

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA



MẠNG MÁY TÍNH

THIẾT KẾ MẠNG MÁY TÍNH CHO BUILDING CỦA NGÂN HÀNG

GVHD : Hoàng Nguyễn Minh Đức

SV :
1. Lê Phương Khuê - 1811015
2. Lê Thị Hà - 1812020
3. Lê Trung Hiếu - 1812167
4. Nguyễn Công Minh - 1813083

NHÓM : MinKHaiue

KHOA : KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

NHÓM : L04 (T5 tiết 7,8)

Tháng 12/2020

MỤC LỤC

I. Tìm hiểu cấu trúc mạng thích hợp cho các tòa nhà	4
Phân tích yêu cầu của hệ thống mạng Trụ sở và Chi nhánh: Xây dựng hệ thống mạng cho một ngân hàng BBB:	4
1.1 Trụ sở chính tại TP. Hồ Chí Minh	4
1.2 Các chi nhánh:	4
1.3 Phân tích ưu điểm, nhược điểm của các phương pháp được chọn:	4
Lập bảng các chi tiết cần khảo sát ở các vị trí cài đặt	6
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)	7
3.1 Trụ sở chính	7
3.2 Chi nhánh	8
Lựa chọn cấu trúc Mạng phù hợp với kiến trúc, sự thuận lợi và thẩm mỹ của tòa nhà	9
II. Danh sách các trang thiết bị tối thiểu, sơ đồ IP và sơ đồ đi dây(cabling)	10
Danh sách thiết bị đề xuất và các đặc điểm kỹ thuật điển hình	10
Access-point	10
Sơ đồ thiết lập vật lý của hệ thống	13
2.1 Trụ sở chính (7 tầng, 100 work station, 5 server)	13
2.2 Chi nhánh (2 tầng: 3 server, 50 workstations)	16
Sơ đồ kết nối WAN giữa Trụ sở và Chi nhánh(dùng giao thức OSPF)	17
III. Tính toán Throughput, bandwidth và các thông số an toàn cho Mạng máy tính	17
IV. Thiết kế sơ đồ mạng dùng phần mềm mô phỏng Cisco Packet Tracer	18
V. Test lại hệ thống bằng những công cụ phổ biến như ping, traceroute,... trên hệ thống được mô phỏng	18
VI. Đánh giá lại hệ thống mạng thông qua các đặc tính	18
Độ tin cậy, an toàn, bảo mật dữ liệu, nâng cấp hệ thống	18
Định hướng phát triển trong tương lai	21

I. Tìm hiểu cấu trúc mạng thích hợp cho các tòa nhà

1. Phân tích yêu cầu của hệ thống mạng Trụ sở và Chi nhánh: Xây dựng hệ thống mạng cho một ngân hàng BBB:

1.1 Trụ sở chính tại TP. Hồ Chí Minh

- Tòa building cao khoảng 7 tầng, tầng 1 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 về hạ tầng mạng 100/1000Mbps, Wired và Wireless
- Tổ chức hệ thống mạng theo cấu trúc VLAN. Tức là chia nhỏ mạng của trung tâm thành các mạng con cho các phòng ban. Các máy tính trong mạng VLAN này có thể truy cập lẫn nhau nhưng những máy thuộc mạng bên ngoài
- 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, dễ dàng nâng cấp hệ thống
- Có khả năng kết nối đến chi nhánh đến ở Nha Trang và Đà Nẵng.
- Có khả năng đáp ứng người dùng trong vòng 5 năm tới

1.2 Các chi nhánh:

Gồm 2 chi nhánh Nha Trang và Đà Nẵng với qui mô nhỏ hơn trụ sở chính:

- Tòa nhà cao khoảng 2 tầng, tầng 1 được trang bị 1 phòng kỹ thuật Mạng và Cabling Central Local.
- BBB dạng chi nhánh: 50 workstations, 3 Servers, 5 Network Equipments

→ Việc thực hiện kết nối giữa trụ sở và chi nhánh thông qua đường links WAN thuê bao bên thứ ba, chúng ta có thể chọn một trong các công nghệ dùng cho đường links này theo tính kinh tế của giải pháp

1.3 Phân tích ưu điểm, nhược điểm của các phương pháp được chọn:

1.3.1 Kiến trúc mạng Vlan

+ *Ưu điểm*

- **Tiết kiệm băng thông của hệ thống mạng:** VLAN chia mạng LAN thành nhiều đoạn (segment) nhỏ, mỗi đoạn đó là một vùng quảng bá (broadcast domain). Khi có gói tin quảng bá (broadcast), nó sẽ được truyền duy nhất trong VLAN tương ứng. Do đó việc chia VLAN giúp tiết kiệm băng thông của hệ thống mạng, giảm overhead trên CPU thiết bị
- **Tăng khả năng bảo mật:** Do các thiết bị ở các VLAN khác nhau không thể truy nhập vào nhau (trừ khi ta sử dụng router nối giữa các VLAN). Ví dụ trong mô hình phát triển lần này, các máy tính trong VLAN kế toán (Accounting) chỉ có thể liên lạc được với nhau. Máy ở VLAN kế toán không thể kết nối được với máy tính ở VLAN kỹ thuật (Engineering).
- **Dễ dàng thêm hay bớt máy tính vào VLAN:** Việc thêm một máy tính vào VLAN rất đơn giản, chỉ cần cấu hình cổng cho máy đó vào VLAN mong muốn. Trong doanh nghiệp việc di chuyển, thay đổi phòng ban là thường xuyên diễn ra nên vlan rất linh động trong việc thay đổi cập nhật
- **Giúp mạng có tính linh động cao:** VLAN có thể dễ dàng di chuyển các thiết bị. Với VLAN, ta chỉ cần cấu hình lại các cổng switch rồi đặt chúng vào các VLAN theo yêu cầu. VLAN có thể được cấu hình tĩnh hay động.
- + **Khuyết điểm:**
 - Nhược điểm của VLAN là chuẩn chính thức IEEE 802.1q chưa được phê duyệt nên việc thiết lập và cấu hình VLAN phải phụ thuộc nhiều vào nhà sản xuất thiết bị mạng.

1.3.2 Leased line

- + **Ưu điểm:**
 - **Kết nối Internet chuyên dụng, tốc độ cao:** Trong quá trình kết nối, Leased line không chia sẻ băng thông với các doanh nghiệp hoặc người dùng khác. Dịch vụ đảm bảo băng thông cố định, hạn chế xảy ra sự cố tắc nghẽn trong giờ cao điểm. Mô hình ngân hàng cần thời gian giao dịch tức thời, và có những khung giờ cao điểm nếu băng thông bị chia sẻ rất bất tiện

- *Đảm bảo tính riêng tư và bảo mật cao:* Leased line là đường truyền kết nối chuyên dụng dành riêng cho doanh nghiệp, công ty nên có thể đảm bảo tính riêng tư và bảo mật cao. Bên cạnh đó, hệ thống kết nối còn được quản lý và bảo vệ từ nhà cung cấp dịch vụ, tránh sự xâm nhập của các đối tượng xấu. Doanh nghiệp còn nhận được sự hỗ trợ 24/7 với dịch vụ ngân hàng bảo mật là điều kiện tiên quyết

2. Lập bảng các chi tiết cần khảo sát ở các vị trí cài đặt

1. Software:

Chúng ta dùng hai loại Licensed và Open Source Software

- Licensed software thường là các phần mềm bản quyền, không thể chỉnh sửa, phần mềm chúng ta phải trả tiền thường phục vụ các chức năng có sẵn không thể thêm xóa bớt tùy ý được. Ưu điểm của loại này là được hỗ trợ từ phía sản xuất và có tính ổn định cao.
- Open Source Software (phần mềm mã nguồn mở) là phần mềm được phát triển sẵn và cho phép chỉnh sửa ngay trong source code và được cộng đồng nâng cấp và phát triển. Loại phần mềm có ích khi ta muốn thêm bớt, chỉnh sửa các chức năng của chúng.

→ Ngân hàng cần có tính chuyên biệt hóa và cần có hệ thống ổn định và bảo mật cao nên ta sẽ chọn phần mềm Licensed software đã được kiểm chứng đảm bảo các yêu cầu cần thiết của ngân hàng.

- Về hệ điều hành: Ta sử dụng hệ điều hành Windows để đơn giản hóa cho việc sử dụng của nhân viên vì đây là hệ điều hành phổ biến và khả năng tương thích cao với hầu hết nhân viên.
- Phần mềm văn phòng: Nhân viên sử dụng phần mềm kế toán Misa và các công cụ soạn thảo của Microsoft Office có bản quyền.
- Phần mềm khác: Nhân viên có sử dụng thêm trình duyệt Chrome hoặc Edge để duyệt web.
- Phần mềm duyệt file server: vì đặc thù của ngân hàng là nó chứa tài liệu theo từng phòng ban. Phòng ban này không có quyền truy xuất vào dữ liệu phòng

ban kia khi chưa được phép, do đó ta dùng cơ chế quản lý theo user và theo group. Vì vậy ta nên chọn hệ điều hành windows server 2003 cho file servers.

- Về phần server: ta chọn hệ điều hành Linux để tối ưu bảo mật cho hệ thống.
- Về phần database server, vì Oracle có khả năng tương thích tốt cho các database lớn như doanh nghiệp và tính bảo mật cao nên ta sẽ cài Oracle database server.

3. 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)

3.1 Trụ sở chính

❖ Tầng 1:

Là nơi diễn ra giao dịch với khách hàng nên cần một tốc độ mạng nhanh và ổn định. Tầng 1 xử lý các nhu cầu giao dịch khách hàng nên các thiết bị phải là chuỗi thiết bị có nhu cầu truy xuất, xử lý dữ liệu nhiều nhất, . Trong bộ phận giao dịch, mỗi nhân viên được trang bị một máy tính riêng. Vì thực hiện giao dịch nên yêu cầu bảo mật ở mỗi máy tính này được đặt lên hàng đầu. Ngoài ra còn có một số máy tính và wifi cho khách hàng truy cập. Những đường truyền internet này không được tham gia thiết bị trong hệ thống. Cụ thể:

- | | |
|-------------------------------|------------|
| + Phòng kỹ thuật | : 3PCs |
| + Phòng Cabling Central Local | : 5 server |
| + Bộ phận giao dịch | : 20PCs |
| + Thư ký | : 2PCs |

❖ Tầng 2:

Bao gồm các phòng ban cơ bản khác, cụ thể:

- | | |
|-----------------------------|--------|
| - Phòng họp | : 2PCs |
| - Phòng thành viên quản trị | : 4PCs |
| - Thư ký | : 2PCs |

❖ Tầng 3: Tầng này sẽ được sử dụng là nơi làm việc của các phòng ban gồm Phòng công quỹ tài chính (10PCs)

❖ **Tầng 4:** Gồm phòng kế toán và phòng kinh doanh. Mỗi phòng ban tương ứng 10 PCs

❖ **Tầng 5:** Phòng nhân sự và phòng thương mại điện tử.

Đối với các phòng ban này, mỗi nhân viên sẽ được trang bị một máy tính được kết nối internet. Các máy được chia thành từng nhóm ứng với các phòng ban nhằm dễ quản lý. Bên cạnh đó, mỗi phòng ban còn được trang bị các thiết bị cần thiết như máy in nhằm vụ công việc in ấn báo cáo của phòng ban đó.

❖ **Tầng 6:**

- Giám đốc, phó giám đốc :2PCs
- Thư ký :2PCs
- Phòng họp :3PCs

❖ **Tầng 7:**

Khu vực dịch vụ, cửa hàng, căn tin dành riêng cho nhân viên ngân hàng, các phòng phục vụ dịch vụ cho nhân viên (thư viện, quán cafe, quán ăn, phòng tập thể dục, phòng y tế,...). Cho phép các thiết bị không trong hệ thống mạng truy cập internet.

3.2 Chi nhánh

Đối với chi nhánh, mỗi trụ sở chi nhánh gồm 2 tầng (50 work stations và 3 server)

❖ **Tầng 1:**

- 10 PCs cho bộ phận giao dịch
- 2 PC cho tiếp tân
- 10 thiết bị cho khách ngoài hệ thống
- 3 PCs cho bộ phận kỹ thuật
- Phòng đặt 3 server

❖ **Tầng 2:**

- 1 phòng họp (5PCs)
- Phòng kế toán (5 PCs)
- Phòng giám đốc và phó giám đốc chi nhánh (2PCs)
- 2 thư ký (2PCs)

- Phòng kinh doanh (6PCs)
- Phòng nhân sự (5PCs)

Vậy theo nhu cầu của ngân hàng, ta phân bố server như sau:

- **Trụ sở chính**

- Database server: 1 cái
- File server: 1 cái
- Web server: 1 cái
- Mail server: 1 cái
- Bank operation processing server (dùng để xử lý các tác vụ chuyên biệt của ngân hàng): 1 cái

Tất cả các server đều được đặt tại phòng tập trung dây mạng và patch panel ở tầng 2 của trụ sở chính.

- **Chi nhánh**

- Database server: 1 cái
- File and mail server: 1 cái
- Backup server: 1 cái

Tất cả các server đều được đặt tại phòng tập trung dây mạng và patch panel ở tầng 2 của chi nhánh.

4. Lựa chọn cấu trúc Mạng phù hợp với kiến trúc, sự thuận lợi và thẩm mỹ của tòa nhà

Cấu trúc hạ tầng mạng trụ sở ngân hàng dự kiến bao gồm các phần sau:

➤ Phân hệ kết nối Internet và truy cập từ xa

- Được trang bị các thiết bị kết nối Gateway Cisco Router riêng kết nối với mạng Internet. Tùy theo nhu cầu phát triển hệ thống mà có thể mở rộng và nâng cấp tốc độ cổng kết nối Internet.
- Người dùng muốn truy cập phải được xác thực theo quyền truy cập để vào mạng nội bộ hoặc Internet và CSDL dùng để xác thực được quản lý tập trung trên máy chủ ACS đặt ở vùng quản trị hệ thống.

➤ Phân hệ mạng DMZ

- Gồm hệ thống máy chủ Web, Email dành cho khách hàng, nội bộ truy cập. Trên máy chủ Web có các hệ thống giao dịch trên Web của ngân hàng, Internet Banking, Home Banking, có thể tra cứu các sản phẩm của ngân hàng, các hệ thống đào tạo, dạy học điện tử nội bộ, các thông tin quảng cáo, ... Máy chủ Web và máy chủ Email của các tài khoản nội bộ hay khách hàng đều được cài các bộ lọc theo các nội dung, các địa chỉ trang Web.
 - Ngoài ra khu vực này còn có các máy chủ Virus để kiểm tra virus đối với các thông tin trong và ngoài Internet.
- Phân hệ mạng nội bộ:
- Bao gồm các clients đặt trên các tầng của tòa nhà, phục vụ cho các nhân viên làm việc, duyệt web, gửi mail, ...

II. Danh sách các trang thiết bị tối thiểu, sơ đồ IP và sơ đồ đi dây(cabling)

1. Danh sách thiết bị đề xuất và các đặc điểm kỹ thuật điển hình

○ Access-point

- Ngân hàng sử dụng access-point nhằm cung cấp hệ thống wifi cho khách hàng để kết nối internet khi tiến hành giao dịch với ngân hàng.



Access Point Linksys 54G

○ Check-Point

- Hạn chế sự tấn công từ bên ngoài vào khi bên ngoài kết nối với các Vlan
- Ngăn chặn một số dịch vụ không cho phép.



Check Point - Firewall 730

- **Switch**

- Ở đây chúng ta sử dụng switch Cisco Catalyst 2960(mỗi switch có 24 port)



Switch Cisco Catalyst 2960

- **Core Switch**

- Core Builder là switch layer 2 nhưng có tốc độ cao dùng để kết nối các switch với nhau.
- Ở đây, ta chọn Core Builder 9000.

- **Firewall**

- Để đảm bảo tính bảo mật thông tin thì việc thiết yếu là xây dựng một firewall, đặc biệt đối với ngân hàng, bảo mật thông tin vô cùng quan trọng.
- Ở đây ta chọn firewall 5540 IDS.

- **Router**

- Đây là một thiết bị không thể thiếu trong việc kết nối ra ngoài đối với bất kỳ một hệ thống mạng nào. Ở đây chúng ta sử dụng router của Cisco.



Router Cisco 4331

- **Server**

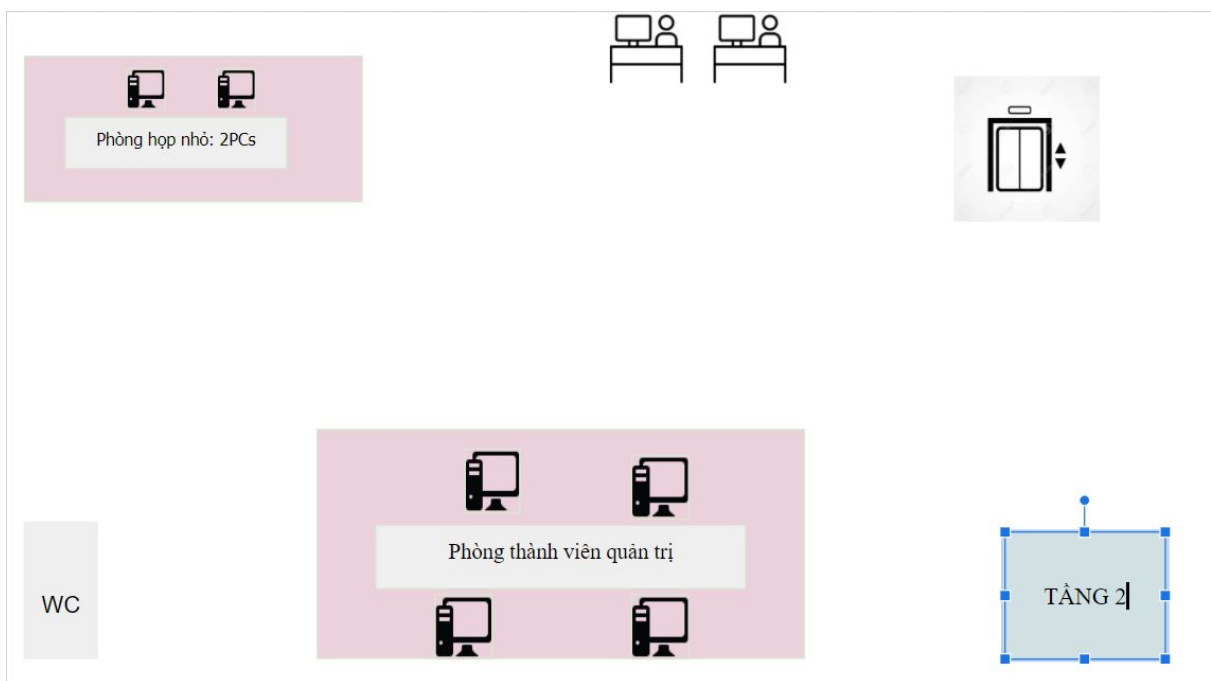
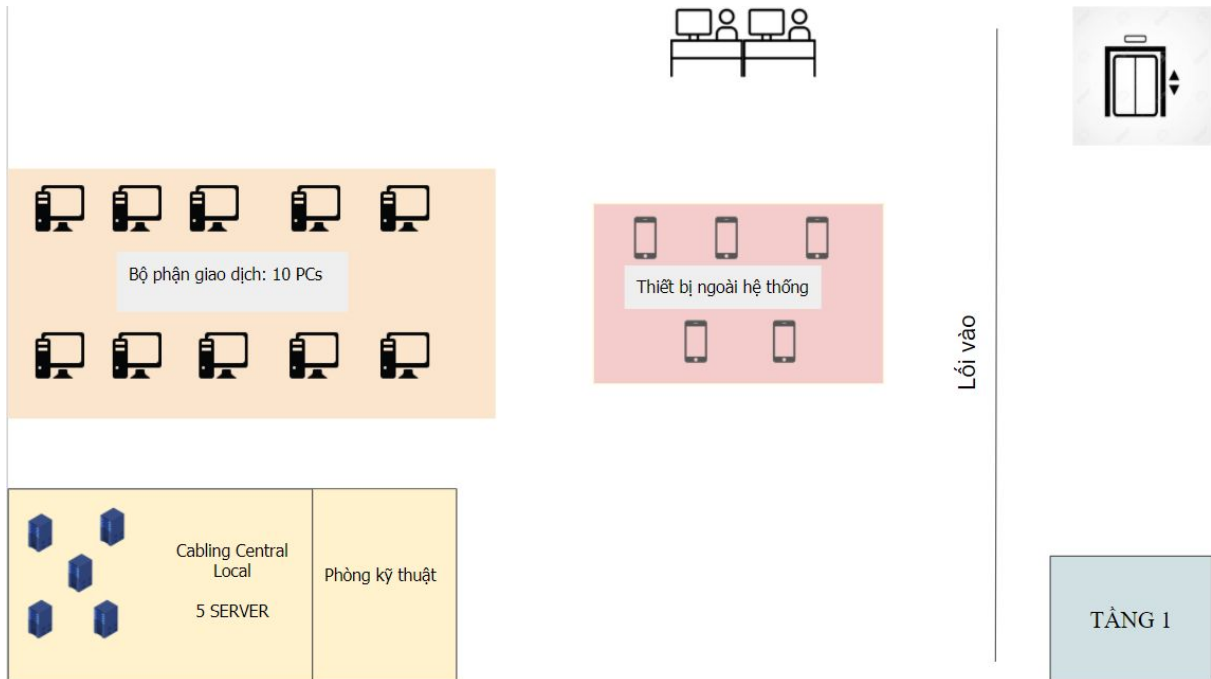
Các server thiết yếu của một ngân hàng bao gồm:

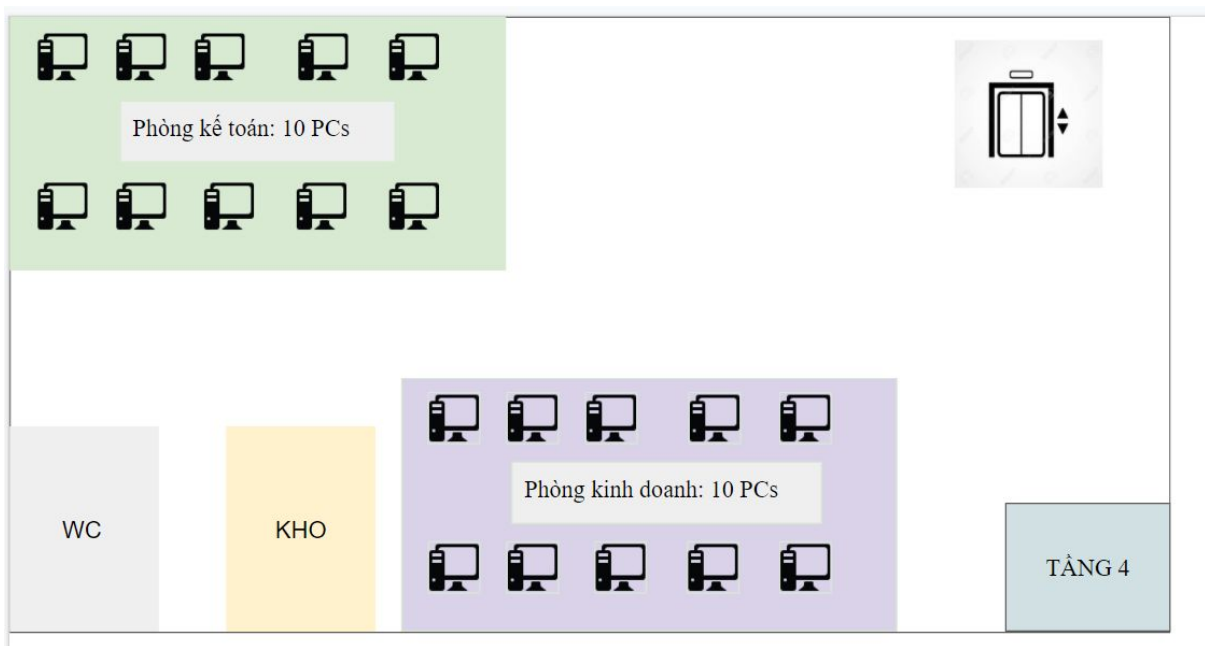
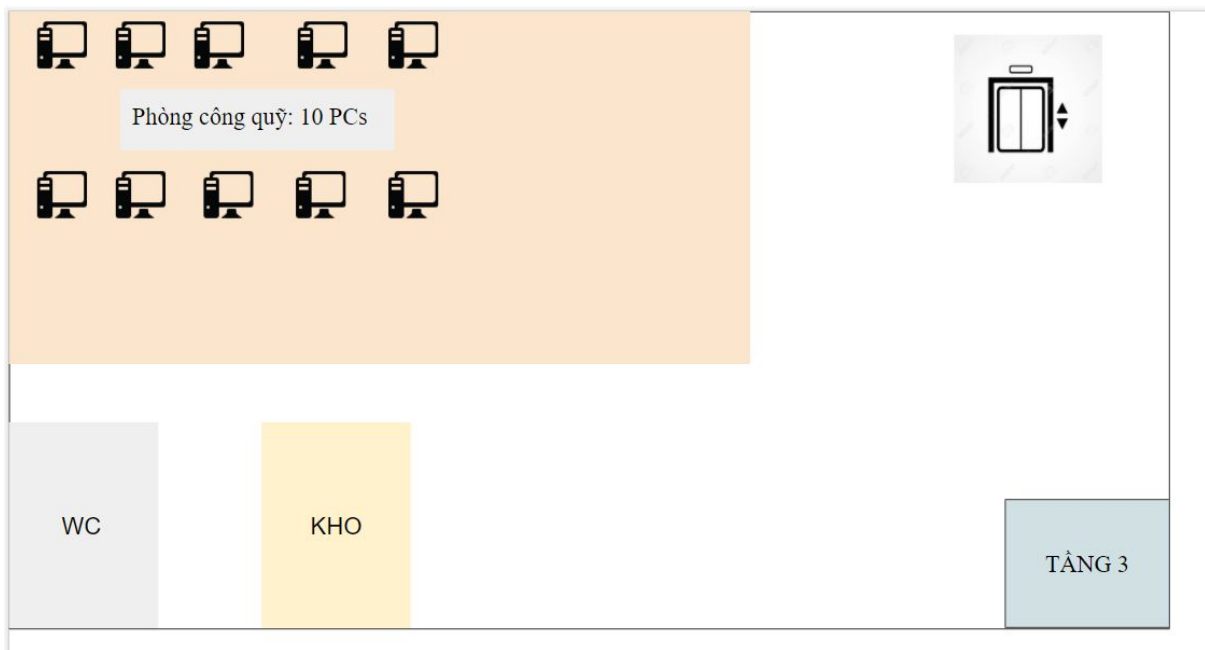
- Web server: Để những khách hàng bên ngoài truy cập để xem thông tin về tài khoản của họ trong ngân hàng, cập nhật thông tin và các dịch vụ khác.
- Mail server: Để gửi và nhận mail.
- DNS server: Dịch tên miền ra địa chỉ IP.
- Database server: Để lưu trữ thông tin.
- Bank Server: Tính toán, xử lý thông tin.

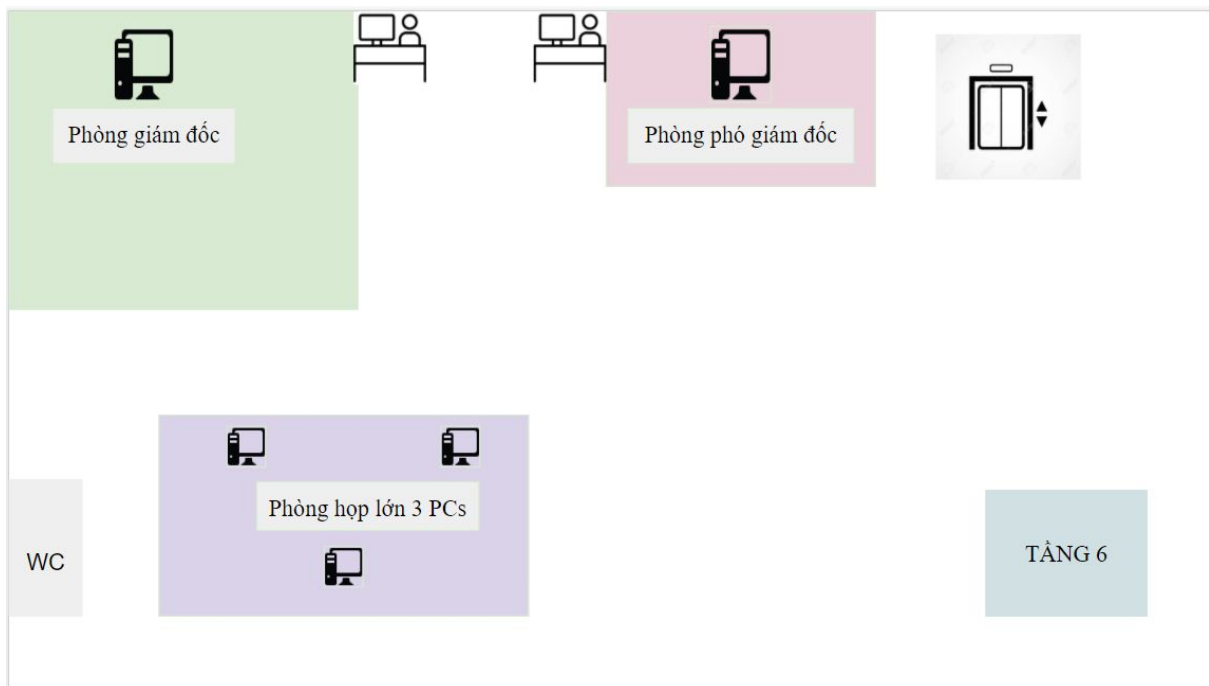
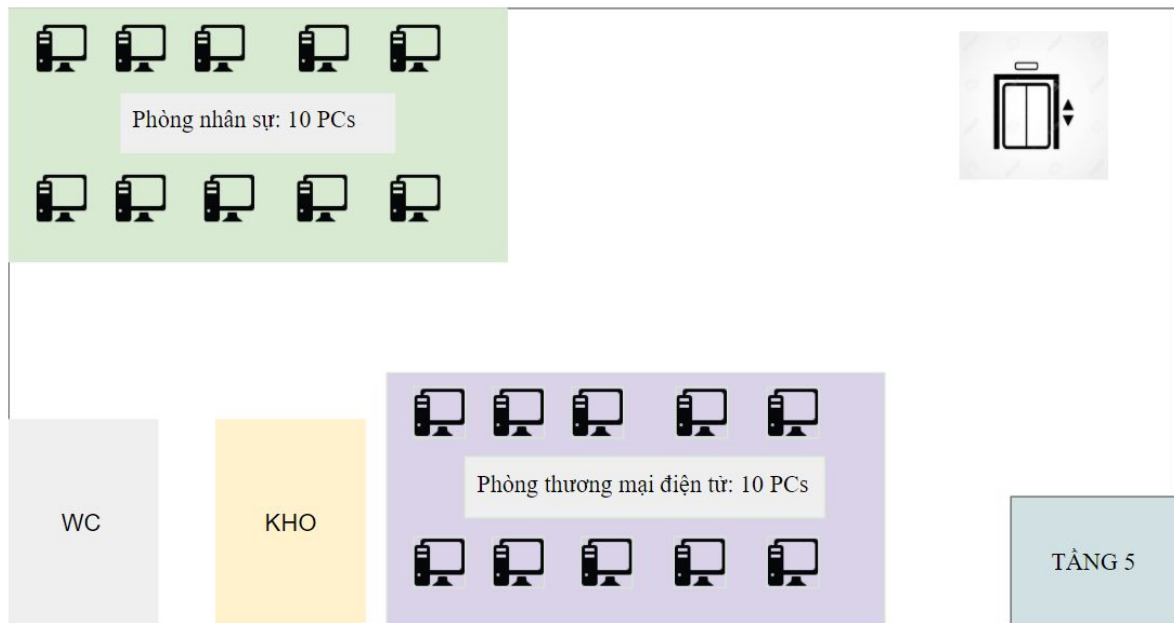
- **Workstation:** máy tính, máy in, ...

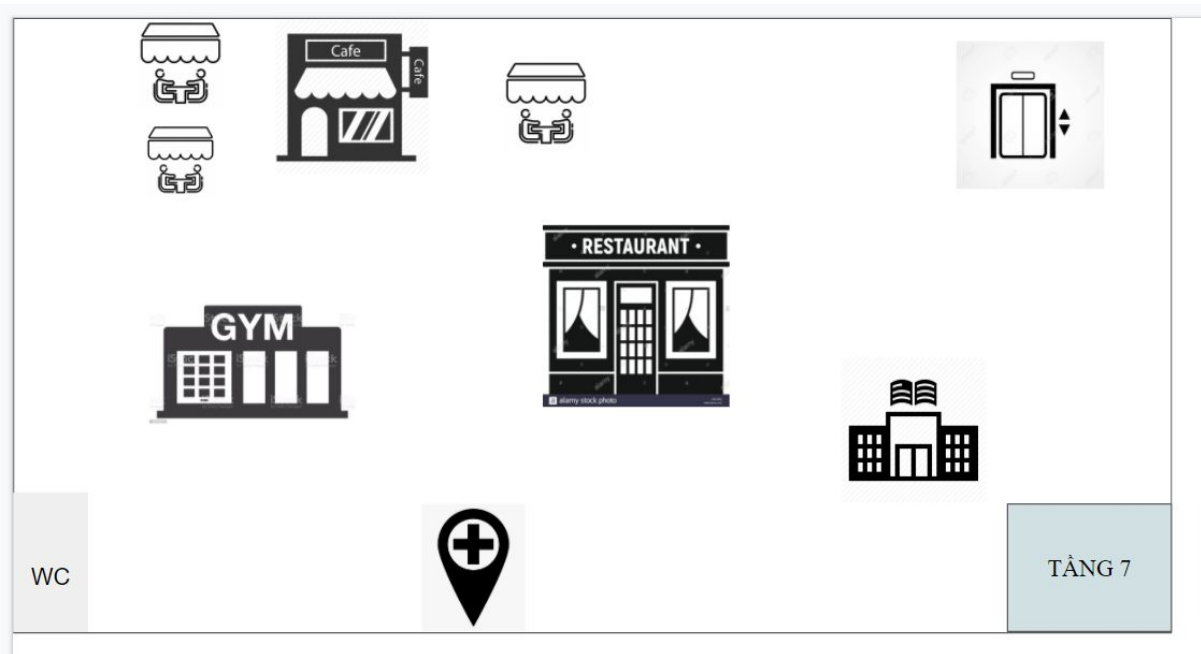
2. Sơ đồ thiết lập vật lý của hệ thống

2.1 Trụ sở chính (7 tầng, 100 work station, 5 server)

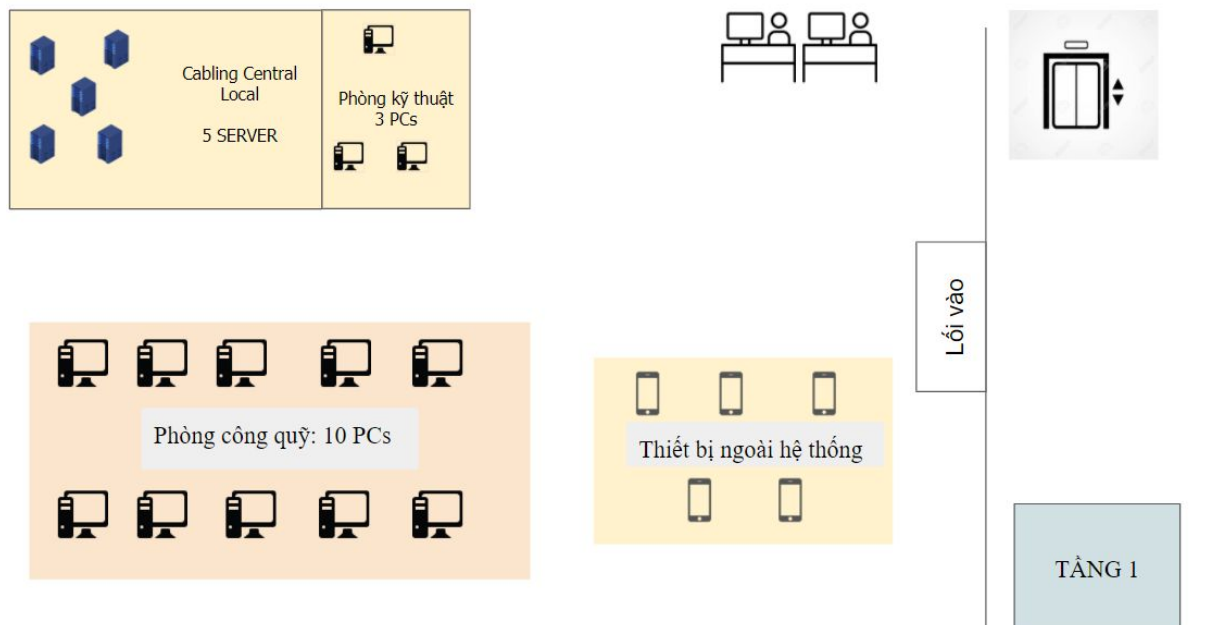


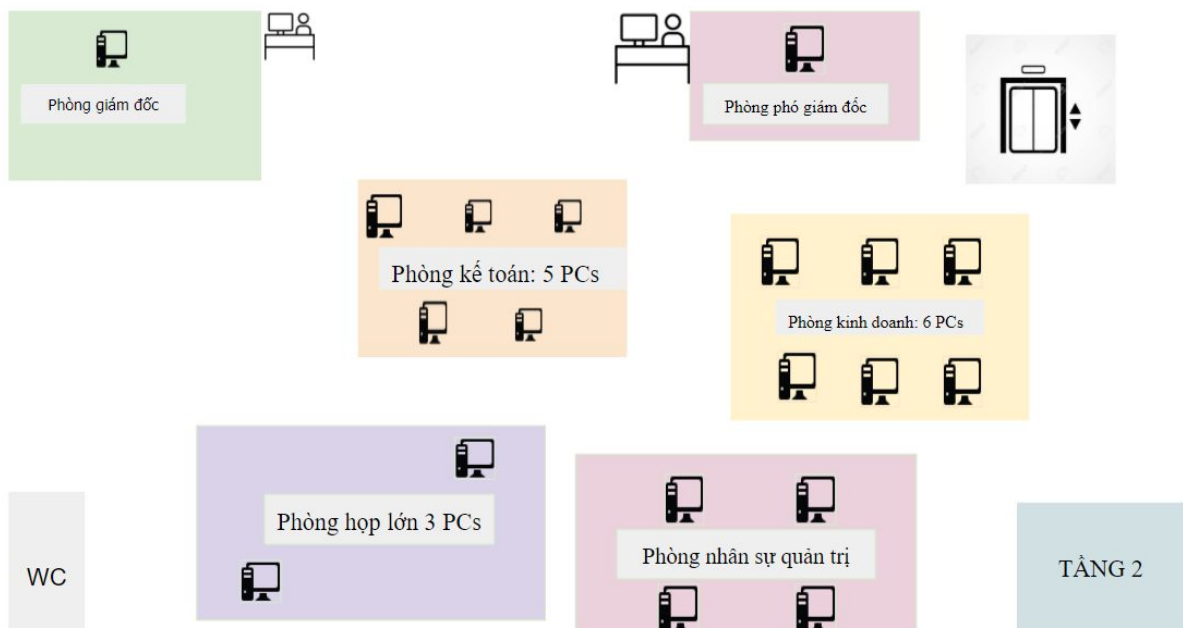






2.2 Chi nhánh (2 tầng: 3 server, 50 workstations)

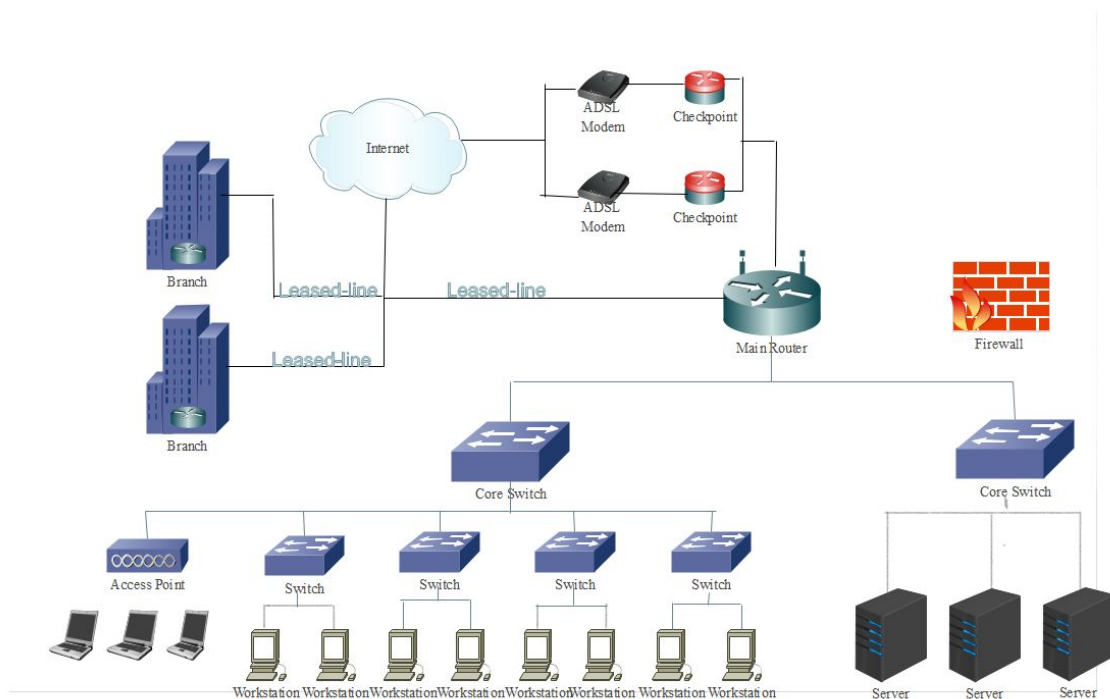




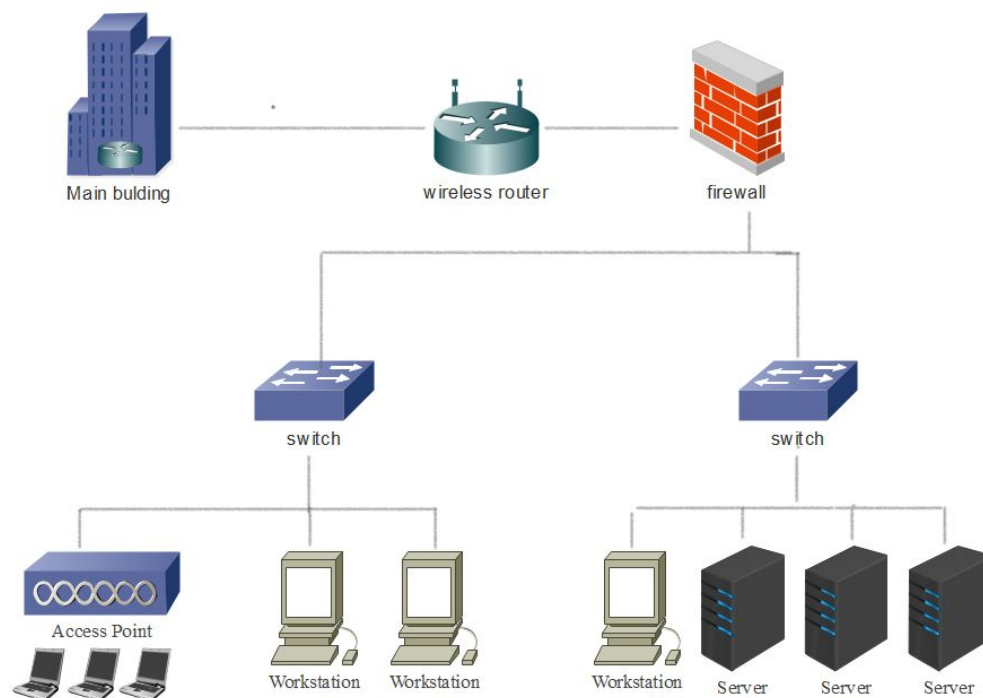
3. Sơ đồ kết nối WAN giữa Trụ sở và Chi nhánh (dùng giao thức OSPF)

○ Sơ đồ thiết bị

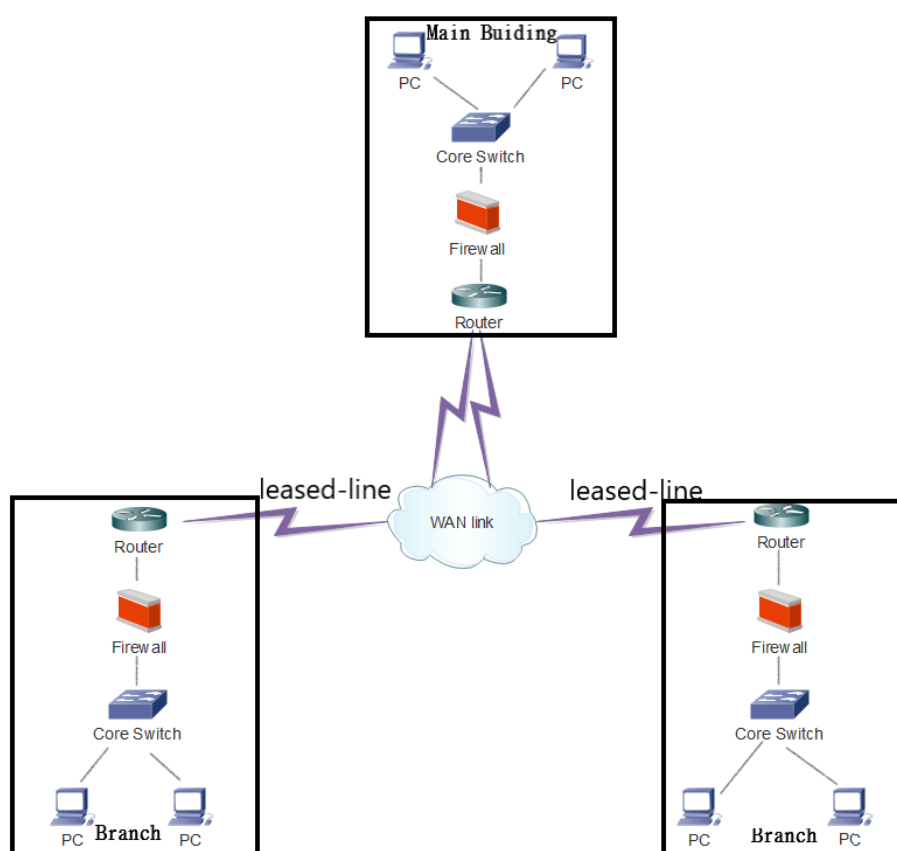
➤ Toàn hệ thống:



➤ Chi nhánh



○ Sơ đồ kết nối WAN giữa trụ sở và chi nhánh



4. Sơ đồ địa chỉ IP

4.1. Sơ đồ VLAN tại trụ sở chính

VLAN	Phòng ban	Địa chỉ IP danh định	Miền cung cấp IP
VLAN1	Phòng Kỹ thuật	192.168.10.0/24	192.168.10.1 ->192.168.10.254
VLAN2	Ban quản trị	192.168.12.0/24	192.168.12.1 ->192.168.12.254
VLAN3	Phòng Công quỹ tài chính	192.168.13.0/24	192.168.13.1 ->192.168.13.254
VLAN4	Phòng Kế toán	192.168.15.0/24	192.168.15.1 ->192.168.15.254
VLAN5	Phòng Kinh doanh	192.168.17.0/24	192.168.17.1 ->192.168.17.254
VLAN6	Phòng Nhân sự	192.168.18.0/24	192.168.18.1 ->192.168.18.254
VLAN7	Phòng Thương mại điện tử	192.168.19.0/24	192.168.19.1 ->192.168.19.254
VLAN8	Phòng Giao dịch	192.168.20.0/24	192.168.20.1 ->192.168.20.254

4.2. Sơ đồ VLAN tại chi nhánh 1

VLAN	Phòng ban	Địa chỉ IP danh định	Miền cung cấp IP
VLAN1	Phòng Kỹ thuật	192.100.2.0/24	192.100.2.1 ->192.100.2.254
VLAN2	Ban quản trị	192.100.3.0/24	192.100.3.1 ->192.100.3.254
VLAN3	Phòng Công quỹ tài chính	192.100.4.0/24	192.100.4.1 ->192.100.4.254
VLAN4	Phòng Kế toán	192.100.6.0/24	192.100.6.1 ->192.100.6.254
VLAN5	Phòng Kinh doanh	192.100.10.0/24	192.100.10.1 ->192.100.10.254
VLAN6	Phòng Nhân sự	192.100.12.0/24	192.100.12.1 ->192.100.12.254

4.3. Sơ đồ VLAN tại chi nhánh 2

VLAN	Phòng ban	Địa chỉ IP danh định	Miền cung cấp IP
VLAN1	Phòng Kỹ thuật	192.200.2.0/24	192.200.2.1 ->192.200.2.254
VLAN2	Ban quản trị	192.200.3.0/24	192.200.3.1 ->192.200.3.254
VLAN3	Phòng Công quỹ tài chính	192.200.4.0/24	192.200.4.1 ->192.200.4.254
VLAN4	Phòng Kế toán	192.200.6.0/24	192.200.6.1 ->192.200.6.254
VLAN5	Phòng Kinh doanh	192.200.10.0/24	192.200.10.1 ->192.200.10.254
VLAN6	Phòng Nhân sự	192.200.12.0/24	192.200.12.1 ->192.200.12.254

III. Tính toán Throughput, bandwidth và các thông số an toàn cho Mạng máy tính

- Số workstation của ngân hàng: $100 + 50 * 2 = 200$ workstations
- Số server của ngân hàng: $5 + 3 * 2 = 11$ server
- Một workstation trong 1 ngày dùng 100MB
- Một server trong 1 ngày dùng 500MB
- Dung lượng dùng trong 1 ngày của ngân hàng là:
 $200 * 100 + 11 * 500 + 50 = 25550 \text{MB}$
- Dung lượng dùng trong 3h cao điểm(9h-11h và 15h-16h) là:
 $25550 * 80\% = 20440 \text{MB}$
- 1 ngày làm việc 8 tiếng => Throughput cần cung cấp ngân hàng là
 $20440 * 8 / (3 * 60 * 60) = 15.14 \text{ Mbps}$
- Ta cần thiết kế an toàn cho việc mở rộng công ty(khoảng thêm 20%):
 $15.14 * 1.2 = 18.17 \text{ Mbps}$
- Ta có thể thuê một đường truyền có ổn định cao, và có bandwidth là 19Mbps (an toàn). Việc tính throughput và bandwidth như vậy đáp ứng được trong điều kiện ở giờ cao điểm, mạng vẫn hoạt động tốt.**

IV. Thiết kế sơ đồ mạng dùng phần mềm mô phỏng Cisco Packet Tracer

V. Test lại hệ thống bằng những công cụ phổ biến như ping, traceroute,.. trên hệ thống được mô phỏng

VI. Đánh giá lại hệ thống mạng thông qua các đặc tính

1. Độ tin cậy, an toàn, bảo mật dữ liệu, nâng cấp hệ thống

Hoạt động của ngân hàng có khối lượng thông tin khổng lồ của các hoạt động nghiệp vụ. Tuy nhiên những thông tin này giới hạn những người có thể truy cập. Do đó nhu cầu thiết yếu của ngân hàng là xây dựng một hệ thống bảo mật phục vụ điều hành, kinh doanh. Cần xác định rõ các yếu tố sau:

➤ Yêu cầu hệ thống bảo mật phải đảm bảo:

- An toàn cho toàn bộ thông tin trên mạng, ngăn cản mọi sự truy cập bất hợp pháp.
- Kiểm soát, quản lý chặt chẽ việc truy cập hệ thống của người dùng.
- Đảm bảo an toàn dữ liệu truyền, nhận qua các dịch vụ đường truyền ra internet.
- Chi phí phù hợp với dự trù của ngân hàng.
- Đáp ứng được khả năng mở rộng trong tương lai của ngân hàng.

➤ Các tài nguyên cần được bảo vệ:

- Phần cứng: các máy chủ mạng, các máy trạm và các thiết bị mạng như Routers, Access Servers.
- Phần mềm: Đầu tiên là các hệ điều hành máy chủ Windows, Linux,... Tiếp theo là các chương trình ứng dụng: quản lý hệ thống tài khoản, tín dụng, các chương trình kế toán, tự động hóa văn phòng, truyền dữ liệu, ATM...
- Dữ liệu: Đây là phần quan trọng cần được bảo vệ. Dữ liệu gồm có dữ liệu tài khoản khách hàng, dữ liệu kế toán, thẻ tín dụng, ATM, ...

- Tài liệu: Các công văn, báo cáo, tài liệu, sách vở, ...

➤ Các mối đe dọa đối với hệ thống:

- Những truy cập bất hợp pháp: Việc truy cập tài nguyên của mạng phải được chia theo từng phân lớp, nhóm người một cách hợp lý.
- Mối đe dọa bởi sự khai thác thông tin: Các thông tin mật của ngân hàng có thể bị xâm phạm khi:
 - Thông tin được lưu trữ trên máy tính, trong tệp sao lưu.
 - Thông tin được truyền từ hệ thống này sang hệ thống khác.
- Mối đe dọa ảnh hưởng hoạt động bình thường của hệ thống:
 - Dữ liệu bị quá tải dẫn đến mạng hoạt động trì trệ, thất thoát dữ liệu và mạng trở nên kém hiệu quả.
 - Tốc độ truy cập mạng, truyền dữ liệu chậm.
 - Mạng không hoạt động hoặc hoạt động bị gián đoạn khi có một thiết bị mạng ngừng hoạt động hoặc một thiết bị bảo vệ mạng bị phá vỡ.
 - Virus phá hoại dữ liệu và làm mạng ngừng hoạt động.
- Mối đe dọa từ bên trong:
 - Đối với hệ thống ngân hàng, đặc thù là do nhiều mạng LAN của trung tâm, chi nhánh kết nối vào. Do đó, nếu những người bên trong hệ thống có ý muốn và cố ý truy cập vào những tài nguyên không được phép của hệ thống sẽ gây mối đe dọa cho mạng.
 - Người sử dụng bên trong có thể vô tình được gán những quyền vượt phạm vi quyền của họ hoặc bị mất mật khẩu, lấy cắp tài khoản truy cập,...
- Mối đe dọa từ bên ngoài:
 - Nguy cơ bị nghe trộm, thay đổi thông tin truyền đi trên mạng công cộng. Điều này ẩn chứa nhiều nguy hiểm và ảnh hưởng trực tiếp đến hoạt động kinh doanh của ngân hàng.
 - Hacker có thể sử dụng các thiết bị đặc biệt để móc nối vào hệ thống cáp truyền thông của ngân hàng để nghe trộm thông tin,

nguy hiểm hơn hacker có thể sửa chữa, thay đổi nội dung thông tin đó – ví dụ nội dung của điện chuyển tiền .. gây ra những hậu quả nghiêm trọng.

➤ An toàn khi xảy ra sự cố:

- Có 2 loại sự cố mạng là sự cố về cơ sở hạ tầng mạng và sự cố về an toàn thông tin. Cần thiết kế hệ thống mạng sao cho ít xảy ra sự cố và nếu có sự cố xảy ra thì thời gian khắc phục ngắn nhất.
- Đường kết nối internet: Ta sử dụng 2 đường leased line 1.2 Mbps và đường ADSL 8 Mbps. Đường kết nối chính là đường leased-line và sử dụng cơ chế load-balancing nhằm chia tải của đường leased-line qua đường ADSL khi đường leased-line bị quá tải hay gặp sự cố.
- Với các thiết bị kết nối ra internet: Các thiết bị phải có cơ chế dự phòng, khi hoạt động bình thường thì tất cả kết nối diễn ra theo đường chính, khi xảy ra sự cố ở một trong các thiết bị mạng thì lập tức phải truyền sang đường dự phòng.
- Dữ liệu: Cần có backup server cho các server web, mail, database, ... và phải backup thường xuyên để phòng trừ việc mất dữ liệu khi xảy ra sự cố trên các server.
- Phân hệ mạng nội bộ: Sử dụng switch có cơ chế spanning-tree giúp chúng ta tạo ra các đường kết nối dự phòng mà không bị loop, ngăn chặn sự gián đoạn của hệ thống ngân hàng khi switch chính gặp sự cố. Khi đó switch dự phòng sẽ hoạt động.
- Xây dựng một phòng kỹ thuật chuyên về hệ thống mạng để giải quyết các vấn đề khi hệ thống ngân hàng xảy ra sự cố.

➤ Nâng cấp hệ thống:

- Việc thiết kế hệ thống mạng phải tính đến những sự tăng thêm sau này. Chẳng hạn như bổ sung nhân sự, tăng số lượng đối tác, số lượng chi nhánh, các server được truy cập nhiều hơn. Bảng thông đã tính đến dự phòng 20% nên có thể đáp ứng được chỉ số an toàn, đảm bảo hệ thống

hoạt động ổn định và chỉ cần đăng kí thay đổi gói cước với nhà cung cấp dịch vụ (ISP) là có thể tăng băng thông. Sử dụng các thiết bị mạng của Cisco – công ty hàng đầu về thiết bị mạng đồng nghĩa mạng được trang bị kỹ thuật tốt hơn, thiết bị ổn định hơn. Đặc biệt trong các sản phẩm của Cisco thường được tích hợp sẵn các công nghệ mới, linh hoạt với yêu cầu sử dụng.

2. Những hạn chế còn vướng mắc cho dự án

- Thiết bị mạng còn hạn chế, không dễ có thay thế trong trường hợp hư hỏng.
- Không có đường dây dự phòng cho mạng LAN.

3. Định hướng phát triển trong tương lai

- Tăng cường thêm dây ADSL kết nối trực tiếp từ chi nhánh ra internet.
- Tăng cường các thiết bị mạng nhằm thay thế trong trường hợp bị hư hỏng.
- Nâng cấp server, đặc biệt là backup server, nâng cấp đường truyền mạng..

VII. Tài liệu tham khảo:

[1]<https://www.cisco.com/c/en/us/td/dg/firewall.pdf>

[2] <http://www.theijes.com/papers/vol6-issue10/Version-2/I0610026377.pdf>

[3] <https://patents.google.com/patent/US8422500B2/en>

[4] <https://patents.google.com/patent/US6975581B1/en>