

ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC BÁCH KHOA  
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



## MẠNG MÁY TÍNH (CO3093)

---

### BÀI TẬP LỚN 2

### Network Designing

---

**Teacher:** Bùi Xuân Giang  
**Students:** Lã Nguyễn Gia Hy 2110231  
Đặng Dương Minh Nhật 2110416  
Trang Sĩ Trọng 2110621  
Trần Lê Quốc Khánh 2111498

TP. Hồ Chí Minh, 15/12/2023

## Mục lục

<b>1</b>	<b>Phân công công việc</b>	<b>3</b>
<b>2</b>	<b>Yêu cầu hệ thống</b>	<b>4</b>
2.1	Yêu cầu hệ thống mạng tại Trụ sở chính và Chi nhánh	4
2.1.1	Trụ sở chính	4
2.1.2	Chi nhánh	4
2.1.3	Thông lượng và tải của hệ thống	4
2.2	Những vấn đề cần khảo sát ở địa điểm lắp đặt	5
2.2.1	Danh sách kiểm tra khảo sát của địa điểm lắp đặt	5
2.3	Xác định khu vực có tải cao	6
2.4	Cấu trúc mạng phù hợp với yêu cầu	6
2.5	Sơ đồ cấu trúc khu vực	7
2.5.1	Trụ sở chính	7
2.5.2	Chi nhánh	11
<b>3</b>	<b>Danh sách thiết bị, sơ đồ IP và sơ đồ nối dây</b>	<b>13</b>
3.1	Danh sách thiết bị mạng sử dụng	13
3.1.1	Switch: Cisco WS-C2960-24TT-L	13
3.1.2	Router: Cisco 2911	13
3.1.3	Access Point: Cisco-Linksys WAP610N Wireless-N Access Point with Dual-Band	14
3.1.4	Thiết bị bảo mật FIREWALL CISCO ASA5506-K9	15
3.1.5	Switch Layer 3 3560	16
3.1.6	Server	16
3.2	Sơ đồ IP và sơ đồ đi dây ở trụ sở chính và chi nhánh	17
3.2.1	Trụ sở chính	17
3.2.2	Tại chi nhánh	18
3.3	Sơ đồ WAN giữa trụ sở và các chi nhánh	19
<b>4</b>	<b>Thiết kế sơ đồ mạng bằng Packet Tracer</b>	<b>20</b>
4.1	Những công nghệ đã sử dụng	20
4.2	Toàn bộ hệ thống	21
4.3	Trụ sở chính	22
4.4	Chi nhánh Đà Nẵng	23
4.5	Chi nhánh Hà Nội	24
<b>5</b>	<b>Tính toán các thông số của hệ thống</b>	<b>25</b>
5.1	Trụ sở chính	25
5.1.1	Server	25
5.1.2	Workstation	25
5.1.3	Người dùng	25
5.1.4	Toàn trụ sở	25
5.1.5	Các thông số an toàn	25
5.2	Chi nhánh	26
5.2.1	Server	26
5.2.2	Workstation	26
5.2.3	Người dùng	26
5.2.4	Toàn chi nhánh	26
5.2.5	Các thông số an toàn	26
<b>6</b>	<b>Kiểm tra hệ thống bằng các công cụ phổ biến như ping, traceroute</b>	<b>27</b>
6.1	PC cùng VLAN	27
6.2	PC khác VLAN tại cùng cơ sở	28
6.3	PC giữa trụ sở chính và chi nhánh	30
6.4	PC truy cập vào server trong DMZ	30
6.5	PC khách hàng không thể truy cập vào PC trong LAN	31
6.6	PC từ ngoài mạng internet truy cập tới server	32



<b>7</b>	<b>Đánh giá hệ thống</b>	<b>33</b>
7.1	Các kết quả đạt được . . . . .	33
7.2	Những hạn chế còn vướng mắc . . . . .	33
7.3	Nâng cấp hệ thống và định hướng cho tương lai . . . . .	33
7.4	Tổng hợp một số công nghệ đã sử dụng cho hệ thống mạng . . . . .	34
7.5	Tính an toàn và bảo mật dữ liệu hệ thống . . . . .	34
<b>8</b>	<b>Tài liệu tham khảo</b>	<b>35</b>



## 1 Phân công công việc

STT	Họ và tên	MSSV	Công việc
1	Đặng Dương Minh Nhật	2110416	Thiết kế hệ thống + Packet Tracer (chính)
2	Trang Sĩ Trọng	2110621	Viết báo cáo (phụ)
3	Lã Nguyễn Gia Hy	2110231	Viết báo cáo (chính)
4	Trần Lê Quốc Khánh	2111498	Thuyết trình + Viết báo cáo(phụ) + Packet Tracer (phụ)

## 2 Yêu cầu hệ thống

### 2.1 Yêu cầu hệ thống mạng tại Trụ sở chính và Chi nhánh

Thiết kế mạng máy tính sử dụng trong trụ sở và hai chi nhánh của một công ty BB đang được xây dựng.

#### 2.1.1 Trụ sở chính

Trụ sở sẽ có các thông số sau:

- Tòa building tại trụ sở cao 7 tầng, tầng 1 được trang bị 1 phòng kỹ thuật mạng và Cabling Central Local (Phòng tập trung dây mạng và patch panel).
- Quy mô: 120 workstations, 5 servers, 12 networking devices.
- Sử dụng các công nghệ mới cho cơ sở hạ tầng mạng bao gồm các kết nối có dây và không dây và cáp sợi (GPON). Mạng được tổ chức theo cấu trúc VLAN và Gigaethernet 1GBE/10GBE.
- Kết nối với bên ngoài bằng 2 Leased Line và 2 xDSL với Load Balancing. Mọi dữ liệu đi ra ngoài Internet đều phải đi qua mạng con của Trụ sở chính.
- Sử dụng kết hợp phần mềm được cấp phép và mã nguồn mở, ứng dụng văn phòng, ứng dụng client-server, đa phương tiện và cơ sở dữ liệu.
- Bảo mật cao, an toàn khi xảy ra sự cố, dễ dàng nâng cấp hệ thống.
- Cấu hình VPN cho site-to-site và cho nhân viên làm việc từ xa kết nối với mạng LAN.
- Đề xuất một hệ thống camera giám sát cho công ty

#### 2.1.2 Chi nhánh

Trụ sở kết nối đến 2 chi nhánh khác ở 2 thành phố lớn là Đà Nẵng và Hà Nội. Mỗi chi nhánh cũng được thiết kế tương tự như trụ sở nhưng ở quy mô nhỏ hơn:

- Tòa nhà cao 2 tầng, tầng 1 được trang bị 1 phòng kỹ thuật Mạng và Cabling Central Local.
- Quy mô chi nhánh: 30 workstations, 3 servers, ít nhất 5 thiết bị mạng.

#### 2.1.3 Thông lượng và tải của hệ thống

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,... Dung lượng tải về khoảng 1000 MB/ngày và dung lượng tải lên khoảng 2000 MB/ngày
- Mỗi workstation dùng cho duyệt Web, tải tài liệu, giao dịch khách hàng,... Tổng dung lượng tải về 500 MB/ngày, tổng dung lượng tải lên khoảng 100MB/ngày.
- Thiết bị kết nối WiFi từ truy cập của khách hàng (dùng để tải về) khoảng 500 MB/ngày.
- Hệ thống Mạng máy tính của Công ty BB 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,...).

## 2.2 Những vấn đề cần khảo sát ở địa điểm lắp đặt

### 2.2.1 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 cấp 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:

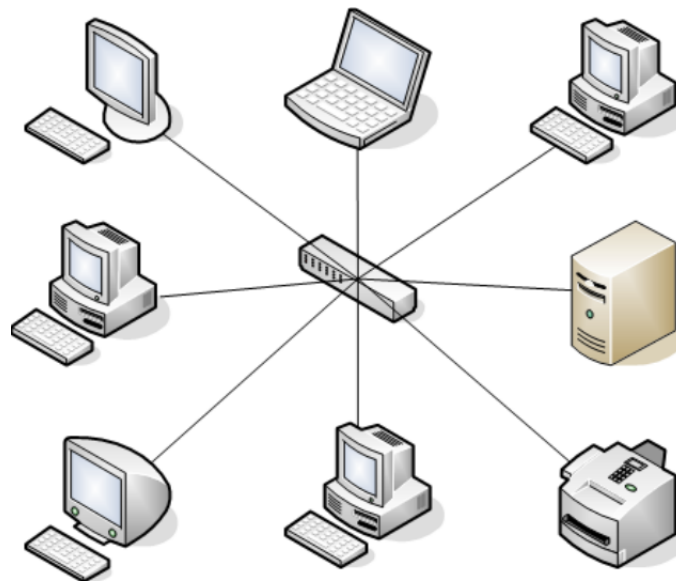
- Phòng IT tầng 1:
  - Kiểm tra các cơ sở hạ tầng sẵn có.
  - Đảm bảo nguồn điện và chuẩn bị các nguồn điện dự phòng khi cần thiết.
  - Xác định điều kiện môi trường và đề ra những giải pháp để tránh ảnh hưởng đến các thiết bị mạng.
  - Xác định tính tương thích của thiết bị mạng hiện có với topology được chọn.
  - Đánh giá khả năng tiếp cận cho công việc bảo dưỡng và sửa chữa.
  - Kiểm tra hệ thống bảo mật
- Trung tâm cấp 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.

## 2.3 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.
- 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.

## 2.4 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 1: 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:

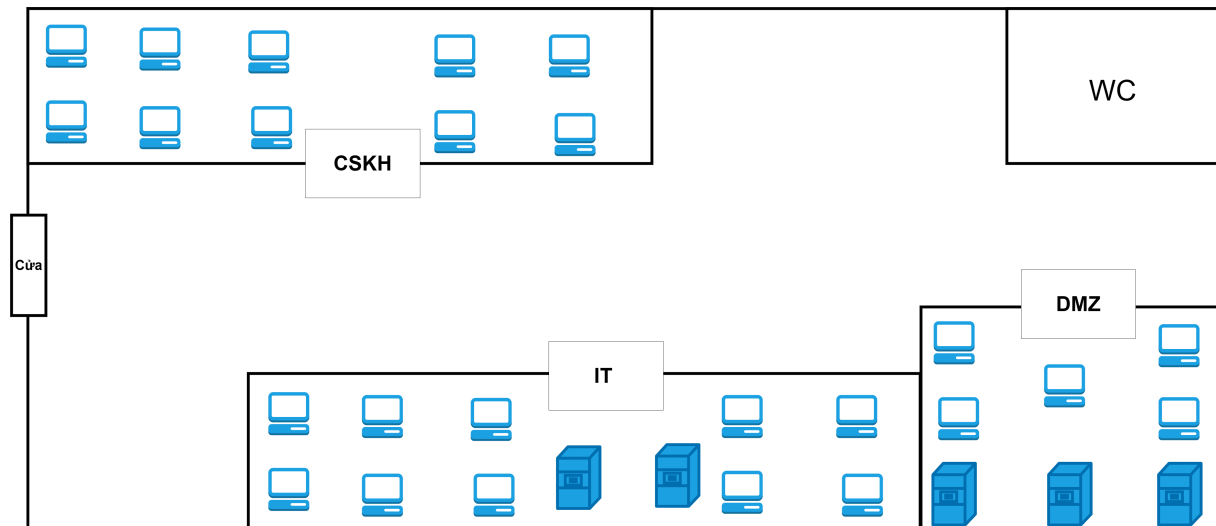
- Nhược điểm chính của trúc này là khi thiết bị trung tâm bị hỏng, các thiết bị kết nối sẽ bị gián đoạn giao tiếp.
- Hiệu suất của toàn mạng phụ thuộc vào hiệu suất của nút trung tâm.

## 2.5 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:

### 2.5.1 Trụ sở chính

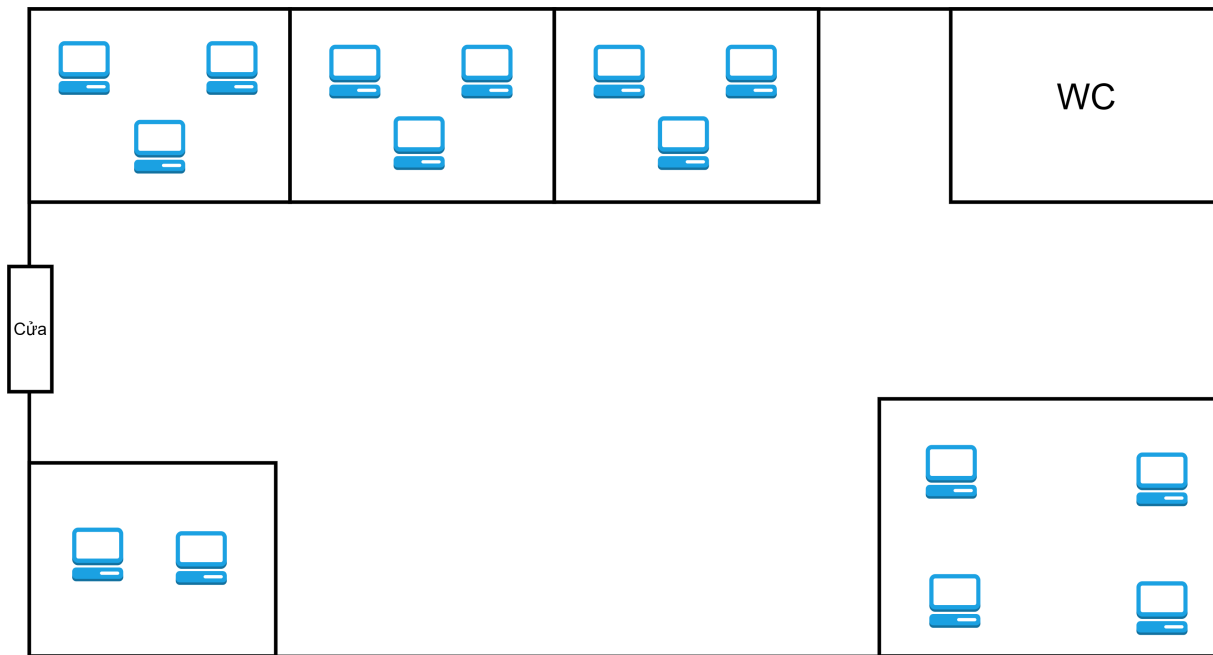
- Tầng 1:
  - Phòng chăm sóc khách hàng trang bị 10 workstation.
  - Phòng server chứa backup server, database server và nơi làm việc của bộ phận DBA (Database Administrator) và bộ phận IT1 trang bị 10 workstations, 7 workstations cho bộ phận DBA và 3 workstations cho bộ phận IT1.
  - Vùng DMZ (chứa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



Hình 2: Tầng 1 - Trụ sở chính

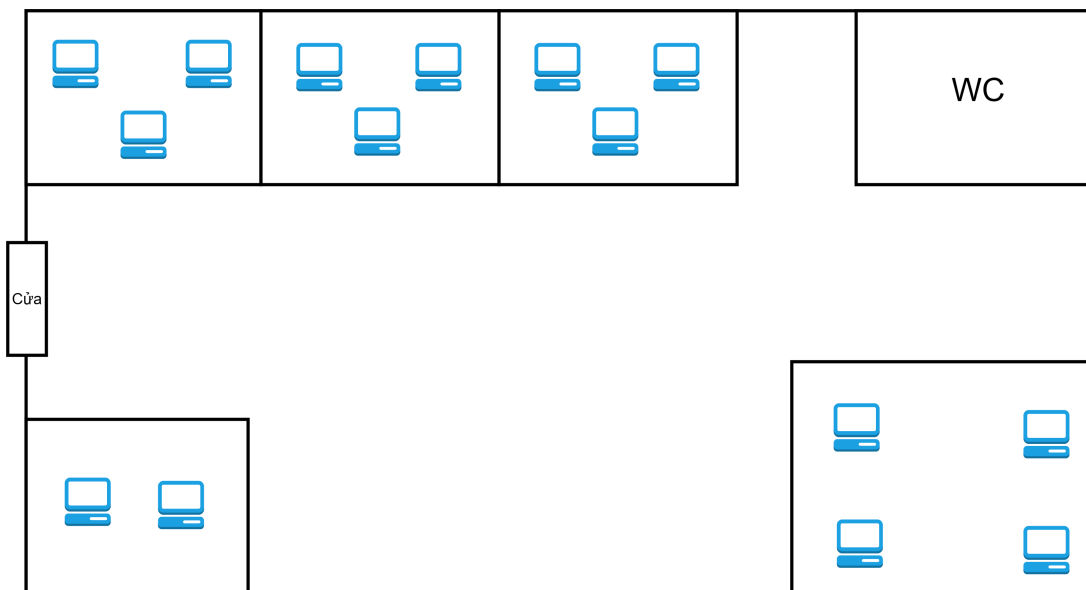
- Tầng 2: Phòng Giao dịch 1, trang bị 15 workstations.





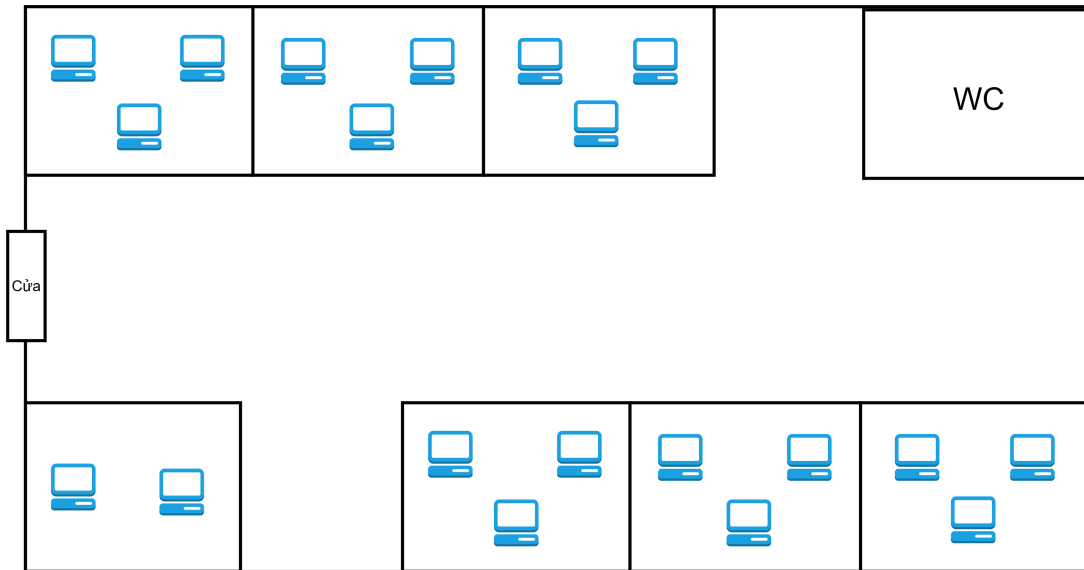
**Hình 3:** Tầng 2 - Trụ sở chính

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



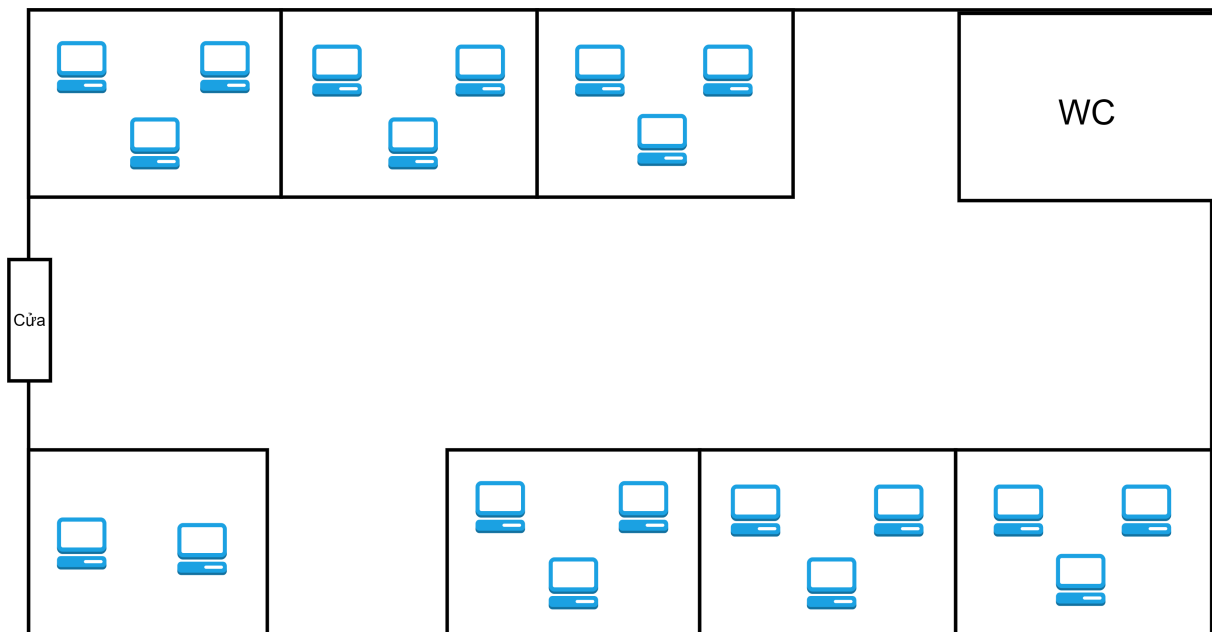
**Hình 4:** Tầng 3 - Trụ sở chính

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



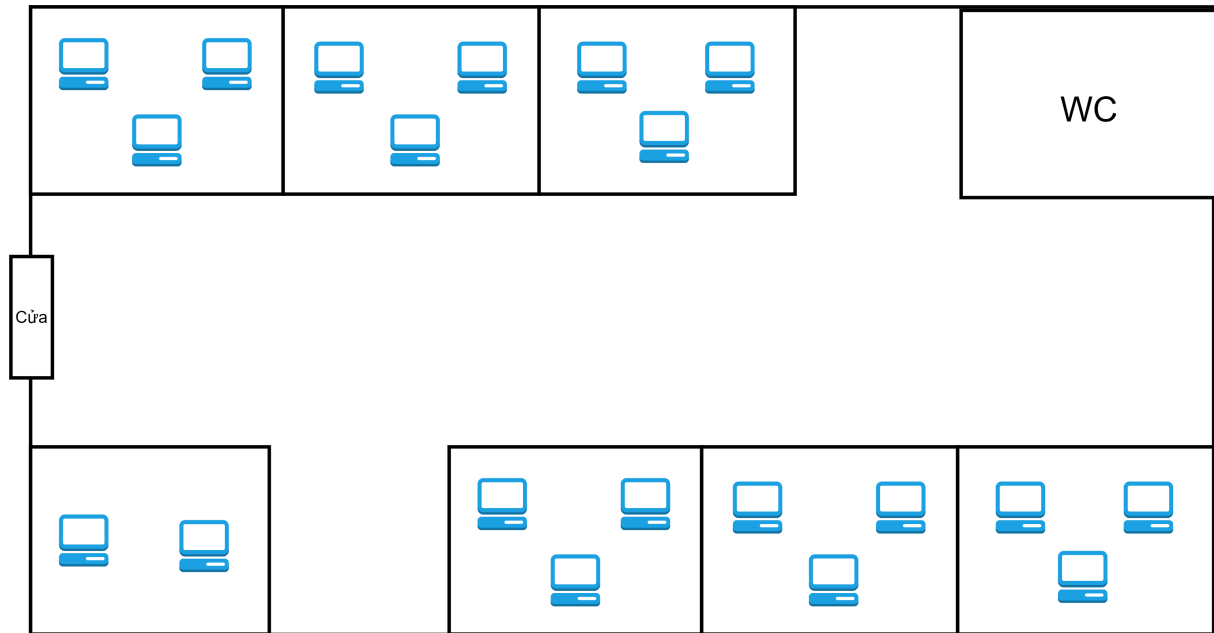
**Hình 5:** Tầng 4 - Trụ sở chính

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



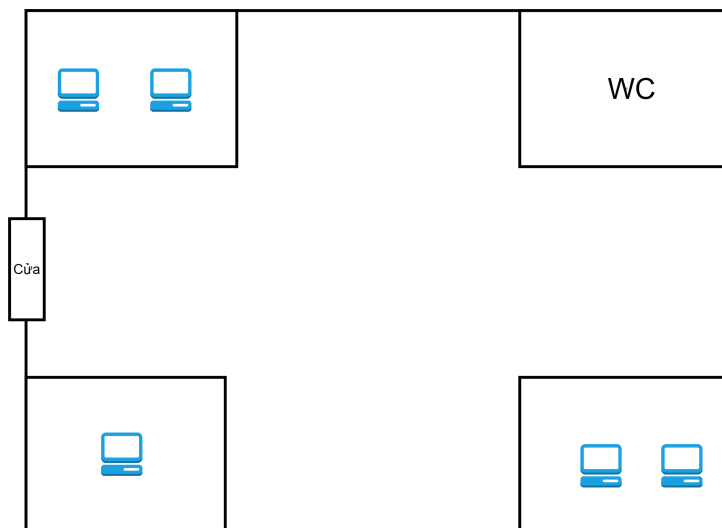
**Hình 6:** Tầng 5 - Trụ sở chính

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



**Hình 7:** Tầng 6 - Trụ sở chính

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



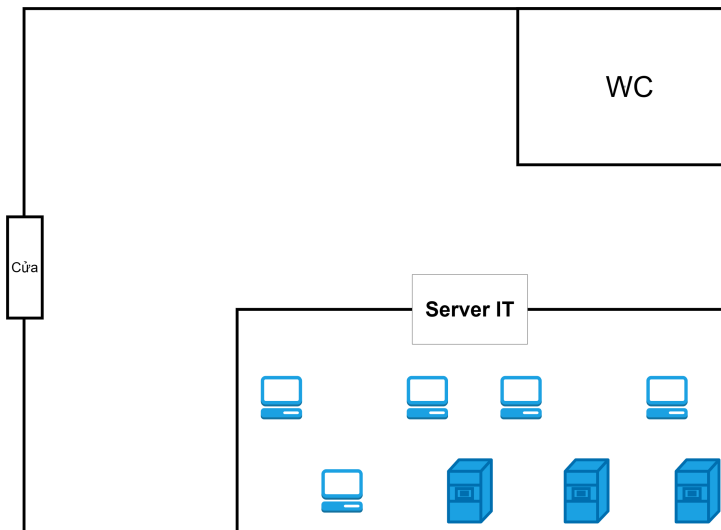
**Hình 8:** Tầng 7 - Trụ sở chính

- 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

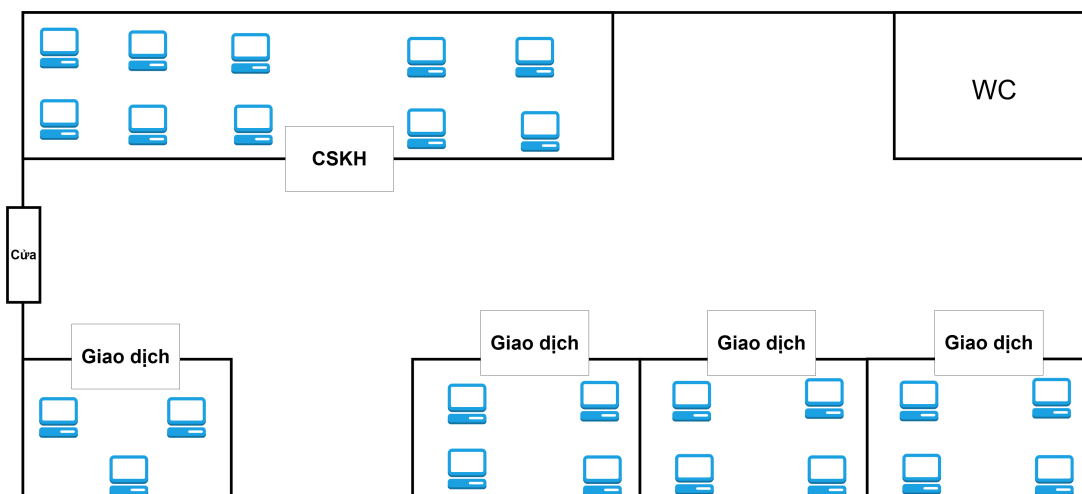
### 2.5.2 Chi nhánh

- 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 9: Tầng 1 - Chi nhánh

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



**Hình 10:** 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

### 3 Danh sách thiết bị, sơ đồ IP và sơ đồ nối dây

#### 3.1 Danh sách thiết bị mạng sử dụng

##### 3.1.1 Switch: Cisco WS-C2960-24TT-L

Switch Cisco WS-C2960-24TT-L được sử dụng làm Switch chính trong hệ thống, dùng để kết nối với các phòng ban và với switch tổng. Thiết bị có độ bảo mật cao cũng như dễ cấu hình, xử lý. Các thông số kỹ thuật như sau:

- Fast Ethernet: Cổng 24 x 10/100 + 2 x 10/100/1000
- RAM: 64 MB
- Bộ nhớ flash: 32 MB flash
- Hiệu suất dung lượng chuyển mạch: 32 Gbps
- Hiệu suất chuyển tiếp(kích thước gói 64 byte): 6,5 Mpps
- Phương pháp xác thực: RADIUS, Vở bảo mật (SSH), TACACS+
- Kích thước: 4.4 x 44.5 x 23.6 cm
- Trọng lượng: 3.6 kg
- Giá bán: 13.650.000 VND

Lý do lựa chọn thiết bị:

- Hỗ trợ công nghệ StackWise-160 (với tốc độ StackRing 32Gbps và hỗ trợ tốc độ downlink port là 100 Mbps.)
- Được trang bị lớp MAC Security trên các cổng downlink / uplink (IP Base/ IP Services models)
- Được trang bị cổng downlink cấp nguồn PoE + (PoE model)
- Tích hợp chức năng bộ điều khiển với khả năng quản lý lên đến 50 điểm truy cập không dây (Hỗ trợ IP Base / IP Services)
- Được trang bị Cisco IOS XE Universal Image (Hỗ trợ Lan Base/ IP Base/ IP Services)
- Được trang bị Unified Access Data Plane (UADP) ASIC được xây dựng để hỗ trợ Cisco ONE (Open Network Environment)



Hình 11: Cisco WS-C2960-24TT-L Switch

##### 3.1.2 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 tới 8GB cho hiệu suất cao và bảo mật. Cisco 2900 cho phép triển khai trong môi trường WAN tốc độ cao với các dịch vụ đồng thời kích hoạt lên đến 75 Mbps để đáp ứng các doanh nghiệp vừa và chi nhánh. Được thiết kế để giải quyết các yêu cầu kinh doanh của khách hàng, cung cấp tăng công suất và hiệu suất như nhu cầu của bạn phát triển mạng lưới. Giao diện Modular cung cấp băng thông tăng lên, một sự đa dạng các tùy chọn kết nối, và khả năng phục hồi mạng. Các thông số kỹ thuật của thiết bị như sau:

- 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)
- Kích thước: 43.8 cm x 30.5 cm x 8.9 cm
- Trọng lượng: 16.15 Kg
- Giá bán: 19.200.000 VND

Lý do lựa chọn:

- Có nhiều giao diện LAN và WAN, bao gồm Gigabit Ethernet và Fast Ethernet.
- Hỗ trợ cổng USB để kết nối và chia sẻ tệp tin hoặc in ấn.
- Hỗ trợ các tính năng bảo mật như VPN (Virtual Private Network) và IPSec.
- Tích hợp firewall và các tính năng bảo mật khác để bảo vệ mạng.
- Sử dụng Cisco IOS (Internetwork Operating System) để quản lý và cấu hình.
- Hỗ trợ SNMP (Simple Network Management Protocol) để giám sát mạng.



Hình 12: Cisco 2911 Router

### 3.1.3 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 ngớt quãng khi xem video quan mạng không dây. Các thông số kỹ thuật như sau:

- 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
- Bandwitch: 2.4GHz – 5 GHz
- Ethernet port: 01 port 10/100Mbps.
- Tốc độ truyền không dây: 270 Mbps
- Trọng lượng: 160g
- Giá tiền: 1.950.000 VND

Lý do lựa chọn thiết bị:

- Hỗ trợ các thiết bị 802.11n, 802.11a, 802.11g và 802.11b.
- Có thể chuyển đổi giữa các băng tần vô tuyến 2.4GHz và 5GHz.
- Hỗ trợ mã hóa WPA2 bằng nút nhấn.
- Trình hướng dẫn thiết lập dễ sử dụng.
- Có một cổng Ethernet 10/100Mbps tự động chuyển đổi duy nhất để kết nối.



**Hình 13:** Cisco-Linksys WAP610N Wireless-N Access Point with Dual-Band

#### 3.1.4 Thiết bị bảo mật FIREWALL CISCO ASA5506-K9

Cisco ASA5506-K9 là một thiết bị tường lửa (firewall) và VPN (Virtual Private Network) thuộc dòng sản phẩm Cisco ASA 5500-X, được thiết kế để cung cấp bảo vệ mạng và giải pháp kết nối an toàn cho doanh nghiệp và tổ chức. Các thông số kỹ thuật của thiết bị như sau:

- Interfaces: 8 x 1 Gigabit Ethernet interface, 1 management port
- Stateful inspection throughput (multiprotocol): 300 Mbps
- Maximum 3DES/AES VPN throughput: 100 Mbps
- Memory: 4GB
- Dimensions (D x H x W): 9.23 in x 1.72 in x 7.871 in

Lý do lựa chọn thiết bị:

- ASA5506-K9 cung cấp hiệu suất lên đến 300 Mbps cho chuyển tiếp dữ liệu.
- Hỗ trợ nhiều tính năng bảo mật như tường lửa, IPS (Intrusion Prevention System), VPN, và content security (bảo mật nội dung).
- Có khả năng xử lý và kiểm soát lưu lượng mạng theo nhiều chiều hướng để ngăn chặn các mối đe dọa tiềm ẩn.
- Sử dụng Cisco ASDM (Adaptive Security Device Manager) hoặc CLI (Command Line Interface) để quản lý và cấu hình.



- Hỗ trợ tính năng quản lý từ xa, giúp người quản trị có thể kiểm soát và theo dõi từ xa.
- Có khả năng mở rộng thông qua các module mô-đun bổ sung như FirePOWER Services để cung cấp khả năng phòng chống mối đe dọa mạnh mẽ.



Hình 14: CISCO ASA5506-K9

### 3.1.5 Switch Layer 3 3560

Gồm 24 cổng FastEthernet 10/100 ports, nhóm sử dụng chúng để kết nối với các Switch tại các node và 2 cổng Gigabit Ethernet để kết nối với tường lửa. Ngoài chức năng chuyển mạch Switch layer 3 còn có thể định tuyến nên khi kết nối các mạng con có nhiều Vlan khác nhau sử dụng Switch layer 3 mà một lựa chọn phù hợp, ngoài ra với yêu cầu chúng ta cũng có thể lựa chọn Router thay thế.

Các thông số kỹ thuật:

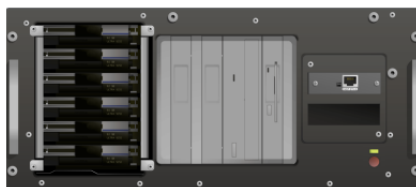
- 48 cổng Ethernet 10/100 và 4 cổng Gigabit Ethernet dựa trên SFP
- Cấu hình cố định 1RU, bộ chuyển mạch đa lớp
- Các dịch vụ thông minh cấp doanh nghiệp được cung cấp tối biên mạng
- Cấp nguồn qua Ethernet tiêu chuẩn IEEE 802.3af và Cisco
- Bộ tính năng phần mềm IP Base (IPB)



Hình 15: CISCO WS-C3560-24PS-S

### 3.1.6 Server

- Số lượng: 11
- Trụ sở cần có 5 server, và mỗi chi nhánh cần có 3 server



Hình 16: Server

Hệ thống bao gồm một số loại server như:

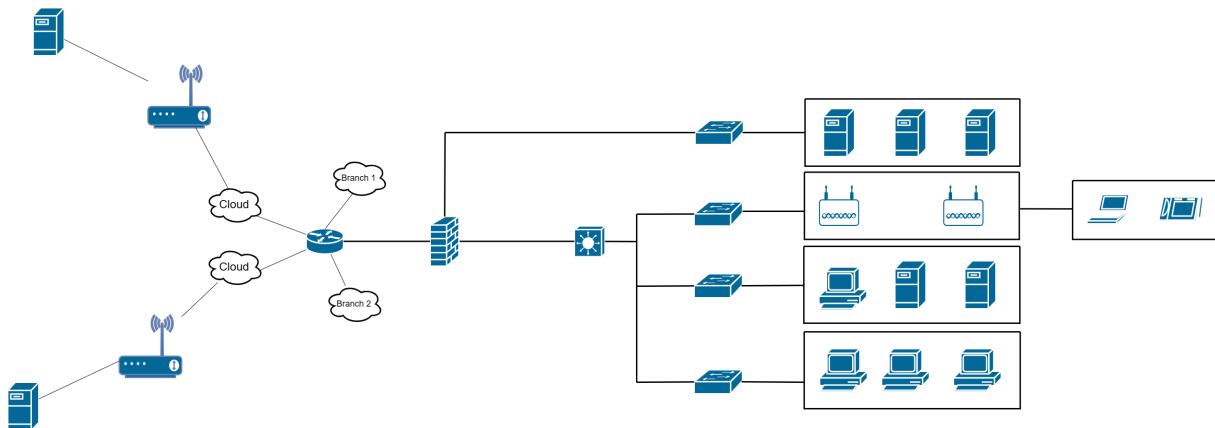
- DNS Server: chuyển đổi tên miền thành địa chỉ IP tương ứng. Điều này giúp các thiết bị trong mạng và trên Internet có thể tìm thấy và kết nối với các máy chủ và dịch vụ bằng cách sử dụng tên thay vì địa chỉ IP.

- Mail Server: quản lý và điều phối việc gửi và nhận thư điện tử. Nó lưu trữ thư trên máy chủ và xác định cách thức truyền và nhận thư trong mạng
- Database Server: chịu trách nhiệm lưu trữ và quản lý cơ sở dữ liệu. Nó cung cấp dịch vụ truy xuất và cập nhật dữ liệu cho các ứng dụng và người dùng có quyền truy cập
- Web Server: nơi lưu trữ và cung cấp các trang web và tài nguyên trên Internet. Khi người dùng truy cập một trang web, web server phản hồi bằng cách cung cấp nội dung của trang web đó.
- DHCP Server: tự động cấp phát địa chỉ IP, cùng với các thông số mạng khác như gateway cho các thiết bị trong mạng. Điều này giúp tự động cấu hình mạng cho các thiết bị mới tham gia mạng mà không cần sự can thiệp thủ công.

### 3.2 Sơ đồ IP và sơ đồ đi dây ở trụ sở chính và chinh nhánh

#### 3.2.1 Trụ sở chính

Sơ đồ đi dây:



Hình 17: Sơ đồ đi dây - Trụ sở chính

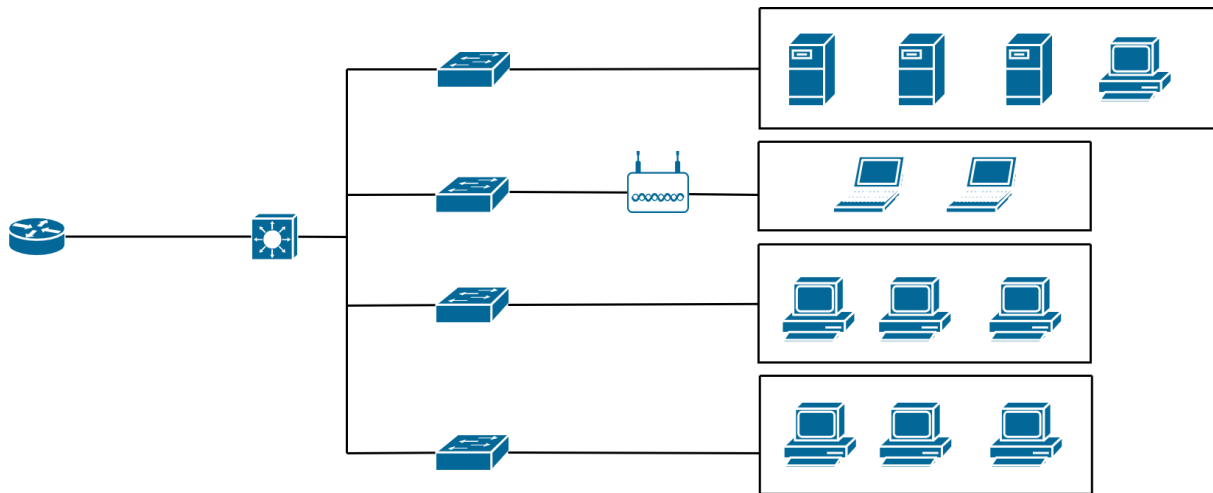
VLAN	Tầng	Phòng ban	Địa chỉ mạng	Default Getway	Địa chỉ khả dụng
80	1	Tiếp tân	192.168.8.0/24	192.168.8.1	192.168.8.1 - 192.168.8.255
10	2	Chăm sóc khách hàng	192.168.1.0/24	192.168.1.1	192.168.1.1 - 192.168.1.255
20	3	Giao dịch	192.168.2.0/24	192.168.2.1	192.168.2.1 - 192.168.2.255
30	4	Tài chính	192.168.3.0/24	192.168.3.1	192.168.3.1 - 192.168.3.255
40	5	Quản trị rủi ro	192.168.4.0/24	192.168.4.1	192.168.4.1 - 192.168.4.255
50	6	Kế toán	192.168.5.0/24	192.168.5.1	192.168.5.1 - 192.168.5.255
60	7	Giám đốc	192.168.6.0/24	192.168.6.1	192.168.6.1 - 192.168.6.255
70	1	DBA + IT Room + Inside Server	192.168.7.0/24	192.168.7.1	192.168.7.1 - 192.168.7.255

IP của các workstation được cấp phát động, tuy nhiên IP của các server được cấp phát tĩnh.

- Transaction Server: 100.0.1.5
- Web Server: 100.0.1.6
- Mail Server: 100.0.1.7
- Database và Backup Server: 192.168.7.8
- DNS Server: 192.168.7.7

### 3.2.2 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	Khách hàng	192.200.1.0/24	192.200.1.1	192.200.1.1 - 192.200.2.255
20	1	IT Room	192.200.2.0/24	192.200.2.1	192.200.2.1 - 192.200.2.255
30	2	Giao dịch + CSKH	192.200.3.0/24	192.200.3.1	192.200.3.1 - 192.200.3.255

IP của các workstation được cấp phát động, tuy nhiên IP của các server được cấp phát tĩnh.

- Mail server: 100.2.1.2
- Database và Backup Server: 192.200.2.8
- DNS server: 192.200.2.7

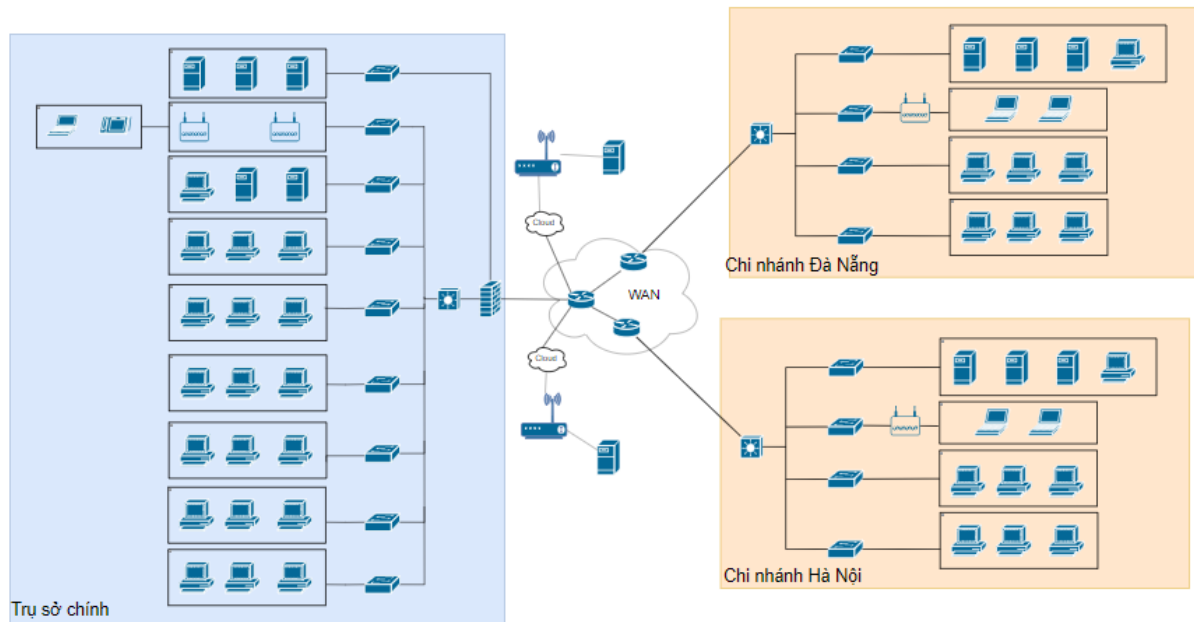
- Chi nhánh Hà Nội

VLAN	Tầng	Phòng ban	Địa chỉ mạng	Default Getway	Địa chỉ khả dụng
10	1	Khách hàng	192.100.1.0/24	192.100.1.1	192.100.1.1 - 192.200.2.255
20	1	IT Room	192.100.2.0/24	192.100.2.1	192.100.2.1 - 192.100.2.255
30	2	Giao dịch + CSKH	192.100.3.0/24	192.100.3.1	192.100.3.1 - 192.100.3.255

IP của các workstation được cấp phát động, tuy nhiên IP của các server được cấp phát tĩnh.

- Mail server: 100.1.1.2
- Database và Backup Server: 192.100.2.8
- DNS server: 192.100.2.7

### 3.3 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.

## 4 Thiết kế sơ đồ mạng bằng Packet Tracer

### 4.1 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 luận lý trên cùng một kiến trúc hạ tầng vật lý. VLAN có một số ưu điểm như sau:

- 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. DHCP có các ưu điểm sau:

- Tự động quản lý 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. ACL có các ưu điểm như sau:

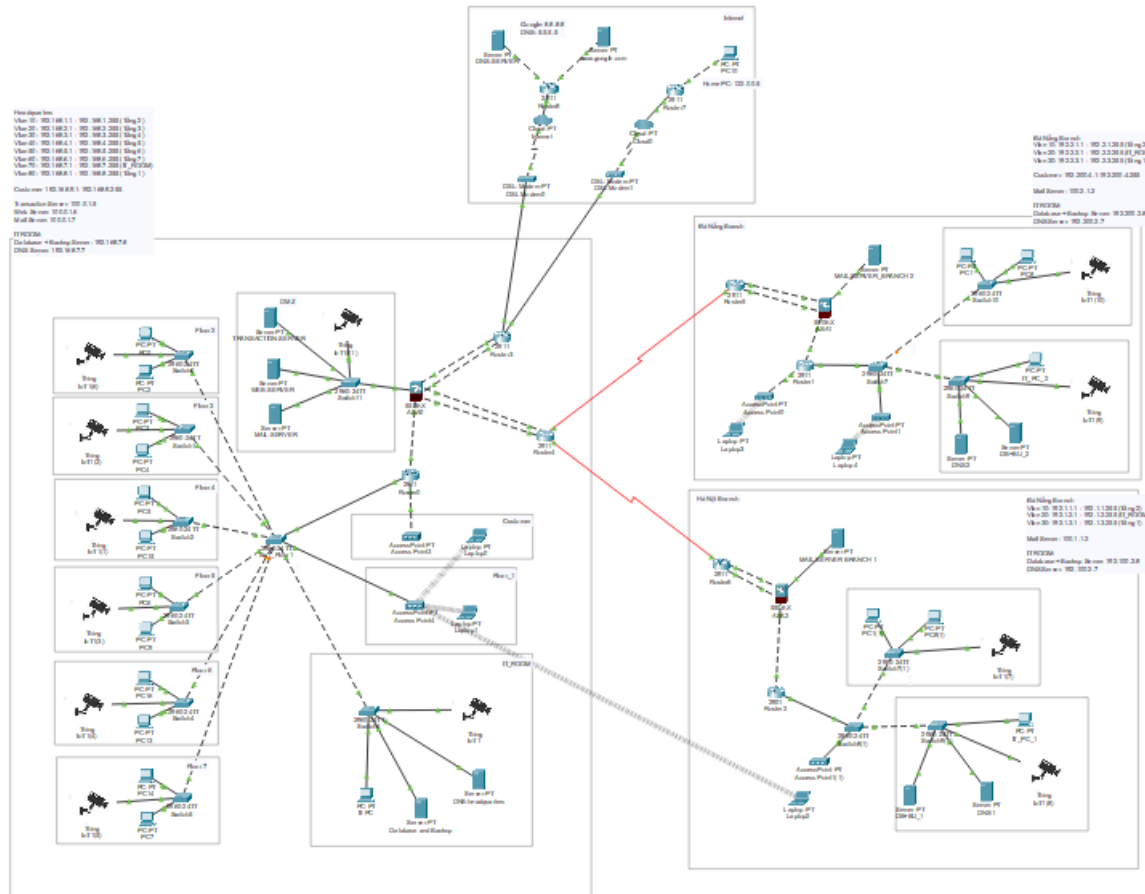
- Cho phép quản trị viên mạng tạo ra các quy tắc tùy chỉnh để kiểm soát truy cập dựa trên địa chỉ IP nguồn và đích, cổng, hay giao thức. Điều này giúp tạo ra các kịch bản linh hoạt để bảo vệ tài nguyên và dữ liệu quan trọng.
- Bằng cách thiết lập ACLs chặt chẽ, mạng có thể đạt được mức độ bảo mật cao 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 (Định tuyến)** 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.

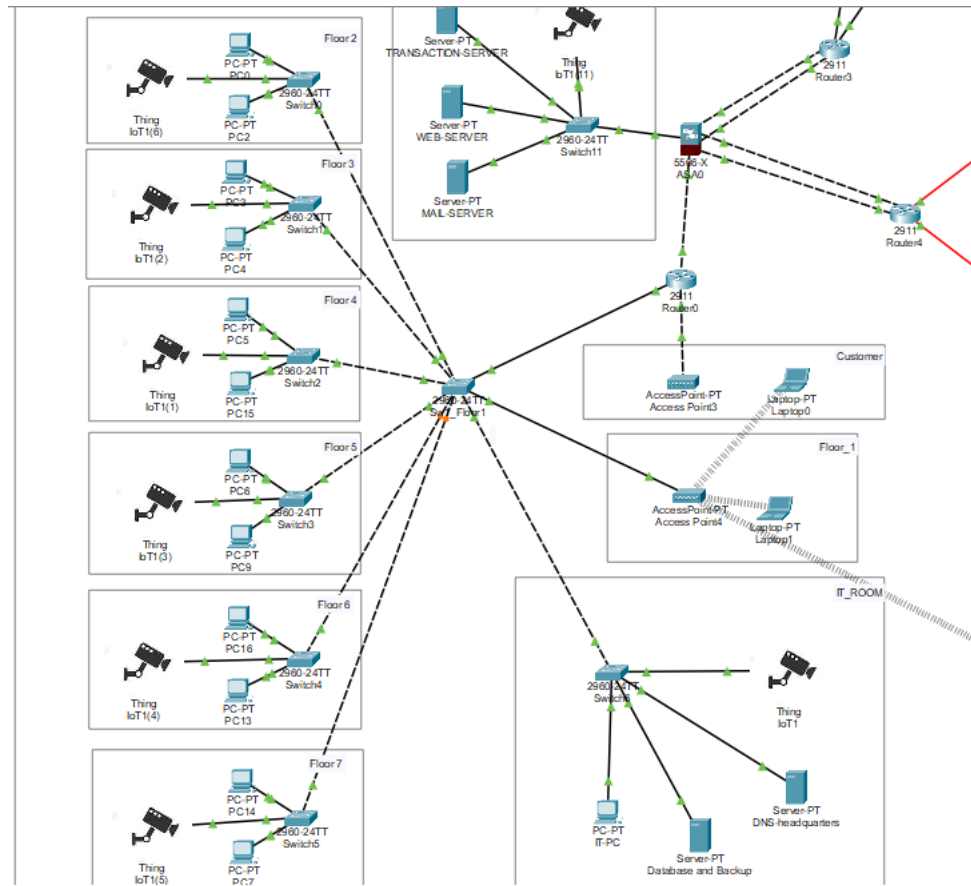
- Bằng cách phân phối tải thông qua nhiều đường truyền, công nghệ định tuyến giúp tối ưu hóa băng thông và ngăn chặn tình trạng quá tải tại một đường truyền duy nhất.
- Các giao thức định tuyến có thể được cấu hình để bảo mật mạng bằng cách kiểm soát quyền truy cập và xác thực dữ liệu, giúp ngăn chặn 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.

## 4.2 Toàn bộ hệ thống



Hình 20: Sơ đồ mạng của toàn bộ hệ thống

### 4.3 Trụ sở chính

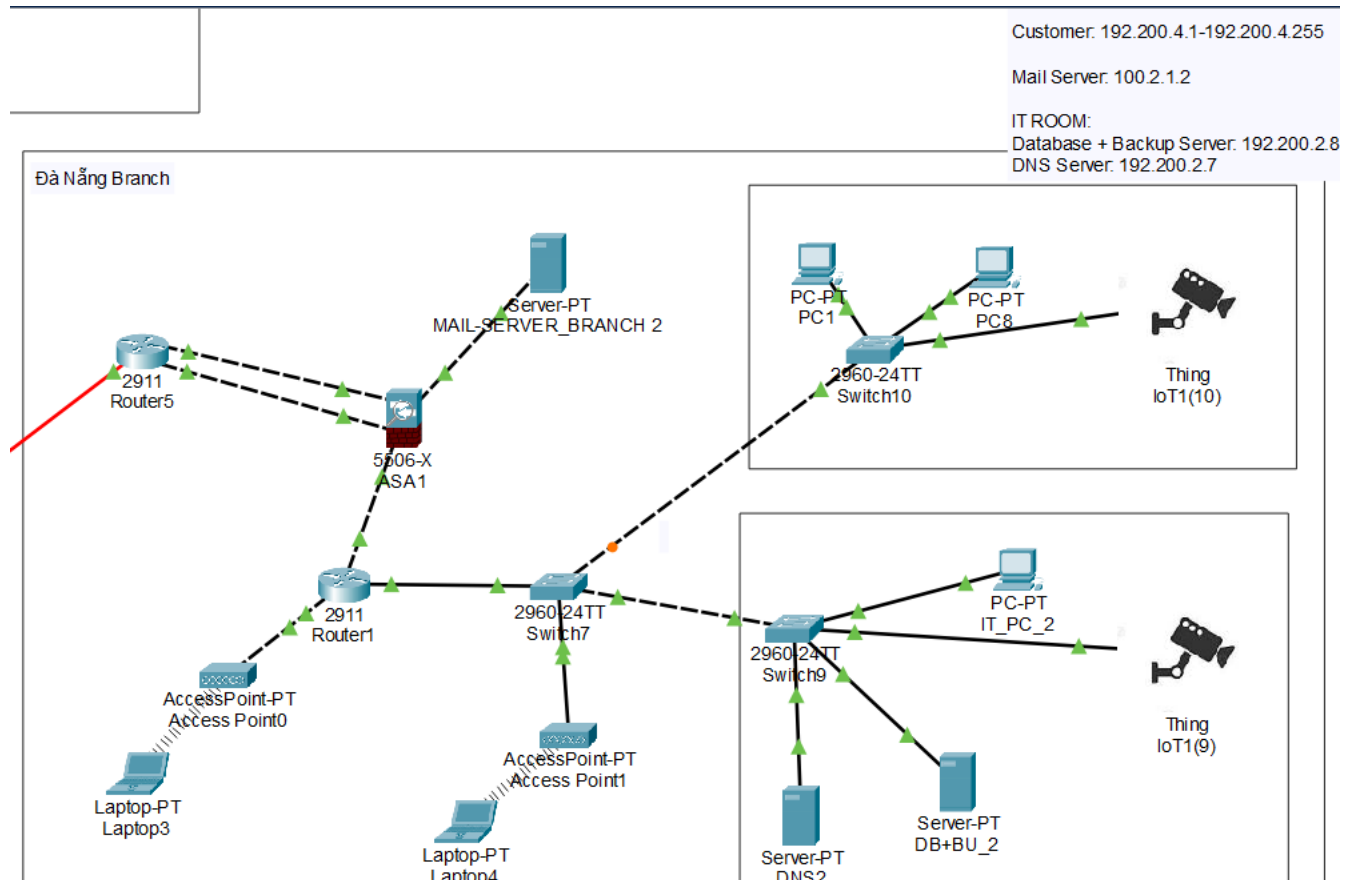


Hình 21: Sơ đồ mạng trụ sở chính

Mô tả:

- 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 lý 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.
- Hệ thống camera an ninh ở mỗi tầng khác nhau để giám sát.

#### 4.4 Chi nhánh Đà Nẵng



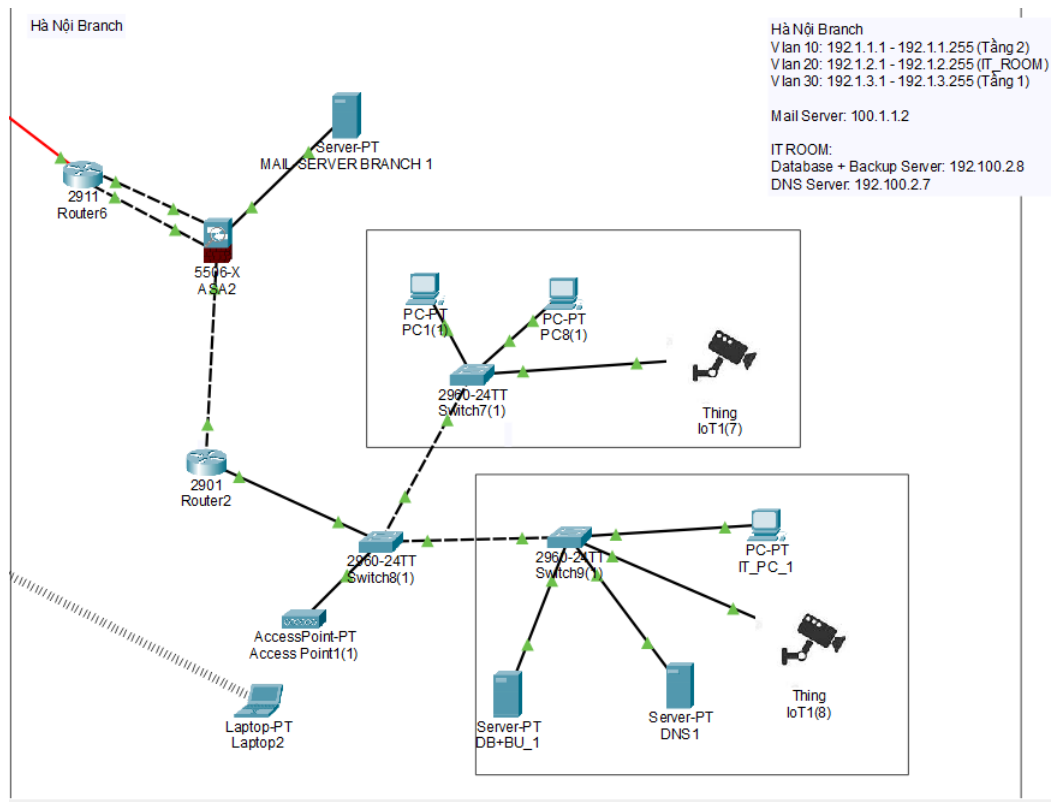
Hình 22: Sơ đồ mạng chi nhánh Đà Nẵng

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 lý 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.
- Hệ thống camera an ninh ở mỗi tầng khác nhau để giám sát.



## 4.5 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 lý 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.
- Hệ thống camera an ninh ở mỗi tầng khác nhau để giám sát.

## 5 Tính toán các thông số của hệ thống

Các thông số về lưu lượng và tải của hệ thống tập trung khoảng 80% vào giờ cao điểm 9h-11h và 15g-16h (3 giờ).

### 5.1 Trụ sở chính

#### 5.1.1 Server

Tổng dung lượng upload và download ước tính là  $2000 + 1000 = 3000\text{MB/ngày}$  cho mỗi server. Throughput của server là:

$$\frac{5 * 3000}{8 * 3600} * 8 = 4.167(Mbps)$$

Bandwidth của server là:

$$\frac{5 * 3000 * 80\%}{3 * 3600} * 8 = 8.889(Mbps)$$

#### 5.1.2 Workstation

Tổng dung lượng upload và download của mỗi workstation là  $100 + 500 = 600$  (MB/ngày) Throughput của các workstations là:

$$\frac{120 * 600}{8 * 3600} * 8 = 20(Mbps)$$

Bandwidth của các workstations là:

$$\frac{120 * 600 * 80\%}{3 * 3600} * 8 = 42.667(Mbps)$$

#### 5.1.3 Người dùng

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. Throughput của mỗi thiết bị người dùng là:

$$\frac{150 * 500}{8 * 3600} * 8 = 20.833(Mbps)$$

Bandwidth của mỗi thiết bị người dùng là:

$$\frac{150 * 500 * 80\%}{3 * 3600} * 8 = 44.444(Mbps)$$

#### 5.1.4 Toàn trụ sở

Giá trị throughput tổng cộng là:

$$4.167 + 20 + 20.833 = 45(Mbps)$$

Giá trị bandwidth tổng cộng là:

$$8.889 + 42.667 + 40.444 = 96(Mbps)$$

#### 5.1.5 Các thông số an toàn

Hệ thống Mạng máy tính của công ty BB được dự đoán cho mức độ phát triển 20% cho nên throughput và bandwidth tối thiểu để hệ thống hoạt động ổn định và có khả năng mở rộng sẽ bằng 120% lượng throughput và bandwidth đã tính ở trụ sở chính và chi nhánh.

Giá trị throughput tổng được tính lại sau 5 năm là:

$$45 * 120\% = 54(Mbps)$$

Giá trị bandwidth tổng được tính lại sau 5 năm là:

$$96 * 120\% = 115.2(Mbps)$$

## 5.2 Chi nhánh

Vì cả hai chi nhánh ở Hà Nội và Đà Nẵng đều có cấu trúc giống nhau, vì thế nên ta chỉ cần tính các thông số của mạng máy tính trên đối với một chi nhánh. Ta giả sử rằng một ngày làm việc của ngân hàng kéo dài 8 tiếng:

### 5.2.1 Server

Đối với chi nhánh, ta có 3 máy chủ với yêu cầu về tổng khả năng upload/download là khoảng 3000MB/ngày. Như vậy có thể tính ra được throughput của server là:

$$\frac{3 * 3000}{8 * 3600} * 8 = 2.5(Mbps)$$

Bandwidth của server là:

$$\frac{3 * 3000 * 80\%}{3 * 3600} = 5.333(Mbps)$$

### 5.2.2 Workstation

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 throughput của các workstations là:

$$\frac{30 * 600}{8 * 3600} * 8 = 5(Mbps)$$

Bandwidth của các workstations là:

$$\frac{30 * 600 * 80\%}{3 * 3600} * 8 = 10.667(Mbps)$$

### 5.2.3 Người dùng

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 throughput của mỗi thiết bị người dùng là:

$$\frac{50 * 500}{8 * 3600} * 8 = 6.944(Mbps)$$

Bandwidth của mỗi thiết bị người dùng là:

$$\frac{50 * 500 * 80\%}{3 * 3600} * 8 = 14.8148(Mbps)$$

### 5.2.4 Toàn chi nhánh

Giá trị throughput tổng cộng là:

$$2.5 + 5 + 6.9994 = 14.4444(Mbps)$$

Giá trị bandwidth tổng cộng là:

$$5.3333 + 10.6667 + 14.8148 = 30.8148(Mbps)$$

### 5.2.5 Các thông số an toàn

Tương tự như trên, ta có giá trị throughput tổng được tính lại sau 5 năm là:

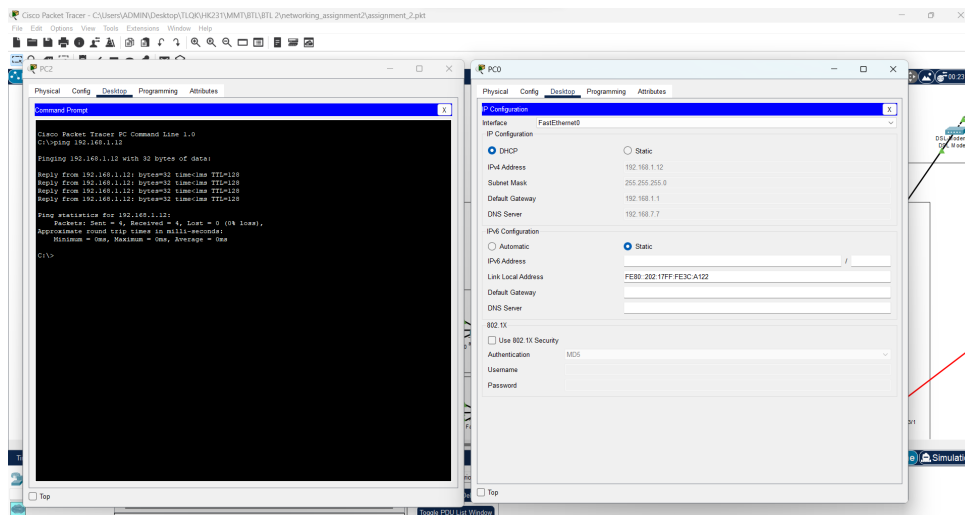
$$14.4444 * 120\% = 17.3333(Mbps)$$

Giá trị bandwidth tổng được tính lại sau 5 năm là:

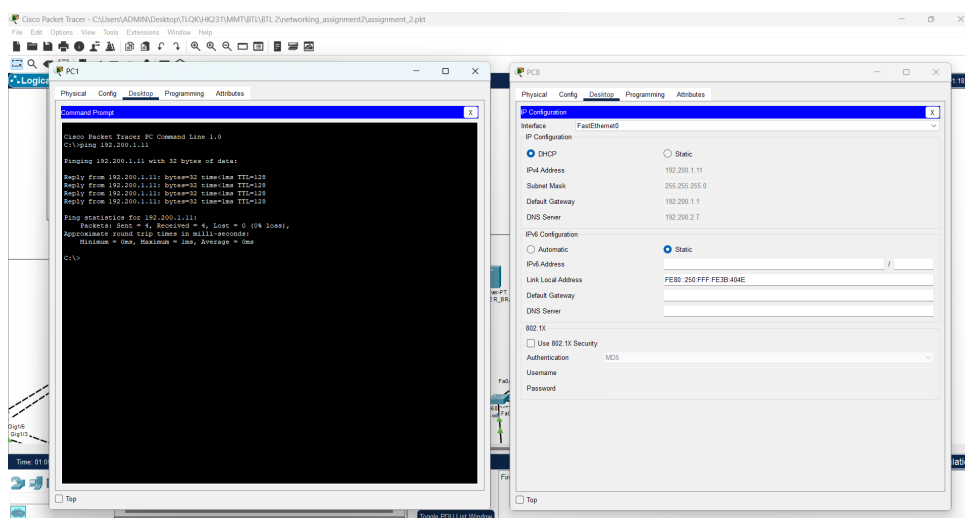
$$30.8148 * 120\% = 36.9778(Mbps)$$

## 6 Kiểm tra hệ thống bằng các công cụ phổ biến như ping, traceroute

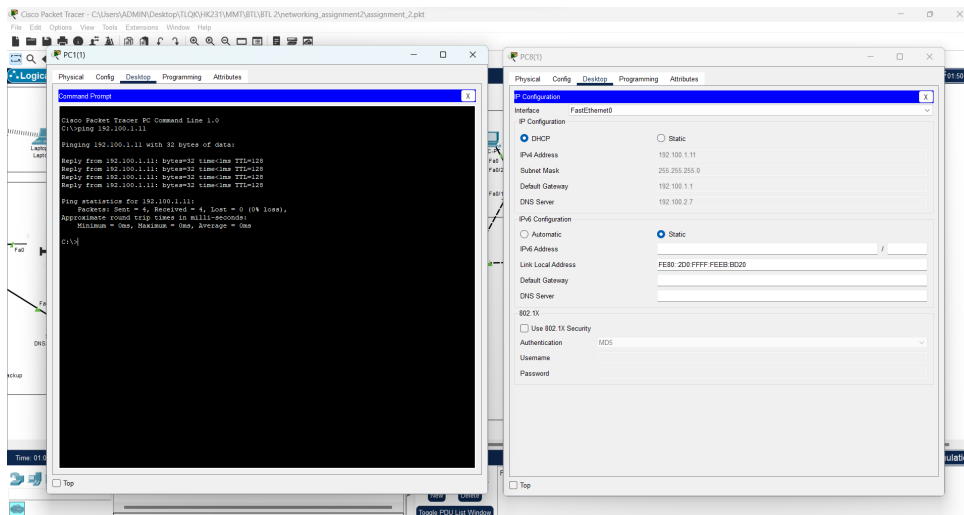
### 6.1 PC cùng VLAN



Hình 24: PC cùng VLAN tại trụ sở chính

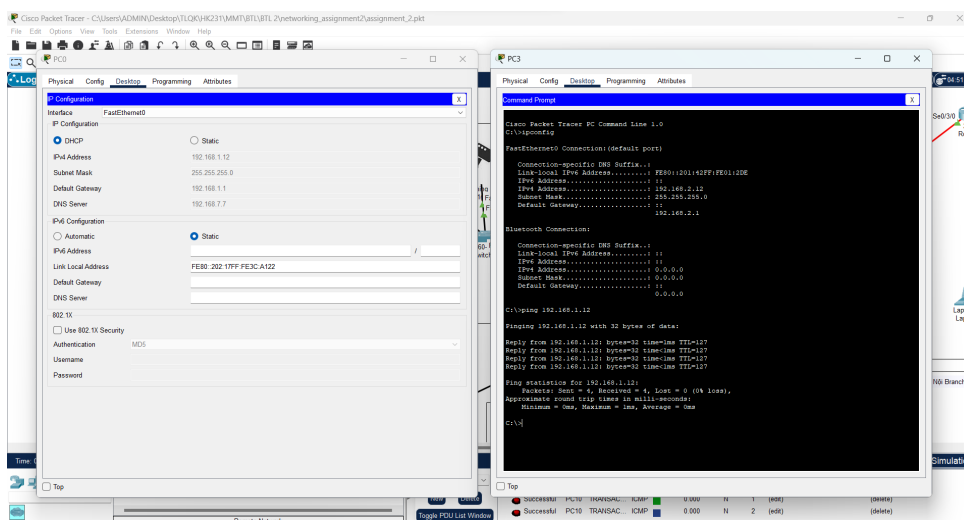


Hình 25: PC cùng VLAN tại chi nhánh Đà Nẵng

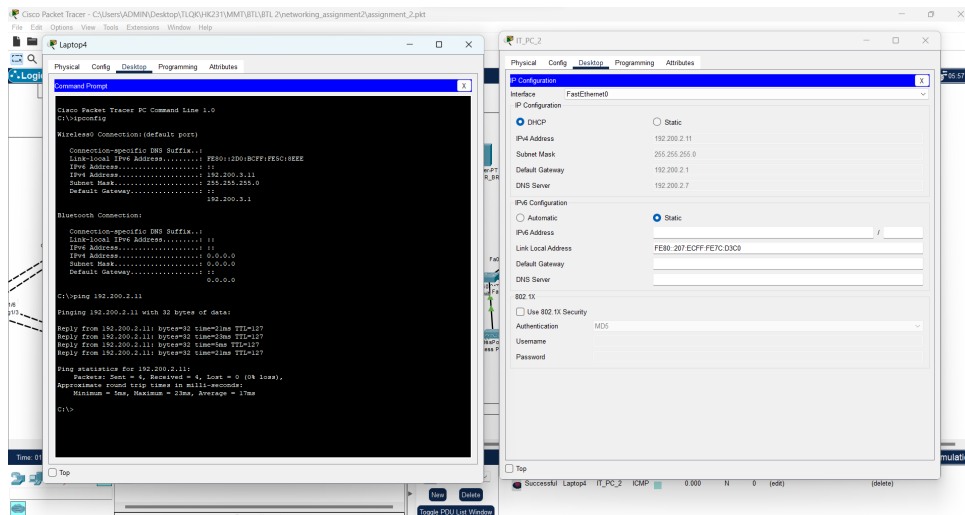


Hình 26: PC cùng VLAN tại chi nhánh Hà Nội

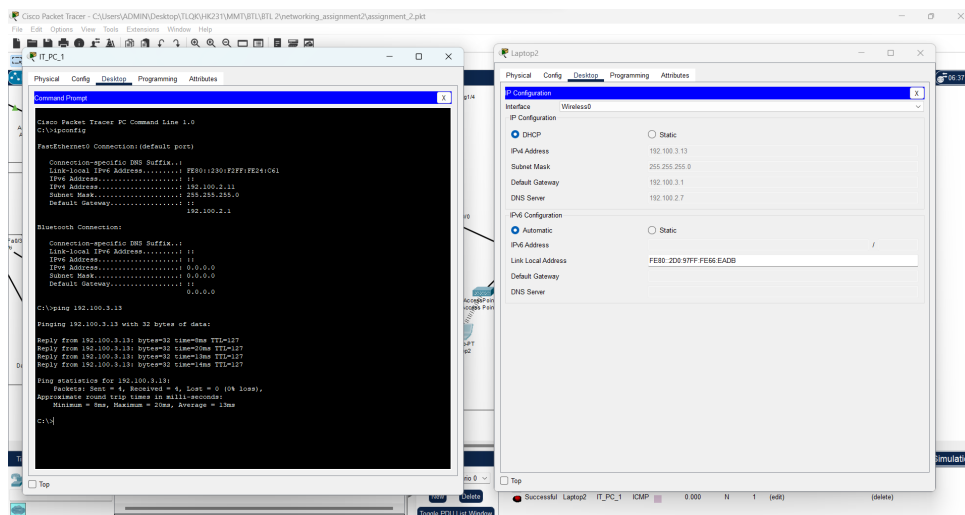
## 6.2 PC khác VLAN tại cùng cơ sở



Hình 27: PC khác VLAN tại trụ sở chính

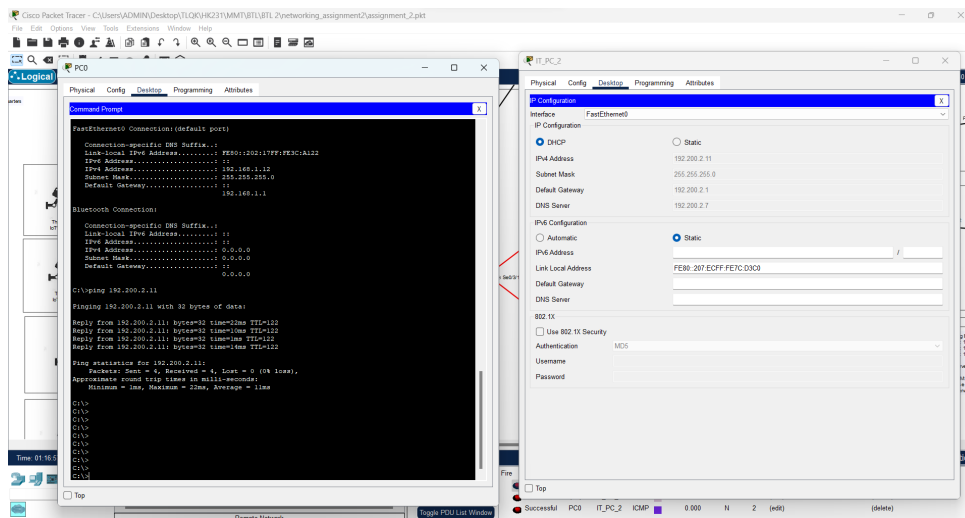


**Hình 28:** *PC cùng VLAN tại chi nhánh Đà Nẵng*



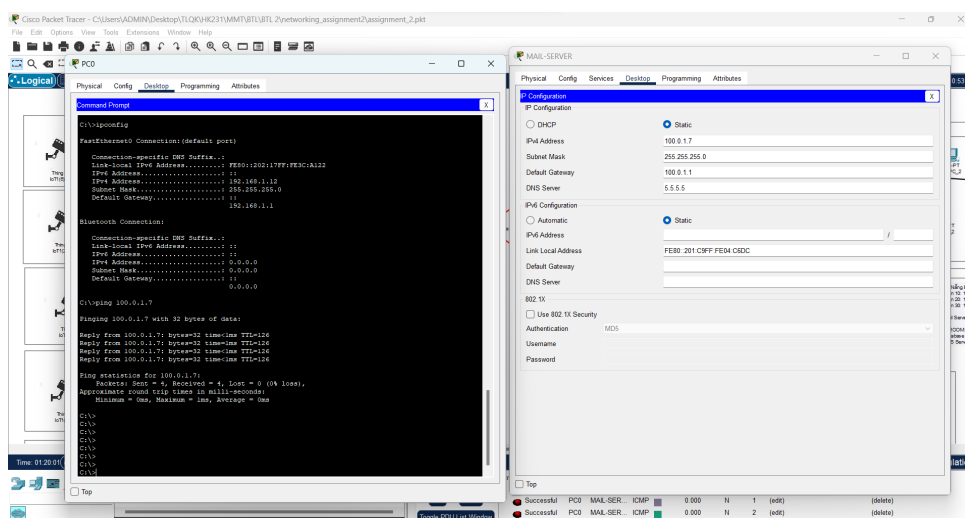
**Hình 29:** PC cùng VLAN tại chi nhánh Hà Nội

### 6.3 PC giữa trụ sở chính và chi nhánh

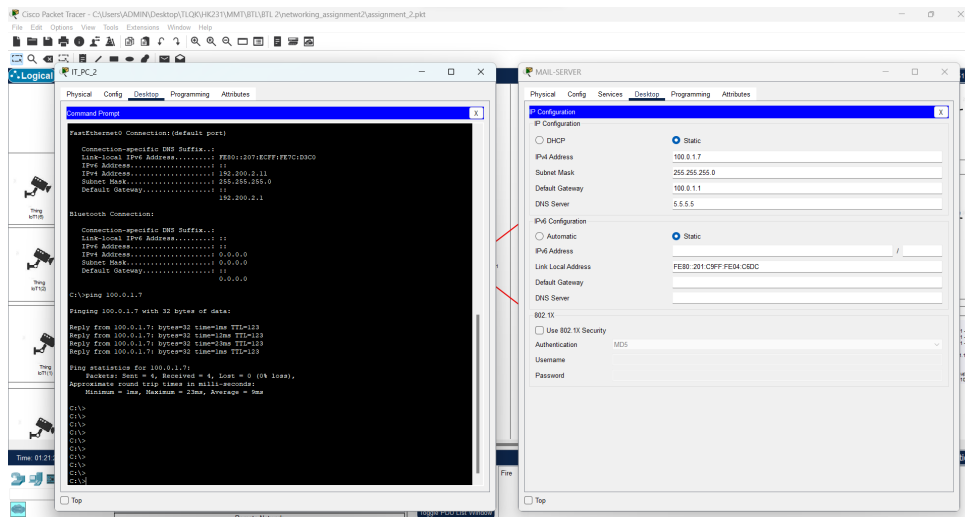


Hình 30: PC giữa trụ sở chính và chi nhánh Đà Nẵng

### 6.4 PC truy cập vào server trong DMZ

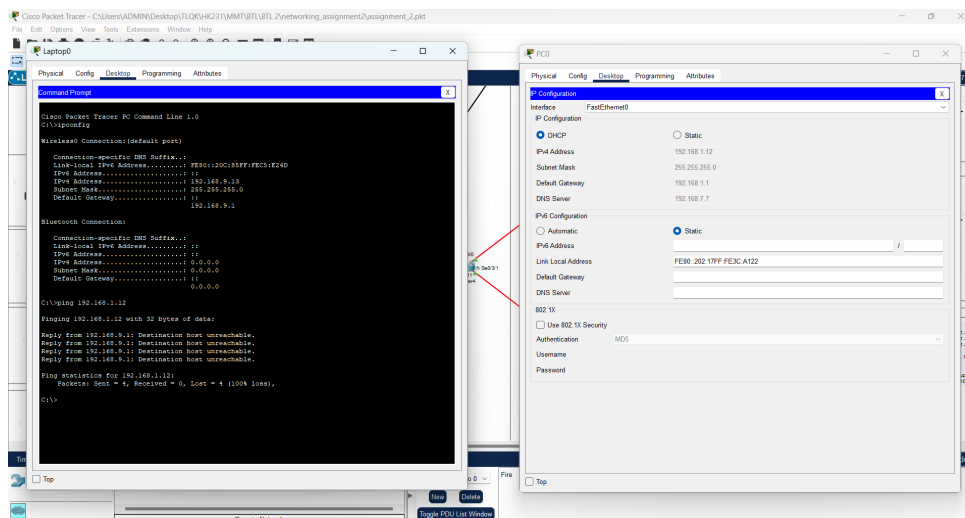


Hình 31: PC tại trụ sở chính vào server trong DMZ



Hình 32: PC tại chi nhánh Đà Nẵng vào server trong DMZ

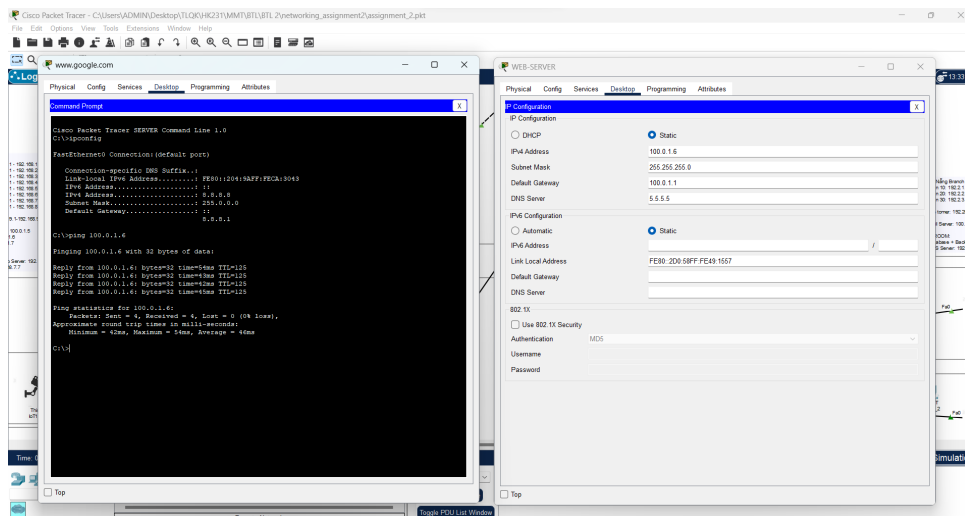
## 6.5 PC khách hàng không thể truy cập vào PC trong LAN



Hình 33: PC khách hàng không thể truy cập vào VLAN tại trụ sở chính



## 6.6 PC từ ngoài mạng internet truy cập tới server



Hình 34: Người dùng từ internet bên ngoài truy cập vào Web Server

## 7 Đánh giá hệ thống

### 7.1 Các kết quả 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 vượt 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.

### 7.2 Những hạn chế còn vướng mắc

- Mặc dù có khả năng mở rộng mạng, nhưng điều này hoàn toàn phụ thuộc vào khả năng hoạt động của bộ phận trung tâm. Một khi trung tâm gặp phải sự cố (switch tổng hoặc router tổng), toàn bộ hệ thống mạng sẽ không thể hoạt động.
- Chưa hoàn thành cấu hình cân bằng tải cho công ty.
- Chưa có kiến thức về một mạng doanh nghiệp cụ thể, khi thiết kế gặp khó khăn về việc quyết định các mô hình, công nghệ, thiết bị nên được sử dụng.

### 7.3 Nâng cấp hệ thống và định hướng cho tương lai

- Phát triển chi nhánh và kết nối
- Phát triển máy trạm ở các phòng ban
- 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.
- 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.
- 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).

## 7.4 Tổng hợp một số công nghệ đã sử dụng cho hệ thống mạng

**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 lý. VLAN có các ưu điểm sau:

- 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. 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. DHCP có một số ưu điểm sau:

- Tự động quản lý 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

## 7.5 Tính an toàn và bảo mật dữ liệu hệ thống

- 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 dùng.
- Đảm bảo an toàn dữ liệu truyền/nhận qua các dịch vụ đường truyền ra Internet.
- Đề xuất được một số cơ chế an toàn 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 công ty 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.



## 8 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, 2004.
- [4] Cisco. (2022). [Configure and Filter IP Access Lists](#)
- [5] Cisco. (2022). [Configure Network Address Translation and ACLs on an ASA Firewall](#).
- [6] Cisco. (2023). [Configure Network Address Translation](#).
- [7] GeeksforGeeks. (2022). [DHCP Server Configuration in Cisco](#).