ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

MẠNG MÁY TÍNH (CO3093)

BÁO CÁO BÀI TẬP LỚN SỐ 2

HK231 - Lớp: L07 - Nhóm: 3

ĐỀ TÀI:

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE COMPANY

GV hướng dẫn: Lê Bảo Khánh

Danh sách thành viên:

STT	Họ và tên	MSSV	Tỷ lệ đóng góp
1	Lìu Ngọc Yến	2115373	120%
2	Trịnh Khải Toàn	2113269	80%
3	Từ Mai Thế Nhân	2114277	100%
4	Lê Hoàng Anh Vũ	2115319	100%

TP. Hồ Chí Minh, Tháng 11/2023

Mục lục

Danh sách hình vẽ

1 Phân công công việc

STT	Họ và tên	MSSV	Nhiệm vụ
1	Lìu Ngọc Yến	2115373	Thiết kế hệ thống, mô phỏng hệ thống
2	Trịnh Khải Toàn	2115036	Thiết kế hệ thống, viết báo cáo, làm slide
3	Từ Mai Thế Nhân	2114277	Thiết kế hệ thống, viết báo cáo, làm slide
4	Lê Hoàng Anh Vũ	2115319	Thiết kế hệ thống, viết báo cáo, làm slide

2 Đặt vấn đề

Công nghệ thông tin đang ngày càng thâm nhập sâu vào các mặt của đời sống con người. Xu hướng cả thế giới đang hướng tới hiện tại là "Internet of Things" - Vạn vật kết nối. Điều này có nghĩa, mọi thứ xung quanh chúng ta hiện tại, đều có tiềm năng trở thành "thành viên" của một hệ thống mạng. Việc liên kết mọi thứ qua mạng đang ngày càng chứng tỏ ưu điểm của nó không chỉ trong quá trình kết nối trên diện rộng mà còn trong hiệu quả kinh tế.

Các ứng dụng mạng, công nghệ kết nối như LAN, WAN ra đời đã hỗ trợ rất nhiều trong công cuộc phát triển của các doanh nghiệp. Chúng đặc biệt cần thiết cho các doanh nghiệp vừa đến lớn, cũng như các doanh nghiệp nhỏ đang có nhu cầu mở thêm chi nhánh và nâng cấp quy mô của mình, giúp đẩy mạnh quá trình chuyển đổi số cho các công ty nói riêng và quốc gia nói chung.

Hình 1: *Hệ thống mạng doanh nghiệp*

Vì những lý do đó, nhóm chọn đề tài "Thiết kế hệ thống mạng cho ngân hàng BBbank" để nghiên cứu. Trong hệ thống này, nhóm tạo khả năng kết nối giữa trụ sở chính, các chi nhánh và cả lực lượng lao động phân tán để cung cấp cho họ khả năng làm việc dù ở bất kỳ đâu (miễn là có kết nối internet).

3 Mục tiêu đề tài

- Nhiệm vụ này là về việc thiết kế cấu trúc liên kết mạng cho một công ty lớn trong đó các bộ phận khác nhau của công ty có một lượng máy tính ở các tòa nhà khác nhau và thiết lập hệ thống mạng cho họ để họ có thể tương tác và liên lạc với nhau bằng cách trao đổi dữ liệu. Mạng được thiết kế và mô phỏng bằng Cisco Packet Tracer.
- Cisco Packet Tracer (CPT) là phần mềm mô phỏng mạng đa nhiệm có thể được sử dụng để hiện thực và phân tích các hoạt động mạng khác nhau như thực hiện các cấu trúc liên kết khác nhau, lựa chọn các đường dẫn tối ưu dựa trên các bộ định tuyến khác nhau và phân tích các cấu hình mạng khác nhau.

4 Tìm hiểu cấu trúc mạng phù hợp cho tòa nhà

4.1 Yêu cầu hệ thống

CCC (Computer & Construction Concept) được yêu cầu thiết kế một mạng máy tính để triển khai tại Trụ sở chính (tại thành phố Hồ Chí Minh) và hai Chi nhánh (tại Đà Nẵng và Hà Nội) của một ngân hàng BB đang được xây dựng. Các đặc điểm chính của việc sử dụng Công nghệ thông tin trong Công ty này như sau.

4.1.1 Trụ sở chính

- Tòa nhà có 7 tầng, tầng đầu tiên được trang bị 1 phòng IT và Cabling Center Local.
- Mô hình tầm trung: 120 máy trạm, 5 servers, 12 (hoặc nhiều hơn nếu có thiết bị bảo mật) thiết bị mạng.
- Sử dụng các công nghệ mới cho cơ sở hạ tầng mạng bao gồm kết nối có dây và không dây, cáp quang (GPON) và GigaEthernet 1GbE/10GbE. Mạng được tổ chức dựa trên cấu trúc VLAN cho các phòng ban khác nhau.
- Phân mạng Trụ sở chính kết nối với hai phân mạng Chi nhánh thông qua 2 đường truyền thuê cho kết nối WAN (có thể áp dụng SD-WAN, MPLS) và 2 xDSL để truy cập Internet với cơ chế cân bằng tải. Toàn bộ lưu lượng đi ra Internet đi qua mạng con Trụ sở chính.
- Tất cả băng thông truy cập vào Internet đều phải đi qua mạng con của trụ sở chính.
- Dùng kết hợp giữa License và Open source Software, Ứng dụng văn phòng, client-server, đa phương tiện, database.
- Yêu cầu về tính bảo mật cao, mạnh mẽ khi có sự cố, dễ dàng nâng cấp hệ thống.
- Đề xuất cầu hình VPN cho site-to-site và cho những người làm việc từ xa để kết nối vào mạng LAN của công ty.
- Đề xuất hệ thống camera an ninh cho công ty.

4.1.2 Chi nhánh

- Ngân hàng có nhu cầu kết nối đến 2 chi nhánh khác ở 2 thành phố lớn Hà Nội và Đà Nẵng. Mỗi chi nhánh cũng được thiết kế tương tự như trụ sở chính nhưng quy mô nhỏ hơn:
  - Tòa nhà có 2 tầng, tầng đầu tiên được trang bị 1 phòng IT và 1 Cabling Center Local.
  - Mô hình tầm trung: 30 máy trạm, 3 servers, 5 (hoặc nhiều hơn nếu có thiết bị bảo mật) thiết bị mạng.
- 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. Phân tích ưu nhược điểm của giải pháp được chọn.

4.1.3 Các thông tin khác

- Các thông số lưu lượng và tải của hệ thống (khoảng 80% vào giờ cao điểm 9g-11g và 15g-16g) có thể dùng chung cho Trụ sở chính và chi nhánh như sau:
  - Server cho cập nhật phần mềm, truy cập web và truy cập cơ sở dữ liệu, với tổng ước tính tải xuống khoảng 1000 MB/ngày và tải lên ước tính là 2000 MB/ngày.
  - Mỗi workstation được sử dụng để duyệt Web, tải tài liệu, giao dịch khách hàng,... Tổng dung lượng tải lên là khoảng 100 MB/ngày và tải xuống khoảng 500 MB/ngày.
  - Kết nối wifi từ các thiết bị của khách hàng sử dụng cho việc tải xuống là khoảng 500 MB/ngày.
- Hệ thống mạng máy tính của Ngân hàng BB được ước tính đạt tốc độ tăng trưởng 20% trong 5 năm (tính theo số lượng người dùng, tải mạng, mở rộng chi nhánh,...).

4.2 Những vấn đề cần khảo sát ở địa điểm lắp đặt

4.2.1 Danh sách kiểm tra khảo sát của địa điểm lắp đặt

1. Trụ sở chính:
   - Phòng IT tầng 1:
     - Kiểm tra các cơ sở hạ tầng sẵn có.
     - Đảm bảo nguồn điện và chuẩn bị các nguồn điện dự phòng khi cần thiết.
     - Xác định điều kiện môi trường và đề ra những giải pháp để tránh ảnh hưởng đến các thiết bị mạng.
     - Xác định tính tương thích của thiết bị mạng hiện có với topology được chọn.
     - Đánh giá khả năng tiếp cận cho công việc bảo dưỡng và sửa chữa.
     - Kiểm tra hệ thống bảo mật
   - Trung tâm cáp tầng 1:
     - Đảm bảo nguồn điện cho thiết bị mạng.
     - Đánh giá các giải pháp quản lý dây cáp để đảm bảo gọn gàng.
     - Đánh giá khả năng tiếp cận cho bảo dưỡng dây cáp.
   - Tầng 2-7:
     - Kiểm tra không gian tòa nhà để sắp xếp thiết bị hợp lý.

  - Xác định số lượng và vị trí thiết bị trong mỗi phòng ban.
  - Kế hoạch cho kết nối có dây và không dây.
  - Kiểm tra hệ thống đường dẫn cáp hiện có hoặc lên kế hoạch cho những đường dẫn mới cho cáp mạng.
  - Kết nối giữa các chi nhánh và nhu cầu trao đổi dữ liệu.

2. Chi nhánh:

   - Phòng IT tầng 1:
     - Kiểm tra các cơ sở hạ tầng sẵn có.
     - Đảm bảo nguồn điện và chuẩn bị các nguồn điện dự phòng khi cần thiết.
     - Xác định điều kiện môi trường và đề ra những giải pháp để tránh ảnh hưởng đến các thiết bị mạng.
     - Xác định tính tương thích của thiết bị mạng hiện có với topology được chọn.
     - Đánh giá khả năng tiếp cận cho công việc bảo dưỡng và sửa chữa.
     - Kiểm tra hệ thống bảo mật
   - Trung tâm cáp tầng 1:
     - Đảm bảo nguồn điện cho thiết bị mạng.
     - Đánh giá các giải pháp quản lý dây cáp để đảm bảo gọn gàng.
     - Đánh giá khả năng tiếp cận cho bảo dưỡng dây cáp.
   - Tầng 2:
     - Kiểm tra không gian tòa nhà để sắp xếp thiết bị hợp lý.
     - Xác định số lượng máy tính và thiết bị trong mỗi phòng ban.
     - Kế hoạch cho kết nối có dây và không dây.
     - Kiểm tra hệ thống đường dẫn cáp hiện có hoặc lên kế hoạch cho những đường dẫn mới cho cáp mạng.
     - Kết nối giữa các chi nhánh và nhu cầu trao đổi dữ liệu.

3. Yêu cầu cụ thể:

   - Xác định các khu vực có mật độ người dùng cao và lên kế hoạch cân bằng tải.
   - Đảm bảo bảo mật của server và kho dữ liệu.

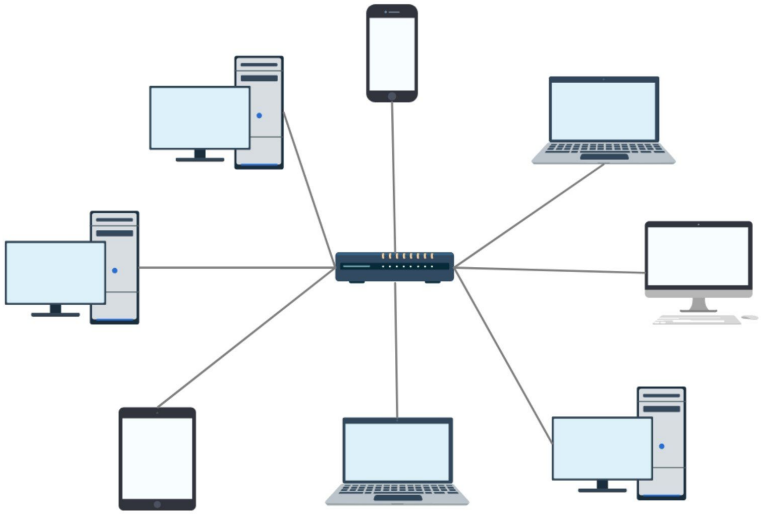
4.3 Xác định khu vực có tải cao

- Về kỹ thuật, hệ thống web server: Cho phép tất cả người dùng Internet đều có thể tìm kiếm thông tin, trao đổi thông tin với website ngân hàng. Do vậy, cần phải đảm bảo về tốc độ truy cập, tính ổn định.
- Theo nhóm nhận thấy, tầng 1 và 2 của trụ sở chính là nơi thường xuyên diễn ra giao dịch và số lượng máy lớn lại là nơi đặt phòng IT trung tâm gồm nhiều server nên đây sẽ là vùng có tải lượng lớn nên cần chú trọng cân bằng tải ở đây.
- Cấu hình thiết bị phù hợp:
  - Triển khai load balancer để phân phối yêu cầu đến nhiều máy chủ, cải thiện khả năng mở rộng và sẵn có.

– Sử dụng kết nối và switch tốc độ cao để kết nối máy chủ và đảm bảo truy cập dữ liệu nhanh chóng.

4.4 Cấu trúc mạng phù hợp với yêu cầu

- Dựa trên các yêu cầu trên của hệ thống, nhóm quyết định xây dựng cấu trúc mạng theo dạng hình sao (Star Topology). cấu trúc mạng dạng hình sao bao gồm một thiết bị làm trung tâm và các nút thông tin chịu sự điều khiển của thiết bị trung tâm đó. Bên trong mạng, các nút thông tin là những trạm đầu cuối. Đôi khi nút thông tin cũng chính là hệ thống các máy tính và những thiết bị khác của mạng LAN.



Hình 2: *Cấu trúc mạng hình sao*

Ưu điểm của cấu trúc:

– Đảm bảo quá trình hoạt động bình thường khi có một nút thông tin bị hư hỏng. Bởi kiểu mạng LAN này hoạt động dựa trên nguyên lý song song.

– Đặc điểm cấu trúc mạng đơn giản giúp cho thuật toán được điều khiển một cách ổn định hơn.

– Dễ dàng thu hẹp hay mở rộng theo nhu cầu, cũng như dễ dàng tăng khoảng cách cũng như độ lớn của mạng hình sao.

– Hạn chế tối đa các yếu tố gây ngưng trệ mạng trong quá trình hoạt động.

Nhược điểm của cấu trúc:

– Nhược điểm chính của trúc này là khi thiết bị trung tâm bị hỏng, các thiết bị kết nối sẽ bị gián đoạn giao tiếp.

– Hiệu suất của toàn mạng phụ thuộc vào hiệu suất của nút trung tâm.

Trong dự án này, nhóm sử dụng các switch làm trung tâm của các mạng hình sao và các nút thông tin là các workstation, server. Khu vực trung tâm đảm nhận nhiệm vụ điều phối mọi hoạt động bên trong hệ thống.

4.5 An ninh và bảo mật

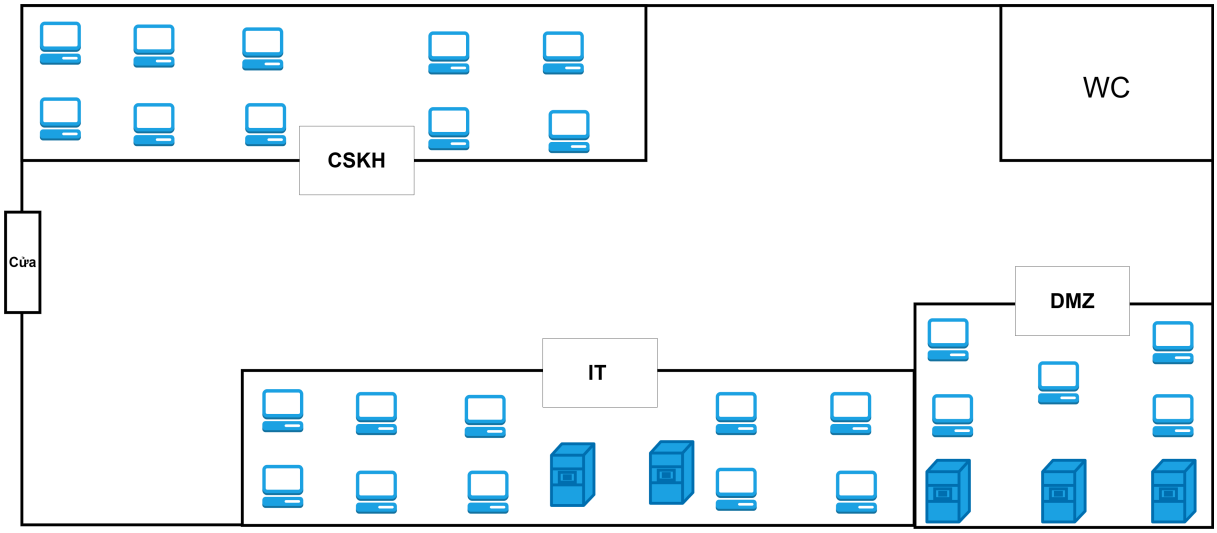
- Mô hình mạng nhóm đề xuất sử dụng tường lửa chia mạng 3 vùng: DMZ, nội bộ và bên ngoài.
- Vùng DMZ là một khu vực an toàn giữa mạng nội bộ và mạng bên ngoài. Vùng này chứa các dịch vụ mà người dùng từ internet có thể truy cập. Thành phần trong DMZ gồm: web server, email server, DNS server.
- Hệ thống có 1 tường lửa đặt sau router từ internet vào mạng nội bộ.
- Sử dụng 1 multi-switch thiết lập access list để ngăn khách hàng truy cập vào mạng nội bộ.
- Chỉ có bộ phận DBA được truy cập vào database, backup server.
- Khách hàng không thể truy cập vào các phòng ban của ngân hàng và các serer nội bộ như database và backup server.
- Thiết bị tường lửa chỉ cho phép các gói tin như ICMP và TCP đi vào vùng mạng nội bộ và vùng DMZ.

4.6 Sơ đồ cấu trúc khu vực

Toàn bộ hệ thống mạng của công ty được tổ chức dưới dạng một mạng LAN (Local Area Network) kết nối với Router trung tâm để truy cập Internet. LAN lớn này được chia thành các VLAN để phân chia và quản lý truy cập mạng cho từng phòng ban. Dưới đây là sự phân chia VLAN cho từng phòng ban cụ thể:

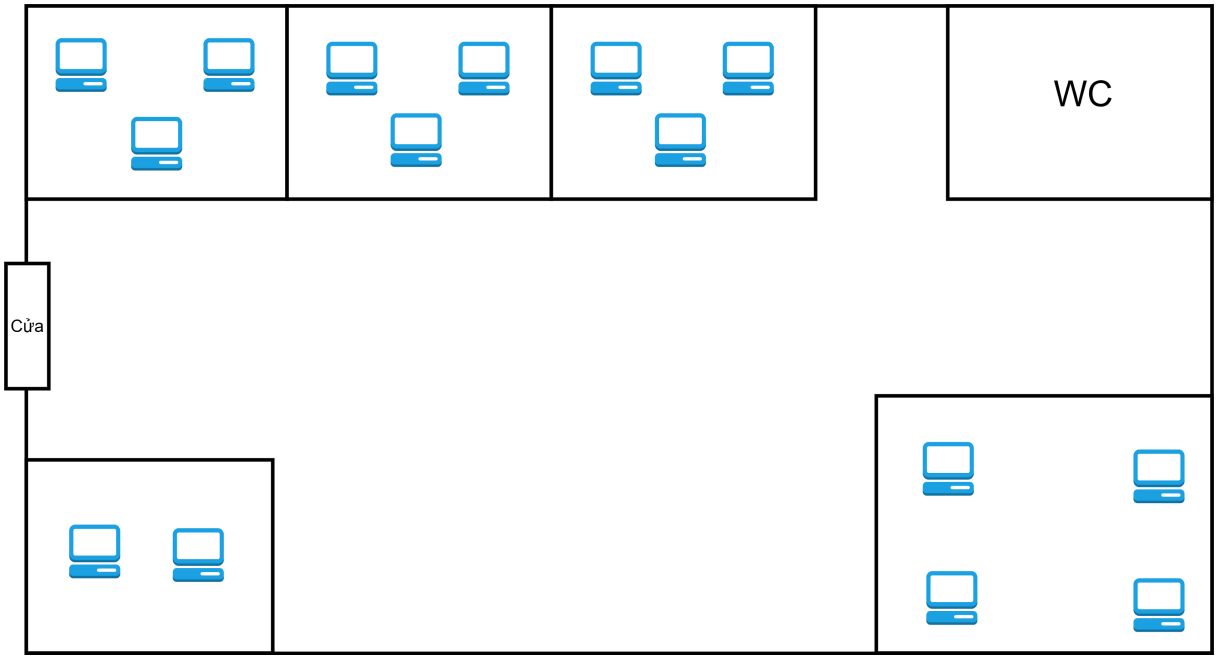
4.6.1 Trụ sở chính

- Tầng 1:
  - Phòng chăm sóc khách hàng trang bị 10 workstation.
  - Phòng server chứa backup server, database server và nơi làm việc của bộ phận DBA (Database Administrator) và bộ phận IT1 trang bị 10 workstations, 7 workstations cho bộ phận DBA và 3 workstations cho bộ phận IT1.
  - Vùng DMZ (chứa Mail Server, Web Server và DNS server) chứa 5 workstations cho bộ phận IT2.



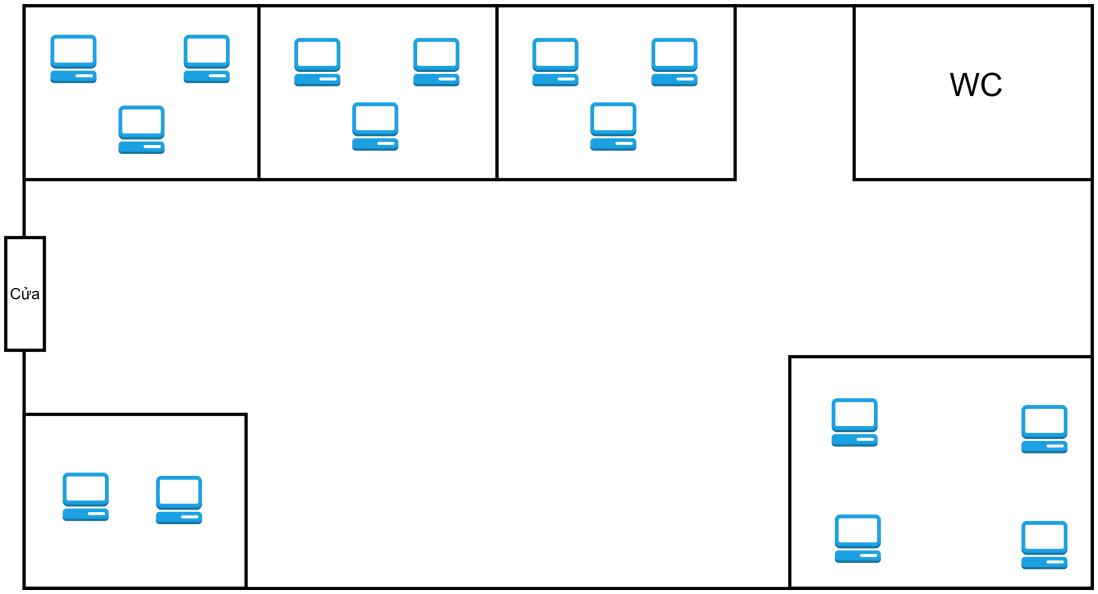
Hình 3: *Tầng 1 - Trụ sở chính*

- Tầng 2: Phòng Giao dịch 1, trang bị 15 workstations.



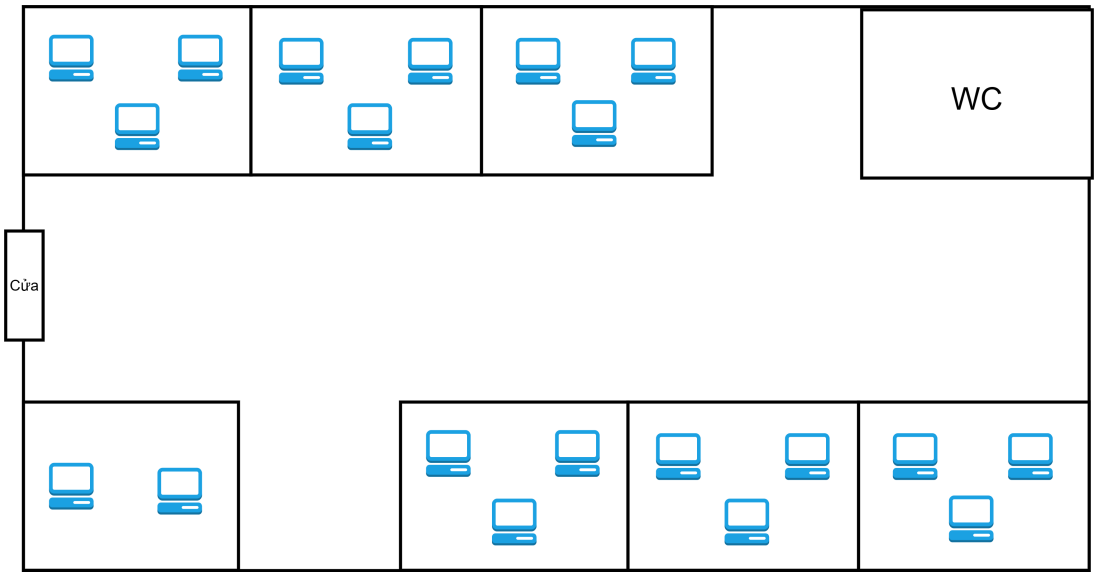
Hình 4: *Tầng 2 - Trụ sở chính*

- Tầng 3: Phòng Giao dịch 2, trang bị 15 workstations.



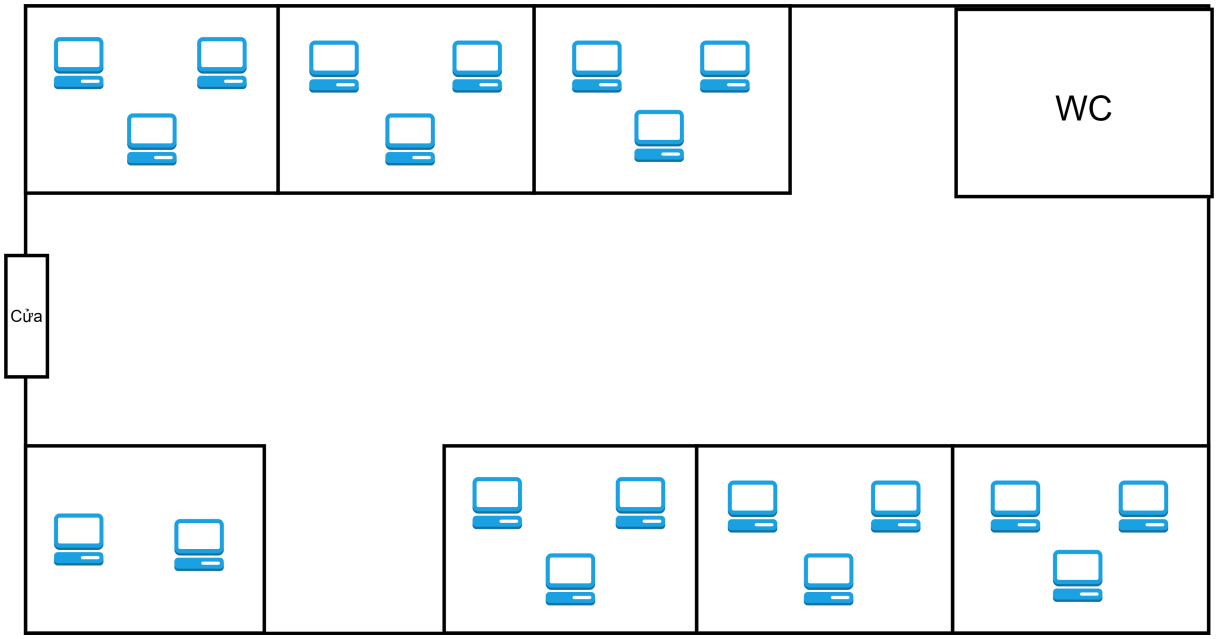
Hình 5: *Tầng 3 - Trụ sở chính*

- Tầng 4: Phòng Tài chính, trang bị 20 workstation.



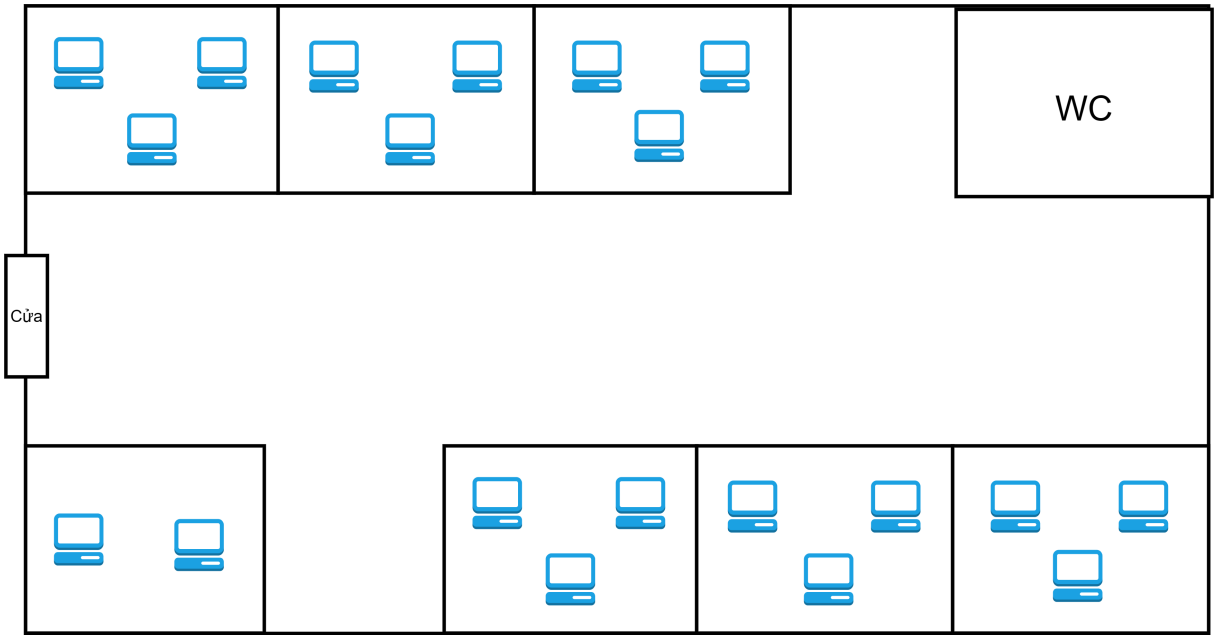
Hình 6: *Tầng 4 - Trụ sở chính*

- Tầng 5: Phòng Quản trị rủi ro, trang bị 20 workstations.



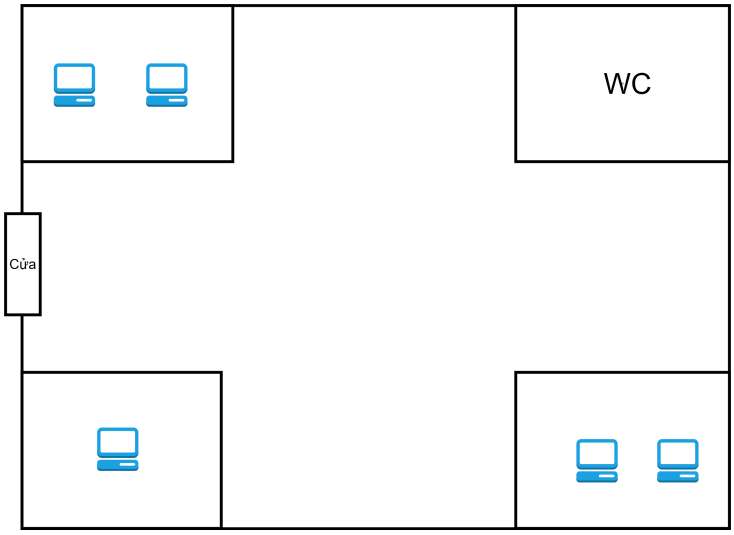
Hình 7: *Tầng 5 - Trụ sở chính*

- Tầng 6: Phòng Kế Toán, trang bị 20 workstation.



Hình 8: *Tầng 6 - Trụ sở chính*

- Tầng 7: Phòng Ban giám độc và thư ký, trang bị 5 workstations.



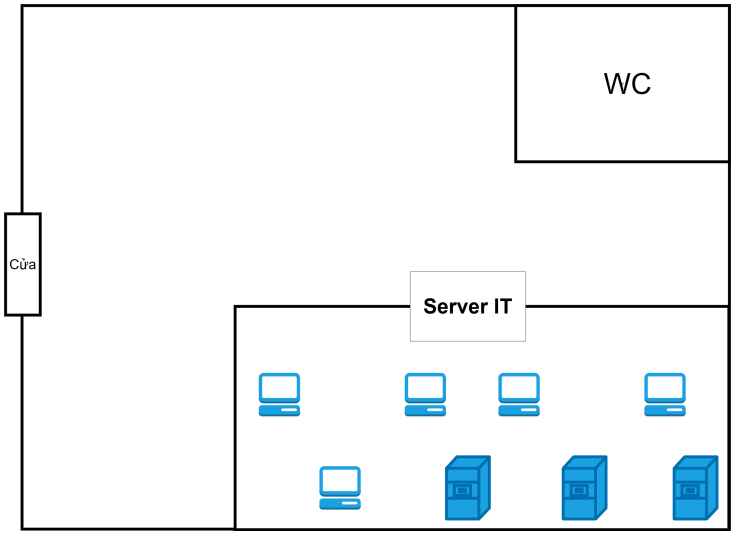
Hình 9: *Tầng 7 - Trụ sở chính*

- Số workstations cho từng phòng ban của trụ sở chính hiện tại và 5 năm sau với mức độ phát triển 20% trong 5 năm.

Phòng ban	Số workstations hiện tại	Số workstations sau 5 năm (+20%)
Chăm sóc khách hàng	10	12
IT1	3	4
IT2	5	6
DBA	7	8
Giao dịch	30	36
Tài chính	20	24
Quản trị rủi ro	20	24
Kế toán	20	24
Giám đốc	5	6
Tổng	120	144

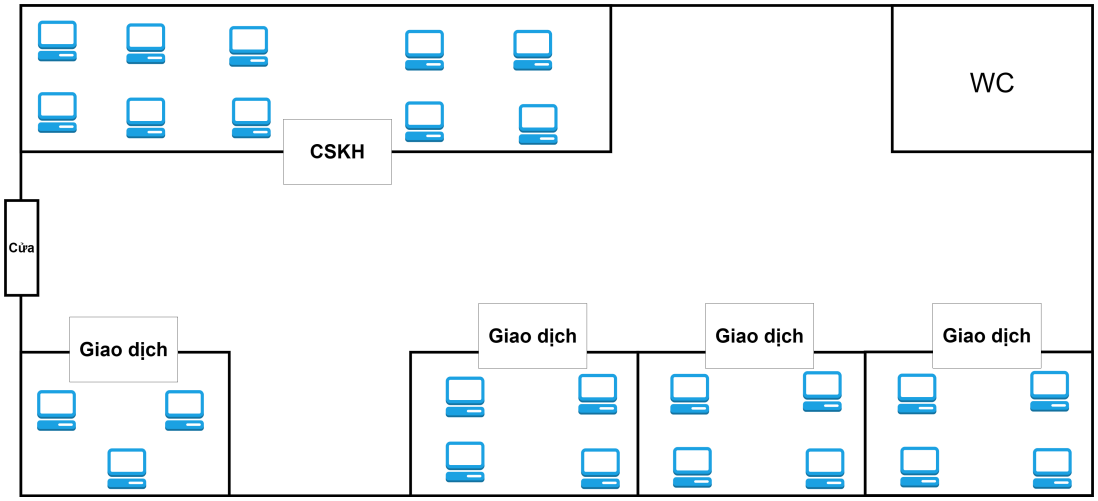
4.6.2 Chi nhánh

- Tầng 1: Phòng server (gồm DNS Server, Mail Server, Web Server) cũng là nơi làm việc của bộ phận IT. Trang bị 5 workstations.



Hình 10: *Tầng 1 - Chi nhánh*

- Tầng 2:
  - Phòng Giao dịch, trang bị 15 workstations.
  - Phòng Chăm sóc khách hàng, trang bị 10 workstations.



Hình 11: *Tầng 2 - Chi nhánh*

- Số workstations cho từng phòng ban của chi nhánh hiện tại và 5 năm sau với mức độ phát triển 20% trong 5 năm.

Phòng ban	Số workstations hiện tại	Số workstations sau 5 năm (+20%)
IT	5	6
Chăm sóc khách hàng	10	12
Giao dịch	15	18
Tổng	30	36

5 Danh sách các thiết bị tối thiểu, sơ đồ IP, sơ đồ đi dây

5.1 Danh sách các thiết bị và các đặc điểm kĩ thuật

- Router: Cisco 2911

Hình 12: *Router: Cisco 2911*

Dùng để kết nối mạng của công ty với Internet và 2 chi nhánh. Có bộ nhớ là 2GB và bộ nhớ Flash có thể tối đa lên đến 8GB cho hiệu suất cao và bảo mật. Bộ định tuyến Router Cisco 2911/K9 có thể cung cấp các ứng dụng ảo hóa và hợp tác bảo mật cao thông qua các mảng rộng nhất của kết nối WAN ở hiệu suất cao, cung cấp dịch vụ đồng thời với tốc độ lên đến 75 Mbps để đáp ứng các doanh nghiệp vừa và chi nhánh.

Thông số kỹ thuật:

- Giao thức kết nối dữ liệu: Ethernet, Fast Ethernet, Gigabit Ethernet
- Định tuyến: OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, static IPv4 IPv6 routing
- Giao thức mạng: IPSec
- Bộ nhớ DRAM: 512 MB (installed) / 2 GB (max)
- Bộ nhớ flash: 256 MB (installed) / 8 GB (max)

- Switch layer 2: Cisco Catalyst WS-C2960-24TT-L

Hình 13: *Switch layer 2: Cisco Catalyst WS-C2960-24TT-L*

Switch 2960 24-port 10/100 + 2-port 1000 được sử dụng làm Switch chính trong hệ thống, dùng để kết nối máy tính các phòng ban và với switch tổng. Thiết bị có độ bảo mật cao, cũng như dễ cấu hình, xử lý. Thông số kỹ thuật:

  - Loại phụ Fast Ethernet: Cổng 24 x 10/100 + 2 x 10/100/1000
  - Hiệu suất: Dung lượng chuyển mạch: 32 Gbps
  - Hiệu suất chuyển tiếp (kích thước gói 64 byte): 6,5 Mbps
  - Phương pháp xác thực: RADIUS, Vỏ bảo mật (SSH), TACACS +
  - RAM: 64 MB
  - Bộ nhớ flash: 32 MB flash

- Switch layer 3: Cisco Catalyst WS-C3650-24TS-S

Hình 14: *Switch layer 3: Cisco Catalyst WS-C3650-24TS-S*

Switch Layer 3 Cisco Catalyst WS-C3650-24TS-S cung cấp khả năng chuyển mạch và định tuyến IP. Nó hỗ trợ quản lý VLAN, giúp phân đoạn mạng một cách an toàn. Đồng thời, với khả năng quản lý băng thông và QoS, switch này đảm bảo ưu tiên cho các dịch vụ quan trọng như giao dịch tài chính. Các tính năng bảo mật như ACLs và quản lý từ xa giúp đảm bảo an toàn và quản lý hiệu quả cho hệ thống mạng

Thông số kỹ thuật:

  - Mật độ cổng tối đa: 24 × 10/100 Ethernet
  - Kích thước bảng địa chỉ MAC: 32000 entry
  - RAM: 4 GB
  - Stack bandwidth: 160 Gbps
  - Forwarding bandwidth: 65.47 Mbps

- Firewall: Cisco ASA 5506-X

Hình 15: *Firewall: Cisco ASA 5506-X*

Hệ thống an ninh mạng có thể dựa trên cả phần cứng và phần mềm, áp dụng các quy tắc để kiểm soát luồng dữ liệu vào và ra khỏi hệ thống. Trong vai trò của một rào chắn giữa mạng an toàn và mạng không an toàn, tường lửa đóng vai trò quan trọng. Nhóm chọn sử dụng tường lửa ASA 5506 của Cisco.

Cisco ASA 5506 là một tường lửa đầy đủ tính năng, được thiết kế đặc biệt để đáp ứng nhu cầu của các môi trường làm việc từ xa của doanh nghiệp và chi nhánh. Nó cung cấp hiệu suất tường lửa cao, hỗ trợ cả VPN SSL và IPsec, cùng với các dịch vụ mạng đa dạng tích hợp trong một thiết bị hoạt động tức thì thông qua mô-đun. Sử dụng Trình quản lý thiết bị bảo mật thích ứng Cisco (ASDM) với giao diện đồ họa tích hợp, Cisco ASA 5506 có thể triển khai nhanh chóng và quản lý một cách dễ dàng, giúp doanh nghiệp giảm chi phí hoạt động.

Đặc biệt, nó trang bị bộ chuyển mạch Gigabit Ethernet và các cổng có khả năng nhóm động, tạo ra tối đa ba VLAN riêng biệt cho gia đình, doanh nghiệp và lưu lượng truy cập internet. Điều này cải thiện phân đoạn mạng và tăng cường khả năng bảo mật của hệ thống.

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

Hình 16: *Access Point: Cisco-Linksys WAP610N Wireless-N Access Point with Dual-Band*

WAP-610N là thiết bị access point không dây chuẩn N với tính năng Dual-Band có thể hoạt động

tại 2 dải tần làm tăng khả năng mở rộng hệ thống mạng có dây hoặc nâng cấp hệ thống mạng không dây lên chuẩn N. WAP-610N có thể làm việc với thiết bị bridge không dây WET610N. Được thiết kế để giảm thiểu sự ngứt quãng khi xem video quan mạng không dây.

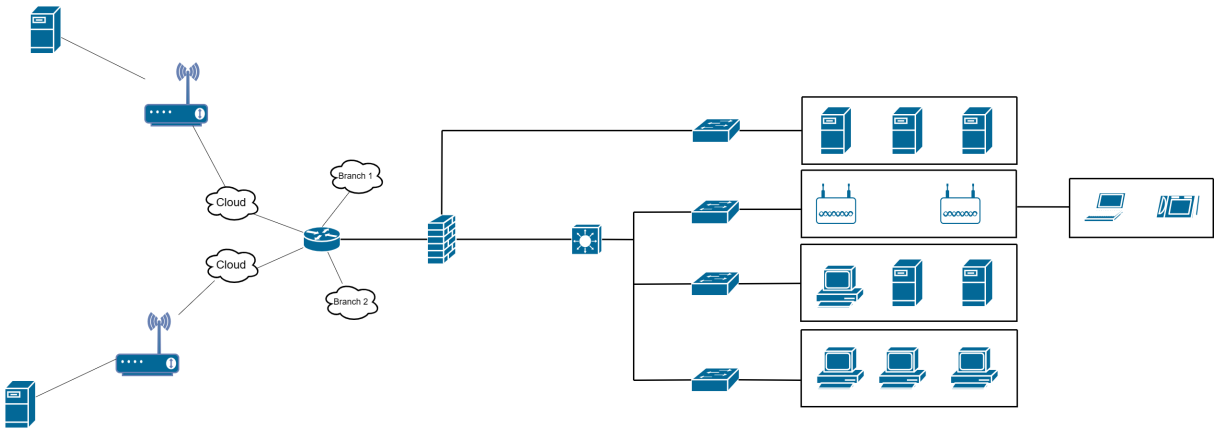
Thông số kỹ thuật:

- Giao thức liên kết dữ liệu: IEEE 802.11n (draft), IEEE 802.11b, IEEE 802.11a, IEEE 802.11g.
- Bảo mật không dây: Giúp bảo vệ dữ liệu an toàn cao với mã hóa xác thực khi kết nối không dây với bảo mật WPA.
- Anten: 03 anten bên trong
- Bandwidth: 2.4GHz – 5 GHz
- Ethernet port: 01 port 10/100Mbps.

5.2 Sơ đồ IP và sơ đồ đi dây ở trụ sở chính và chi nhánh

5.2.1 Trụ sở chính

Sơ đồ đi dây:



Hình 17: *Sơ đồ đi dây - Trụ sở chính*

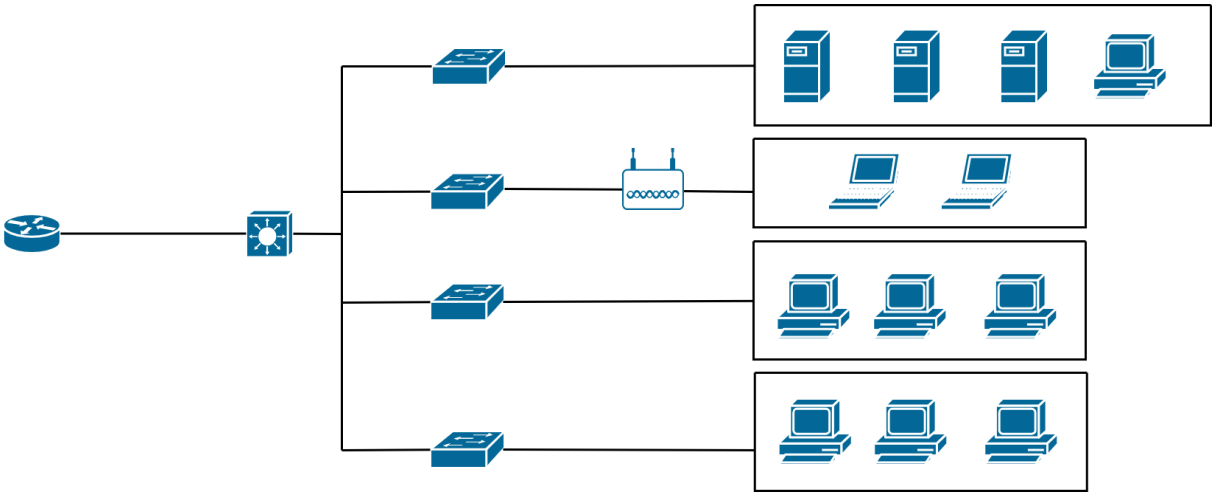
VLAN	Tầng	Phòng ban	Địa chỉ mạng	Default Getway	Địa chỉ khả dụng
4	1	IT2 + DMZ	192.168.4.2/24	192.168.4.2	192.168.4.3 - 192.168.10.254
10	1	Chăm sóc khách hàng	192.168.10.0/24	192.168.10.1	192.168.10.2 - 192.168.10.254
20	2, 3	Giao dịch	192.168.20.0/24	192.168.20.1	192.168.20.2 - 192.168.20.254
30	4	Tài chính	192.168.30.0/24	192.168.30.1	192.168.30.2 - 192.168.30.254
40	5	Quản trị rủi ro	192.168.40.0/24	192.168.40.1	192.168.40.2 - 192.168.40.254
50	6	Kế toán	192.168.50.0/24	192.168.50.1	192.168.50.2 - 192.168.50.254
60	7	Giám đốc	192.168.60.0/24	192.168.60.1	192.168.60.2 - 192.168.60.254
70	1	DBA + IT1 + Inside Server	192.168.70.0/24	192.168.70.1	192.168.70.2 - 192.168.70.254
80	1	Khách hàng	192.168.80.0/24	192.168.80.1	192.168.80.2 - 192.168.80.254

IP của các workstation được cấp phát động bằng Switch layer 3, tuy nhiên IP của các server và các workstations của DBA và IT được cấp phát tĩnh.

- Web server: 192.168.4.4
- Mail server: 192.168.4.3
- DNS server: 192.168.4.6
- PC IT2: 192.168.4.6
- Database server: 192.168.70.2
- Backup server: 192.168.70.6
- PC IT1: 192.168.70.3
- PC DBA1: 192.168.70.7

5.2.2 Tại chi nhánh

Sơ đồ đi dây:



Hình 18: *Sơ đồ đi dây - Chi nhánh*

- Chi nhánh Đà Nẵng

VLAN	Tầng	Phòng ban	Địa chỉ mạng	Default Getway	Địa chỉ khả dụng
10	1	IT + Server	192.100.10.0/24	192.100.10.1	192.100.10.2 - 192.100.10.254
20	2	Khách hàng	192.100.20.0/24	192.100.20.1	192.100.20.2 - 192.100.20.254
30	2	Giao dịch + CSKH	192.100.30.0/24	192.100.30.1	192.100.30.2 - 192.100.30.254

IP của các workstation được cấp phát động bằng Switch layer 3, tuy nhiên IP của các server và các workstations IT được cấp phát tĩnh.

  - PC IT1 : 192.100.10.2
  - Web server: 192.100.10.5
  - Mail server: 192.100.10.4
  - DNS server: 192.100.10.3

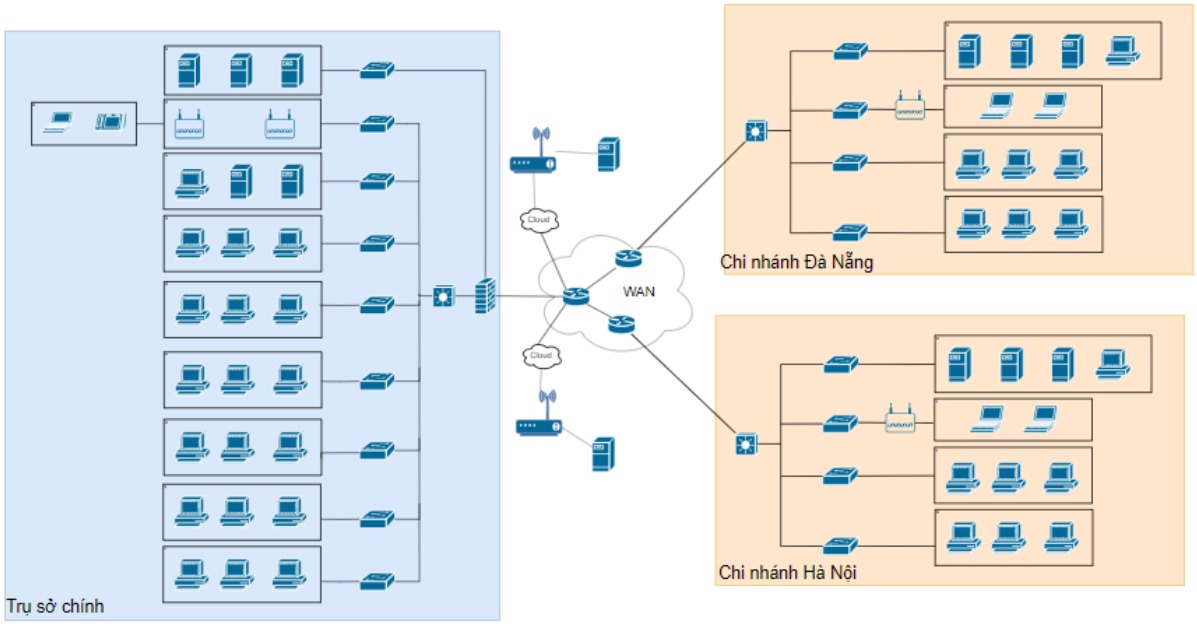
- Chi nhánh Hà Nội

VLAN	Tầng	Phòng ban	Địa chỉ mạng	Default Getway	Địa chỉ khả dụng
10	1	IT + Server	192.200.10.0/24	192.200.10.1	192.200.10.2 - 192.200.10.254
20	2	Khách hàng	192.200.20.0/24	192.200.20.1	192.200.20.2 - 192.200.20.254
30	2	Giao dịch + CSKH	192.200.30.0/24	192.200.30.1	192.200.30.2 - 192.200.30.254

IP của các workstation được cấp phát động bằng Switch layer 3, tuy nhiên IP của các server và các workstations IT được cấp phát tĩnh.

- PC IT1 : 192.200.10.3
- Web server: 192.200.10.5
- Mail server: 192.200.10.4
- DNS server: 192.200.10.2

5.3 Sơ đồ WAN giữa trụ sở và các chi nhánh



Hình 19: *Sơ đồ WAN giữa trụ sở và các chi nhánh*

Các đơn vị trung tâm và chi nhánh của hệ thống được liên kết thông qua mạng WAN, sử dụng đường truyền riêng do nhà cung cấp dịch vụ cung cấp. Hình trên mô tả cách kết nối này, trong đó mỗi đơn vị kết nối với internet thông qua một Router. Tại các Router này, được thiết lập 2 đường truyền để kết nối với mạng WAN - kết nối trụ sở chính với 2 chi nhánh và hai đường ADSL liên kết với Modem để kết nối với Internet. Mục đích của việc sử dụng 2 đường ADSL là để giảm tải trên các đường truyền, tránh tình trạng quá tải hoặc lãng phí, các giải thuật định tuyến được triển khai tại Router.

6 Tính toán throughput, bandwidth và cấu hình cho mạng máy tính.

6.1 Khái niệm

- *Thông lượng (throughput)* là số lượng dữ liệu thực tế được truyền qua mạng trong một khoảng thời gian nhất định. Nó đo lường khả năng truyền dữ liệu hiệu quả của mạng và thể hiện tốc độ truyền dữ liệu thực tế. Thông lượng được tính bằng đơn vị bit/giây (bps) hoặc byte/giây (Bps).
- *Băng thông (bandwidth)* là khả năng truyền tải dữ liệu thông qua một kênh truyền hoặc một đường truyền mạng trong một khoảng thời gian xác định. Nó đo lường khả năng truyền dữ liệu tối đa của mạng và được đo bằng đơn vị bit/giây (bps) hoặc byte/giây (Bps).

6.2 Trụ sở chính

- Có tổng cộng 5 servers được đặt tại tầng 1, dùng cho updates, web access, database access,... Tổng dung lượng upload và download mỗi server vào khoảng 3000 MB/ngày. Tổng thời gian làm việc 1 ngày là 8 giờ và vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày.Ta tính được bandwidth và throughput:

$$Bandwidth = \frac{5 \times 3000 \times 0.8}{3 \times 3600} = 1.1111MBps = 8.8889Mbps \quad (1)$$

$$Throughput = \frac{5 \times 3000}{8 \times 3600} = 0.5208MBps = 4.1667Mbps \quad (2)$$

- Có tổng cộng 120 workstations. Tổng dung lượng upload và download mỗi workstation vào khoảng 600 MB/ngày. Tổng thời gian làm việc 1 ngày là 8 giờ và vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày.Ta tính được bandwidth và throughput:

$$Bandwidth = \frac{120 \times 600 \times 0.8}{3 \times 3600} = 5.3333MBps = 42.6667Mbps \quad (3)$$

$$Throughput = \frac{120 \times 600}{8 \times 3600} = 2.5MBps = 20Mbps \quad (4)$$

- Lượng truy cập WiFi bằng laptop khoảng 500 MB/ngày với giả sử là lượng khách truy cập là 150 người/ngày. Tổng thời gian làm việc 1 ngày là 8 giờ và vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày.Ta tính được bandwidth và throughput:

$$Bandwidth = \frac{150 \times 500 \times 0.8}{3 \times 3600} = 5.5556MBps = 44.4444Mbps \quad (5)$$

$$Throughput = \frac{150 \times 500}{8 \times 3600} = 2.6042MBps = 20.8333Mbps \quad (6)$$

- Trong thời điểm nếu toàn bộ hệ thống mạng của trụ sở chính hoạt đồng thời truy cập dữ liệu thì Bandwidth và Throughput cao nhất có thể đạt tới là:

$$Bandwidth = 8.8889 + 42.6667 + 44.4444 = 96Mbps \quad (7)$$

$$Throughput = 4.1667 + 20 + 20.8333 = 45Mbps \quad (8)$$

- 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,..) nên hệ số an toàn sẽ là 20%. Băng thông và thông lượng tối thiểu nên sử dụng bằng 120% băng thông và thông lượng cao nhất:

$$Bandwidth = 96 * 120\% = 115.2Mbps \tag{9}$$
$$Throughput = 45 * 120\% = 54Mbps \tag{10}$$

6.3 Chi nhánh

- Có tổng cộng 3 servers được đặt tại tầng 1, dùng cho DNS, mail và web. Tổng dung lượng upload và download mỗi server vào khoảng 3000 MB/ngày. Tổng thời gian làm việc 1 ngày là 8 giờ và vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày.Ta tính được bandwidth và throughput:

$$Bandwidth = \frac{3 \times 3000 \times 0.8}{3 \times 3600} = 0.6667MBps = 5.3333Mbps \tag{11}$$
$$Throughput = \frac{3 \times 3000}{8 \times 3600} = 0.3125MBps = 2.5Mbps \tag{12}$$

- Có tổng cộng 30 workstations. Tổng dung lượng upload và download mỗi workstation vào khoảng 600 MB/ngày. Tổng thời gian làm việc 1 ngày là 8 giờ và vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày.Ta tính được bandwidth và throughput:

$$Bandwidth = \frac{30 \times 600 \times 0.8}{3 \times 3600} = 1.3333MBps = 10.6667Mbps \tag{13}$$
$$Throughput = \frac{30 \times 600}{8 \times 3600} = 0.625MBps = 5Mbps \tag{14}$$

- Lượng truy cập WiFi bằng laptop khoảng 500 MB/ngày với giả sử là lượng khách truy cập là 50 người/ngày. Tổng thời gian làm việc 1 ngày là 8 giờ và vào giờ cao điểm là 3 giờ. Giờ cao điểm tập trung 80% trong ngày.Ta tính được bandwidth và throughput:

$$Bandwidth = \frac{50 \times 500 \times 0.8}{3 \times 3600} = 1.8519MBps = 14.8148Mbps \tag{15}$$
$$Throughput = \frac{50 \times 500}{8 \times 3600} = 0.8681MBps = 6.9444Mbps \tag{16}$$

- Trong thời điểm nếu toàn bộ hệ thống mạng của chi nhánh hoạt đồng thời truy cập dữ liệu thì Bandwidth và Throughput cao nhất có thể đạt tới là:

$$Bandwidth = 5.3333 + 10.6667 + 14.8148 = 30.8148Mbps \tag{17}$$
$$Throughput = 2.5 + 5 + 6.9994 = 14.4444Mbps \tag{18}$$

- 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,..) nên hệ số an toàn sẽ là 20%. Băng thông và thông lượng tối thiểu nên sử dụng bằng 120% thông băng thông và thông

lượng cao nhất:

$$Bandwidth = 30.8148 * 120\% = 36.9778 Mbps \tag{19}$$

$$Throughput = 14.4444 * 120\% = 17.3333 Mbps \tag{20}$$

7 Thiết kế sơ đồ mạng bằng Packet Tracer

7.1 Những công nghệ đã sử dụng

- VLAN (Virtual Local Area Network): 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. Ưu điểm:
  - Gia tăng tính bảo mật.
  - Linh hoạt trong việc 1 switch có thể tạo ra nhiều switch ảo.
  - 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.
  - Dễ dàng thêm bớt các máy PC vào VLAN.
- 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. Giao thức DHCP thường được sử dụng 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:
  - 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 tái sử dụng cho hệ thống khác.
- Access Control Lists (ACLs) là một phần quan trọng trong thiết kế mạng, giúp quản lý và kiểm soát quyền truy cập vào tài nguyên mạng. ACLs là một tập hợp các quy tắc được áp dụng trên thiết bị mạng để xác định liệu một gói dữ liệu nào có được chấp nhận, từ chối, hoặc chuyển tiếp. Được tích hợp cả ở mức đường truyền và mức lớp 3 của mô hình OSI, ACLs cung cấp khả năng kiểm soát chi tiết đối với việc chia sẻ tài nguyên mạng. Ưu điểm:
  - Cho phép quản trị viên mạng tạo ra các quy tắc tùy chỉnh để kiểm soát truy cập dựa trên địa chỉ IP nguồn và đích, cổng, hay giao thức. Điều này giúp tạo ra các kịch bản linh hoạt để bảo vệ tài nguyên và dữ liệu quan trọng.
  - Bằng cách thiết lập ACLs chặt chẽ, mạng có thể đạt được mức độ bảo mật cao hơn, giảm thiểu rủi ro về việc truy cập trái phép hay tấn công mạng từ bên ngoài.
  - ACLs cho phép quản trị viên mạng quản lý và ưu tiên truy cập vào các tài nguyên mạng quan trọng. Điều này giúp tối ưu hóa băng thông và đảm bảo hiệu suất mạng tốt nhất.
  - ACLs có thể được sử dụng để chống lại các loại tấn công mạng như DDoS (Distributed Denial of Service) bằng cách hạn chế lưu lượng đến từ các nguồn không đáng tin cậy.
  - Bằng cách sử dụng ACLs, quản trị viên mạng có thể quản lý tài nguyên và định rõ các quy tắc truy cập một cách dễ dàng, giúp đơn giản hóa quá trình quản lý và bảo trì hệ thống.
- Routing là một thành phần quan trọng trong thiết kế mạng, chịu trách nhiệm điều hướng các gói dữ liệu từ nguồn đến đích thông qua mạng. Các giao thức định tuyến như RIP, OSPF, và BGP giúp tạo ra các bảng định tuyến, quyết định con đường tối ưu cho dữ liệu truyền qua mạng. Dưới đây là những ưu điểm quan trọng của công nghệ định tuyến. Ưu điểm:
  - Công nghệ định tuyến giúp tối ưu hóa con đường truyền dẫn dữ liệu, đảm bảo rằng nó sẽ đi qua đường tối ưu nhất để đạt được hiệu suất cao và giảm độ trễ.

– Định tuyến hỗ trợ mạng mở rộng linh hoạt, cho phép thêm vào các thiết bị mới mà không ảnh hưởng đến hoạt động chung của mạng.

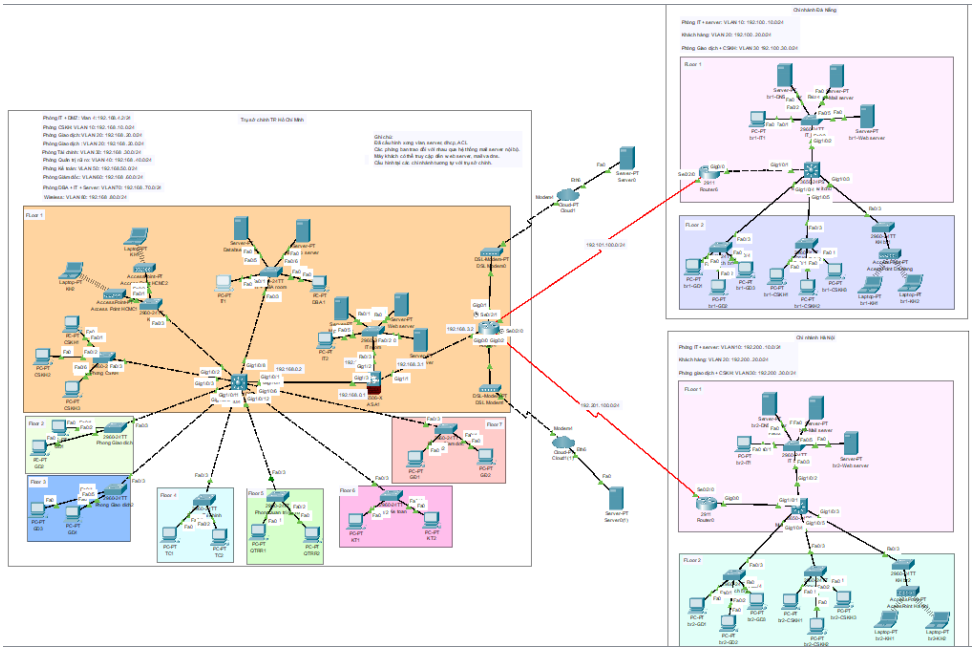
– Công nghệ định tuyến cung cấp khả năng chịu đựng lỗi, tự động chuyển đổi con đường nếu một đường truyền hoặc thiết bị bị lỗi, giúp duy trì tính sẵn sàng cao của mạng.

– Bằng cách phân phối tải thông qua nhiều đường truyền, công nghệ định tuyến giúp tối ưu hóa băng thông và ngăn chặn tình trạng quá tải tại một đường truyền duy nhất.

– Các giao thức định tuyến có thể được cấu hình để bảo mật mạng bằng cách kiểm soát quyền truy cập và xác thực dữ liệu, giúp ngăn chặn các mối đe dọa an ninh mạng.

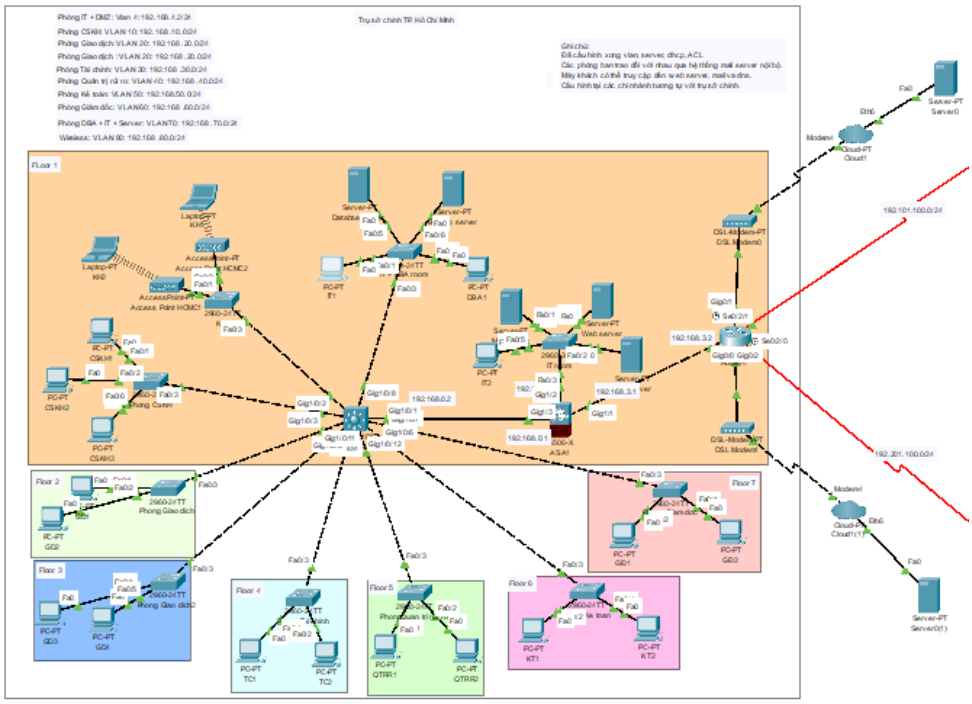
– Công nghệ định tuyến cung cấp sự linh hoạt trong việc quản lý và phân bổ tài nguyên mạng, giúp tối ưu hóa sự sử dụng của chúng.

7.2 Toàn bộ hệ thống



Hình 20: *Sơ đồ mạng của toàn bộ hệ thống*

7.3 Trụ sở chính

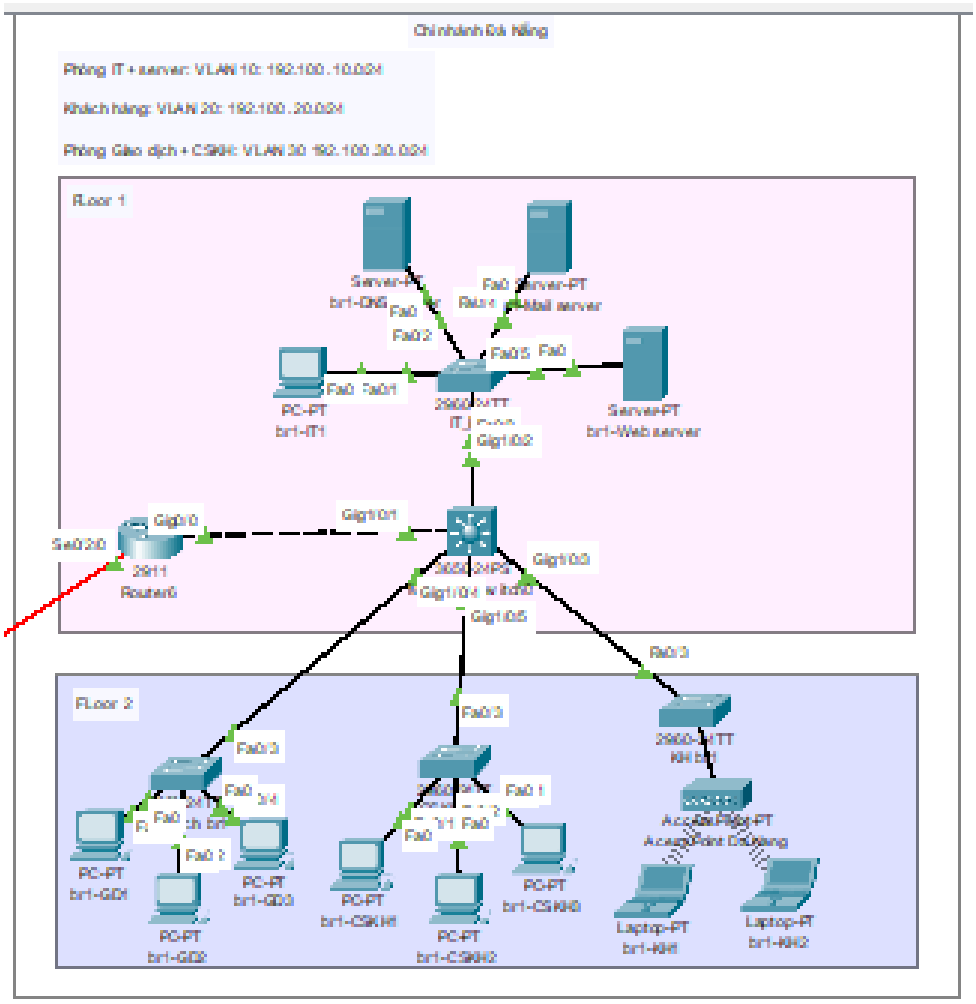


Hình 21: *Sơ đồ mạng trụ sở chính*

Mô tả:

- Một switch layer 3 làm switch trung tâm. Nhóm cấu hình hai access-list tại đây. Một access-list có tác dụng ngăn không cho các VLAN dành cho khách truy cập vào các thiết bị nội bộ. Acces-list còn lại dùng để ngăn các VLAN khác ngoài VLAN của bộ phận DBA truy cập vào server database và server backup.
- Tường lửa ASA5506 được sử dụng để ngăn chặn truy cập không ủy quyền vào dữ liệu hệ thống, đồng thời giữ cho quyền truy cập của chi nhánh chính có thể mở rộng đến cả hệ thống của hai chi nhánh.
- Tầng 1 nơi mà phòng IT quản lí các thiết bị router, switch, tường lửa của chi nhánh. Phòng ban lễ tân cũng nằm ở tầng này để phục vụ khách hàng. Bên cạnh đó còn có phòng ban DBA (Database Administrator) để quản lý các server tại đây.
- Các tầng còn lại phân chia đều cho các phòng ban của hệ thống ngân hàng.
- Tầng 1 sẽ có các access point để truy cập laptop, tablet, smartphone ,... dành riêng cho khách hàng.
- DSL modem chuyển đổi tín hiệu giữa mạng nội bộ và đường dây DSL, kết nối router với internet. Nó giải mô đun tín hiệu, bảo vệ mạng qua tính năng tường lửa, và cung cấp giao diện cấu hình để quản lý kết nối và đảm bảo an toàn cho mạng.

7.4 Chi nhánh Đà Nẵng

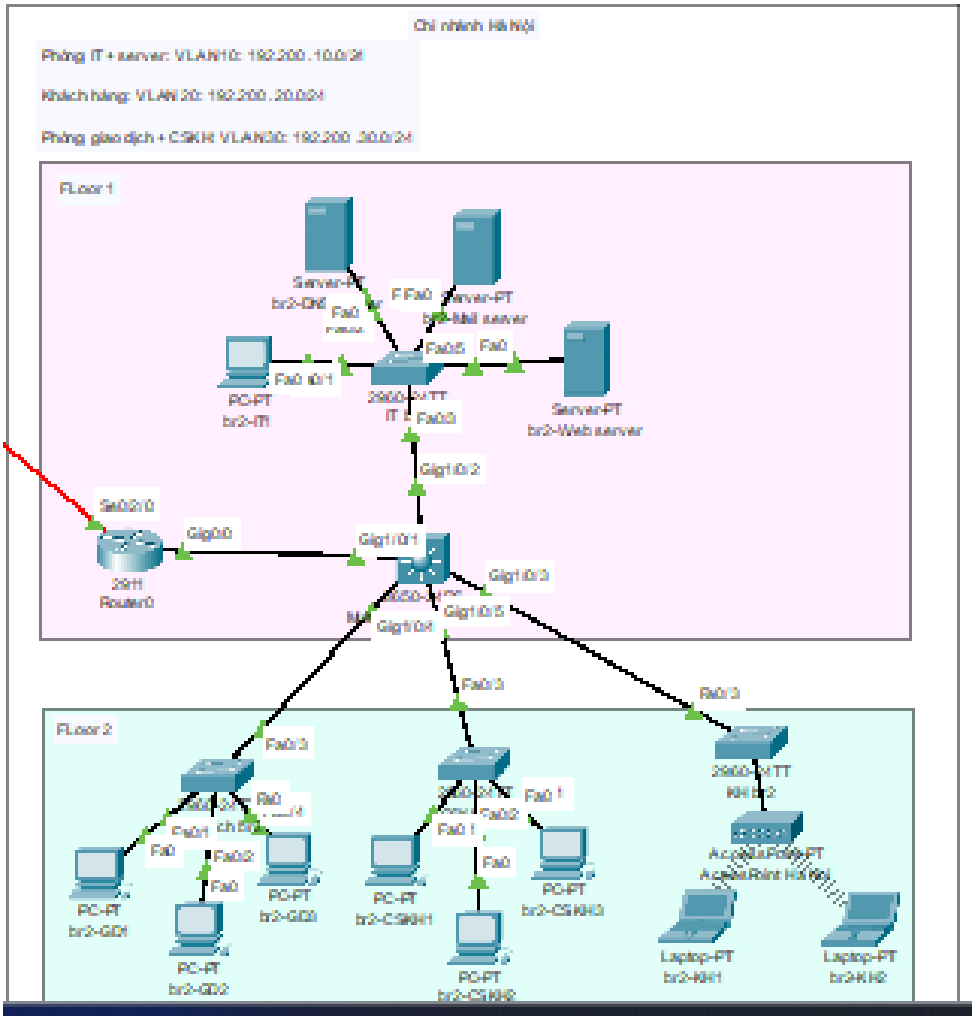


Hình 22: *Sơ đồ mạng chi nhánh Đà Nẵng*

Mô tả:

- Tương tự như ở trụ sở chính, chi nhánh Đà Nẵng cũng có một switch layer3 làm switch trung tâm.
- Tầng một sẽ nơi lưu trữ server và là nơi mà phòng IT quản lí các thiết bị router, switch, tường lửa của chi nhánh. Phòng ban lễ tân cũng nằm ở tầng này để phục vụ khách hàng
- Tầng 2 phân chia đều cho các phòng ban của hệ thống ngân hàng.
- Tầng 1 có một Access Point để truy cập từ laptop, tablet.

7.5 Chi nhánh Hà Nội



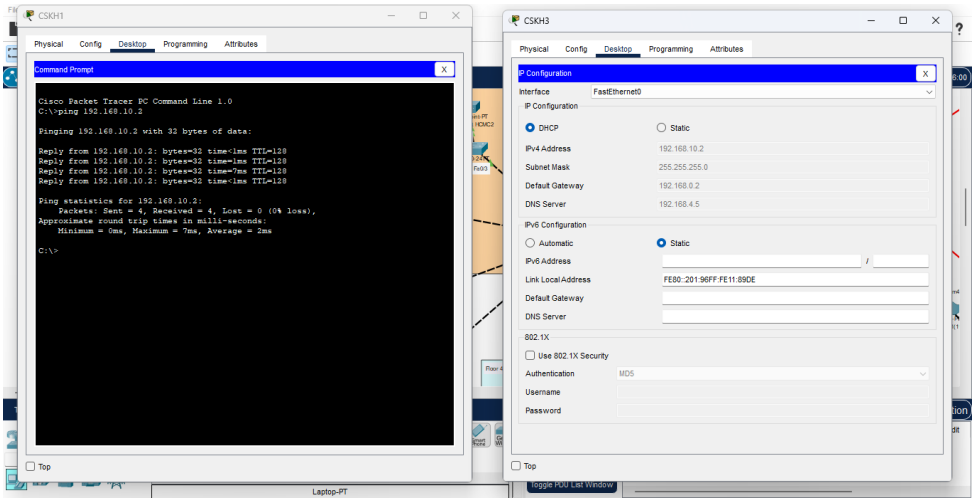
Hình 23: *Sơ đồ mạng chi nhánh Hà Nội*

Mô tả:

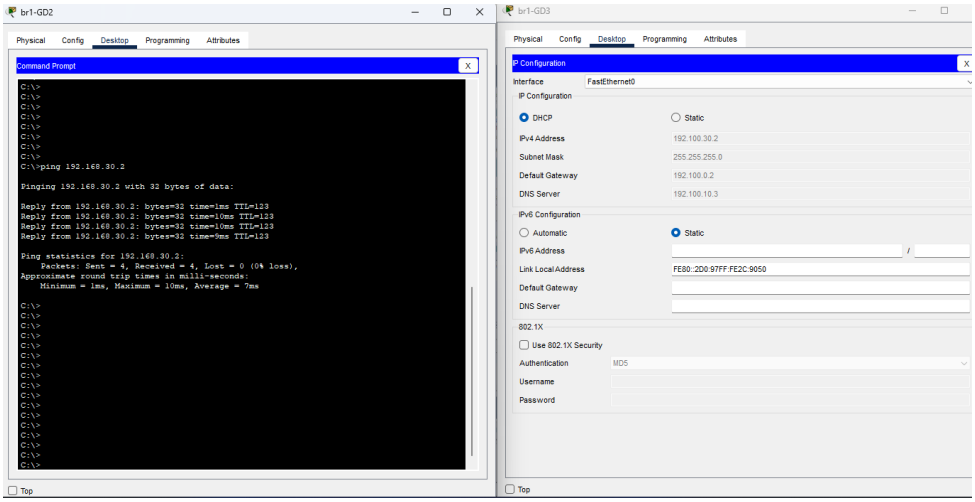
- Tương tự như ở trụ sở chính, chi nhánh Đà Nẵng cũng có một switch layer3 làm switch trung tâm.
- Tầng một sẽ nơi lưu trữ server và là nơi mà phòng IT quản lí các thiết bị router, switch, tường lửa của chi nhánh. Phòng ban lễ tân cũng nằm ở tầng này để phục vụ khách hàng
- Tầng 2 phân chia đều cho các phòng ban của hệ thống ngân hàng.
- Tầng 1 có một Access Point để truy cập từ laptop, tablet.

8 Kiểm tra hệ thống mạng bằng các công cụ phổ biến như ping, traceroute,...

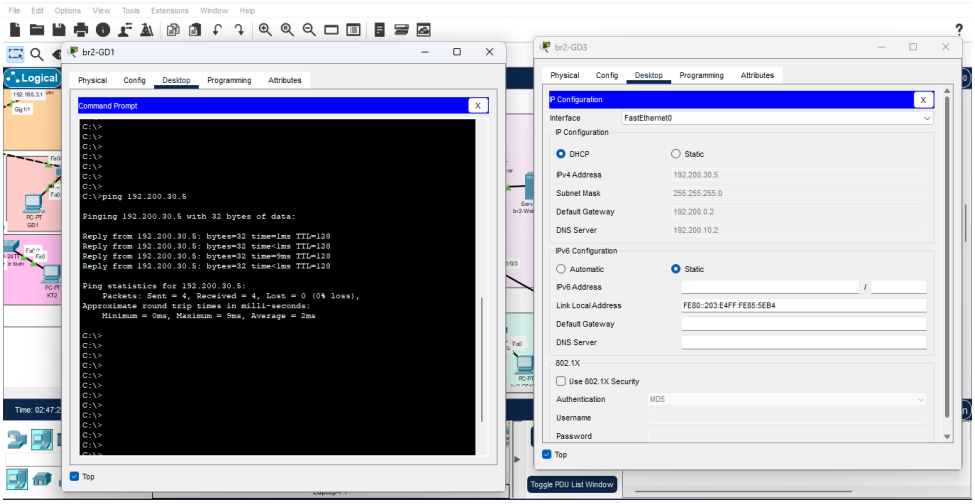
8.1 PC cùng VLAN



Hình 24: *PC cùng VLAN tại trụ sở chính*

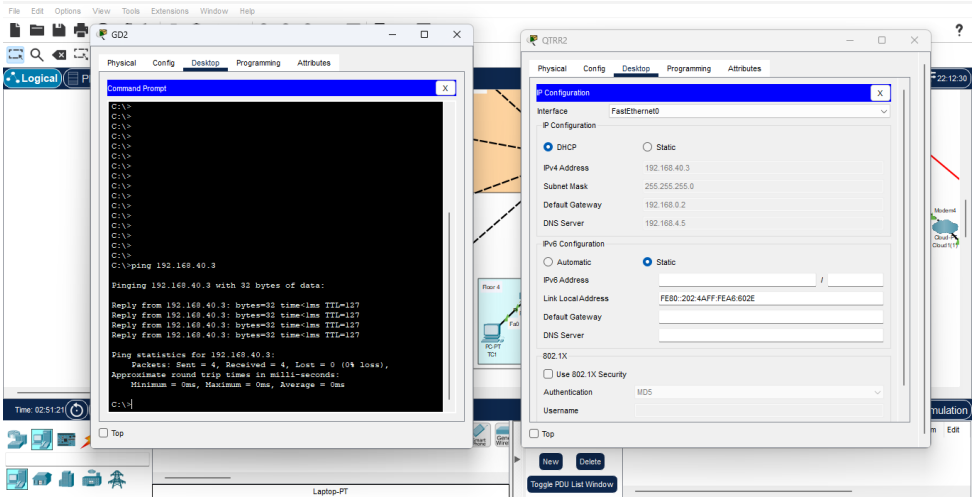


Hình 25: *PC cùng VLAN tại chi nhánh Đà Nẵng*

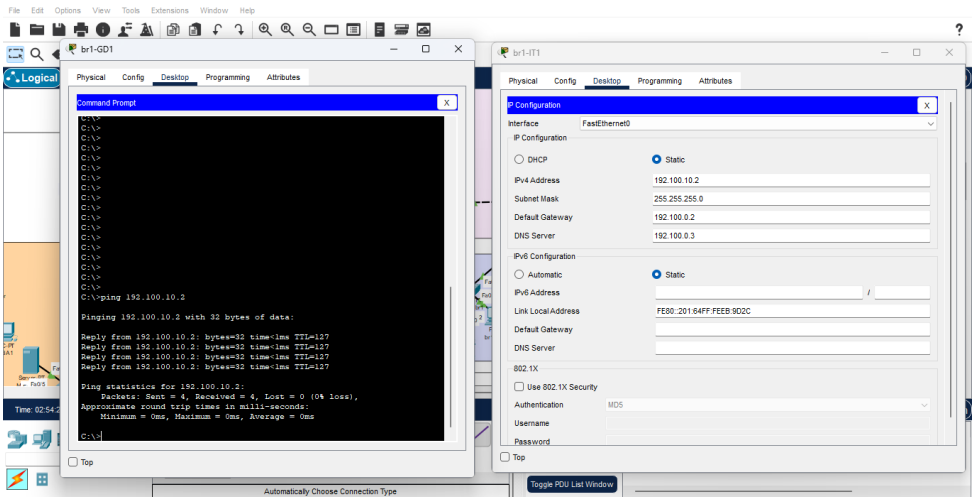


Hình 26: *PC cùng VLAN tại chi nhánh Hà Nội*

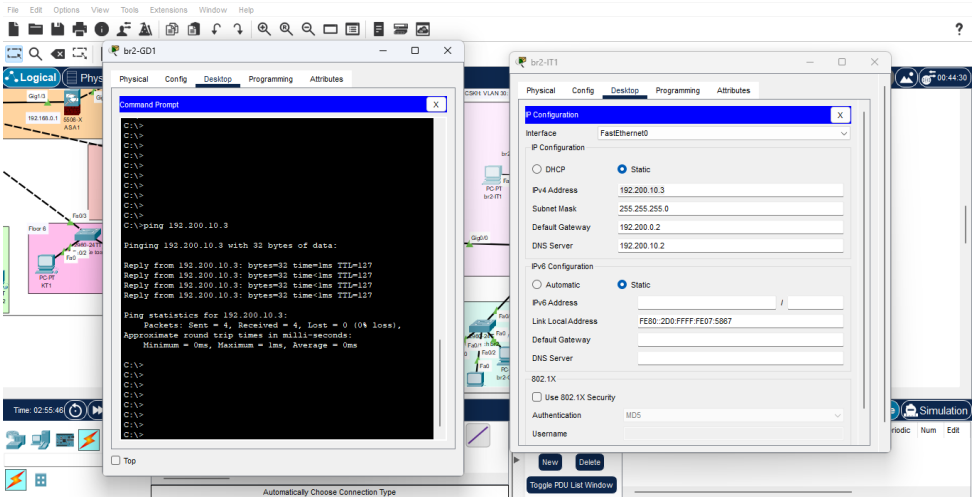
8.2 PC khác VLAN được truy cập tới nhau



Hình 27: *PC khác VLAN tại trụ sở chính được truy cập tới nhau*

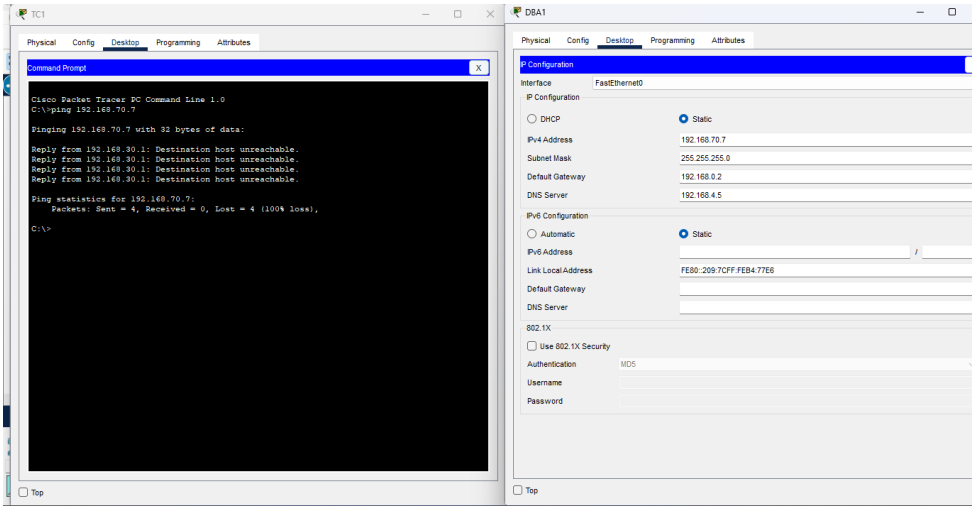


Hình 28: *PC khác VLAN tại chi nhánh Đà Nẵng được truy cập tới nhau*



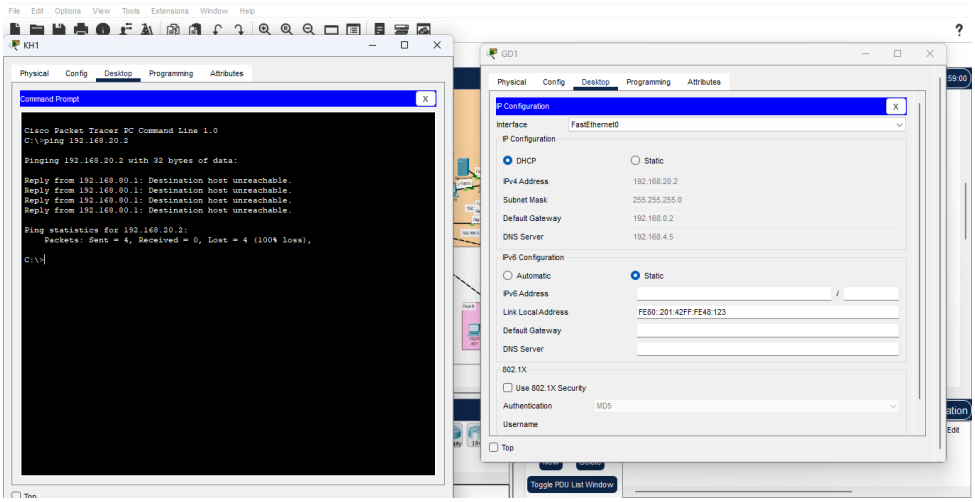
Hình 29: *PC khác VLAN tại chi nhánh Hà Nội được truy cập tới nhau*

8.3 PC khác VLAN không được truy cập tới nhau



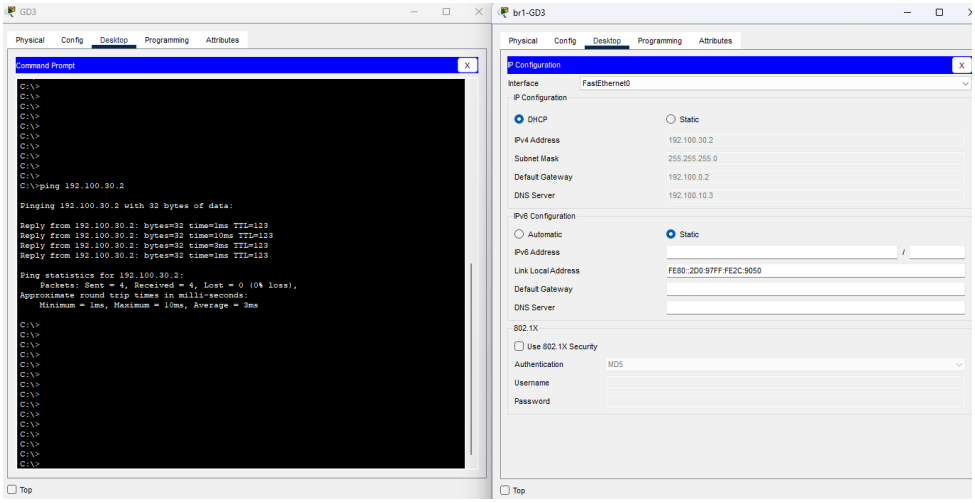
Hình 30: *PC khác VLAN tại trụ sở chính không được truy cập tới nhau*

8.4 Khách không thể truy cập tới các VLAN khác

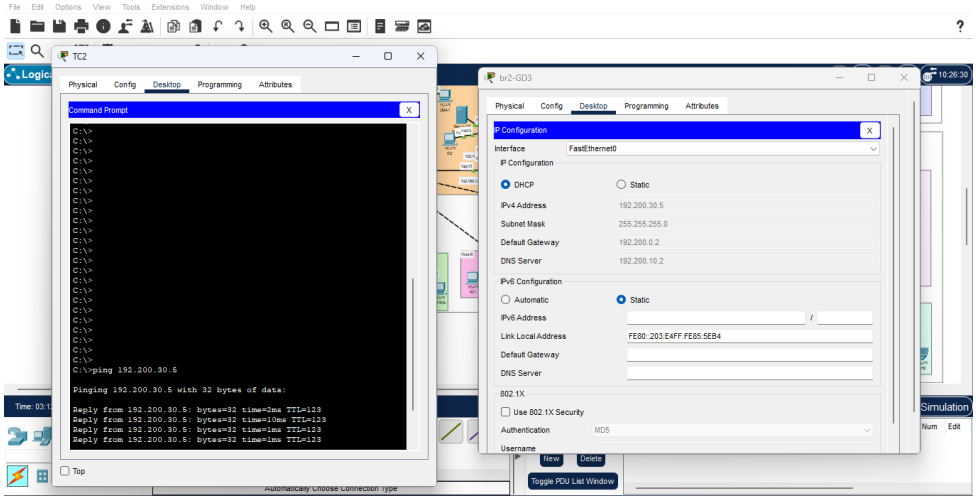


Hình 31: *PC khách không thể truy cập tới VLAN trong trụ sở chính*

8.5 PC ở trụ sở chính và chi nhánh được truy cập tới nhau

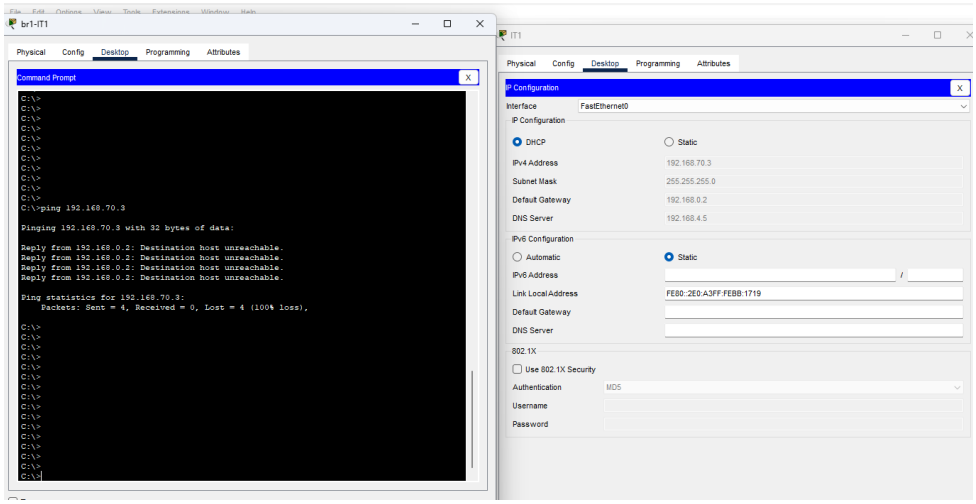


Hình 32: *PC ở trụ sở chính và chi nhánh Đà Nẵng được truy cập tới nhau*

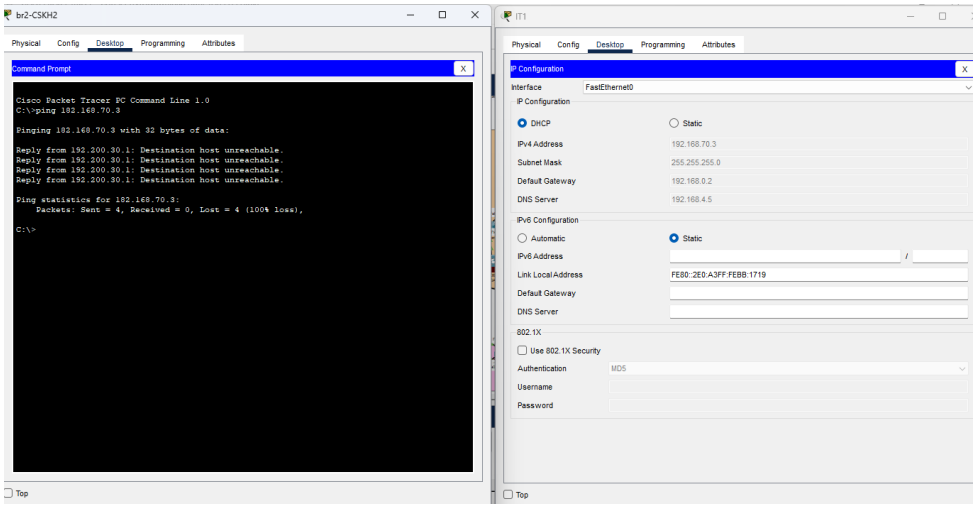


Hình 33: *PC ở trụ sở chính và chi nhánh Hà Nội được truy cập tới nhau*

8.6 PC ở trụ sở chính và chi nhánh không được truy cập tới nhau

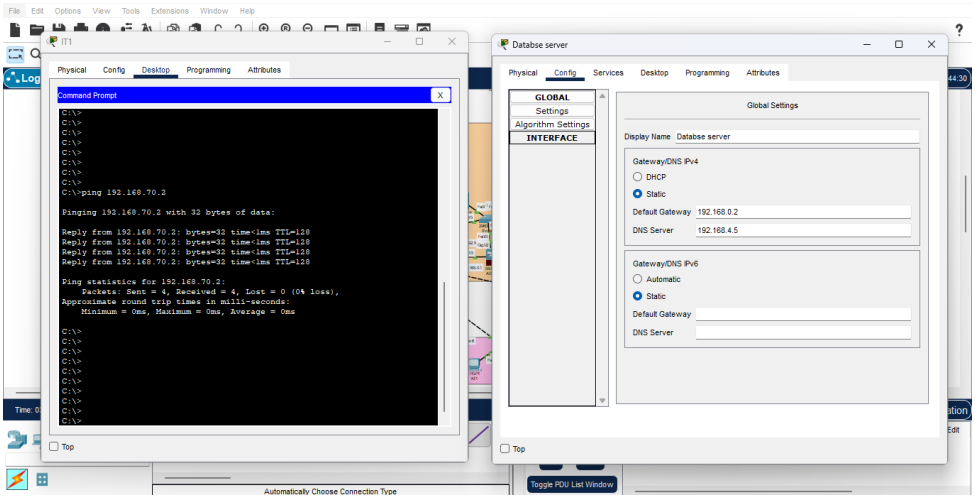


Hình 34: *PC ở trụ sở chính và chi nhánh Đà Nẵng không được truy cập tới nhau*

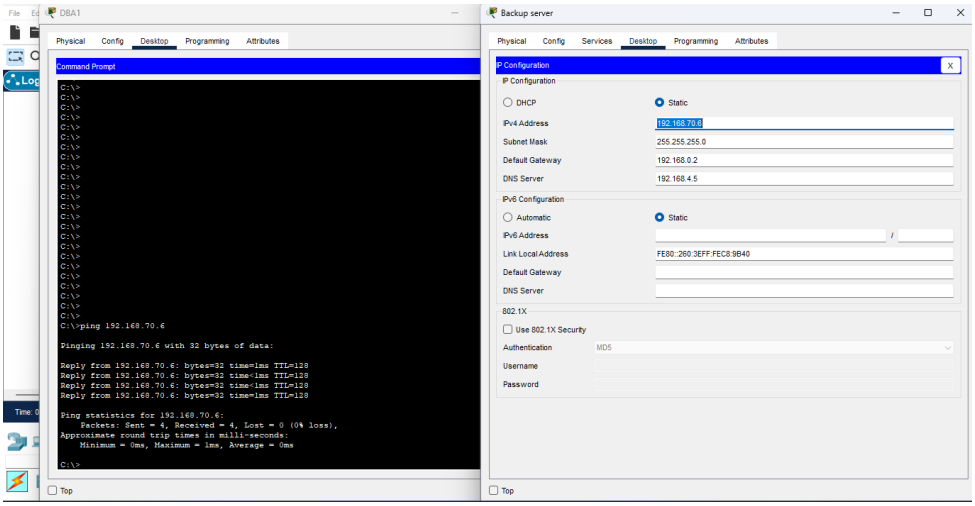


Hình 35: *PC ở trụ sở chính và chi nhánh Hà Nội không được truy cập tới nhau*

8.7 PC được truy cập vào backup server và database server

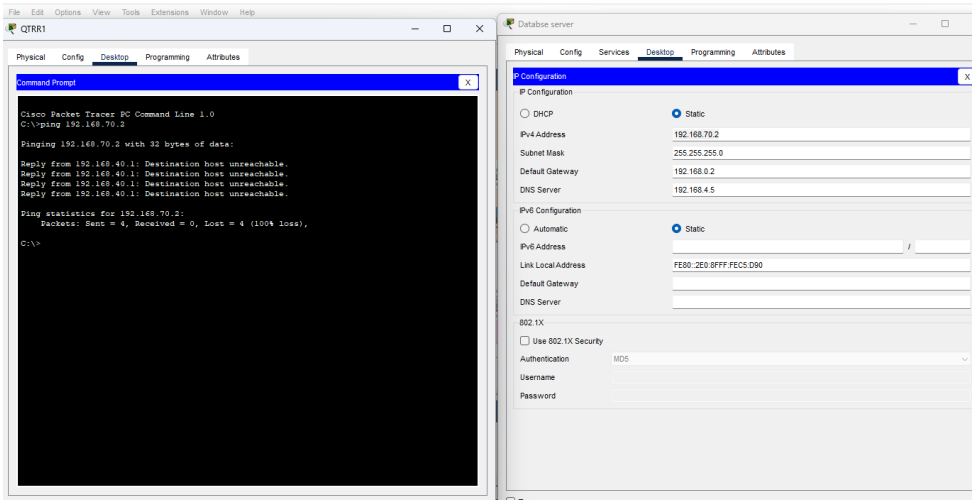


Hình 36: *PC ở trụ sở chính được truy cập đến Database Server*

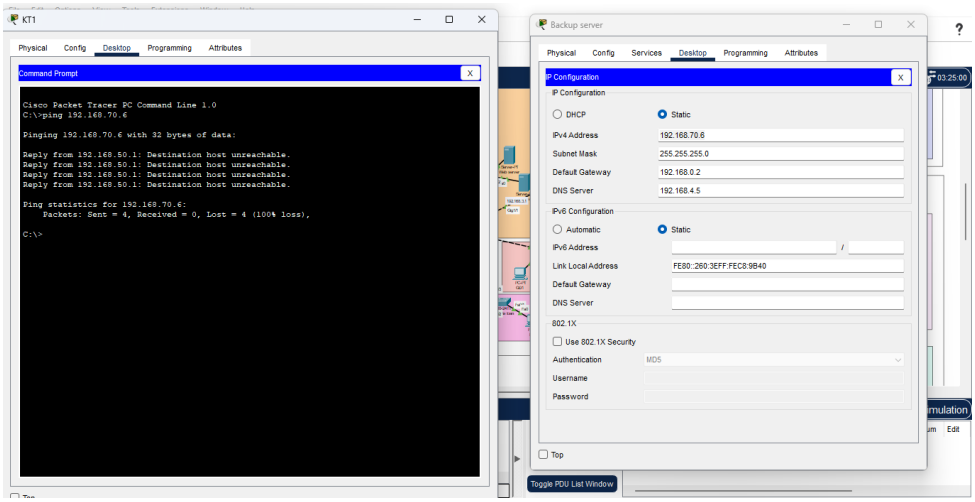


Hình 37: *PC ở trụ sở chính được truy cập đến Backup Server*

8.8 PC không được truy cập vào backup server và database server

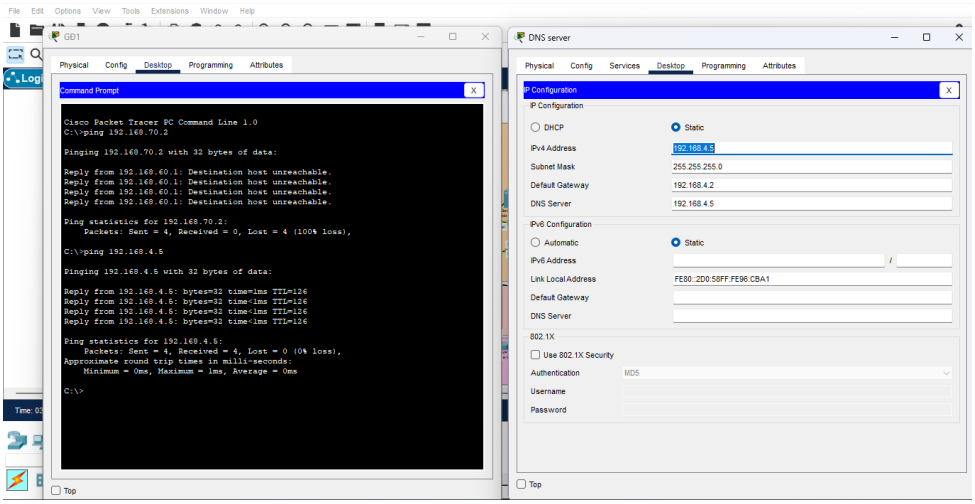


Hình 38: *PC ở trụ sở chính không được truy cập đến Database Server*

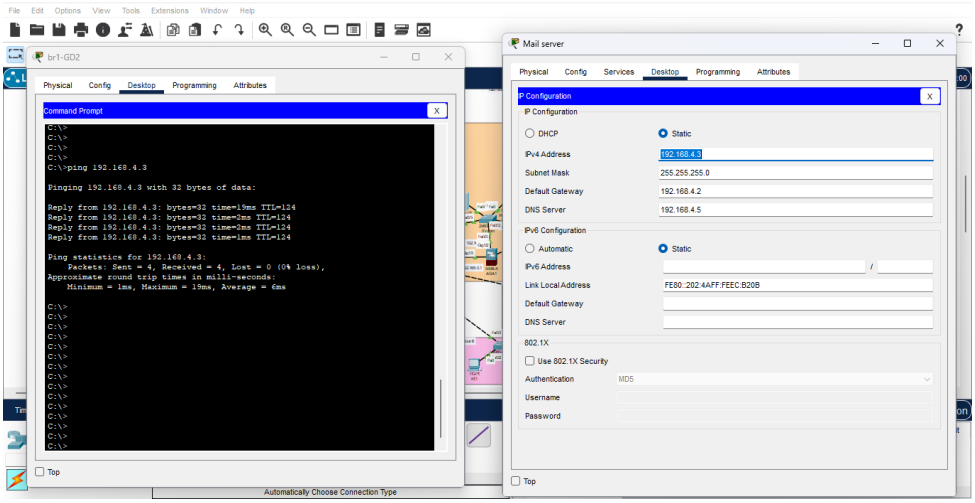


Hình 39: *PC ở trụ sở chính không được truy cập đến Backup Server*

8.9 PC được truy cập vào DMZ



Hình 40: *PC ở trụ sở chính được truy cập đến DMZ ở trụ sở chính*



Hình 41: *PC ở chi nhánh Đà Nẵng được truy cập đến DMZ ở trụ sở chính*

9 Kết luận và đánh giá

9.1 Những ưu điểm mà hệ thống đạt được

Các thiết bị mạng được triển khai với chất lượng cao, đảm bảo tuổi thọ dài và khả năng hoạt động ổn định. Hệ thống mạng này đáp ứng mượt mà các yêu cầu về lưu lượng dữ liệu, cho phép các thiết bị trong mạng LAN kết nối và giao tiếp hiệu quả.

Với sự tích hợp của mạng VLAN, dữ liệu và thông tin nội bộ của các phòng ban được bảo mật hiệu quả và quản lý một cách dễ dàng. Sự linh hoạt của hệ thống cho phép chuyển đổi giữa các VLAN một cách thuận tiện, cùng với khả năng nâng cấp và sửa chữa mà không gây ra rắc rối.

Hệ thống này được thiết kế để duy trì hiệu suất tốt mà không bị quá tải, thậm chí khi có sự mở rộng 20 % (hoặc hơn) trong vòng 5 năm tới. Sự sử dụng tường lửa giúp đảm bảo an toàn thông tin và bảo vệ tính toàn vẹn của hệ thống.

Backup và Recovery:

- Phát triển một backup server đặc biệt cho các máy chủ trong DMZ, đặc biệt là máy chủ cơ sở dữ liệu để giảm thiểu rủi ro mất dữ liệu.
- Thực hiện kiểm tra định kỳ để đảm bảo khả năng khôi phục dữ liệu nhanh chóng và hiệu quả.

9.2 Những vấn đề còn tồn tại đối với dự án

Mặc dù đã triển khai tường lửa, nhưng vẫn tồn tại rủi ro cao về vi-rút do khả năng lây lan của một hệ thống bị nhiễm có thể lan ra khắp mạng.

Các giải pháp đưa ra vẫn chưa phản ánh chặt chẽ thực tế do phải đặt nhiều giả định.

Chi phí thực hiện giải pháp là khá lớn, đặc biệt khi sử dụng các thiết bị hàng đầu trên thị trường.

Trong trường hợp một switch chính hoặc router chính gặp sự cố, toàn bộ hệ thống mạng sẽ trở nên không thể hoạt động.

Gặp khó khăn trong việc tích hợp các dạng NAT như Static, Dynamic, và PAT. Cần thêm nghiên cứu để áp dụng NAT hiệu quả trong quản lý địa chỉ IP. Thực hiện VPN trên Packet Tracer:

Còn thách thức trong việc triển khai VPN trên Packet Tracer. Yêu cầu tìm hiểu cách cài đặt VPN cho thiết bị mạng cụ thể và ứng dụng trong truy cập từ xa hoặc kết nối giữa các chi nhánh.

Thử nghiệm lắp đặt camera giám sát, nhưng gặp khó khăn trên Packet Tracer. Nghiên cứu thêm về giao thức như RTSP và ONVIF để tích hợp camera giám sát vào mạng.

Chưa giải quyết được cách tích hợp giữa NAT, VPN và camera giám sát. Nghiên cứu để bảo vệ mạng khi truyền dữ liệu từ camera giám sát qua mạng công cộng.

9.3 Định hướng tương lai

9.3.1 Bảo mật hệ thống

Với việc thiết kế một hệ thống mạng hoạt động trong lĩnh vực tài chính ngân hàng, việc tăng cường bảo mật là hết sức quan trọng.

- Firewall và IDS:
  - Kế hoạch để tích hợp thêm Firewall vào hệ thống để lọc và kiểm soát lưu lượng mạng.
  - Sử dụng hệ thống phát hiện xâm nhập (IDS) để theo dõi và cảnh báo về các hành vi đáng ngờ trên mạng.

- VoIP Security:
  - Triển khai hệ thống VoIP với đường truyền riêng, đặc biệt dẫn tới VoIP server.
  - Đảm bảo rằng các cuộc gọi trực tuyến giữ được tính bảo mật, có thể sử dụng mã hóa để bảo vệ thông tin trong quá trình truyền tải.
- Bảo mật hệ điều hành và ứng dụng:
  - Thực hiện việc sao lưu định kỳ và cập nhật các bản vá lỗi cho hệ điều hành và ứng dụng.
  - Sử dụng phần mềm bổ sung (Patch) để đóng các lỗ hổng và đảm bảo hệ thống hoạt động ổn định.
- Bảo mật access layer:
  - Xây dựng các kênh VPN để đảm bảo an toàn trong quá trình truy cập đối với các nhân viên làm việc từ xa.

9.3.2 Phát triển chi nhánh và kết Nối

- Kết nối chi nhánh mới:
  - Thiết lập kết nối chi nhánh mới với trụ sở chính để đảm bảo việc chia sẻ dữ liệu và tài nguyên mạng một cách hiệu quả.
  - Sử dụng thiết bị router để tạo mạng riêng ảo (VPN) và đảm bảo kết nối an toàn và bảo mật.
- Kết nối chi nhánh mới với chi nhánh cũ
  - Liên kết chi nhánh mới với các chi nhánh hiện tại thông qua router để tạo một môi trường mạng đồng nhất.
  - Thực hiện cấu hình chặt chẽ để đảm bảo tính an toàn và khả năng mở rộng.

9.3.3 Phát triển máy trạm ở các phòng ban

- Sử dụng switch 48 port:
  - Đối với mỗi phòng ban, triển khai switch 48 port để đảm bảo sự linh hoạt trong việc kết nối máy trạm và thiết bị mạng khác.
  - Cấu hình switch để quản lý băng thông và tối ưu hóa hiệu suất mạng.
- Gấp đôi số lượng máy trạm:
  - Nếu có nhu cầu phát triển, gấp đôi số lượng máy trạm để đảm bảo rằng mỗi phòng ban có đủ tài nguyên để hoạt động hiệu quả.
  - Tính toán và cấu hình mạng sao cho nó có thể mở rộng dễ dàng khi cần thiết.
- Bảo mật và quản lý máy trạm:
  - Áp dụng biện pháp bảo mật để ngăn chặn truy cập trái phép và bảo vệ thông tin quan trọng.
  - Sử dụng phần mềm quản lý mạng để giám sát và duy trì máy trạm một cách hiệu quả.

9.3.4 Triển khai hệ thống VPN

- Thiết lập một hệ thống Virtual Private Network (VPN) để cung cấp một kênh kết nối an toàn cho nhân viên khi làm việc từ xa hoặc kết nối từ các chi nhánh khác.
- Sử dụng các giao thức VPN mạnh mẽ để đảm bảo tính bảo mật cao, chẳng hạn như OpenVPN hoặc IPsec.

9.3.5 Cải thiện NAT (Network Address Translation)

- Kết hợp cải thiện NAT để giúp quản lý địa chỉ IP và tăng cường bảo mật của hệ thống mạng.
- Sử dụng các kỹ thuật NAT dynamic và static để tối ưu hóa việc gán địa chỉ IP và giảm rủi ro từ các cuộc tấn công mạng.

9.3.6 Hệ thống camera giám sát

- Triển khai hệ thống camera giám sát để theo dõi và bảo vệ vùng quan trọng của tòa nhà, đặc biệt là khu vực có giá trị tài sản cao.
- Sử dụng công nghệ camera có độ phân giải cao và khả năng quay hình trong điều kiện ánh sáng yếu để đảm bảo thu được hình ảnh chất lượng cao mọi lúc.

9.3.7 Áp dụng công nghệ mới

Theo dõi và nghiên cứu các xu hướng công nghệ mới trong lĩnh vực mạng và ngân hàng. Áp dụng thêm những công nghệ như SD-WAN, các giải pháp load balancing tốt hơn và giải pháp tốt hơn cho vấn đề truy cập (thay cho ACL).

10 Tài liệu tham khảo

[1] Kurose, J. R., & Ross, K. (2021b). Computer Networking [Global Edition].

[2] Jesin A. Packet Tracer Network Simulator. Packt Publishing, 2014.

[3] Michal Pioro, Deepankar Medhi. Routing, Flow, and Capacity Design in Communication and Computer Networks. Elsevier/Morgan Kaufmann, 200.

[4] PowerCert Animated Videos. Truy cập từ: https://www.youtube.com/@PowerCertAnimatedVideos

[5] Cisco. (2022). Configure and Filter IP Access Lists. Truy cập từ https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

[6] Cisco. (2022). Configure Network Address Translation and ACLs on an ASA Firewall. Truy cập từ: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.html.

[7] Cisco. (2023). Configure Network Address Translation. Truy cập https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html

[8] Kai Nguyen. Truy cập từ: https://www.youtube.com/watch?v=9mWgDLEwt-k.

[9] NetworkChuck. Truy cập từ: https://bit.ly/nc-ccna.

[10] GeeksforGeeks. (2022). DHCP Server Configuration in Cisco. Truy cập từ: https://www.geeksforgeeks.org/dhcp-server-configuration-in-cisco/ [11] Nessi. (2020, February 9). Lab 7.0 Cấu hình HSRP Cisco [Online forum post]. Truy cập từ https://securityzone.vn/t/lab-7-0-cau-hinh-hsrp-cisco.2749/

[12] Quyền Nguyễn. (2023, August 29). Giao thức OSPF là gì? Cách thức hoạt động và cấu hình định tuyến OSPF. Truy cập từ https://hostingviet.vn/giao-thuc-ospf

[13] CCNASEC. (2018, June 21). 9.3.1.2 Lab A: Configuring ASA Basic Settings and Firewall Using CLI (Instructor Version). Truy cập từ https://ccnasec.com/9-3-1-2-lab-a-configuring-asa-basic-settings-and-firewall-using-cli-instructor-version.html

[14] Viễn thông xanh C. D. (2023, September 25). Mạng Hình Sao (Star Topology) Chi Tiết về Cấu Trúc, Ưu Điểm và Hạn Chế. Viễn Thông Xanh. Truy cập từ https://vienthongxanh.vn/mang-hinh-sao-star-topology-cau-truc-uu-diem-va-han-che/

[15] Dương Văn Thông. (2017, October 17). CẤU TRÚC MÔ HÌNH MẠNG PHÂN CẤP. Truy cập từ https://vnpro.vn/thu-vien/cau-truc-mo-hinh-mang-phan-cap-2014.html