KHOA KỸ THUẬT VÀ CÔNG NGHỆ
BỘ MÔN CÔNG NGHỆ THÔNG TIN

ĐỒ ÁN CƠ SỞ NGÀNH

HỌC KỲ I, NĂM HỌC 2023 - 2024

THIẾT KẾ HỆ THỐNG MẠNG MÁY TÍNH TẠI TRƯỜNG THPT DƯƠNG HÁO HỌC

Giáo viên hướng dẫn:
Ths. Dương Ngọc Vân Khanh

Sinh viên thực hiện:
Họ tên: Trương Nguyễn Hoàng Thanh
MSSV: 110121101
Lớp: DA21TTB

Trà Vinh, tháng 01 năm 2024.

KHOA KỸ THUẬT VÀ CÔNG NGHỆ
BỘ MÔN CÔNG NGHỆ THÔNG TIN

ĐỒ ÁN CƠ SỞ NGÀNH

HỌC KỲ I, NĂM HỌC 2023 - 2024

THIẾT KẾ HỆ THỐNG MẠNG MÁY TÍNH TẠI TRƯỜNG THPT DƯƠNG HÁO HỌC

Giáo viên hướng dẫn:
Ths. Dương Ngọc Vân Khanh

Sinh viên thực hiện:
Họ tên: Trương Nguyễn Hoàng Thanh
MSSV: 110121101
Lớp: DA21TTB

Trà Vinh, tháng 01 năm 2024.

NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....

Trà Vinh, ngày ..... tháng …… năm ……

Giáo viên hướng dẫn

(Ký tên và ghi rõ họ tên)

NHẬN XÉT CỦA THÀNH VIÊN HỘI ĐỒNG

....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....

Trà Vinh, ngày ….. tháng …… năm ……

Thành viên hội đồng

(Ký tên và ghi rõ họ tên)

LỜI CẢM ƠN

Trước hết, em xin gửi lời cảm ơn chân thành nhất đến thầy Dương Ngọc Vân Khanh, giảng viên hướng dẫn của em. Thầy đã hỗ trợ và chỉ dẫn tận tình cho em trong suốt quá trình thực hiện đồ án này. Những kiến thức, kỹ năng mà thầy đã truyền đạt không chỉ giúp em hoàn thành đồ án mà còn là bước đệm quan trọng cho sự nghiệp tương lai của em. Thầy đã tạo điều kiện cho em học hỏi, thực hành và giải đáp những thắc mắc trong quá trình thực hiện đồ án.

Tiếp theo, em xin gửi lời cảm ơn đến Khoa Kỹ thuật và Công Nghệ, Trường Đại học Trà Vinh. Khoa đã tạo điều kiện và cung cấp những kiến thức bổ ích và là nền tảng vững chắc cho em trong quá trình học tập và thực hiện đồ án. Những quyển giáo trình và tài liệu tham khảo mà Khoa cung cấp đã trở thành nguồn tri thức quý giá, giúp em định hình và mở rộng kiến thức của mình.

Với những kiến thức đã được học tập và tìm hiểu, cùng với sự hướng dẫn nhiệt tình của thầy đã giúp em đã hoàn thành bài báo cáo đồ án cơ sở ngành. Tuy nhiên, em nhận thức được rằng trong quá trình thực hiện đề tài, em vẫn còn nhiều thiếu sót. Điều này không chỉ là do hạn chế về kiến thức và kỹ năng của bản thân, mà còn do sự phức tạp của đề tài. Em đã cố gắng học hỏi và khắc phục những khó khăn này, nhưng vẫn còn nhiều điều cần cải thiện.

Do đó, em mong nhận được đóng góp ý kiến của quý thầy cô để em có thể học tập thêm được nhiều kinh nghiệm, nâng cao kỹ năng và kiến thức của mình. Em tin rằng, với sự hỗ trợ và chỉ dẫn của quý thầy cô, em sẽ hoàn thành tốt hơn trong những bài báo cáo sắp tới.

Em xin chân thành cảm ơn!

TÓM TẮT NIÊN LUẬN/ĐỒ ÁN CƠ SỞ NGÀNH

Đồ án Thiết kế hệ thống mạng máy tính tại một trường trung học phổ thông (THPT) nhằm cung cấp cơ sở hạ tầng kỹ thuật để hỗ trợ các hoạt động giáo dục và quản lý nội bộ. Cấu trúc mạng .Để triển khai một hệ thống mạng máy tính hiệu quả, việc hợp tác với các chuyên gia IT và tuân thủ các quy chuẩn bảo mật và quản lý mạng là cực kỳ quan trọng. Thiết kế mạng cần phải linh hoạt để đáp ứng nhu cầu ngày càng thay đổi của cộng đồng học đường và đảm bảo tính ổn định, bảo mật và hiệu suất cho các hoạt động giáo dục và quản lý.

MỞ ĐẦU

Lí do chọn đề tài

Việc thiết kế hệ thống mạng máy tính tại một trường THPT có thể được lựa chọn vì nó đem lại nhiều lợi ích và có ảnh hưởng đáng kể đối với môi trường học tập. Dưới đây là một số lý do có thể giúp bạn hiểu rõ hơn:

Tăng cường hiệu suất học tập: Hệ thống mạng máy tính hiện đại có thể cải thiện hiệu suất học tập thông qua việc cung cấp tài nguyên trực tuyến, nâng cao khả năng tiếp cận thông tin và giáo dục.

Tính linh hoạt và tiện ích: Một hệ thống mạng tốt có thể tạo điều kiện cho việc tiếp cận tài nguyên giáo dục từ xa, giúp học sinh và giáo viên dễ dàng truy cập vào tài liệu, sách và tài nguyên giáo dục trực tuyến.

Quản lý dữ liệu và thông tin: Hệ thống mạng có thể giúp trường quản lý thông tin học sinh, giáo viên, tài liệu giảng dạy và hành chính một cách hiệu quả hơn.

Tạo điều kiện cho việc học tập sáng tạo: Mạng máy tính có thể hỗ trợ việc học tập tương tác và sáng tạo thông qua việc kết nối các thiết bị, chia sẻ tài nguyên và hợp tác trong các dự án học tập.

Tăng cường kỹ năng công nghệ cho học sinh: Việc tiếp xúc với hệ thống mạng máy tính sẽ giúp học sinh nắm vững kiến thức về công nghệ thông tin, kỹ năng sử dụng máy tính và internet một cách hiệu quả.

Giao tiếp và tương tác tốt hơn: Hệ thống mạng có thể tạo ra cơ hội để học sinh và giáo viên kết nối, trao đổi thông tin và học hỏi từ nhau thông qua các nền tảng trực tuyến.

An toàn và bảo mật thông tin: Một hệ thống mạng máy tính tốt cũng đảm bảo an toàn thông tin, bảo vệ dữ liệu cá nhân của học sinh và giáo viên khỏi các mối đe dọa trực tuyến.

Hiệu quả quản lý hệ thống: Việc thiết kế một hệ thống mạng tốt sẽ giúp trường quản lý và vận hành hệ thống mạng một cách hiệu quả, tiết kiệm chi phí và tối ưu hóa hoạt động.

Mục đích nghiên cứu

Mục đích của việc nghiên cứu và thiết kế hệ thống mạng máy tính tại trường THPT có thể bao gồm các mục tiêu sau đây:

Nâng cao chất lượng giáo dục: Tạo điều kiện tốt nhất để hỗ trợ quá trình giảng dạy và học tập thông qua việc tối ưu hóa việc truy cập thông tin, tài liệu giáo dục và công cụ học tập trực tuyến.

Tăng cường sự linh hoạt và tiện ích: Xây dựng một hệ thống mạng linh hoạt, dễ mở rộng và dễ quản lý, giúp trường dễ dàng thích nghi với sự phát triển và nhu cầu mới trong giáo dục.

Cải thiện tương tác giữa giáo viên và học sinh: Xây dựng các nền tảng trực tuyến để hỗ trợ tương tác giữa giáo viên và học sinh, cũng như tạo điều kiện cho học sinh tham gia vào quá trình học tập tương tác và hợp tác.

Tối ưu hóa an ninh mạng: Bảo vệ thông tin cá nhân, dữ liệu quan trọng và hệ thống mạng của trường tránh khỏi các mối đe dọa mạng.

Đào tạo kỹ năng công nghệ cho học sinh: Xây dựng một môi trường học tập sử dụng công nghệ, giúp học sinh nắm vững kiến thức về công nghệ thông tin và phát triển kỹ năng cần thiết để sử dụng công nghệ hiệu quả.

Tối ưu hóa quản lý hệ thống: Thiết kế hệ thống mạng máy tính sao cho việc quản lý và vận hành trở nên hiệu quả hơn, tiết kiệm chi phí và thời gian của trường.

Nghiên cứu và áp dụng công nghệ mới: Tìm hiểu và sử dụng các công nghệ mới nhất để cải thiện hiệu suất và tính đáng tin cậy của hệ thống mạng máy tính.

Tạo điều kiện cho học sinh phát triển sáng tạo: Hỗ trợ việc sáng tạo và phát triển cá nhân của học sinh thông qua việc sử dụng công nghệ trong các dự án học tập và nghiên cứu.

Đối tượng nghiên cứu

Đối tượng nghiên cứu trong việc thiết kế hệ thống mạng máy tính tại trường THPT có thể bao gồm các nhóm chính sau:

Học sinh: Học sinh là một trong những đối tượng chính trong việc nghiên cứu này. Hệ thống mạng máy tính được thiết kế để hỗ trợ quá trình học tập của họ, cung cấp tài nguyên giáo dục, cơ hội học tập trực tuyến và khuyến khích sự tương tác và hợp tác giữa các học sinh.

Giáo viên và nhân viên giáo dục: Giáo viên và nhân viên của trường là một đối tượng quan trọng trong việc sử dụng và quản lý hệ thống mạng máy tính. Họ cần được đào tạo để sử dụng các công nghệ mới, tận dụng các công cụ giáo dục trực tuyến và hỗ trợ trong quá trình dạy học

Ban quản lý và quản lý hệ thống: Những người đảm nhiệm vai trò quản lý cấp cao tại trường, bao gồm các quản lý hệ thống mạng, quản lý công nghệ thông tin, quản lý hành chính và tài chính, cũng đóng vai trò quan trọng trong quá trình nghiên cứu và thiết kế hệ thống mạng máy tính tại trường.

Phụ huynh: Phụ huynh cũng có thể được xem xét trong nghiên cứu, đặc biệt là trong việc đánh giá sự hiệu quả và đáp ứng của hệ thống mạng đối với việc giáo dục và phát triển của học sinh. Ý kiến và phản hồi từ phụ huynh có thể đóng vai trò quan trọng trong việc cải thiện và tối ưu hóa hệ thống

Phạm vi nghiên cứu

Phạm vi nghiên cứu đề tài "Thiết kế hệ thống mạng máy tính tại trường THPT" có thể bao gồm các khía cạnh cụ thể sau đây:

Kiến trúc Hệ thống Mạng:

- Xác định và mô tả kiến trúc hệ thống mạng phù hợp cho trường THPT.
- Đánh giá và lựa chọn các loại mạng (LAN, WAN, WLAN) và cấu hình mạng phù hợp với nhu cầu của trường.

Công nghệ và Thiết bị Mạng:

- Nghiên cứu và lựa chọn các công nghệ, thiết bị (bộ định tuyến, switch, máy chủ) phù hợp với yêu cầu của trường THPT.
- Đánh giá hiệu suất và tính năng của các thiết bị để đảm bảo chúng đáp ứng được nhu cầu sử dụng.

An ninh và Bảo mật Mạng:

- Xác định các biện pháp an ninh mạng để bảo vệ dữ liệu quan trọng và thông tin cá nhân của học sinh, giáo viên.
- Phát triển chính sách và cơ chế bảo mật để ngăn chặn các cuộc tấn công mạng và đảm bảo an toàn thông tin.

Dịch vụ và Ứng dụng Mạng:

- Triển khai các dịch vụ mạng như email, hệ thống quản lý học tập, và các ứng dụng hỗ trợ giáo dục.
- Đánh giá hiệu suất của các dịch vụ và ứng dụng để cải thiện trải nghiệm người dùng.

Quản lý và Vận hành Hệ thống:

- Xác định các quy trình quản lý và vận hành hệ thống mạng một cách hiệu quả, bao gồm sao lưu, phục hồi, và giám sát.
- Đánh giá và cải thiện hiệu suất hệ thống, đồng thời xác định các vấn đề kỹ thuật để giải quyết.

Đào tạo và Hỗ trợ Người dùng:

- Phân tích nhu cầu đào tạo và hỗ trợ người dùng về việc sử dụng hệ thống mạng và các ứng dụng kỹ thuật số.
- Phát triển các tài liệu hướng dẫn và chương trình đào tạo cho giáo viên và học sinh.

Đánh giá và Đề xuất Cải thiện:

- Thu thập phản hồi từ người dùng để đánh giá hiệu suất và sự hài lòng với hệ thống mạng.

MỤC LỤC

CHƯƠNG 1: TỔNG QUAN

1.1. Giới thiệu chung

Tên gọi: Trường THPT Dương Háo Học

Địa chỉ:xã Tân An huyện Càng Long tỉnh Trà Vinh

Điện thoại:

1.2. Tiếp cận đơn vị

1.1.1. Nhận xét về hệ thống hiện tại và dự án của hệ thống mới

* Ưu điểm

Hiện tại, trường THPT Dương Háo Học 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 LAN 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

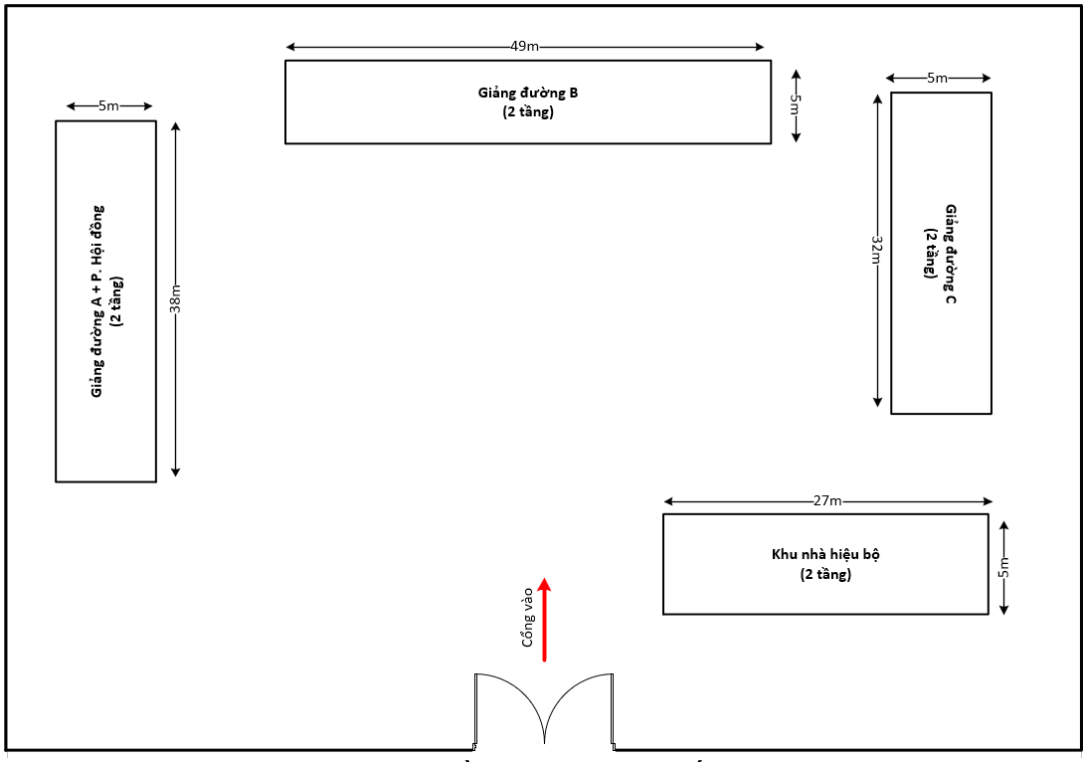
1.1.2. Yêu cầu của hệ thống

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.

1.1.3. Khảo sát thực tế trường THPT Dương Háo Học

- Sơ đồ khảo sát thực tế:

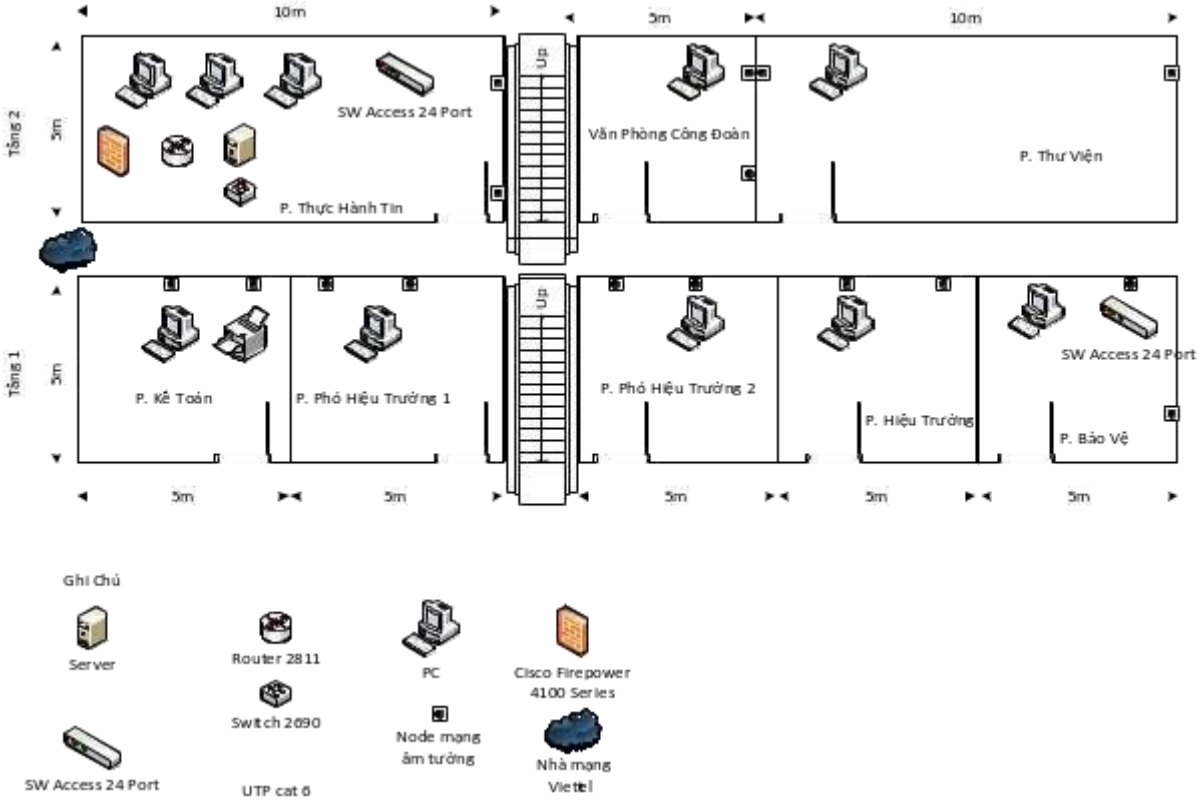


Sơ đồ khảo sát thực tế

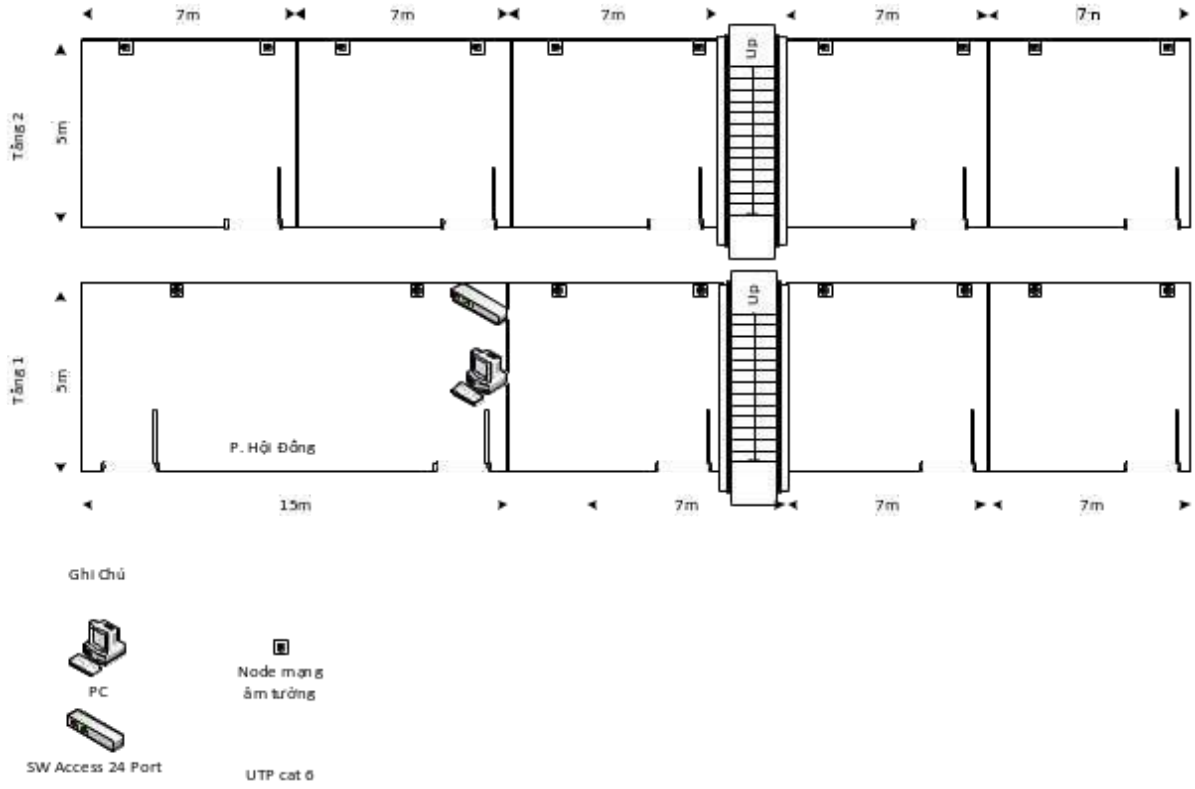
1.1.4. Kế hoạch phân bố IP và VLAN

Vlan_ID	Tên Vlan	Ghi chú
1	Vlan 1	Không dùng
10	Vlan 10	Phòng thực hành tin
20	Vlan 20	Văn phòng công đoàn
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

- Sơ đồ vật lý và đi dây:



Khu nhà Hiệu Bộ



Giảng đường A

- Dự kiến xây dựng 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	01	25m
3	Thư viện	02	01	20m
4	Kế toán	02	01	35m
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

- Thông tin về địa chỉ 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

CHƯƠNG 2: NGHIÊN CỨU LÝ THUYẾT

2.1. 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.

2.2. 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

2.3. 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 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.

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.

2.4. 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).

2.5. Mô hình mạng chia sẻ

Đầu các năm 1990, mạng Campus được xây dựng theo kiểu truyền thống chỉ có một LAN đơn giản cho tất cả các user kết nối đến và sử dụng. Tất cả các thiết bị trên LAN bắt buộc phải chia sẻ băng thông sẵn có. Môi trường truyền như Ethernet và TokenRing đều có giới hạn về khoảng cách cũng như giới hạn số thiết bị được kết nối vào LAN.

Khả năng hoạt động và tính sẵn sàng của mạng sẽ giảm nếu số thiết bị kết nối tăng dần. Ví dụ như tất cả các thiết bị của Ethernet LAN đều chia sẻ băng thông bán song công 10Mbps. Ethernet cũng sử dụng CSMA/CD để quyết định khi nào một thiết bị có thể truyền dữ liệu trên đoạn LAN chia sẻ này. Trong cùng thời điểm nếu có nhiều hơn một thiết bị có nhu cầu truyền thì sẽ xảy ra đụng độ, và tất cả các thiết bị phải "lắng nghe" và chờ để truyền lại, người ta gọi nó là miền đụng độ.

Trong khi TokenRing LAN thì không xảy ra đụng độ vì các trạm chỉ được phép truyền khi nhận được thẻ bài. Có một cách làm giảm tắt nghẽn mạng là phân đoạn mạng, hoặc chia một LAN thành nhiều miền đụng độ riêng biệt bằng cách sử dụng bridge chuyển tiếp frame dữ liệu ở lớp 2 . Bridge cho phép giảm số thiết bị trên một đoạn, do đó sẽ giảm được xác suất đụng độ trên các đoạn đồng thời tăng giới hạn khoảng cách vật lý vì nó hoạt động như là một repeater.

Tuy nhiên, các frame chứa địa chỉ broadcast (FF:FF:FF:FF:FF:FF) đều đến tất các các đoạn. Các frame broadcast thường được dùng để kết hợp các yêu cầu về thông tin hoặc dịch vụ, bao gồm các thông báo về dịch vụ mạng. IP sử dụng broadcast cho giao thức ARP gửi yêu cầu để hỏi địa chỉ MAC tương ứng với địa chỉ IP. Các frame broadcast còn được dùng để gửi các yêu cầu DHCP, IPX, GNS (Get Nearest Server), SAP (Service Advertising Protocol), RIP, tên NetBIOS.

Một miền broadcast là một nhóm các đoạn mạng mà broadcast được tràn qua. Lưu lượng multicast là lưu lượng được định trước cho một nhóm các user được thiết lập cụ thể, mà không quan tâm đến vị trí của nó trong mạng Campus. Các frame multicast cũng qua tất cả các đoạn mạng bởi vì nó là một hình thức của broadcast. Mặc dù trạm đầu cuối phải chọn một nhóm multicast để cho phép nhận dữ liệu multicast, nhưng bridge phải cho lưu lượng tràn qua tất cả các đoạn mạng vì nó không biết được trạm nào là thành viên của nhóm multicast. Các frame multicast chia sẻ băng thông

trên một đoạn mạng, nhưng không bắt buộc sử dụng tài nguyên CPU trên mỗi thiết bị kết nối.

Chỉ có các CPU đăng ký là thành viên của nhóm multicast mới thực sự xử lý các frame này. Lưu lượng broadcast sẽ gây nên hai vấn đề: thứ nhất là độc quyền băng thông sẵn có, và thứ hai là tất cả các trạm đầu cuối đều phải lắng nghe để giải mã và xử lý mỗi frame broadcast.

2.6. Mô hình phân đoạn LAN

Phân đoạn mạng sẽ giảm lưu lượng và số trạm trên một đoạn để khắc phục vấn đề đụng độ và broadcast. Việc giảm số lượng trạm sẽ giảm được miền đụng độ vì có ít máy hơn cùng có nhu cầu truyền. Đối với việc ngăn chặn broadcast, giải pháp là cung cấp một hàng rào tại biên của đoạn LAN để broadcast không qua được hoặc chuyển tiếp trên đó. Người thiết kế có thể dùng router hoặc switch. Ta có thể dùng router để kết nối các mạng con nhỏ và định tuyến các gói lớp 3. Router không cho phép lưu lượng broadcast đi qua, do đó broadcast không thể chuyển tiếp qua các mạng con khác.

Ngoài ra ta còn phân đoạn LAN bằng switch. Switch cung cấp khả năng thực thi cao hơn với băng thông chuyên dụng trên mỗi port (không chia sẽ băng thông). Người ta gọi switch là multi-bridge. Mỗi port của switch là một miền đụng độ riêng lẻ và không truyền đụng độ qua port khác, tuy nhiên các frame broadcast và multicast vẫn tràn qua tất cả các port của switch. Để phân chia miền broadcast ta sẽ dùng VLAN bên trong mạng chuyển mạch. Một switch sẽ chia các port một cách logic thành các đoạn riêng biệt. VLAN là một nhóm các port vẫn chia sẽ môi trường truyền của đoạn LAN. Vấn đề về VLAN sẽ được tìm hiểu rõ ở phần sau.

2.7. Mô hình lưu lượng mạng

Để thiết kế và xây dựng thành công mạng Campus thì ta phải hiểu lưu lượng sinh ra bởi việc sử dụng các ứng dụng cộng với luồng lưu lượng đi và đến từ toàn thể user. Tất cả các thiết bị sẽ truyền dữ liệu qua mạng với các kiểu dữ liệu và tải khác nhau. Các ứng dụng như: email, word, print, truyền file, và duyệt web, sẽ mang các kiểu dữ liệu đã biết trước từ nguồn đến đích. Tuy nhiên các ứng dụng mới hơn như video, TV, VoIP… có kiểu lưu lượng khó đoán trước được.

- Gán lại tài nguyên sẵn có để mang các user và các server lại gần với nhau
- Chuyển các ứng dụng và các file đến các server khác nhau ở trong một nhóm

2.8. 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 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 trình thiết kế.

2.9. 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.

2.10. 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.

2.11. 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.

2.12. 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)

2.13. 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).

2.14. 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.

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.

2.15. 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: MÔ HÌNH MẠNG BACKUP

3.1. 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.

3.2. 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),…

3.3. 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.

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

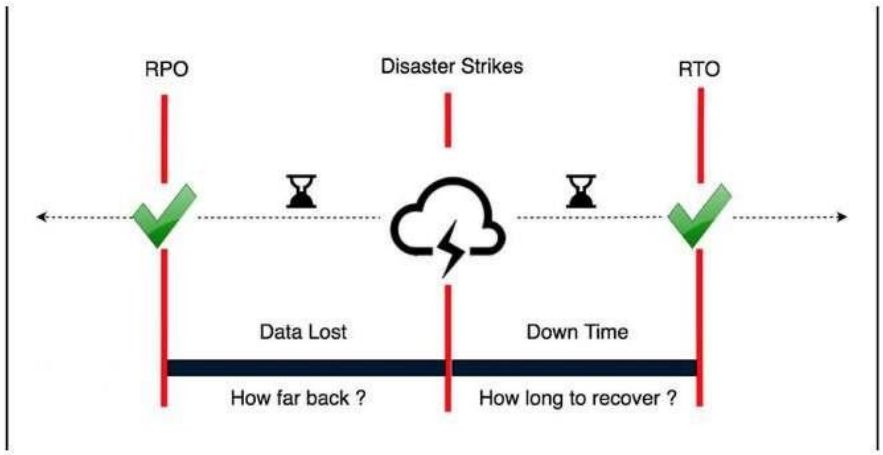
Khi đã quyết định được phạm vi backup của mình, thì quyết định quan trọng tiếp theo là tần suất cần backup và xác định lịch để backup dữ liệu. Có 2 yếu tố chính để quyết định việc này là RTO và RPO.

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.



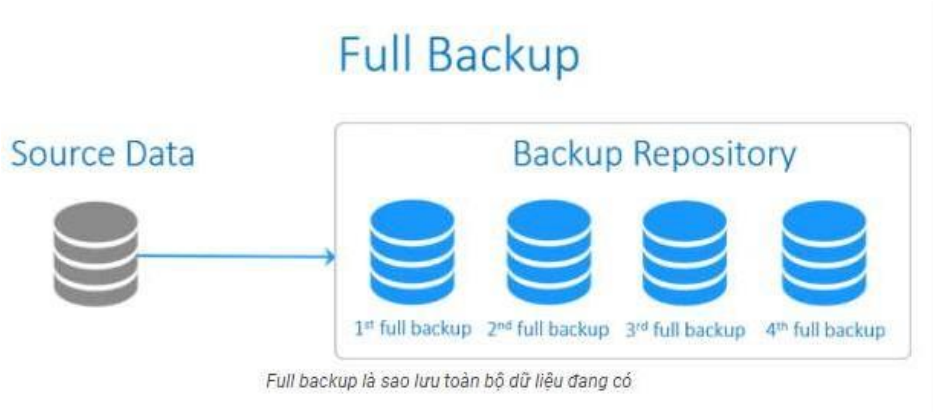
Một biến quan trọng khác là Recovery Time Objective (RTO) - Thời gian phục hồi - Ví dụ như phòng nhân sự mất file tính lương và họ yêu cầu DN trong vòng 1 tiếng phải phục hồi cho họ ngay, như vậy RTO = 1 giờ. RTO càng nhỏ thì chi phí càng cao.

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:

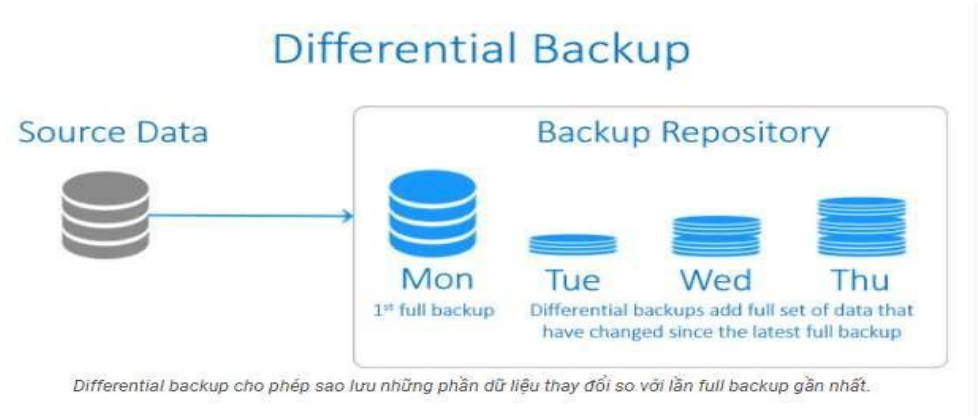


+ Full Backup:

- 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 cho phép sao lưu những phần dữ liệu thay đổi so vớilần full backup gần nhất.



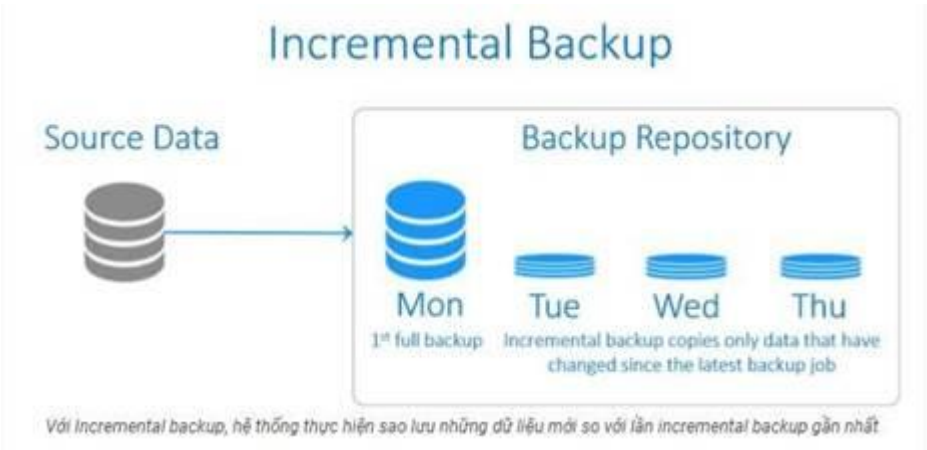
- Ưu điểm của differential backup

- 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:

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



Ưu điểm của Incremental backup

- So với hai dạng trên thì incremental backup có thời gian thực hiện nhanh
- 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.
- Full backup hàng tháng
- Differential backup hàng tuần
- Incremental backup hàng ngày.
- Differential backup cho phép sao lưu những phần dữ liệu thay đổi so với lần full backup gần nhất.

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.

Ưu điểm của Incremental backup

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

- Full backup hàng tháng
- Differential backup hàng tuần
- Incremental backup hàng ngày

3.5. 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.

3.6. Backup dữ liệu lên Cloud

Với giải pháp này, bạn đăng ký một dung lượng lưu trữ tại nhà cung cấp dịch vụ. Việc backup này không yêu cầu doanh nghiệp phải đầu tư phần cứng, ngoài việc

sở hữu kết nối đến internet để lưu trữ các dữ liệu lên cloud của đơn vị cung cấp dịch vụ.

Đối với các doanh nghiệp gặp vấn đề trong lần đầu di chuyển dữ liệu lên Cloud do dung lượng quá lớn, thì một số đơn vị cung cấp dịch vụ sẽ có các giải pháp để xử lý việc này với chi phí không quá tốn kém.

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).

4.1. Thiết kế cơ sở hạ tầng theo mô hình SOA

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.

4.2. 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.

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

4.3. 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.

4.2. 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.

4.3. 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

4.4. 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

4.5. 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.

4.6. Nhóm giải pháp về hệ thống ngăn chặn, phát hiện tấn công

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 lửal 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.

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 nhiều và 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

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

4.7.1. 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.

4.7.2. 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.

4.8. Nhóm giải pháp khác

4.8.1 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

4.8.2. Ghi nhật ký, theo dõi, giám sát hệ thống

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.

CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN:

5.1. Kết Luận:

Trong quá trình nghiên cứu và thiết kế hệ thống mạng máy tính tại Trường THPT Dương Hạo Học, em đã đạt được những kết quả quan trọng nhất như sau:

- Hiểu rõ nhu cầu và yêu cầu cụ thể của trường trong việc xây dựng hệ thống mạng máy tính.
- Thiết kế một hệ thống mạng đáp ứng đầy đủ các tiêu chí về tốc độ, bảo mật và ổn định.
- Triển khai thành công hệ thống mạng tại Trường THPT Dương Hạo Học và đảm bảo sự liên kết mạnh mẽ giữa các thiết bị.

Với những kết quả trên, em tin rằng hệ thống mạng máy tính sẽ mang lại nhiều lợi ích cho cả học sinh và giáo viên, giúp tối ưu hóa quá trình học tập và quản lý tại trường.

5.2. Hạn Chế:

Tuy nhiên, trong quá trình thực hiện đề tài, em đã gặp một số hạn chế nhất định:

- Hạn chế về nguồn lực: Dự án gặp khó khăn trong việc mobilize nguồn lực cần thiết, ảnh hưởng đến tốc độ triển khai.
- Thiếu sự hỗ trợ chủ động từ phía người quản lý và người sử dụng: Điều này có thể gây khó khăn trong việc đảm bảo hiệu suất và tính ổn định của hệ thống.

5.3. Phương Hướng Phát Triển:

Để nâng cao hiệu suất và khắc phục những hạn chế đã đề cập, có một số phương hướng phát triển mà em đề xuất:

- Mở rộng hệ thống mạng để đáp ứng với sự gia tăng về số lượng người sử dụng và thiết bị.
- Tăng cường đào tạo và hỗ trợ người sử dụng để tối ưu hóa hiệu suất của hệ thống.
- Liên tục cập nhật và nâng cấp cả về phần cứng và phần mềm để đảm bảo tính bảo mật và ổn định.

Những hướng phát triển này sẽ giúp đảm bảo rằng hệ thống mạng máy tính tại Trường THPT Dương Hạo Học luôn đáp ứng được nhu cầu và tiêu chí ngày càng cao trong tương lai.