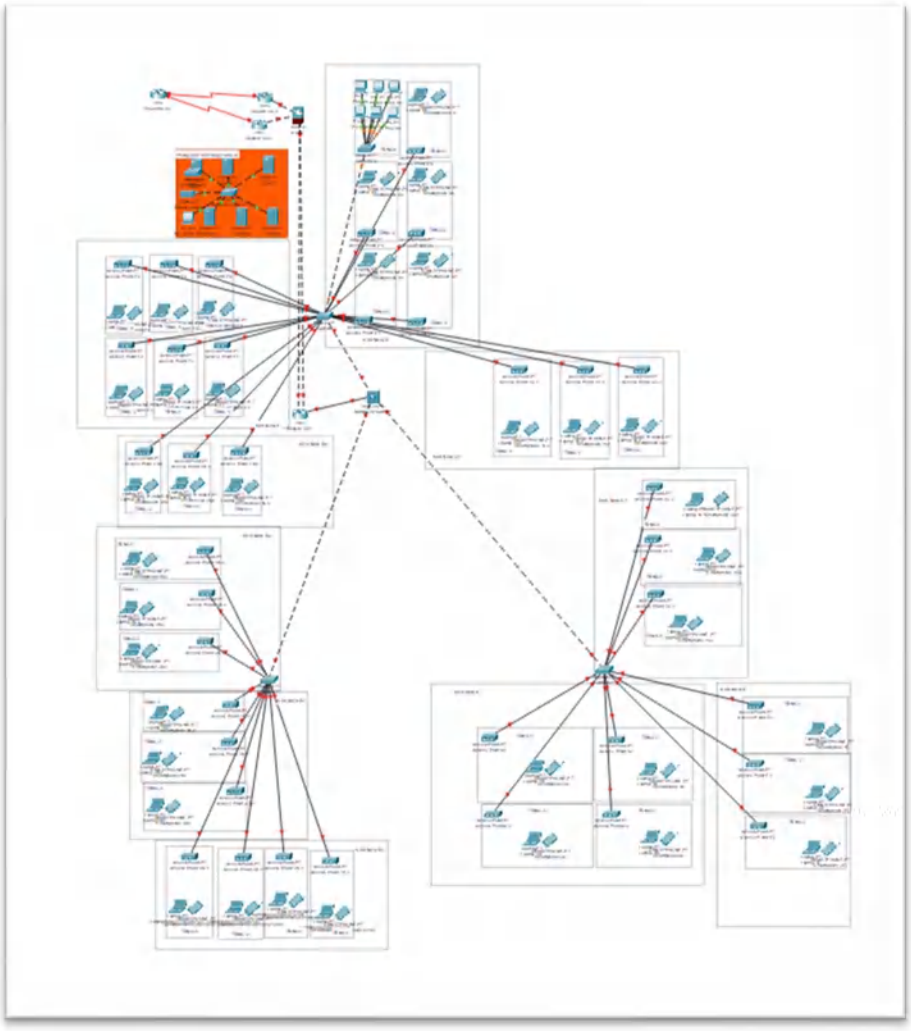
VLAN dành riêng cho hệ thống phòng Lab và giảng viên với ưu tiên băng thông.

- Kết nối giữa các tầng thông qua switch Layer 3, giúp cải thiện khả năng mở rộng.

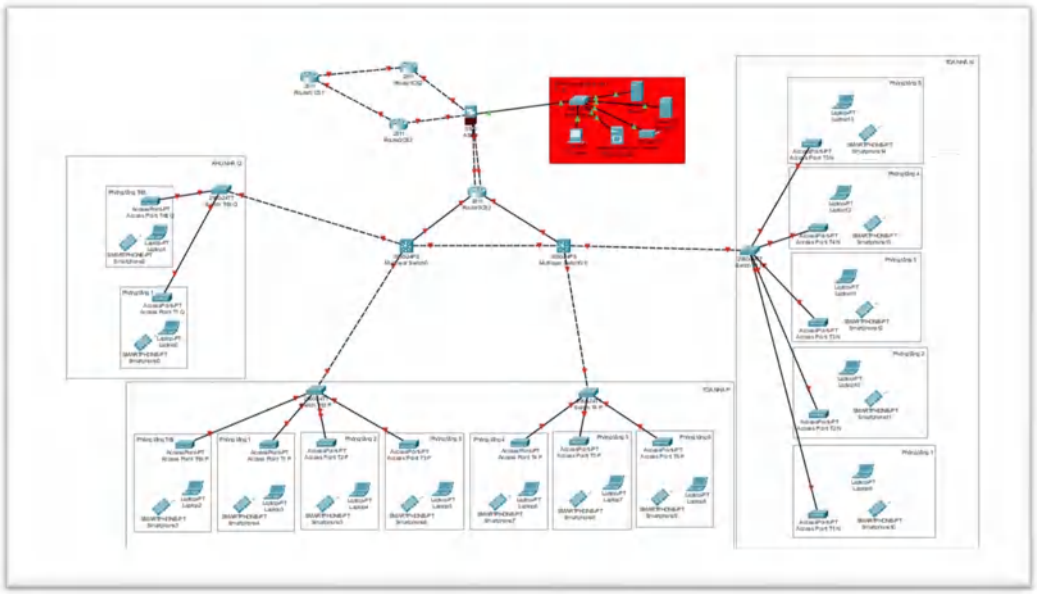
3.5.1.3 Cơ sở Quận 12 (CS3)

- Mạng được phân vùng để tối ưu hiệu suất cho sinh viên và nhân viên hành chính.

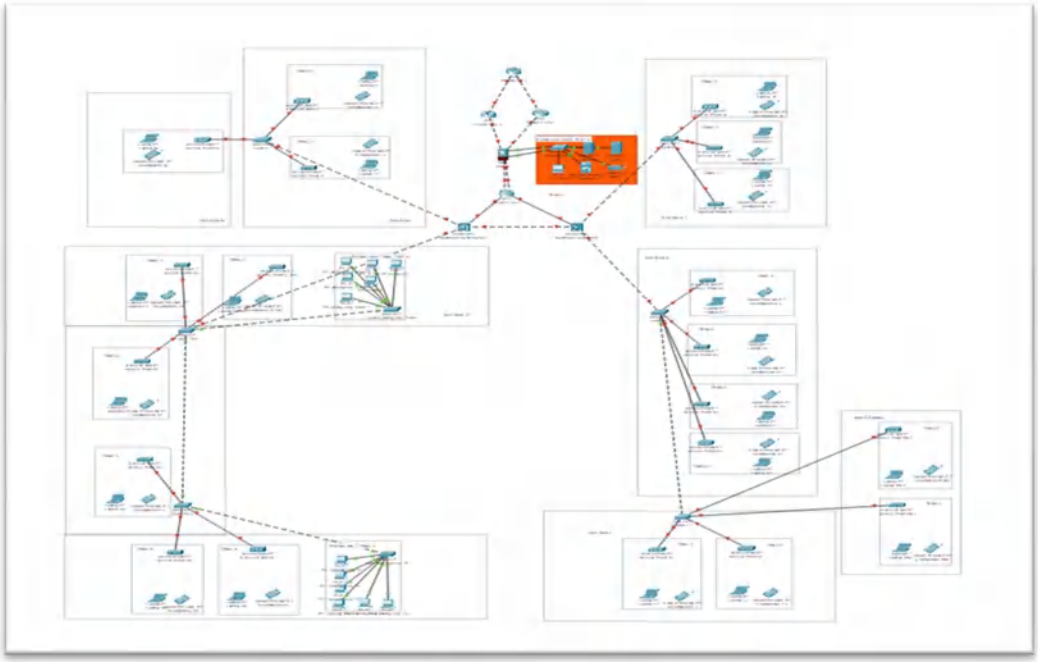
- Cấu trúc mạng cân bằng giữa kết nối có dây (Ethernet) và không dây (Wi-Fi 6).
- Switch Access có hỗ trợ PoE để cấp nguồn cho các AP, camera an ninh.



Hình 1. Sơ đồ tổng thể mạng cho cơ sở 1



Hình 2. Sơ đồ tổng thể mạng cho cơ sở 2



Hình 3. Sơ đồ tổng thể mạng cho cơ sở 3

3.5.2 Công Nghệ Sử Dụng

3.5.2.1 Mạng LAN và WAN

- Mỗi cơ sở có mạng LAN riêng, sử dụng VLAN để phân chia người dùng.
- Kết nối giữa các cơ sở qua mạng WAN VPN (IPSec hoặc MPLS) đảm bảo an toàn và ổn định.

3.5.2.2 Cấu trúc mạng theo mô hình Star

- Core Layer: Router chính kết nối với nhà cung cấp dịch vụ Internet (ISP).
- Distribution Layer: Switch Layer 3 chịu trách nhiệm routing VLAN.
- Access Layer: Switch Layer 2 và AP phục vụ kết nối đầu cuối.

3.5.2.3. Công nghệ không dây (Wi-Fi 6, 802.11ax)

- Hỗ trợ tốc độ cao, giảm độ trễ, tối ưu cho kết nối đông người.
- AP được triển khai theo sơ đồ mạng Mesh giúp mở rộng phạm vi phủ sóng.

3.5.2.4. Hệ thống bảo mật

- Firewall bảo vệ khỏi tấn công mạng, kiểm soát truy cập Internet.
- Hệ thống IDS/IPS giám sát và phát hiện nguy cơ bảo mật.

3.5.3 Mô Hình Vật Lý

3.5.3.1 Thiết bị mạng

Hệ thống mạng tại mỗi cơ sở được thiết kế để đảm bảo hiệu suất cao, bảo mật mạnh mẽ và khả năng mở rộng linh hoạt**.** Dưới đây là phân tích chi tiết về từng loại thiết bị mạng được sử dụng trong hệ thống.

Router – Kết Nối Internet và Quản Lý Mạng WAN

Vai trò:

- Kết nối mạng nội bộ (LAN) của cơ sở với Internet và các cơ sở khác qua mạng WAN.
- Xử lý định tuyến tĩnh (Static Routing) và động (OSPF, BGP, EIGRP) để tối ưu lưu lượng.
- Hỗ trợ VPN IPSec, GRE Tunnel, MPLS để đảm bảo kết nối bảo mật giữa các cơ sở.
- Tích hợp QoS (Quality of Service) để ưu tiên lưu lượng quan trọng (giảng dạy, hội nghị trực tuyến).

Mẫu thiết bị đề xuất:

Model	Thông số kỹ thuật chính	Ưu điểm
Cisco ISR 4000 Series (ISR 4331, ISR 4351, ISR 4451-X)	Hỗ trợ VPN, tường lửa ích hợp, QoS, 3-10Gbps	Bảo mật cao, quản lý ạnh, mở rộng linh hoạt
MikroTik CCR1036-8G-2S+	36 lõi CPU, 8 cổng Gigabit, 2 cổng SFP+ (10GbE)	Hiệu suất cao, giá thành ợp lý, phù hợp mạng lớn
FortiGate 100F (Tích hợp Firewall)	Tường lửa, VPN, IDS/IPS, 10GbE WAN	Bảo mật mạnh, tối ưu cho kết nối liên cơ sở

Kết nối:

- WAN: Cổng quang 10GbE hoặc 1GbE kết nối nhà mạng (FTTH, MPLS, Metro Ethernet).
- LAN: Kết nối với Switch Core (Layer 3) qua cổng quang 10GbE, đảm bảo tốc độ cao.

Switch Core (Layer 3) – Định Tuyến VLAN & Quản Lý Lưu Lượng
Vai trò:
- Định tuyến VLAN (Inter-VLAN Routing) giữa các nhóm người dùng như sinh viên, giảng viên, hành chính, phòng lab**.**
- Quản lý các kết nối tốc độ cao (10GbE - 40GbE) giữa các switch Distribution và Router.
- Hỗ trợ STP (Spanning Tree Protocol), VRRP/HSRP (dự phòng router), ACL (Access Control List) để bảo mật.
- Tích hợp PoE (Power over Ethernet) để cấp nguồn cho các thiết bị như Access Point, Camera IP.

Mẫu thiết bị đề xuất:

Model	Thông số kỹ thuật chính	Ưu điểm
Cisco Catalyst 9500 Series	24-48 cổng 10GbE/40GbE, Modular, Layer 3	Định tuyến nhanh, bảo mật tốt, hỗ trợ nhiều VLAN
Aruba CX 6400 Series	Modular, 10GbE/40GbE, Hỗ trợ PoE++	Hiệu suất cao, bảo mật mạnh, dễ mở rộng
Juniper EX4650	25GbE/100GbE, Hỗ trợ VXLAN, EVPN	Hiệu suất mạnh, hỗ trợ mạng SDN

Kết nối:
- Với Switch Core: Cáp quang 10GbE để giảm nghẽn mạng.
- Với thiết bị đầu cuối: Cáp đồng Cat6a / Cat7 (1GbE/10GbE).

Access Point (AP) – Hỗ Trợ Wi-Fi 6, Phủ Sóng Toàn Cơ Sở
Vai trò:
- Cung cấp Wi-Fi 6 (802.11ax) tốc độ cao, giảm nhiễu và hỗ trợ nhiều kết nối đồng thời.
- Hỗ trợ MU-MIMO, OFDMA để tăng hiệu suất kết nối khi có nhiều người dùng.
- Tích hợp Mesh Networking, giúp mở rộng vùng phủ sóng mà không cần dây mạng bổ sung.
- Quản lý SSID, VLAN, Captive Portal (đăng nhập mạng Wi-Fi qua xác thực).
- Hỗ trợ WPA3, RADIUS authentication, đảm bảo bảo mật khi truy cập.

Mẫu thiết bị đề xuất:

Model	**Chuẩn Wi-Fi**	**Ưu điểm**
Cisco Aironet 9130AX	Wi-Fi 6, 4x4 MU-MIMO, PoE+	Bảo mật cao, hiệu suất mạnh, phù hợp không gian lớn
Aruba AP 515	Wi-Fi 6, Dual-band, PoE	Giá hợp lý, hiệu suất ổn định

Model	Chuẩn Wi-Fi	Ưu điểm
Ubiquiti UniFi 6 LR	Wi-Fi 6, 5GHz/2.4GHz, 4x4 MU-MIMO	Giá rẻ, phù hợp trường học, văn phòng

Bố trí AP:

- Lắp đặt trên trần nhà hoặc trong phòng hoặc trên bờ tường để tránh vật cản, tối ưu vùng phủ sóng.
- Triển khai theo Mesh Wi-Fi để mở rộng vùng phủ sóng mà không bị mất tín hiệu.
- Kết nối qua switch Access Layer 2 bằng PoE, giảm dây nguồn rườm rà.

Tổng Kết Sơ Bộ

Thiết Bị	Mẫu Đề Xuất	Chức Năng Chính
Router	Cisco ISR 4000, MikroTik CCR1036	Kết nối WAN, định tuyến liên cơ sở
Switch Core (Layer 3)	Cisco Catalyst 9500, Aruba CX 6400	Định tuyến VLAN, quản lý lưu lượng lớn
Switch Access (Layer 2)	Cisco Catalyst 9200, Aruba 2930F	Kết nối thiết bị đầu cuối, hỗ trợ PoE
Access Point (Wi-Fi 6)	Cisco Aironet 9130AX, Aruba AP 500	Cung cấp Wi-Fi tốc độ cao

Hệ thống này đảm bảo tốc độ, bảo mật và dễ dàng mở rộng trong tương lai**.**

3.5.3.2 Cáp Kết Nối Giữa Các Thiết Bị Mạng

+ Cáp Quang – Kết Nối Trục Chính (Backbone Connection)

Vai trò:

- Dùng để kết nối Router ⇄ Switch Core **và** Switch Core ⇄ Switch Access với băng thông cao (10GbE - 40GbE).
- Giảm độ trễ, chống nhiễu điện từ (EMI/RFI), truyền dữ liệu xa hơn (100m - 10km).
- Bảo đảm tốc độ ổn định cho hệ thống mạng nội bộ và liên kết giữa các khu vực.

Loại cáp quang đề xuất:

Loại Cáp	Chuẩn Sợi Quang	Băng Thông Hỗ Trợ	Khoảng Cách Tối Đa	Ứng Dụng
Cáp quang Single-Mode (OS2)	9µm	10Gbps - 100Gbps	10km - 40km	Kết nối Router - Switch Core, liên kết giữa các cơ sở
Cáp quang Multi-Mode (OM3, OM4)	50µm	10Gbps - 40Gbps	300m - 500m	Kết nối Switch Core - Switch Access

Nên sử dụng:
- Router → Switch Core: Cáp quang Single-Mode (OS2), chuẩn LC-LC hoặc SC LC, tốc độ 10GbE - 40GbE.
- Switch Core → Switch Access: Cáp quang Multi-Mode (OM3/OM4), chuẩn LC-LC, tốc độ 10GbE để tối ưu chi phí.

Module quang (Transceiver) đề xuất:
- Cisco SFP-10G-LR (Single-Mode, khoảng cách lên đến 10km).
- Cisco SFP-10G-SR (Multi-Mode, khoảng cách 300m).
- Aruba J9150D (10GbE SR), J8177C (1GbE SX).

Cáp Đồng Ethernet – Kết Nối Thiết Bị Đầu Cuối:

- Sử dụng cáp Dây Cáp Đồng Trục Cat6e FTP và cap quang để kết nối các thiết bị mạng trong từng cơ sở, đảm bảo tốc độ truyền tải cao và ổn định.

a) Bố trí thiết bị

Việc bố trí thiết bị mạng hợp lý tối ưu hóa hiệu suất, đảm bảo vùng phủ sóng rộng rãi và duy trì kết nối ổn định. Dưới đây là kế hoạch chi tiết về cách bố trí Router, Switch, Access Point (AP) và các thiết bị mạng khác trong mỗi cơ sở.

Nguyên Tắc Bố Trí Thiết Bị Mạng

Router, Switch Core:
- Đặt trong Phòng Máy Chủ (Server Room) để bảo vệ thiết bị và dễ dàng quản lý.
- Có hệ thống tản nhiệt, UPS dự phòng, đảm bảo nguồn điện ổn định.
- Kết nối bằng cáp quang để tối ưu tốc độ giữa các khu vực.

Switch Access:
- Lắp đặt trong Tủ Rack (Network Cabinet) tại mỗi tầng/khu vực, tránh tiếp xúc môi trường bên ngoài.
- Kết nối Switch Core bằng cáp quang để đảm bảo băng thông cao.
- Hỗ trợ PoE (Power over Ethernet) để cấp nguồn cho Access Point, Camera IP, Điện thoại IP.

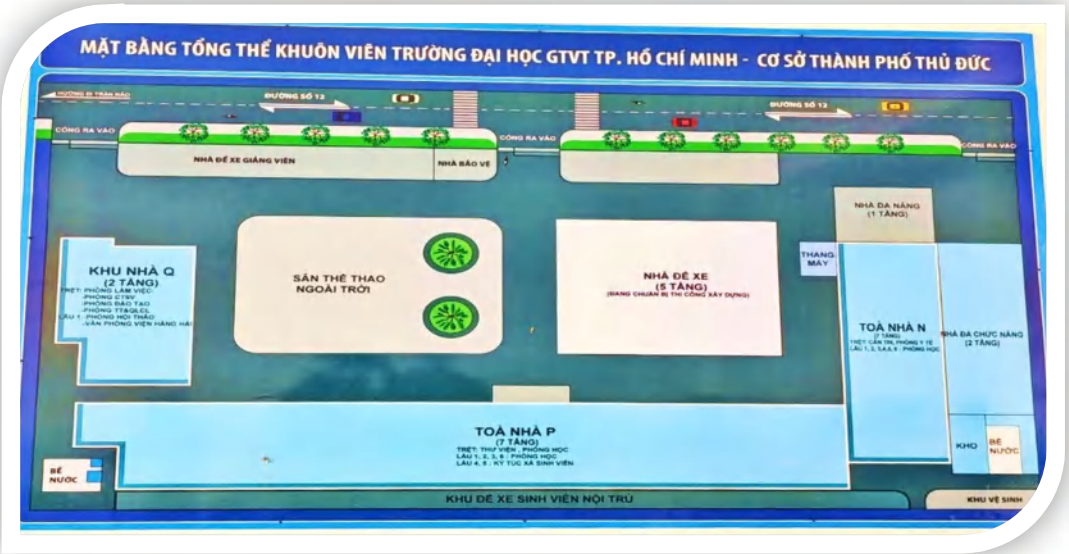
Access Point (AP) – Wi-Fi 6:

- Mô hình tập trung (Hub-and-Spoke): Đây là mô hình chính được sử dụng trong cả 3 thiết kế. Có một hoặc vài thiết bị trung tâm (router/switch) đóng vai trò là trung tâm điều phối và kết nối tất cả các thiết bị khác. Các nhánh (spokes) từ trung tâm tỏa ra đến các phòng ban, khu vực.
- Phân cấp (Hierarchical): Mô hình này cũng được sử dụng, đặc biệt ở phần kết nối giữa các router/switch trung tâm. Có thể thấy một vài router/switch trung tâm kết nối với nhau theo một cấu trúc phân cấp.- AP treo trần (Ceiling Mount) hoặc gắn tường ở hành lang, phòng học, phòng Lab.
- Mỗi AP hỗ trợ tối đa 250 - 300 người dùng, phân bổ hợp lý theo mật độ người dùng.

b) Mô hình vật lý

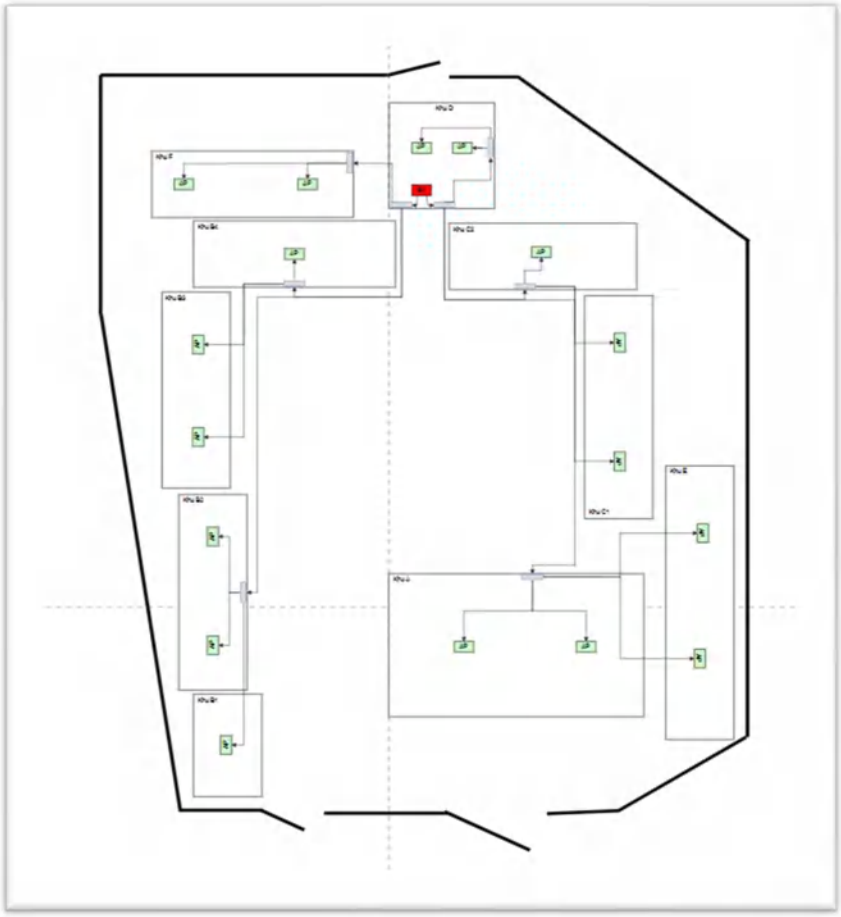
Nguyên tắc thiết kế mô hình vật lý dựa theo mặt bằng tổng thể: Tầng kiến trúc mạng 3 lớp (Three-Tier Architecture):

Hình 4. Mặt bằng tổng thể CS1

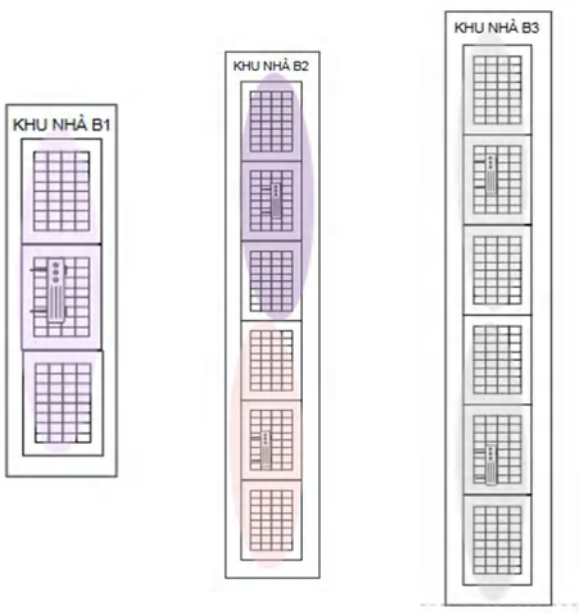


Hình 5. Mặt bằng tổng thể CS2

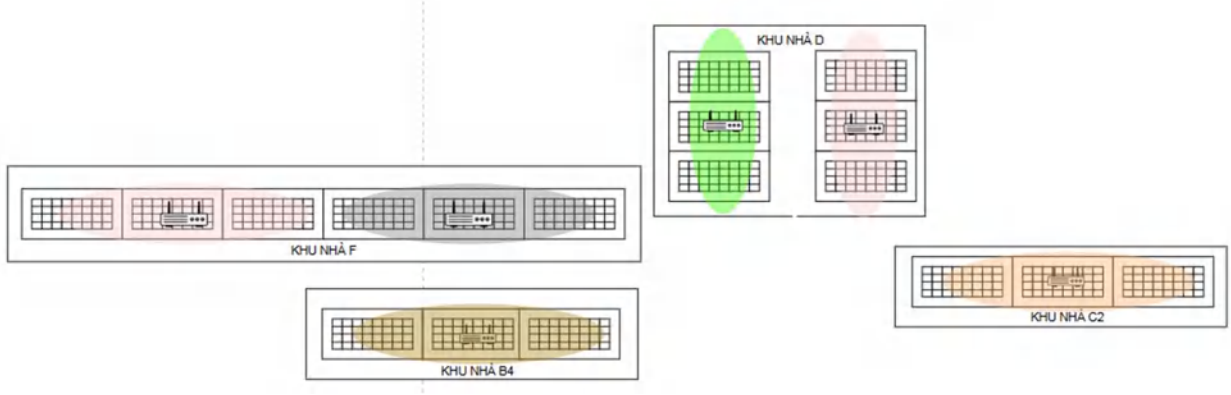
Hình 6. Mặt bằng tổng thể CS3



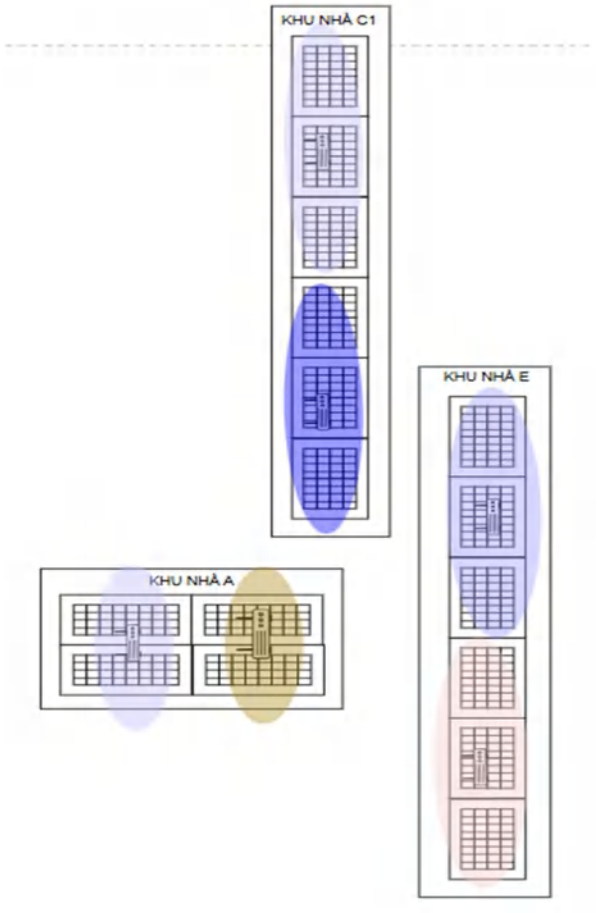
Hình 7. Sơ đồ vật lý CS1



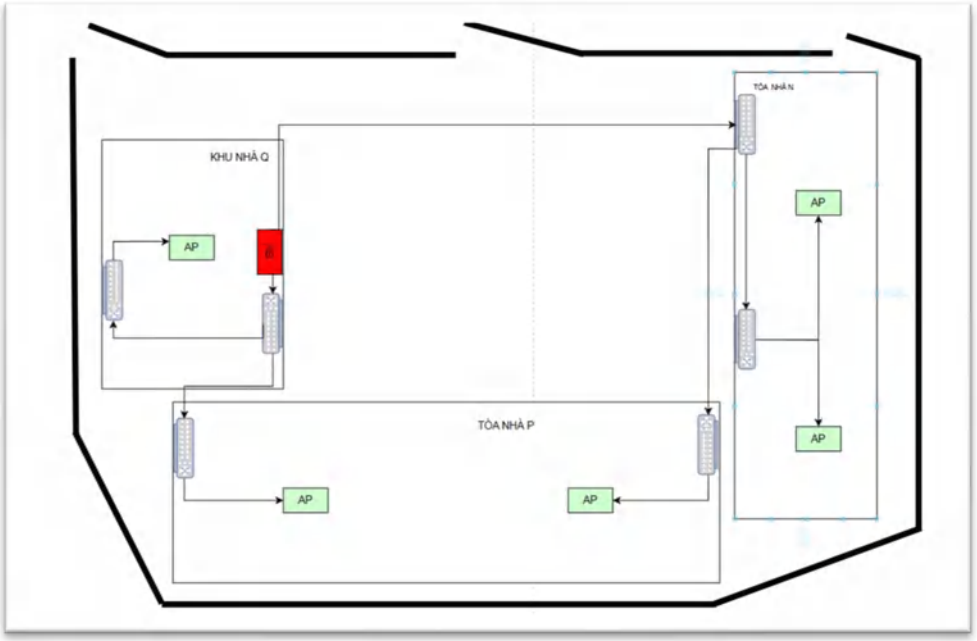
Hình 8. Sơ đồ chi tiết Khu B1 – B2 – B3 - CS1



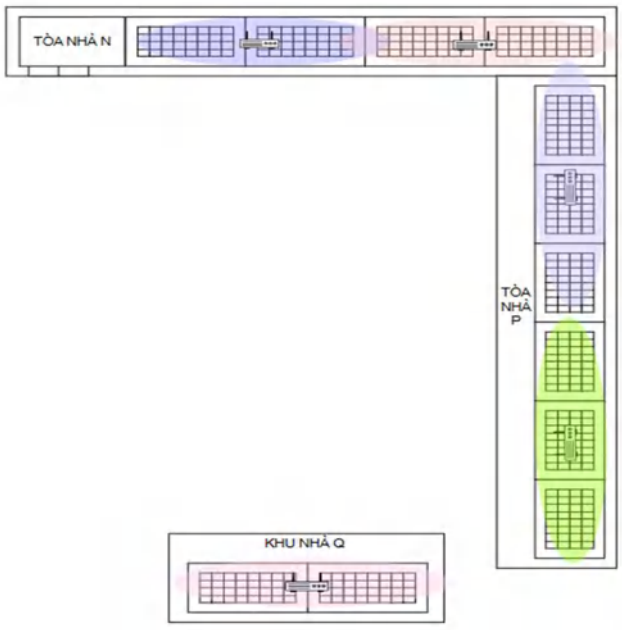
Hình 9. Sơ đồ chi tiết Khu B4 – F – D – C2 - CS1



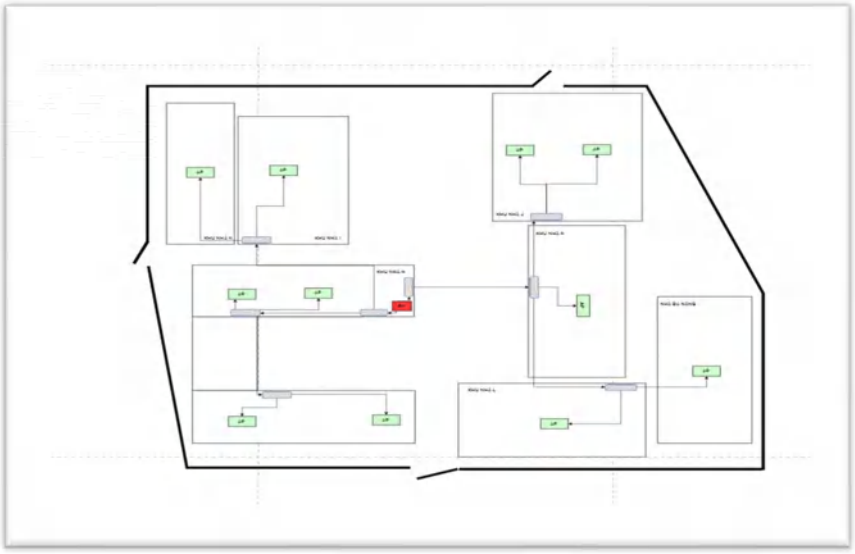
Hình 10. Sơ đồ chi tiết Khu A – E – C1 - CS1



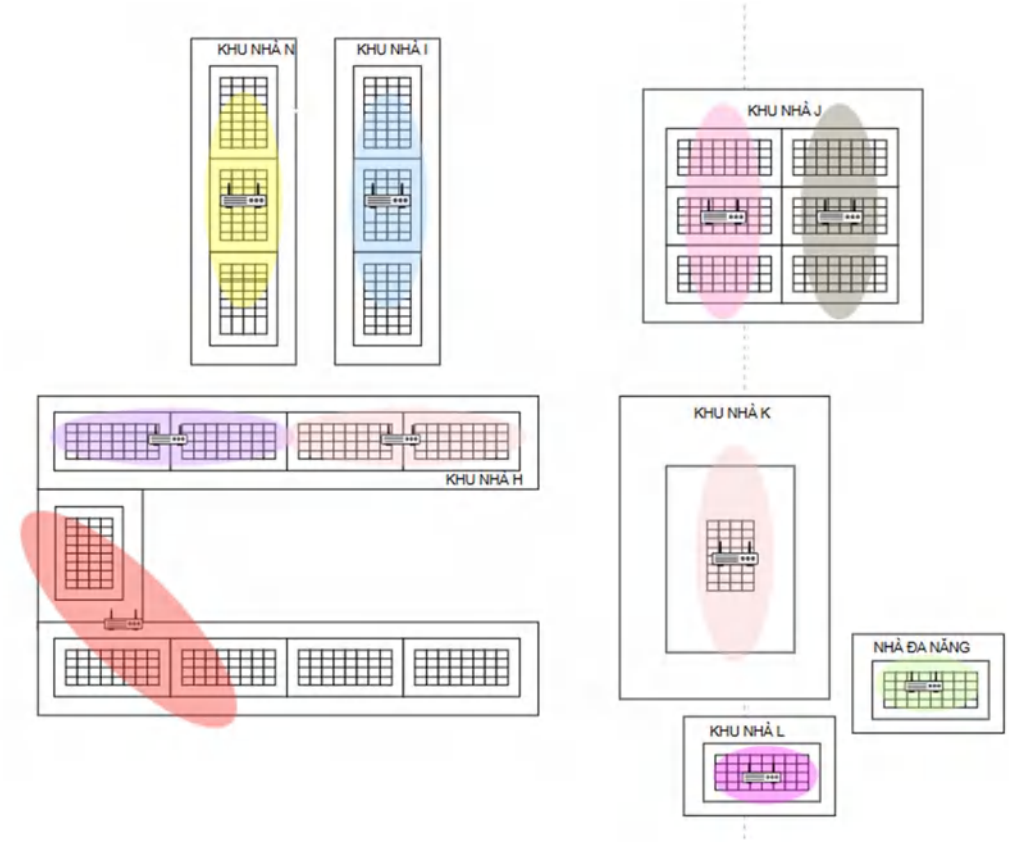
Hình 11. Sơ đồ vật lý CS2



Hình 12. Sơ đồ chi tiết các tòa – CS2



Hình 13. Sơ đồ vật lý CS3



Hình 14. Sơ đồ chi tiết các tòa - CS3

Phân chia VLAN:

- Tạo VLAN cho từng nhóm người dùng (giảng viên, sinh viên, nhân viên) nhằm quản lý lưu lượng và bảo mật tốt hơn.

Kết nối VPN:

- Sử dụng công nghệ VPN để bảo mật kết nối giữa các cơ sở và đảm bảo tính riêng tư trong việc truyền tải dữ liệu.

3.6 Lựa Chọn Thiết Bị

Thiết bị mạng:

- Chọn router, switch và Access Point hiện đại hỗ trợ chuẩn Wi-Fi 6 để đảm bảo tốc độ và độ ổn định cao.
- Các thiết bị phải có khả năng quản lý băng thông, hỗ trợ các tính năng bảo mật và tương thích với nhau.

3.7 Triển Khai Hạ Tầng Mạng

Lắp đặt thiết bị mạng:

- Cấu hình các thiết bị như router, switch, firewall và server tại mỗi cơ sở
- Thiết lập hệ thống server tập trung để lưu trữ dữ liệu và quản lý truy cập
- Cài đặt các thiết bị Wi-Fi cho các khu vực trong và ngoài khuôn viên.
- Kiểm tra và tối ưu hóa vị trí lắp đặt để đảm bảo tín hiệu mạnh và ổn định cho toàn bộ người dùng.

CHƯƠNG 4: CÁC THIẾT BỊ VÀ ỨNG DỤNG DỰ KIẾN SỬ DỤNG

4.1 Các thiết bị

- Router: Router Cisco ISR4431-SEC/K9
- Access Point (AP): Access Point Ubiquiti UniFi AP AC LR
- Switch: NETGEAR GS748T
- Dây cáp Đồng Trục Cat5e FTP, Cat6e FTP
- Cáp quang Singlemode 12Fo (DB 12 core)

4.1.1 Phân tích nhu cầu sử dụng cho ba cơ sở

a) File Server

- Chức năng: Lưu trữ dữ liệu quan trọng như tài liệu, hình ảnh, cơ sở dữ liệu.
- Tính năng: Đảm bảo tính bảo mật và khả năng truy cập cao cho 100 nhân viên.
- Yêu cầu mở rộng: Khả năng mở rộng dung lượng lưu trữ trong tương lai.

b) Application Server

- Chức năng: Chạy các ứng dụng quan trọng như phần mềm quản lý bán hàng, nhân sự, kế toán.
- Tính năng: Đảm bảo hiệu năng cao và khả năng xử lý nhanh cho các ứng dụng.
- Khả năng chịu tải: Đáp ứng cho nhiều người sử dụng đồng thời.

c) Web Server/Mail Server

- Chức năng: Cung cấp dịch vụ web và email cho doanh nghiệp.
- Tính năng: Đảm bảo tính ổn định và khả năng truy cập cao.
- Khả năng bảo mật: Đảm bảo an toàn trước các tấn công mạng.

d) DHCP Server

- Chức năng: Cung cấp địa chỉ IP tự động cho các thiết bị trong mạng để đảm bảo kết nối ổn định.
- Tính năng: Quản lý và phân phối địa chỉ IP một cách hiệu quả cho tất cả các thiết bị, giảm thiểu khả năng xung đột địa chỉ.
- Khả năng mở rộng: Đáp ứng nhu cầu mở rộng trong tương lai khi có thêm thiết bị mới kết nối vào mạng.

e) Data Server

- Chức năng: Lưu trữ và quản lý dữ liệu lớn, phục vụ cho các ứng dụng phân tích và báo cáo.
- Tính năng: Cung cấp khả năng truy cập nhanh chóng và hiệu quả cho người dùng để xử lý các truy vấn dữ liệu phức tạp.
- Khả năng mở rộng: Hỗ trợ mở rộng dung lượng lưu trữ và khả năng xử lý khi nhu cầu dữ liệu tăng lên trong tương lai.

f) DNS Server (thuê dịch vụ của FPT)

- Chức năng: Chuyển đổi tên miền thành địa chỉ IP để các thiết bị có thể truy cập vào dịch vụ mạng dễ dàng hơn.
- Tính năng: Cung cấp khả năng phân giải tên miền nhanh chóng và chính xác cho

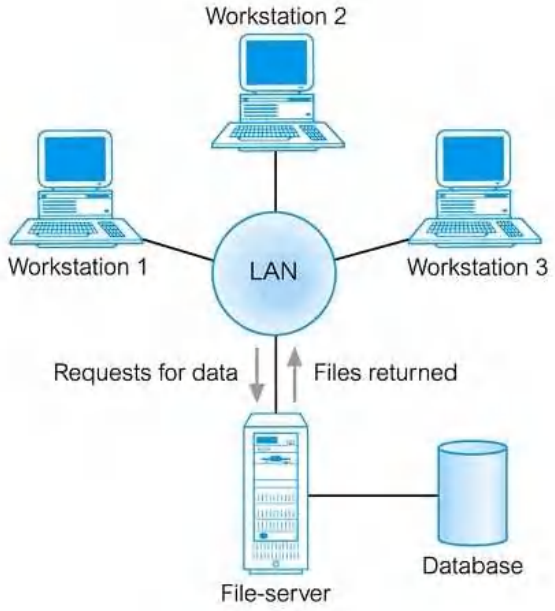
các ứng dụng và dịch vụ của doanh nghiệp.
- Khả năng bảo mật: Đảm bảo thông tin tên miền được bảo vệ trước các cuộc tấn công và rò rỉ dữ liệu.

4.2 Đề xuất cấu hình chi tiết

4.2.1 Cấu hình chi tiết cụ thể cho từng thiết bị

a) File Server:

Cơ sở	Cấu hình	Ghi chú
Tất cả	- CPU: Intel Xeon E3/E5 - RAM: 8GB DDR4 - HDD: 2x240GB SSD (RAID 1) - NIC: 2x1Gbps	Có thể thuê ngoài (FPT, Viettel), hoặc cài đặt DNS nội bộ với BIND/Windows DNS Server

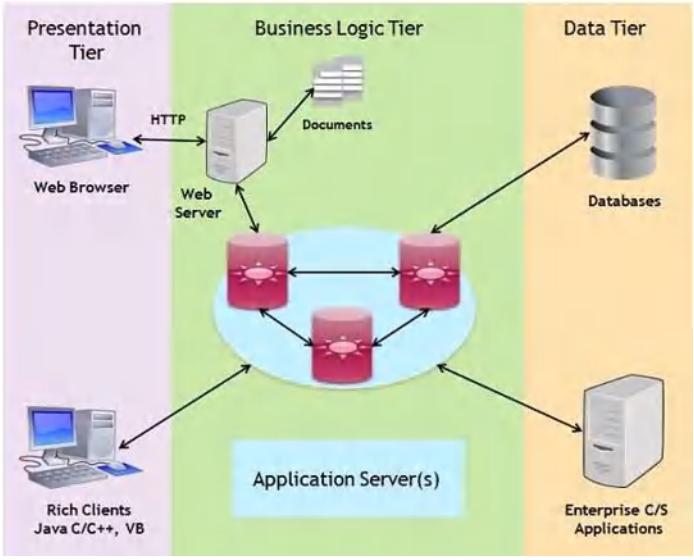


Hình 20. File Server

a) Application Server: Dell PowerEdge

Cơ sở	Cấu hình	Ghi chú
CS1	- CPU: Xeon Silver - RAM: 32GB - SSD: 512GB	Triển khai API backend, xử lý nghiệp vụ nội bộ (học vụ, điểm danh, lịch thi)

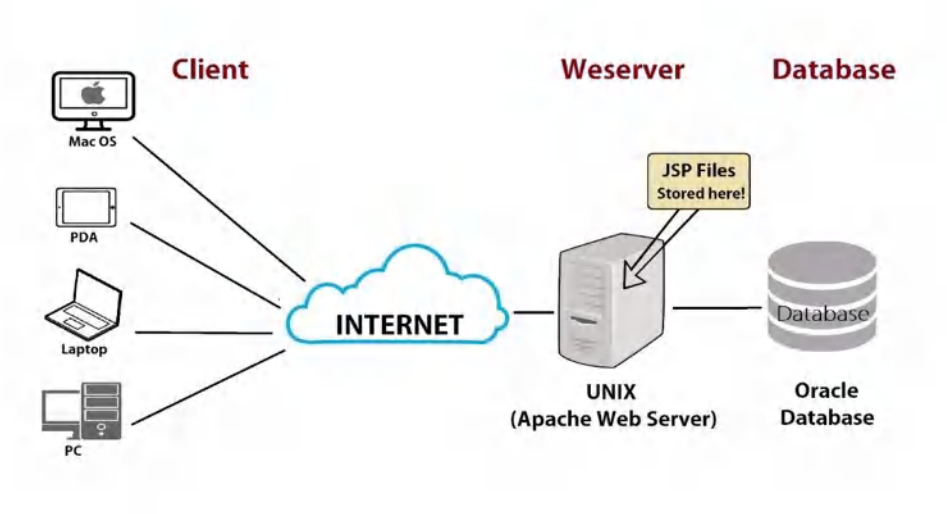
Cơ sở	Cấu hình	Ghi chú
CS2, CS3	- CPU: Intel Xeon E3 - RAM: 16GB - SSD: 240GB	Nếu cần ứng dụng độc lập, có thể cài app microservice riêng



Hình 21. Application Server

c) Web Server/Mail Server: Dell PowerEdge

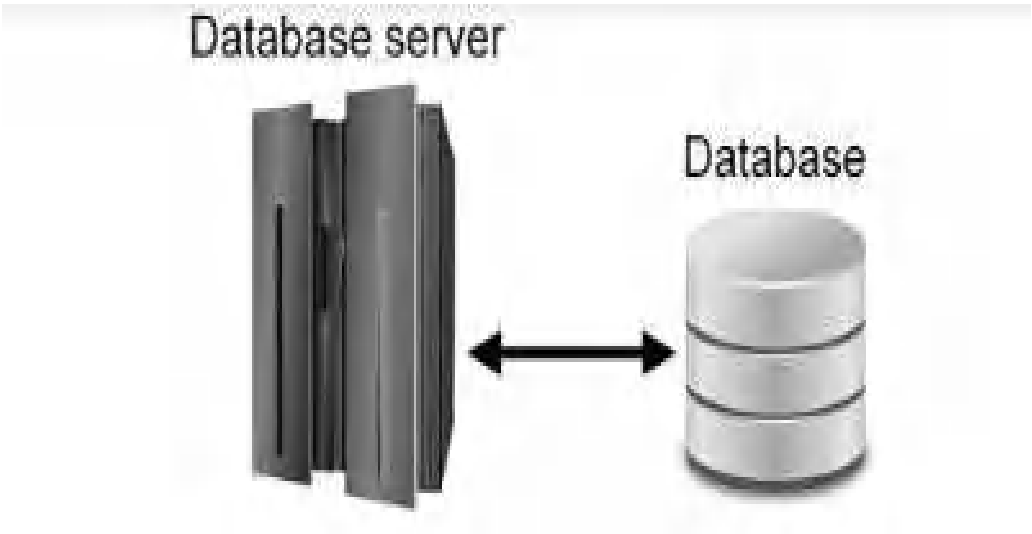
Cơ sở	Cấu hình	Ghi chú
CS1 (Bình Thạnh)	- CPU: Intel Xeon E-2288G - RAM: 32GB - SSD: 2x512GB - NIC: 2x1Gbps	- Chạy các ứng dụng web (quản lý đào tạo, tài khoản nội bộ, thông báo học vụ) - Mail Server sử dụng Postfix + Dovecot hoặc Microsoft Exchange
CS2, CS3	Không cần triển khai riêng, sử dụng dịch vụ từ CS1 hoặc cloud	



Hình 22. Web Server/Mail Server

d) Database Server:

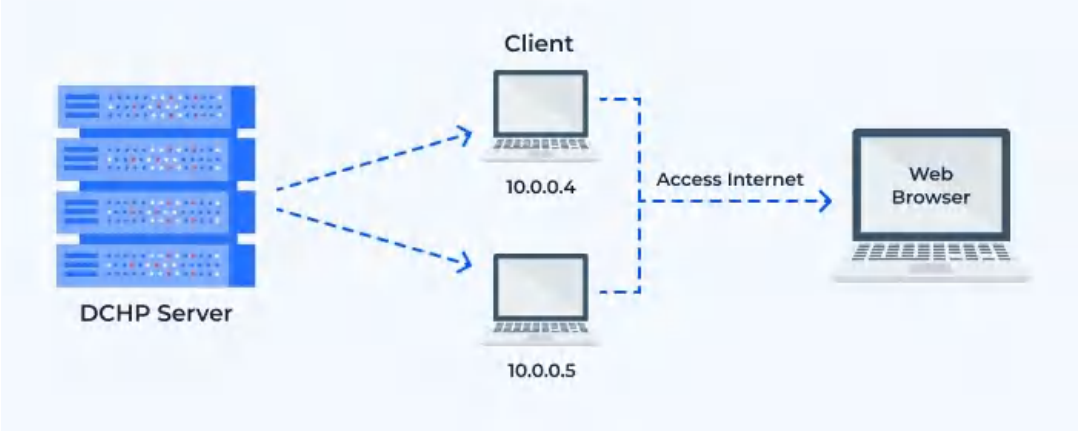
Cơ sở	Cấu hình	Ghi chú
CS1 (Bình Thạnh - trung tâm dữ liệu chính)	- CPU: 2x Intel Xeon Silver 4210 - RAM: 64GB ECC - Storage: 4x1TB SSD (RAID 10) - NIC: 2x10Gbps	Chứa toàn bộ CSDL của hệ thống: điểm danh, quản lý sinh viên, thiết bị, tài khoản, ứng dụng nội bộ
CS2, CS3	Chỉ cần truy cập CSDL trung tâm (CS1)	Backup định kỳ hoặc Mirroring



Hình 23. Database Server

e) DHCP Server:

Cơ sở	Cấu hình	Ghi chú
CS1 (Bình Thạnh)	- CPU: Xeon Silver 4210 - RAM: 16GB ECC - SSD: 240GB - NIC: 2x1Gbps	Phục vụ ~1.500 user
CS2 (Thủ Đức)	- CPU: Xeon E-2224G - RAM: 12GB - SSD: 240GB - NIC: 2x1Gbps	Phục vụ ~1.800 user
CS3 (Q.12)	- CPU: Xeon E-2224G - RAM: 12GB - SSD: 240GB - NIC: 2x1Gbps	Phục vụ ~2.200 user



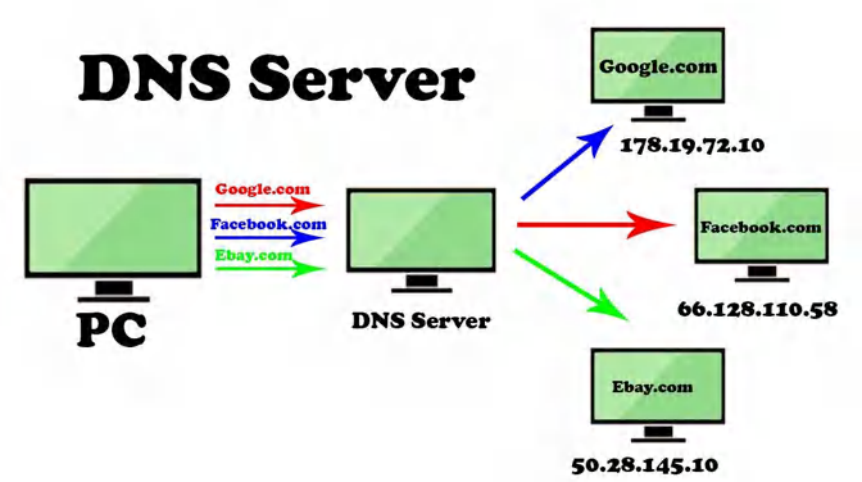
Hình 24. DHCP Server

f) DNS Server:

Cơ sở	Cấu hình	Ghi chú
Tất cả	- CPU: Intel Xeon E3/E5 - RAM: 8GB DDR4	Có thể thuê ngoài (FPT, Viettel), hoặc cài đặt DNS nội bộ với

Cơ sở	Cấu hình	Ghi chú
	- HDD: 2x240GB SSD (RAID 1) - NIC: 2x1Gbps	BIND/Windows DNS Server

Hình 25. DNS Server



4.3 Một số công nghệ được sử dụng

4.3.1 VLAN (Virtual Local Area Network)

Khái niệm:

- VLAN là mạng LAN ảo, cho phép tạo ra các miền quảng bá trên switch mà không cần đến router. Điều này giúp các thiết bị trong cùng một VLAN giao tiếp với nhau mà không cần phải truyền tải thông tin qua mạng LAN lớn hơn.

Phân loại VLAN:

- Port-based VLAN: Các cổng trên switch được cấu hình thành các VLAN khác nhau.
- MAC address-based VLAN: VLAN được phân chia dựa trên địa chỉ MAC của thiết bị.
- Protocol-based VLAN: VLAN được phân chia theo giao thức mạng.

Lợi ích:

- Tiết kiệm băng thông: VLAN giúp phân chia mạng LAN thành các đoạn khác nhau, giảm thiểu lưu lượng quảng bá.
- Tăng cường bảo mật: Các VLAN khác nhau không thể truy cập vào nhau trừ khi có định tuyến được cấu hình.
- Tính linh động cao: Có thể dễ dàng di chuyển và cấu hình các thiết bị trong VLAN.

Kết luận:

Việc áp dụng VLAN trong thiết kế mạng cho ba cơ sở của trường giúp tăng hiệu suất mạng LAN và bảo mật thông tin, đặc biệt khi số lượng máy tính và lưu lượng truyền tải tăng cao.

4.3.2 VPN (Virtual Private Network)

Khái niệm:

- VPN tạo ra kết nối mạng riêng tư giữa các thiết bị thông qua Internet, cho phép truyền dữ liệu an toàn và ẩn danh.

Phân loại:

- Site-to-Site: Kết nối mạng giữa hai hoặc nhiều địa điểm khác nhau.
- Remote Access: Kết nối từ xa cho người dùng cá nhân và nội bộ.

Công dụng:

- Quyền riêng tư: Bảo vệ dữ liệu cá nhân qua mã hóa.
- Tính ẩn danh: Ẩn địa chỉ IP của người dùng.
- Bảo mật: Bảo vệ kết nối Internet khỏi truy cập trái phép.

Ưu - Nhược điểm:

- Ưu điểm: Bảo vệ an ninh cho dữ liệu cá nhân, khó xâm nhập từ tin tặc.
- Nhược điểm: Một số trang web có thể hạn chế truy cập từ VPN; có thể bị lạm dụng cho các hoạt động trái pháp luật.

4.3.3 DHCP và DNS Server

Khái niệm:

- DHCP (Dynamic Host Configuration Protocol): Giao thức tự động gán địa chỉ IP cho các thiết bị trong mạng.
- DNS (Domain Name System): Hệ thống dịch tên miền thành địa chỉ IP, hoạt động như một "danh bạ" trên Internet.

Công dụng:

- DHCP: giảm thời gian cấu hình mạng và quản lý địa chỉ IP một cách hiệu quả.
- DNS: Giúp định vị và địa chỉ hóa các thiết bị trên Internet.

Ưu - Nhược điểm:

- DHCP: Tăng tốc độ kết nối mạng, nhưng không phù hợp với thiết bị cố định như máy in.
- DNS: Tăng tốc độ Internet nhưng có thể sự cố nếu máy chủ DNS gặp vấn đề.

4.3.4 MIMO (Multiple Input Multiple Output)

Khái niệm:

- MIMO là công nghệ sử dụng nhiều ăng-ten để phát và thu tín hiệu trong kết nối không dây, giúp cải thiện hiệu suất mạng Wi-Fi.

Lợi ích:

- Tăng tốc độ truyền dữ liệu: Sử dụng nhiều anten cho phép tăng cường tốc độ truyền dữ liệu mà không cần tăng tần số.
- Cải thiện hiệu suất kết nối: Giảm tắc nghẽn mạng bằng cách cung cấp nhiều

đường truyền song song.
- Tăng cường độ phủ sóng: Cải thiện khả năng phủ sóng của mạng WiFi.
Phân loại:
- SU-MIMO (Single-User MIMO): Phục vụ một thiết bị người dùng duy nhất.
- MU-MIMO (Multi-User MIMO): Cho phép truyền dữ liệu cho nhiều thiết bị cùng lúc.
Ưu điểm của công nghệ MU-MIMO:
- Giảm độ trễ và tăng băng thông, giúp nâng cao trải nghiệm người dùng.
Tăng tốc độ truyền tải dữ liệu cho cả thiết bị cũ và mới.

4.4 Ứng dụng của MIMO trong mạng không dây:

- Wi-Fi: MIMO được sử dụng phổ biến trong các tiêu chuẩn Wi-Fi hiện đại như 802.11n và 802.11ac, giúp cải thiện tốc độ và độ ổn định của kết nối.
- Mạng di động: Công nghệ MIMO cũng được ứng dụng trong mạng di động 4G LTE và 5G, cho phép truyền dữ liệu nhanh hơn và hiệu quả hơn giữa các thiết bị di động.

KẾT LUẬN

1. Đã đạt được:

Sau quá trình nghiên cứu, thiết kế và mô phỏng, hệ thống mạng đã được triển khai thành công với các kết quả chính sau:

***Thiết kế mô hình mạng IP tối ưu**:* Hệ thống mạng được phân chia hợp lý theo từng cơ sở, đảm bảo khả năng mở rộng, tính ổn định và hiệu suất cao. Việc phân đoạn mạng dựa trên số lượng người dùng tại mỗi địa điểm giúp tối ưu tài nguyên và giảm tắc nghẽn.

***Cấu hình VLAN khoa học**:* Mạng nội bộ được chia thành các VLAN riêng biệt cho sinh viên, giảng viên, phòng lab, hành chính và các dịch vụ khác, giúp tăng cường bảo mật, quản lý lưu lượng hiệu quả và nâng cao chất lượng truy cập.

***Kết nối định tuyến tối ưu**:* Các router đã được cấu hình để đảm bảo lưu lượng giữa các phân đoạn mạng tại mỗi cơ sở và kết nối giữa các cơ sở hoạt động trơn tru. Điều này giúp duy trì sự liền mạch trong hệ thống và tối đa hóa tốc độ truyền tải dữ liệu.

***Lựa chọn và cấu hình thiết bị mạng phù hợp**:* Hệ thống sử dụng các thiết bị switch, router và access point có khả năng chịu tải cao, phù hợp với nhu cầu sử dụng thực tế, đảm bảo hiệu suất hoạt động ổn định cho hàng nghìn người dùng đồng thời.

***Mô phỏng và kiểm thử thực tế trên Packet Tracer**:* Dự án đã được thử nghiệm với các mô hình giả lập trên Cisco Packet Tracer, cho phép kiểm tra hiệu quả thiết kế, phát hiện và điều chỉnh các điểm chưa tối ưu trước khi triển khai thực tế.

2. Tổng quan hệ thống mạng

Hệ thống mạng được thiết kế để phục vụ ba cơ sở chính của Đại học Giao thông Vận tải TP.HCM, đảm bảo kết nối ổn định và hiệu quả cho tổng số hơn 18.000 sinh viên, giảng viên và nhân viên.

***Cơ sở Bình Thạnh (CS1)**:* Quy mô 4.500 – 5.500 người, hỗ trợ 2.300 – 2.800 kết nối đồng thời.

***Cơ sở Thủ Đức (CS2)**:* Quy mô 3.500 – 4.500 người, hỗ trợ 1.300 – 1.800 kết nối đồng thời.

***Cơ sở Quận 12 (CS3)**:* Quy mô 3.800 – 4.200 người, hỗ trợ 1.700 – 2.200 kết nối đồng thời.

Mỗi cơ sở đều có các khu vực được phân tách rõ ràng như phòng học, phòng giảng viên, phòng lab, khu hành chính và các dịch vụ khác.

3. Kiến trúc mạng và phân chia tài nguyên:

Hệ thống IP được thiết kế với quy hoạch hợp lý, đảm bảo mở rộng trong tương lai mà không ảnh hưởng đến hiệu suất.

Mô hình VLAN được triển khai nhằm phân bổ tài nguyên theo nhu cầu sử dụng, giúp kiểm soát lưu lượng và bảo vệ dữ liệu.

Cấu trúc mạng đảm bảo tính bảo mật, hạn chế rủi ro truy cập trái phép và tối ưu hiệu suất hệ thống.

4. Kết nối định tuyến và quản lý hệ thống

- Các router được cấu hình với giao thức định tuyến phù hợp, giúp tối ưu hóa tốc độ truy cập và duy trì tính liền mạch giữa các phân đoạn mạng.
- Hệ thống switch và access point được lựa chọn với công suất phù hợp để đáp ứng nhu cầu sử dụng đồng thời của hàng nghìn người dùng mà không làm giảm hiệu suất.

5. Thách thức và hạn chế

Mặc dù hệ thống mạng đã được thiết kế và mô phỏng thành công, vẫn còn một số thách thức cần được giải quyết khi triển khai thực tế:

Khả năng kiểm thử thực tế hạn chế: Do môi trường mô phỏng không thể hoàn toàn tái hiện điều kiện thực tế, việc đánh giá hiệu suất khi hệ thống chịu tải lớn vẫn cần được theo dõi trong quá trình vận hành.

Quản lý băng thông và tối ưu hóa hiệu suất: Khi số lượng người dùng tăng đột biến, đặc biệt trong giờ cao điểm, cần có các cơ chế giám sát và điều chỉnh tài nguyên linh hoạt hơn.

6. Giá trị đạt được

Dự án không chỉ giúp hoàn thiện hệ thống mạng cho một tổ chức có quy mô lớn mà còn mang lại nhiều kinh nghiệm thực tiễn quan trọng:

Hiểu sâu về thiết kế và triển khai mạng doanh nghiệp: từ lý thuyết đến mô phỏng thực tế.

Nắm vững kỹ năng cấu hình thiết bị mạng: bao gồm router, switch và access point.

Cải thiện kỹ năng làm việc nhóm và lập kế hoạch: khi phối hợp để triển khai dự án từ đầu đến cuối.

Phát triển kỹ năng phân tích và giải quyết vấn đề: đặc biệt trong việc tối ưu hóa hiệu suất và bảo mật mạng.

Dự án này là nền tảng quan trọng cho các triển khai thực tế sau này, đồng thời góp phần nâng cao khả năng ứng dụng công nghệ mạng trong thực tiễn.

TÀI LIỆU THAM KHẢO

[1] Akamai Technologies. (n.d.). *Akamai Network: Content Delivery Network and the Internet*. Coursera. https://www.coursera.org/learn/akamai-networking

[2] Cisco. (n.d.). *What is network design?*. Cisco. https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-design.html#~features

[3] Cisco. (n.d.). *Cloud-managed Catalyst: The future of networking* [Infographic]. Cisco. https://www.cisco.com/c/m/en_us/solutions/enterprise-networks/nb-06-cloud-managed-catalyst-infograph.html

[4] Cisco. (n.d.). *Networking products*. Cisco. https://www.cisco.com/site/us/en/products/networking/index.html

[5] Cisco. (n.d.). *Site survey guidelines for WLAN deployment*. Cisco. https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html

[6] Cisco Systems. (n.d.). *Cisco validated design: Campus LAN and wireless LAN design guide*. Cisco. Retrieved April 9, 2025, from https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html

[7] Cisco Systems. (n.d.). *WLAN Site Survey and Planning Considerations*. Cisco. Retrieved April 9, 2025, from https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html

[8] Huawei. (n.d.). *Site survey*. Huawei Support. https://support.huawei.com/enterprise/en/doc/EDOC1000113315/445b8ff2/site-survey

[9] Huawei Technologies Co., Ltd. (n.d.). *iMaster NCE-Campus*. Huawei Enterprise Support. Retrieved April 9, 2025, from https://support.huawei.com/enterprise/en/network-management-control-analysis/imaster-nce-campus-pid-250852420

[10] Microsoft. (n.d.). *Introduction to networking fundamentals*. Microsoft Learn. https://learn.microsoft.com/en-us/training/modules/network-fundamentals/

[11] Microsoft. (n.d.). *Windows network architecture and the OSI model*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-

hardware/drivers/network/windows-network-architecture-and-the-osi-model

[12] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., & Lear, E. (1996). *Address Allocation for Private Internets* (RFC 1918). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc1918

[13] Saylor, P. (1991). *TCP/IP tutorial* (RFC 1180). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc1180