Trường Đại học Bách Khoa Thành phố Hồ Chí Minh

**GVHD: Nguyễn Hồng Nam**

Nhóm: L09\_ST3\_Alias

Thành viên:

1/ Nguyễn Bá Tiến 1810578

2/ Châu Thanh Tân 1810501

3/ Nguyễn Phi Thông 1814205

4/ Nguyễn Văn Thuần 1814220

**TP.HCM, 12/2020**

Khoa Khoa học và Kĩ thuật Máy tính

**-------------------------------------------------------------------**



**MẠNG MÁY TÍNH**

**BÀI TẬP LỚN 2**

**THIẾT KẾ MẠNG MÁY TÍNH CHO**

**HỆ THỐNG NGÂN HÀNG**

Mục lục

[1/ Tìm hiểu cấu trúc mạng thích hợp cho các tòa nhà: 2](#_Toc59456830)

[2/ Danh sách các trang thiết bị tối thiểu, sơ đồ IP và sơ đồ đi dây (cabling): 4](#_Toc59456831)

[3/ Tính toán throughput, bandwidth và các thông số an toàn cho Mạng máy tính: 8](#_Toc59456832)

[4/ Thiết kế sơ đồ mạng dùng phần mềm mô phỏng Cisco Packet Tracer: 10](#_Toc59456833)

[5/ Đánh giá hệ thống mạng đã thiết kế: 12](#_Toc59456834)

[6/ Kết luận của nhóm: 14](#_Toc59456835)

# 1/ Tìm hiểu cấu trúc mạng thích hợp cho các tòa nhà:

a) Phân tích yêu cầu của hệ thống mạng Trụ sở và Chi nhánh:

- Mạng máy tính dùng trong trụ sở của một Ngân hàng BBB (B Bank Building) chuẩn bị xây mới. Các thông số quan trọng của việc sử dụng CNTT trong Ngân hàng này là:

+ Tòa building cao khoảng 7 tầng, tầng 7 được trang bị 1 phòng kỹ thuật Mạng và Cabling Central Local (Phòng tập trung dây mạng và patch panels)

+ BBB dạng Small Enterprise: 100 workstations, 5 Servers, 10 Network devices

+ Dùng công nghệ mới (new technology) về hạ tầng mạng, 100/1000 Mbps và Wireless

+ Tổ chức hệ thống mạng theo cấu trúc VLAN

+ Dùng kết hợp giữa Licensed và Open source Softwares

+ Kết nối với bên ngoài bằng 2 Leased line và 1 ADSL, dùng Load-balancing

+ Ứng dụng văn phòng, client-server, đa phương tiện, database

+ Bảo mật cao, an toàn khi xảy ra sự cố, dể dàng nâng cấp hệ thống

- Ngân hàng có nhu cầu kết nối đến 2 chi nhánh khác ở 2 thành phố lớn như Nha Trang và Đà Nẵng. Mỗi chi nhánh cũng được thiết kế tương tự như trụ sở nhưng quy mô nhỏ hơn:

+Tòa nhà cao khoảng 2 tầng, tầng 2 được trang bị 1 phòng kỹ thuật Mạng và Cabling Central Local.

+ BBB dạng chi nhánh: 50 workstations, 3 Servers, 5 Network Equipments

- Các thông số về lưu lượng và tải của hệ thống (tập trung khoảng 80% vào giờ cao điểm 9g-11g và 15g-16g) có thể dùng chung cho Trụ sở và Chi nhánh như sau:

+ Servers dùng cho updates, web access, database access, ... Tổng dung lượng upload và download vào khoảng 500 MB/ngày.

+ Mỗi workstation dùng cho duyệt Web, tải tài liệu, giao dịch khách hàng,...Tổng dung lượng upload và download vào khoảng 100 MB/ngày.

+ Máy laptop kết nối WiFi dùng cho khách hàng truy xuất khoảng 50 MB/ngày.

- Hệ thống Mạng máy tính của Ngân hàng BBB được dự toán cho mức độ phát triển 20% trong 5 năm (về số lượng người sử dụng, tải trọng mạng, mở rộng nhiều chi nhánh,..).

b) Lập bảng các chi tiết cần khảo sát ở các vị trí cài đặt:

- Đối với trụ sở chính:

+ Từ tầng 1 đến 6: mỗi tầng 15 workstation

+ Tầng 7: 10 workstation

- Đối với chi nhánh:

+ Tầng 1: 40 workstation

+ Tầng 2: 10 workstation

c) Xác định các vùng có tải lớn (Network Load) để đặc biệt lựa chọn cấu hình thiết bị phù hợp (Cân bằng tải được đặt ở những vị trí cần thiết):

- Tầng 2 ở các chi nhánh và tầng 7 ở trụ sở, ta đặt các server. Do mọi hoạt động giao dịch diễn ra tại tầng 1 nên ta lắp đặt 1 mạng Wireless để cung cấp mạng cho khách hàng.

d) Lựa chọn cấu trúc Mạng phù hợp với kiến trúc, sự thuận lợi và thẩm mỹ của tòa nhà:

Tổ chức hệ thống mạng theo VLAN: chia nhỏ hệ thống mạng thành các mạng con cho các phòng ban. Các máy tính giữa các VLAN khác nhau không thể xâm nhập lẫn nhau.

Kết nối Internet: Mạng của trụ sở chính sẽ kết nối với hệ thống Internet bằng đường truyền ADSL và với 2 chi nhánh bằng đường truyền Lease Line.

# 2/ Danh sách các trang thiết bị tối thiểu, sơ đồ IP và sơ đồ đi dây (cabling):

- Các trang thiết bị tối thiểu cho cả hệ thống:

+ Switch:

**20-Port Gigabit Managed Switch CISCO SG300-20 (SRW2016-K9):**

****

+ Router:

**Router Cisco RV340-K9-G5**



+ Access Point:

**Wireless-N Access Point with PoE Cisco WAP121**

****

a) Trụ sở chính:

- Các server:

+ Web server: Để khách hàng có thể truy cập vào các dịch vụ web như đăng nhập, xem thông tin, lịch sử giao dịch…

+ Mail server: Để gửi mail và nhận mail.

+ DNS server: Dịch tên miền ra địa chỉ IP.

+ Database server: Lưu trữ dữ liệu.

+ Backup server: Chứa dữ liệu backup.

- Các server cần có cấu hình đủ mạnh để phục vụ cho nhiều truy xuất đồng thời và liên tục.

- Toàn bộ mạng của trụ sở chính là một LAN. Mạng này kết nối với Router trung tâm và từ đó kết nối ra Internet.

+ LAN được chia thành 7 VLAN cho 7 tầng (10, 20… 70). Các workstations của mỗi tầng được đưa vào cùng một VLAN. Hệ thống server được đưa vào VLAN của tầng 7:

|  |  |  |
| --- | --- | --- |
|  | Chức năng | Số lượng thiết bị |
| Tầng 7 | Tầng chứa server | - 10 workstations  - 1 Switch  - 5 servers  - 1 tường lửa |
| Tầng 6 | Tầng làm việc | - 15 workstations  - 1 Switch |
| Tầng 5 | Tầng làm việc | - 15 workstations  - 1 Switch |
| Tầng 4 | Tầng làm việc | - 15 workstations  - 1 Switch |
| Tầng 3 | Tầng làm việc | - 15 workstations  - 1 Switch |
| Tầng 2 | Tầng làm việc | - 15 workstations  - 1 Switch |
| Tầng 1 | Tầng giao dịch | - 15 workstations  - 1 access point  - 2 Switch  - 1 Router  - 10 laptop |

Ở tầng 7, ta sử dụng 1 Switch để nối 5 server và 10 workstations.

Từ tầng 6 đến tầng 2, ta sử dụng 1 Switch để nối 15 workstations.

Ở tầng 1, ta sử dụng 1 Switch để nối 15 workstations và 1 access point. 10 laptop sẽ kết nối wifi từ access point.

7 Switch ở 7 tầng đã nêu trên sẽ nối vào Switch tổng đặt ở tầng 1. Switch tổng này sẽ nối ra Router để nối ra Internet.

- Sơ đồ chia VLAN bởi địa chỉ IP tại trụ sở chính:

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN | Chức năng | Địa chỉ IP danh định | Chi tiết - Miền cung cấp IP |
| VLAN10 | Tầng 1 | 192.168.0.1/24 | 192.168.0.2 -> 192.168.0.254 |
| VLAN20 | Tầng 2 | 192.168.1.1/24 | 192.168.1.2 -> 192.168.1.254 |
| VLAN30 | Tầng 3 | 192.168.2.1/24 | 192.168.2.2 -> 192.168.2.254 |
| VLAN40 | Tầng 4 | 192.168.3.1/24 | 192.168.3.2 -> 192.168.3.254 |
| VLAN50 | Tầng 5 | 192.168.4.1/24 | 192.168.4.2 -> 192.168.4.254 |
| VLAN60 | Tầng 6 | 192.168.5.1/24 | 192.168.5.2 -> 192.168.5.254 |
| VLAN70 | Tầng 7 | 192.168.6.1/24 | 192.168.6.2 -> 192.168.6.254 |

b) Chi nhánh:

- Các server:

+ Web server: Để khách hàng có thể truy cập vào các dịch vụ web như đăng nhập, xem thông tin, lịch sử giao dịch…

+ Mail server: Để gửi mail và nhận mail.

+ DNS server: Dịch tên miền ra địa chỉ IP.

- Các server cần có cấu hình đủ mạnh để phục vụ cho nhiều truy xuất đồng thời và liên tục.

- Toàn bộ mạng của chi nhánh là một LAN. Mạng này kết nối với Router trung tâm và từ đó kết nối ra Internet.

+ LAN được chia thành 2 VLAN cho 2 tầng (10, 20). Các workstations của mỗi tầng được đưa vào cùng một VLAN. Hệ thống server được đưa vào VLAN của tầng 2:

|  |  |  |
| --- | --- | --- |
|  | Chức năng | Số lượng thiết bị |
| Tầng 1 | Tầng làm việc | - 40 workstations  - 3 Switch  - 1 Router  - 1 access point  - 5 laptop |
| Tầng 2 | Tầng kỹ thuật mạng | - 3 server  - 10 workstations  - 1 Switch  - 1 tường lửa |

Ở tầng 2, ta sử dụng 1 Switch để nối 3 server và 10 workstations.

Ở tầng 1, ta sử dụng 2 Switch, Switch 1 nối 20 workstations và 1 access point, Switch 2 nối 20 workstations. 5 laptop sẽ kết nối wifi từ access point.

1 Switch ở tầng 2 và 2 Switch ở tầng 1 sẽ nối vào Switch tổng đặt ở tầng 1. Switch tổng này sẽ nối ra Router để nối ra Internet.

- Sơ đồ chia VLAN bởi địa chỉ IP tại chi nhánh 1:

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN | Chức năng | Địa chỉ IP danh định | Chi tiết - Miền cung cấp IP |
| VLAN10 | Tầng làm việc | 192.100.0.1/24 | 192.100.0.2 -> 192.100.0.254 |
| VLAN20 | Phòng Server | 192.100.1.1/24 | 192.100.1.2 -> 192.100.1.254 |

- Sơ đồ chia VLAN bởi địa chỉ IP tại chi nhánh 2:

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN | Chức năng | Địa chỉ IP danh định | Chi tiết - Miền cung cấp IP |
| VLAN10 | Tầng làm việc | 192.200.0.1/24 | 192.200.0.2 -> 192.200.0.254 |
| VLAN20 | Phòng Server | 192.200.1.2/24 | 192.200.1.2 -> 192.200.1.254 |

# 3/ Tính toán throughput, bandwidth và các thông số an toàn cho Mạng máy tính:

a) Các khái niệm:

- Thông lượng (Throughput) là lượng thông tin hữu ích được truyền đi trên mạng trong một đơn vị thời gian; là chỉ số để đánh giá mạng nhanh hay chậm. Đơn vị: bps hay Bps

- Băng thông (Bandwidth) là đại lượng được dùng để chỉ một khối lượng dữ liệu có thể truyền tải được trong một thời gian nhất định. Đơn vị: bps hay Bps.

b) Tính toán các thông số:

- Các thông số về lưu lượng và tải của hệ thống (tập trung khoảng 80% vào giờ cao điểm 9-11h và 15-16h) có thể dùng chung cho Trụ sở và Chi nhánh.

=> Tổng giờ cao điểm là 3h.

\* Tại Trụ sở chính:

- Tầng 7 có :

+ Tổng cộng 5 servers dùng cho updates, web access, database access,... Tổng dung lượng upload và download vào khoảng 500 MB/ngày.

+ Tổng cộng 10 máy workstations. Tổng dung lượng upload và download vào khoảng 100 MB/ngày

=> Ta tính được Throughput vào lúc sử dụng đường truyền cao nhất (tập trung 80%) trong 3h cao điểm tại tầng 7 là:

Throughput = ((5 \* 500 + 10 \* 100) \* 80%) / (3 \* 3600) = 0.259 MB/s = 2.074 Mbps

- 5 tầng từ tầng 2 đến tầng 6 có tất cả 75 máy workstation (mỗi tầng 15 máy). Tổng dung lượng và upload và download vào khoảng 100 MB/ngày.

=> Ta tính được Throughput lúc sử dụng đường truyền cao nhất tại 5 tầng trên là:

Throughput = (75 \* 100 \* 80%) / (3 \* 3600) = 0.555 MB/s = 4.444 Mbps

- Tầng 1 có:

+ 15 máy workstation.

+ Lắp đặt wifi cung cấp mạng cho khoảng 10 máy laptop, mỗi laptop truy xuất khoảng 50MB/ngày.

=> Ta tính được Throughput lúc sử dụng đường truyền cao nhất tại tầng 1 là:

Throughput = ((15 \* 100 + 10 \* 50) \* 80%) / (3 \* 3600) = 0.148 MB/s = 1.185 Mbps

Vậy trong thời điểm nếu toàn bộ hệ thống mạng của trụ sở chính hoạt động đồng thời truy cập dữ liệu thì Throughput cao nhất có thể đạt tới là, hay Bandwidth: 2.074(T7) + 4.444(T2->6) + 1.185(T1) = 7.703 Mbps

\* Tại chi nhánh:

- Tầng 2 có :

+ Tổng cộng 3 servers dùng cho updates, web access, database access,... Tổng dung lượng upload và download vào khoảng 500 MB/ngày.

+ Tổng cộng 10 máy workstations. Tổng dung lượng upload và download vào khoảng 100 MB/ngày

=> Ta tính được Throughput vào lúc sử dụng đường truyền cao nhất (tập trung 80%) trong 3h cao điểm tại tầng 1 là:

Throughput = ((3 \* 500 + 10 \* 100) \* 80%) / (3 \* 3600) = 0.185 MB/s = 1.481 Mbps

- Tầng 1 có:

+ 40 máy workstation.

+ Lắp đặt wifi cung cấp mạng cho khoảng 5 máy laptop, mỗi laptop truy xuất khoảng 50MB/ngày

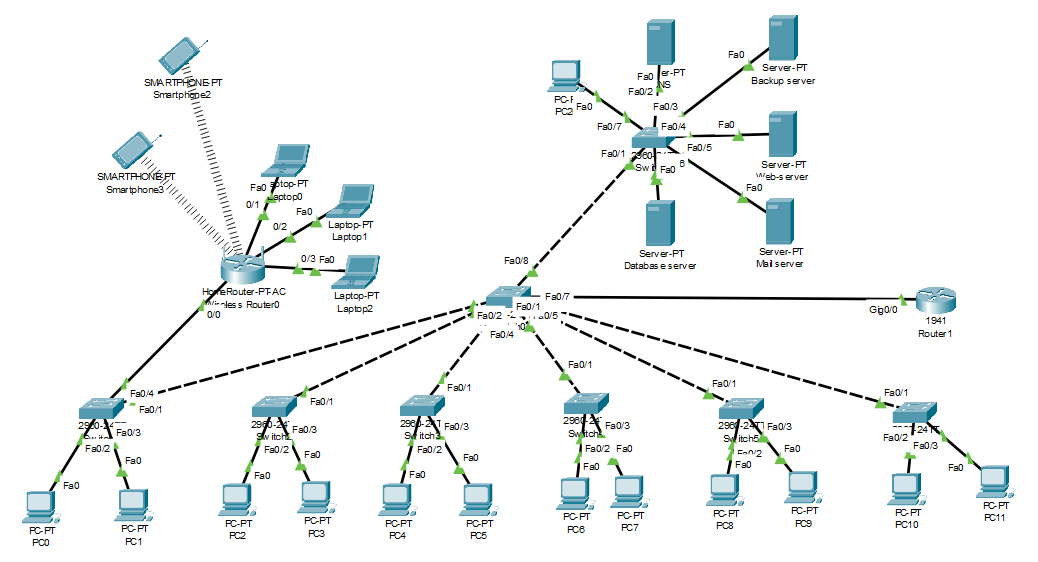
=> Ta tính được Throughput lúc sử dụng đường truyền cao nhất tại 6 tầng trên là:

Throughput = ((40 \* 100 + 5 \* 50) \* 80%) / (3 \* 3600) = 0.315 MB/s = 2.519 Mbps

Vậy trong thời điểm nếu toàn bộ hệ thống mạng của chi nhánh hoạt động đồng thời truy cập dữ liệu thì Throughput cao nhất có thể đạt tới là, hay Bandwidth: 1.481 + 2.519 = 4.000 Mbps

# 4/ Thiết kế sơ đồ mạng dùng phần mềm mô phỏng Cisco Packet Tracer:

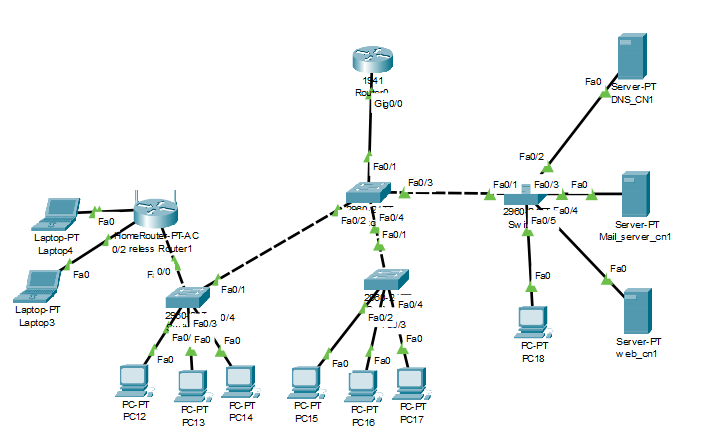
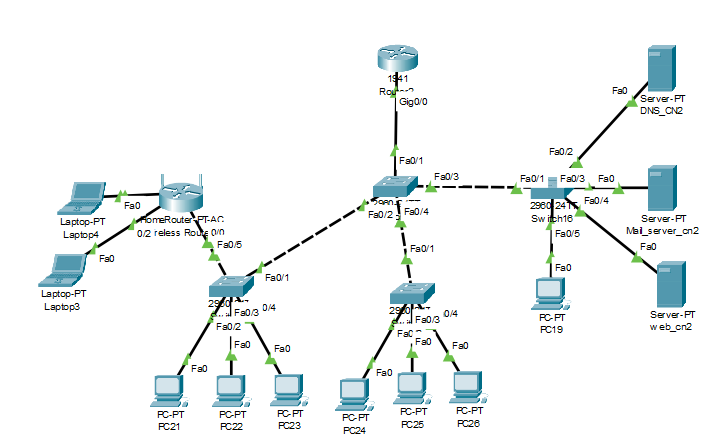
\* Sơ đồ trụ sở chính:



Tầng 7

Tầng 1 Tầng 2 Tầng 3 Tầng 4 Tầng 5 Tầng 6

\* Sơ đồ chi nhánh 1:

 \* Sơ đồ chi nhánh 2:

Tầng 2

Tầng 1

# 5/ Đánh giá hệ thống mạng đã thiết kế:

a) Tính an toàn và bảo mật của dữ liệu và hệ thống:

- Hệ thống bảo mật tương đối đảm bảo:

+ An toàn cho toàn bộ thông tin trên mạng, chống lại mọi sự truy cập bất hợp pháp vào mạng.

+ Kiểm soát được việc truy cập của người sử dụng.

+ Bảo đảm an toàn dữ liệu truyền, nhận qua các dịch vụ đường truyền ra Internet.

+ Chi phí phù hợp với dự trù kinh phí của ngân hàng.

- Các tài nguyên đảm bảo được bảo mật:

+ Máy chủ, máy trạm, các thiết bị mạng (Router, Access Point, ....)

+ Các chương trình ứng dụng quản lí tài khoản, tín dụng, các chương trình kế toán, ATM, …

+ Các thông tin tài khoản của khách hàng.

+ Công văn, báo cáo, tài liệu của ngân hàng.

- Các phương pháp giải quyết khi xảy ra sự cố trong hệ thống mạng:

+ Đường mạng kết nối Internet: Sử dụng đường leased-line và ADSL với

cơ chế load-balancing nhằm chia tải của leased-line qua ADSL khi leased-line gặp sự cố hay quá tải.

+ Các thiết bị kết nối Internet: Có cơ chế dự phòng, thực hiện set thông số priority cho các thiết bị (thiết bị càng lớn, priority càng lớn). Khi thiết bị chính gặp sự cố, hệ thống lập tức sử dụng thiết bị dự phòng đảm bảo kết nối không bị trì hoãn.

+ Miền DMZ: Có backup server cho các server web, mail, database, … và thường xuyên backup để đảm bảo không bị mất dữ liệu khi gặp sự cố.

+ Mạng nội bộ: Sử dụng Switch có cơ chế spanning-tree tạo ra các kết nối dự phòng, giúp ngân hàng không bị gián đoạn khi sự cố.

+ Xây dựng cho ngân hàng một phòng kỹ thuật giải quyết kịp thời các sự cố không mong muốn.

b) Thuê đường mạng hợp lí phục vụ cho cả ngân hàng và chi nhánh:

- Để giải quyết tốc độ mạng cho cả ngân hàng và chi nhánh một cách tối ưu, sau khi tính được Bandwidth cho cả trụ sở chính và chi nhánh, chúng ta cần thuê đường mạng cho trụ sở chính và chi nhánh như sau:

+ Đối với trụ ở chính: Bandwidth tối thiểu 8 Mbps

+ Đối với chi nhánh: Bandwidth tối thiểu 5 Mbps

c) Những hạn chế còn vướng mắc:

- Ta chưa giải quyết triệt để phần Firewall nên không thể loại bỏ một số vấn đề về đe dọa đến hệ thống mạng như:

+ Không kiểm soát được truy cập từ các nguồn bên ngoài vào mạng nội bộ dẫn đến việc các đối tượng tấn công, làm tê liệt hệ thống của ngân hàng như hacker, một số loại virus nguy hiểm

+ Đặc biệt đối với hệ thống của một ngân hàng thì việc kiểm soát các lượt truy cập vào hệ thống là một việc quan trọng nhằm tránh ảnh hưởng đến thông tin khách hàng, tài sản,...

+ Không thể kiểm soát được các dịch vụ truy cập ra bên ngoài, từ đó không đảm bảo thông tin nội bộ của ngân hàng

d) Nâng cấp hệ thống và phát triển cho tương lai:

- Hệ số an toàn trong Bandwidth là 20% đảm bảo hệ thống ổn định. Khi có nhu cầu tăng Bandwidth, ta cần đăng kí thêm gói với nhà cung cấp dịch vụ.

- Trong tương lai, chúng ta hướng đến sử dụng các thiết bị mạng của Cisco giúp hỗ trợ kĩ thuật tốt hơn, các thiết bị được ổn định hơn. Đặc biệt, các thiết bị của công ty Cisco thường được tích hợp sẵn các công nghệ mới, phù hợp với yêu cầu sử dụng như:

+ Switch Cisco các loại

+ Cisco ASR 1001 Router

+ Cisco-Linksys WAP610N Wireless-N Access Point with Dual-Band

+ Cisco Firewall ASA 5540

…

e) Tổng hợp một số công nghệ sử dụng cho hệ thống mạng:

\* VLAN (Virtual Local Area Network):

- VLAN là một miền quảng bá được tạo bởi Switch hay được hiểu như là một mạng LAN ảo.

- VLAN là một kỹ thuật cho phép tạo lập các mạng LAN độc lập một cách logic trên cùng một kiến trúc hạ tầng vật lí.

- Ứng dụng:

+ Ngăn chặn vùng quảng bá.

+ Gia tăng tính bảo mật.

+ Linh hoạt trong việc 1 Switch có thể tạo ra nhiều Switch ảo.

+ Tạo ra vùng quảng bá (Broadcast Domain) để sử dụng chung một ứng dụng nào đó.

- Ưu điểm:

+ Tiết kiệm băng thông của mạng do VLAN chia nhỏ LAN thành các vùng Broadcast Domain. Khi một gói tin quảng bá, nó sẽ lan truyền trong một mạng VLAN duy nhất, không truyền sang các VLAN khác nên tiết kiệm được băng thông đường truyền.

+ Tăng khả năng bảo mật: Các VLAN khác nhau không truy cập nhau được.

+ Dễ dàng thêm bớt các máy PC vào VLAN

\* DHCP server: (chưa triệt để)

- DHCP (Dynamic Host Configuration Protocol): giao thức này được thiết kế để giảm thời gian chỉnh cấu hình cho mạng TCP/IP bằng cách tự động gán các địa chỉ IP cho các máy tính khi chúng vào mạng. Ta nên sử dụng DHCP cho mô hình mạng có nhiều máy không cố định (Wifi) hoặc với số lượng máy lớn mà việc chia IP bằng tay là rất khó khăn, phức tạp.

- Ưu điểm:

+ DHCP tự động quản lí các địa chỉ và loại bỏ được các lỗi.

+ DHCP cho thuê địa chỉ trong một khoảng thời gian, nên các địa chỉ này sẽ còn được dùng cho hệ thống khác.

# 6/ Kết luận của nhóm:

a) Việc đã hoàn thành:

- Thiết kế được mô hình mạng cho công ty bao gồm IP và đi dây.

- Mô phỏng và test thử trên phần mềm Cisco Packet Tracer.

- Chia VLAN cho các tầng của trụ sở chính và chi nhánh.

- Định tuyến các Router.

b) Những khó khăn, công việc chưa hoàn thành:

- Chưa hoàn thành cấu hình Firewall cho ngân hàng.

c) Các kiến thức đạt được:

- Hiểu biết sâu về mạng máy tính đặc biệt đối với hệ thống mạng VLAN, WLAN.

- Nắm một số phần về thiết kế quy mô mạng cho một công ty lớn.

- Tích lũy kinh nghiệm lựa chọn, phân chia thiết bị cho mô hình mạng.

- Tích lũy khả năng tính toán, giải quyết vấn đề về lưu lượng băng thông cho giờ cao điểm.

d) Đánh giá hoạt động thành viên trong nhóm:

Đánh giá theo mức độ tham gia đóng góp và tinh thần trách nhiệm:

|  |  |
| --- | --- |
| Họ tên | Công việc phân chia |
| Nguyễn Bá Tiến | Thiết kế, mô phỏng |
| Châu Thanh Tân | Hỗ trợ thiết kế, viết báo cáo, tính toán các số liệu |
| Nguyễn Phi Thông | Thiết kế, mô phỏng |
| Nguyễn Văn Thuần | Hỗ trợ thiết kế, viết báo cáo |