ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
Khoa Khoa học và kỹ thuật máy tính


# BÀI TẬP LỚN MÔN
# MẠNG MÁY TÍNH
# (CO3093)

**Lớp: TN01 – Học kỳ: 241**

# NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE HOSPITAL

**Giảng viên hướng dẫn:** **TS. NGUYỄN LÊ DUY LAI**

**Sinh viên thực hiện:** Lê Vân Anh Khoa, 2211605
Võ Thanh Tâm, 2213046

Tp. Hồ Chí Minh, tháng 11 năm 2024.

# Mục lục

# Danh sách hình vẽ

# 1 Bảng phân công nhiệm vụ

| Tên thành viên | Nhiệm vụ | Mức độ đóng góp |
|---|---|---|
| Lê Văn Anh Khoa | Thiết kế khu vực chính và SPN | 50% |
| Võ Thanh Tâm | Thiết kế khu vực phụ và Internet | 50% |

# 2 Kiến trúc mạng lưới

## 2.1 Phân tích yêu cầu

- Địa điểm chính gồm 600 máy trạm, 10 máy chủ và 12 thiết bị mạng.
- Kết nối không dây phủ sóng toàn bộ khu vực.
- Sử dụng công nghệ mới cho hạ tầng mạng bao gồm kết nối có dây và không dây, cáp quang (GPON), và Ethernet tốc độ cao (1GbE/10GbE/40GbE).
- Mạng được tổ chức theo cấu trúc VLAN cho từng phòng ban.
- Khu vực chính kết nối với hai khu vực phụ bằng 2 leased lines cho kết nối WAN (sử dụng SD-WAN, MPLS) và 2 DSL cho kết nối Internet với cơ chế load-balancing.
- Bảo mật, dễ dàng nâng cấp hệ thống.
- Ở các khu vực phụ thì mỗi chỗ sẽ có 2 tầng, tầng đầu có phòng IT và 1 cáp kết nối trung tâm, bên cạnh đó là số lượng thiết bị ít hơn: 60 máy trạm, 2 servers và ít nhất 5 thiết bị kết nối mạng.

## 2.2 Danh sách khảo sát tại địa điểm lắp đặt

Bảng 1: Danh sách khảo sát tại địa điểm lắp đặt hệ thống mạng bệnh viện

| Check | Nội dung | Chi tiết thông số |
|---|---|---|
| ☐ | Đánh giá tổng quan | • Đánh giá kiến trúc tổng thể của các tòa nhà A, B và các phòng ban<br>• Cơ sở hạ tầng mạng hiện có, bao gồm Data Center và Cabling Central Local<br>• Dự đoán các vùng khó khăn trong lắp đặt và kết nối: tầng cao, khoảng cách 50m<br>• Phân loại và lựa chọn mô hình khảo sát phù hợp: Dữ liệu, Giọng nói, Định vị |

*Còn tiếp ở trang sau...*

| Check | Nội dung | Chi tiết thông số |
|---|---|---|
| ☐ | Đặc điểm triển khai | • Quy mô kết nối: 600 máy trạm, 10 server, 12+ thiết bị mạng<br>• Hạ tầng mạng có dây và không dây: GPON, 1GbE/10GbE/40GbE<br>• Phân chia VLAN cho từng phòng ban, cơ sở dữ liệu<br>• Khoảng cách kết nối giữa các chi nhánh qua WAN: DBP, BHTQ<br>• Yêu cầu lắp đặt camera giám sát tại các khu vực đặc biệt |
| ☐ | Công cụ khảo sát | • Xây dựng bản đồ khảo sát: sơ đồ tòa nhà A, B và chi nhánh phụ<br>• Công cụ phân tích tầm phủ sóng WiFi, đo đạc khoảng cách và băng thông<br>• Định vị các thiết bị kiểm thử, đo đạc tại hiện trường |
| ☐ | Số lượng thiết bị | • Thống kê số lượng máy trạm, phòng ban, thiết bị kết nối tại mỗi tòa nhà<br>• Xác định số lượng thiết bị truy cập WiFi (khách hàng, nhân viên làm việc từ xa)<br>• Lưu lượng sử dụng: trung bình và giờ cao điểm (80% từ 9h-11h và 15h-16h)<br>• Phân loại lưu lượng tải xuống/tải lên cho các dịch vụ: web, cơ sở dữ liệu |

*Còn tiếp ở trang sau...*

| Check | Nội dung | Chi tiết thông số |
|---|---|---|
| ☐ | Yêu cầu vật lý | • Điện năng tiêu thụ cho máy trạm, thiết bị mạng, server<br>• Đường dẫn điện và mạng: tối ưu cho không gian 50m giữa Data Center và các tòa nhà<br>• Loại dây cáp (GPON, Ethernet), giá đỡ, dây buộc phù hợp<br>• Điều kiện khí hậu môi trường: bảo vệ thiết bị khỏi ẩm ướt, nhiệt độ cao |
| ☐ | Giải pháp mở rộng và bảo mật | • Kế hoạch mở rộng hệ thống: tăng trưởng 20% trong 5 năm<br>• Yêu cầu bảo mật: tường lửa, IPS/IDS, VPN site-to-site, teleworker VPN<br>• Cân nhắc công nghệ WAN: SD-WAN, MPLS, xDSL (cân bằng tải)<br>• Hệ thống giám sát và phát hiện sự cố: độ sẵn sàng cao, phục hồi nhanh |

## 2.3 Hướng giải quyết

### 2.3.1 Khu vực chính

Hệ thống mạng lưới sẽ được chia thành 3 lớp chính:

- Core layer: cung cấp kết nối giữa các lớp phân phối cho mô hình mạng lớn, nằm ngoài cùng của mạng lưới (gồm router, firewal...)
- Distribution layer: gồm các Switch Layer 3, là cầu nối với Core layer và Access layer, nhằm cấp IP cho VLAN qua DHCP server.
- Access layer: gồm các Switch Layer 2, nhiệm vụ kết nối các thiết bị vào từng VLAN

Điều này giúp hệ thống có khả năng chịu lỗi cao, ổn định kết nối và dễ nâng cấp sau này.
Với khu vực chính gồm 2 toà nhà A, B. Mỗi toà gồm 5 tầng, mỗi tầng gồm 10 phòng. Vậy tổng cộng gồm 100 phòng, cùng với khoảng 600 máy trạm thì mỗi phòng sẽ gồm 6 máy trạm.
Như vậy, với việc mỗi tầng gồm 60 máy trạm, sẽ cần sử dụng 3 switch 24 cổng (2960) để có thể thiết lập kết nối với các máy này, các cổng còn dư sẽ được dùng cho việc mở rộng và nâng cấp mạng lưới.
Với số lượng thiết bị nhiều như vậy, cần có các tầng riêng biệt với các thiết bị khác để xử lý việc kết nối giữa các máy với nhau, và với bên ngoài mạng lưới, đồng thời có thể đáp ứng và chịu được lưu lượng dày đặc từ mạng lưới.
Ở Core Layer:

- **2 router trung tâm**, mỗi router phục vụ cho một tòa nhà, 2 Router này sẽ kết nối WAN với 2 Router bên ngoài để có được kết nối mạng diện rộng, với 2 khu vực phụ (DBP và BHTQ). Sở dĩ cần tới 2 router phục vụ cho việc kết nối khu vực chính và các khu vực phụ là để phòng trường hợp 1 Router bị hỏng, sẽ còn 1 cái để thay thế.
  - Router này giúp điều phối và định tuyến lưu lượng lớn giữa các phân đoạn mạng nội bộ, giúp kiểm soát lưu lượng giữa các VLAN và các tòa nhà.
- **2 Firewall**, mỗi Firerwall tương ứng với mỗi router, với mục đích bảo mật và quản lý tất các các kết nối từ trong nội bộ 2 toà của bệnh viện, và từ bên ngoài vào mạng nội bộ này. Là cầu nối giữa các Switch Layer 3 với 2 Router bên trên để kết nối với bên ngoài.
- **2 switch Layer 3 (Catalyst 3650)**, đóng vai trò như thiết bị định tuyến/điều phối các kết nối từ Distribution layer với bên ngoài. Được kết nối với các Router thông qua Firewall.
  - Các switch Layer 3 này sẽ thực hiện định tuyến nội bộ trong mạng LAN với tốc độ cao, với lưu lượng nhận từ các Switch Layer 3 bên dưới ở Distribution Layer.

Distribution Layer:

- **4 switch Layer 3** được chia thành 2 nhóm chính:
  - **2 switch Layer 3 đầu tiên (Catalyst 3560)** kết nối trực tiếp với các switch Layer 3 ở Core Layer, mỗi cái phụ trách một tòa nhà. Các Switch này làm nhiệm vụ điều phối lưu lượng giữa các VLAN từ các Switch Layer 2, giúp các VLAN ở các Switch khác nhau có thể giao tiếp được với nhau, và chuyển tiếp lưu lượng từ Access layer lên các Switch Layer 3 ở Core Layer cho các mục đích khác như kết nối với bên ngoài.
  - **2 switch Layer 3 còn lại (Catalyst 3650)** kết nối với các máy chủ, quản lý lưu lượng giữa máy chủ và các phần còn lại của mạng.
    - Switch 1: Kết nối với các server nội bộ, như DHCP server, Application server, Database server, Backup Server và File server, định tuyến các kết nối giữa các server này với các thiết bị trong 2 toà nhà, như cung cấp IP cho các máy tính qua DHCP thông qua các yêu cầu từ thiết bị, truy cập dữ liệu nội bộ,... Vì vậy, Switch này sẽ chỉ kết nối trực tiếp với 2 Switch Layer 3 ở Core Layer, từ đó kết nối với các thiết bị nội bộ.
    - Switch 2: Kết nối với các server có kết nối ra bên ngoài, như Web Server, DNS Server hay mail Server. Vì vậy Switch này sẽ chỉ cần kết nối với các Router (thông qua kết nối trực tiếp với các Firewall) để cung cấp dịch vụ kết nối với bên ngoài cho các thiết bị trong 2 toà nhà.

Access Layer:
**30 switch Layer 2**, mỗi tòa nhà có 15 switch, phân bổ theo từng tầng và phòng. Mỗi switch Layer 2 sẽ chịu trách nhiệm kết nối các máy trạm (có dây) ở các tầng tương ứng, và mỗi bộ phận sẽ là 1 VLAN, được chia như sau:

- Ở toà A (khu hành chính):
  - Tầng 1:
    - Bộ phận lễ tân (phòng 1 tới 4): VLAN 10
    - Bộ phận hành chính, kế toán (phòng 5-7) : VLAN 20
    - Bộ phận an ninh và bảo trì (phòng 8-10): VLAN 30

  - Tầng 2:
    * Bộ phận quản lý (phòng 1-5): VLAN 40
    * Bộ phận kỹ thuật (phòng 6-10): VLAN 50
  - Tầng 3:
    * Các phòng hội thảo và tập huấn (phòng 1-5): VLAN 60
    * Bộ phận quản lý và lưu trữ hồ sơ (phòng 6-10): VLAN 70
  - Tầng 4:
    * Khu vực điều trị ngoại trú (phòng 1-5): VLAN 80
    * Khu trữ thuốc (phòng 6-10): VLAN 90
  - Tầng 5:
    * Bộ phận phân tích dữ liệu (phòng 1-5): VLAN 100
    * Bộ phận hành chính cao cấp/ban điều hành (phòng 6-10): VLAN 110

- Ở toà B (khu khám chữa bệnh):
  - Tầng 1:
    * Khoa Cấp cứu (phòng 1-5): VLAN 120
    * Khoa Chẩn đoán hình ảnh (phòng 6-10): VLAN 130
  - Tầng 2:
    * Khu vực Điều trị nội trú (phòng 1-5): VLAN 140
    * Khoa vật lý trị liệu (phòng 6-10): VLAN 150
  - Tầng 3:
    * Khoa Phẫu thuật (phòng 1-5): VLAN 160
    * Khu vực Hồi sức (phòng 6-10): VLAN 170
  - Tầng 4:
    * Khoa Điều trị đặc biệt (phòng 1-5): VLAN 180
    * Các phòng nghiên cứu (phòng 6-10): VLAN 190
    * Khoa Hồi sức tích cực và Chống độc (phòng 1-5): VLAN 200
    * Khoa Sản Nhi (phòng 6-10): VLAN 210

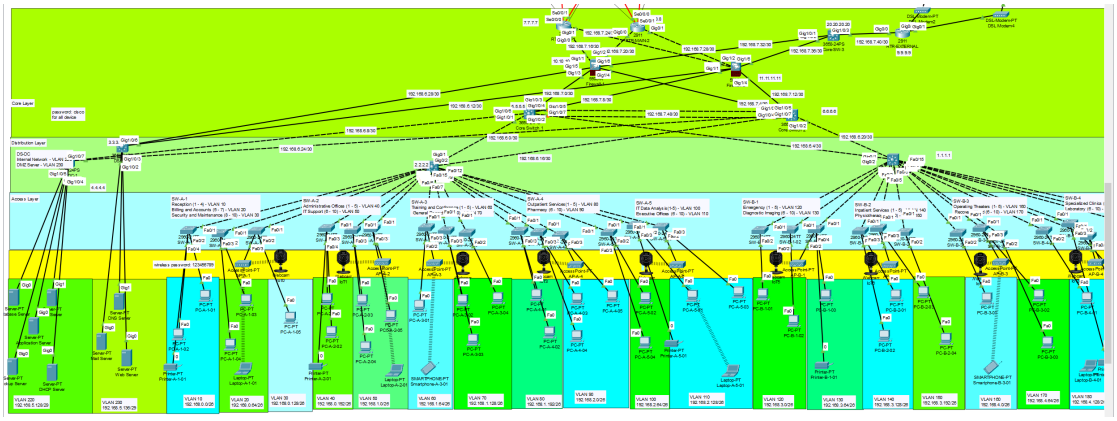
Các switch này kết nối với switch Layer 3 ở Distribution Layer tương ứng với từng tòa nhà. Switch Layer 3 này sẽ đóng vai trò là trung tâm định tuyến, để các VLAN khác nhau từ các Switch Layer 2 khác nhau có thể giao tiếp với nhau, và kết nối với mạng bên ngoài bệnh viện.
**Access Points**:

- Mỗi tầng có một access point, tổng cộng 10 access point cho 2 tòa nhà.
- Mỗi access point kết nối với một switch bất kỳ trong tầng để cung cấp kết nối WiFi.
- Access point giúp tăng cường vùng phủ sóng và đảm bảo kết nối không dây cho các thiết bị di động hoặc laptop.

Với hệ thống bệnh viện, sẽ có các Servers sau:

- Web server: Người dùng/bệnh nhân có thể truy cập để có các thông tin mới nhất từ bệnh viện.

- Database server: Lưu trữ dữ liệu của bệnh viện như hồ sơ bệnh án, dữ liệu nhân viên,...
- Mail server: Để các phòng ban có thể gửi mail nội bộ
- DHCP server: nhằm cung cấp tự động IP cho các thiết bị kết nối mạng
- DNS server: Dịch tên miền thành địa chỉ IP
- File server: Để chia sẻ các tập tin trong nội bộ
- Backup server: Sao lưu hệ thống
- Application server

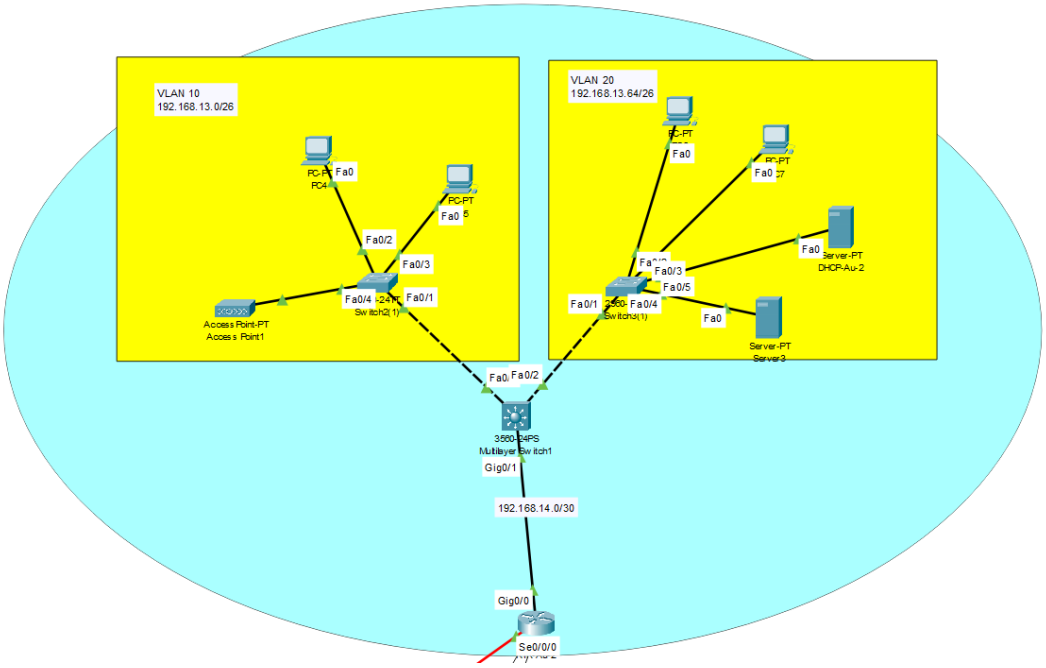


Hình 1: Sơ đồ mạng lưới khu vực chính

### 2.3.2 Các khu vực phụ

Với số lượng thiết bị ít hơn nhiều so với khu vực chính (chỉ gồm 60 máy trạm, 2 servers và 5 thiết bị mạng), sẽ chỉ cần sử dụng thiết kế đơn giản:

- Gồm 2 VLAN, tương ứng với 2 tầng: Tầng 1 là phòng IT, tầng 2 là phòng kết nối với mạng trung tâm.
  - Tầng 1: gồm các máy trạm, 1 switch để phân vùng VLAN và 1 Access Point phục vụ việc truy cập Wifi.
  - Tầng 2: Gồm các máy trạm khắc, 1 switch để phân vùng VLAN, và 2 server, trong đó có 1 DHCP server để tự động cấp IP cho các thiết bị của khu vực.
- Ngoài ra, còn có 1 switch Layer 3 kết nối với 2 switch ở 2 phòng, và 1 router, với vai trò cầu nối giao tiếp giữa các thiết bị trong khu vực với bên ngoài. Đồng thời là nơi mà các máy trạm ở tầng 1 gửi yêu cầu sang DHCP server ở tầng 2 để được cung cấp IP.
- Ở ngoài cùng sẽ là 1 router, kết nối với router SPN để có thể tiếp nhận và truyền đi các kết nối từ trong ra ngoài, với các khu vực khác. Lưu ý để có thể kết nối Internet, yêu cầu kết nối sẽ phải đi từ khu vực phụ sang SPN, từ đó sang khu vực chính rồi mới có thể kết nối Internet, điều này đảm bảo sự bảo mật, tất cả yêu cầu được gửi đi từ bất kì khu vực nào của bệnh viện đều phải đi qua các firewall ở khu vực chính.




Hình 2: Kiến trúc mạng khu vực phụ

## 2.4 Khu vực SPN

Đây là khu vực nhận trách nhiệm kết nối các khu vực của bệnh viện với nhau, gồm có 3 router để chịu được lưu lượng kết nối giữa các khu vực.

## 2.5 Các khu vực chịu tải cao

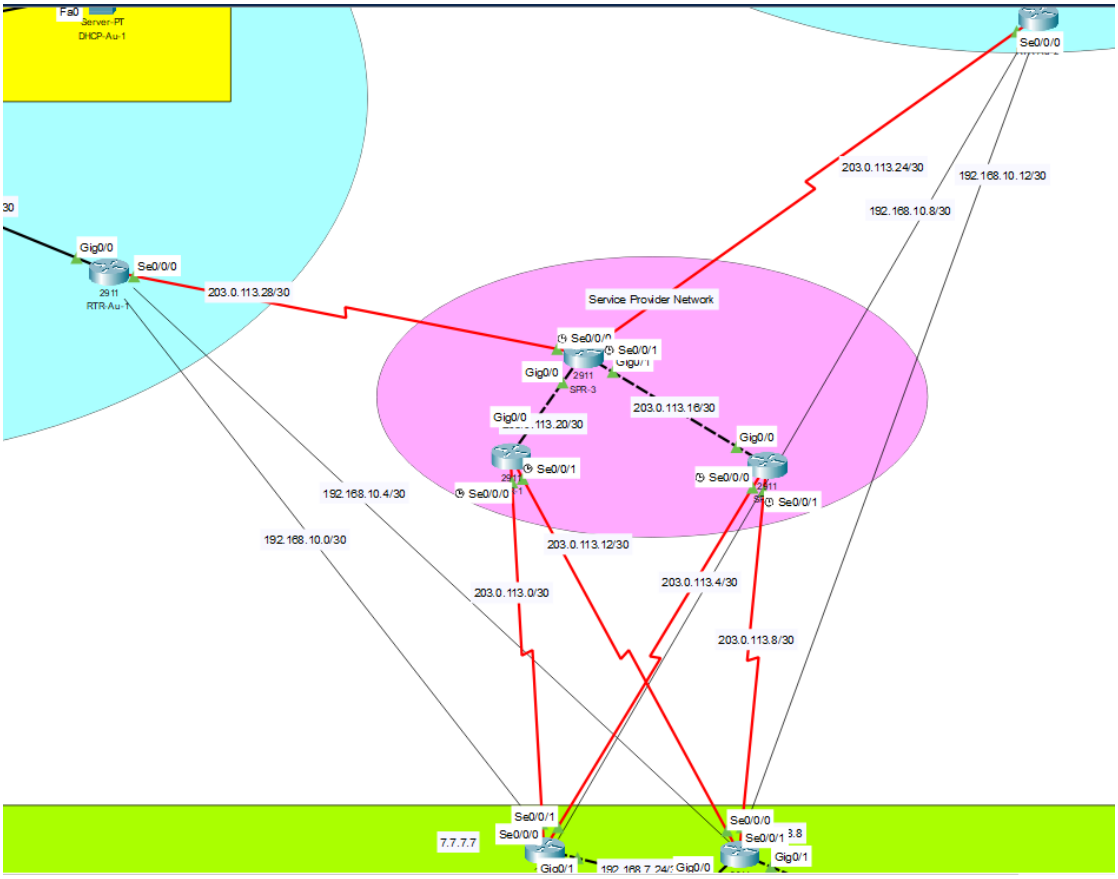
#### 2.5.0.1 Các router kết nối với SPN (Service Provider Network) và thế giới bên ngoài (dịch vụ Internet)

Bởi vì:

- Router kết nối với SPN xử lý toàn bộ lưu lượng giữa mạng nội bộ của bệnh viện (bao gồm các khu vực chính, phụ) và bên ngoài.
- Chúng xử lý các yêu cầu web bên ngoài, kết nối VPN, và trao đổi dữ liệu với các dịch vụ bên thứ ba.
- Kết nối WAN (các đường thuê bao) thường có băng thông giới hạn, khiến router này trở thành nút thắt cổ chai quan trọng trong quản lý lưu lượng.

Chiến lược giảm tải:

- Sử dụng nhiều router (ở đây là 3) để giảm tải hoạt động, lưu lượng phải nhận bởi mỗi router.


Fa0
Server-PT
DHCP-Au-1
Se0/0/0
203.0.113.24/30
192.168.10.12/30
192.168.10.8/30
Gig0/0
Se0/0/0
2911
RTR-Au-1
203.0.113.28/30
Service Provider Network
Se0/0/0
Se0/0/1
Gig0/0
2911
SPR-3
203.0.113.16/30
Gig0/0
Gig0/0
Se0/0/1
Se0/0/0
Se0/0/0
Se0/0/1
192.168.10.4/30
192.168.10.0/30
203.0.113.12/30
203.0.113.4/30
203.0.113.0/30
203.0.113.8/30
Se0/0/1
Se0/0/0
7.7.7.7
Gig0/1
Se0/0/0
Se0/0/1
Gig0/1

Hình 3: SPN

#### 2.5.0.2 Tường lửa (Firewall)

- Tường lửa kiểm tra và lọc lưu lượng, áp dụng các chính sách bảo mật cho cả dữ liệu đi vào và đi ra.
- Xử lý lượng lớn lưu lượng từ các máy trạm (lưu lượng nội bộ) và yêu cầu từ bên ngoài.
- Firewall khi thực hiện các nhiệm vụ kiểm tra gói tin đi vào/đi ra, phát hiện/ngăn chặn xâm nhập (IDS/IPS), hay ghi logs cũng tốn tài nguyên đáng kể.

Chiến lược giảm tải: sử dụng 2 Firewall để giảm lưu lượng chia sẻ cho mỗi máy.

#### 2.5.0.3 Máy chủ DHCP

- Máy chủ DHCP phân bổ địa chỉ IP cho hàng trăm máy trạm và thiết bị tại khu chính và các phân khu.
- Lượng thiết bị kết nối thay đổi liên tục và số lượng nhiều như khách khám bệnh, mỗi người đều có thiết bị di động để kết nối wifi, hay khi có các thiết bị mới được nhập vào cũng sẽ kết nối vào mạng nội bộ của bệnh viện, những điều này làm tăng lưu lượng yêu cầu cấp phát IP tự động từ những thiết bị này tới DHCP server.

#### 2.5.0.4 Máy chủ Web và DNS

Bệnh viện có nhiều ứng dụng web, như cổng thông tin, các tính năng đặt lịch online cho bệnh nhân,... sẽ được sử dụng nhiều, điều này tạo ra lượng lưu lượng đáng kể đến máy chủ web. Bên cạnh đó, máy chủ DNS đảm nhiệm việc xử lý việc phân giải tên miền cho tất cả lưu lượng web nội bộ và bên ngoài. Với mô tả bên trên về việc web được truy cập nhiều, đồng nghĩa lưu lượng và các request tới DNS server cũng là tương đương với Web server.
Chiến lược giảm tải: Sử dụng cân bằng tải và chia ra nhiều server Web và DNS để tránh một máy chủ phải chịu quá nhiều tải.

#### 2.5.0.5 Switch Layer 3 ở Tầng Core

- Switch Layer 3 ở tầng Core quản lý định tuyến liên VLAN cho hàng trăm máy trạm, đồng thời cũng là kênh vận đưa thông tin IP tới các máy trạm từ DHCP server.
- Các switch này cũng tập hợp lưu lượng từ tầng phân phối để chuyển tiếp ra bên ngoài (tới các site phụ hoặc internet), cũng như nhận các yêu cầu từ bên ngoài và đưa vào bên trong.

Chiến lược giảm tải: Sử dụng load balancing khi kết nối giữa 2 Switch này, ở đây dùng thêm 2 cáp kết nối chúng với nhau

#### 2.5.0.6 Liên kết WAN và Router SPN

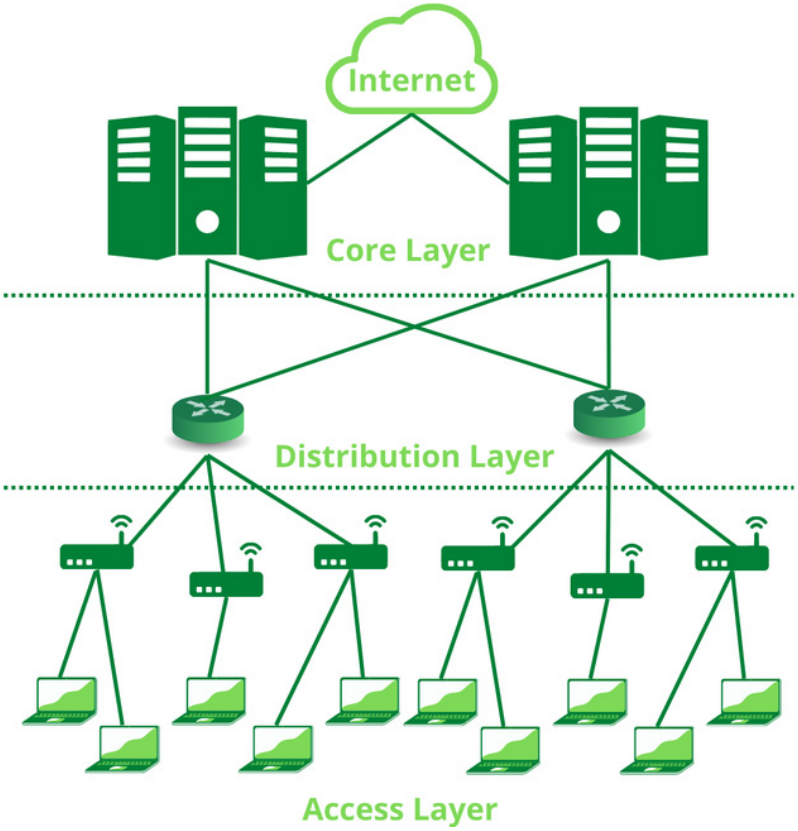
- Các đường thuê bao kết nối khu chính và các phân khu thông qua SPN có thể trở thành nút thắt cổ chai nếu băng thông không đủ.
- Router SPN giao tiếp với các đường này cũng xử lý lưu lượng cho tất cả các khu vực, có thể làm quá tải năng lực xử lý.

Chiến lược giảm tải:

- Tăng băng thông cho các đường thuê bao.
- Triển khai quản lý lưu lượng và ưu tiên trên các liên kết WAN.

## 2.6 Cấu trúc lựa chọn

Mạng của bệnh viện được thiết kế theo **3-tier LAN Architecture**, bao gồm ba tầng: *Access Layer*, *Distribution Layer*, và *Core Layer*. Đây là một mô hình phổ biến trong các hệ thống mạng lớn, mang lại nhiều lợi ích về quản lý, hiệu năng và khả năng mở rộng.




Hình 4: Mô hình kiến trúc 3-tier

**Lý do lựa chọn**

- **Quản lý phân cấp:** Việc phân chia thành 3 tầng cho phép quản lý lưu lượng một cách tập trung tại tầng Core, xử lý tổng hợp tại tầng Distribution và triển khai thiết bị người dùng tại tầng Access. Điều này giúp đơn giản hóa việc quản trị và khắc phục sự cố.
- **Khả năng mở rộng:** 3-tier LAN Architecture hỗ trợ việc mở rộng mạng dễ dàng, từ việc thêm các máy trạm ở tầng Access đến nâng cấp các thiết bị tại tầng Distribution hoặc Core.

- **Hiệu suất cao:** Mỗi tầng trong kiến trúc được thiết kế để xử lý một loại lưu lượng cụ thể, giúp tối ưu hóa tài nguyên và đảm bảo hiệu năng cao cho toàn bộ hệ thống.
- **An toàn và linh hoạt:** Dễ dàng triển khai các công nghệ bảo mật (Firewall, IDS/IPS) và định tuyến lưu lượng qua các tầng để đảm bảo an toàn và hiệu quả.

**Ưu điểm**

- **Phân tách vai trò rõ ràng:** Mỗi tầng thực hiện một nhiệm vụ cụ thể:
  - *Access Layer:* Kết nối các thiết bị đầu cuối như máy trạm, điện thoại IP, thiết bị IoT.
  - *Distribution Layer:* Xử lý tổng hợp lưu lượng từ Access Layer, thực hiện định tuyến liên VLAN và áp dụng chính sách bảo mật.
  - *Core Layer:* Chuyển tiếp lưu lượng với tốc độ cao và đảm bảo tính sẵn sàng cao.
- **Khả năng sẵn sàng cao:** Sử dụng các giao thức dự phòng (như HSRP, VRRP) và liên kết dự phòng giữa các tầng giúp giảm nguy cơ gián đoạn dịch vụ khi có lỗi xảy ra.
- **Khả năng mở rộng linh hoạt:** Mô hình này dễ dàng mở rộng theo cả chiều ngang (thêm thiết bị ở Access Layer) và chiều dọc (nâng cấp thiết bị ở Core Layer).
- **Hỗ trợ hiệu năng cao:** Tầng Core được thiết kế để xử lý lưu lượng với tốc độ cao, đảm bảo mạng hoạt động mượt mà ngay cả trong giờ cao điểm.
- **Triển khai bảo mật dễ dàng:** Tầng Distribution và Core cung cấp các điểm kiểm soát tập trung (Firewall,...) để triển khai chính sách bảo mật.

**Nhược điểm**

- **Chi phí cao:** Cần đầu tư vào các thiết bị hiệu suất cao, đặc biệt ở tầng Core và Distribution.
- **Phức tạp trong cấu hình thiết bị:** Cấu hình VLAN, định tuyến liên VLAN, và các giao thức định tuyến yêu cầu kiến thức chuyên môn cao từ đội ngũ quản trị mạng.
- **Tầng Core là nút thắt :** Lưu lượng từ toàn bộ hệ thống đều đi qua tầng Core. Nếu xảy ra sự cố tại đây, mạng có thể bị ảnh hưởng nghiêm trọng, nhưng đã được hạn chế bớt nguy cơ bằng cách sử dụng các thiết bị dự phòng như 2 Router, 2 Firewall và 2 Switch Layer 3.
- **Khó khăn nếu tầng core ban đầu không đáp ứng đủ nhu cầu của bệnh viện:** Khi lưu lượng vượt quá khả năng xử lý của thiết bị ở tầng Core, việc nâng cấp có thể phức tạp và tốn kém.

## 2.7 Thiết kế mạng không dây

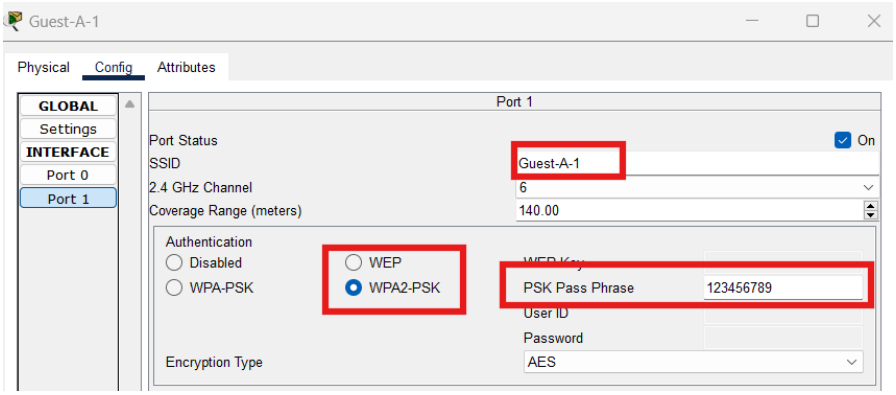
### 2.7.1 Thiết kế mạng không dây

- **Triển khai Access Point (AP) băng tần kép:**
  - Sử dụng các AP hỗ trợ đồng thời băng tần 2.4 GHz và 5 GHz để tăng khả năng phủ sóng và cải thiện hiệu suất của các thiết bị hiện đại.
- **Mạng lưới Mesh (Mesh Networking):**

– Sử dụng công nghệ mesh để mở rộng vùng phủ sóng trong trường hợp không thể kéo thêm dây cáp. Điều này giúp giảm chi phí và đảm bảo sự liên tục của kết nối.

- **Áp dụng QoS (Quality of Service):**
  – Cấu hình QoS để ưu tiên các loại lưu lượng quan trọng như VoIP và hội nghị truyền hình nhằm đảm bảo hiệu suất cao trong các tình huống tải lớn.

### 2.7.2 Tiêu chuẩn bảo mật




Hình 5: Mã hóa WPA2-PSK

- **Mã hóa WPA2-PSK:**
  – Cấu hình mạng Wi-Fi với chuẩn bảo mật WPA2-PSK để bảo vệ dữ liệu khỏi các cuộc tấn công tiềm tàng.
- **Phân đoạn VLAN:**
  – Sử dụng VLAN để tách biệt lưu lượng mạng khách và mạng nội bộ, đảm bảo rằng khách không thể truy cập vào các tài nguyên quan trọng.
- **Lọc địa chỉ MAC và ẩn SSID:**
  – Kích hoạt lọc địa chỉ MAC để giới hạn các thiết bị được phép kết nối vào mạng.
  – Tắt tính năng phát SSID đối với các mạng quan trọng để giảm nguy cơ tấn công từ bên ngoài.

## 2.8 Phân vùng các server và thiết bị mạng

### 2.8.1 Server Farm

- **Tập trung hóa máy chủ:**
  – Các máy chủ được đặt tại khu vực trung tâm với cấu hình dự phòng (failover clustering) để đảm bảo khả năng sẵn sàng cao.
- **Phân VLAN cho các loại máy chủ:**

- VLAN dành riêng cho máy chủ cơ sở dữ liệu.
- VLAN dành riêng cho máy chủ ứng dụng.
- VLAN dành riêng cho máy chủ lưu trữ.

### 2.8.2 DMZ Server

- **Đặt máy chủ công khai:**
  - Các máy chủ như web server, email server, và VPN server được đặt trong DMZ để tách biệt khỏi mạng nội bộ.
- **Áp dụng quy tắc tường lửa nghiêm ngặt:**
  - Chỉ cho phép lưu lượng cần thiết được phép đi qua giữa DMZ và mạng nội bộ.

### 2.8.3 Firewalls

Đặt tường lửa tại biên giới giữa Internet và mạng nội bộ để kiểm soát lưu lượng ra/vào.

# 3 Danh sách thiết bị và sơ đồ kết nối

## 3.1 Các thiết bị và cấu hình

### 3.1.1 Access Point

Sử dụng Access Point để làm điểm phát và kết nối mạng không dây cho mỗi tầng, dành cho các thiết bị cần kết nối Wifi. Trong hệ thống mạng này, sẽ sử dụng Cisco Access Point-PT.

Hình 6: Access Point

- **Data Link Protocol** IEEE 802.11n (draft), IEEE 802.11b, IEEE 802.11a, IEEE 802.11g.
- **Wireless Security** WEP, Wi-Fi Protected AccessTM 2 (WPA2), Wireless MAC Filtering.
- **Interfaces** 1 x Network - Ethernet 10Base-T/100Base-TX/1000Base-T-RJ-45.
- **Bandwidth** 2.4GHz - 5GHz

### 3.1.2 Switch Cisco 2960

Với thiết kế kiến trúc hạ tầng mạng đã nêu, sẽ sử dụng Cisco Switch 2960 vì có thông số phù hợp:

Hình 7: Switch Cisco 2960

- Loại: LAN Lite
- Giao diện Uplink: 2 (SFP or 1000BASE-T)
- Ports: 24 x 10/100Mbps Ethernet
- Chuyển tiếp băng thông: 16 Gbps
- DRAM: 128 MB
- Flash Memory: 64 MB

### 3.1.3 Switch Layer 3

Các mẫu Switch Layer 3 sẽ được sử dụng trong hạ tầng mạng là Catalyst 3560 và Catalyst 3650, đều gồm 24 cổng kết nối. Điểm khác biệt giữa hai loại này là:

- **Catalyst 3560:** Là dòng cũ hơn, hỗ trợ các tác vụ định tuyến cơ bản và các tính năng Layer 2 như switch bình thường gồm cấu hình VLAN, trunking. Được kết nối với các Switch Layer 2 ở tầng Access Layer đóng vai trò như trung tâm định tuyến giữa các VLAN khác nhau nằm trên các Switch layer 2 khác nhau,
- **Catalyst 3650:** Là dòng mới hơn, hỗ trọ các tác vụ định tuyến nâng cao, bao gồm cả định tuyến động (dynamic router) với OSPF và EIGRP. Hỗ trợ nhiều module linh hoạt và cho phép triển khai nhiều kịch bản mạng phức tạp hơn, được dùng để kết nối giữa vùng DMZ (server) tới các router, và giữa Catalyst 3560 ở tầng Distribtuion Layer với Router và Firewall ở tầng Core Layer.

Hình 8: Switch Layer 3

- 24-port 10/100/1000BASE-T RJ45 copper
- 4 100/1000BASE-X mini-GBIC/SFP slots, shared with Port-21 to Port-24
- 4 khe cắm 10GBASE-SR/LR SFP+, tương thích với 1000BASE-SX/LX/BX SFP
- Giao diện console RJ45 sang RS232 để quản lý và cài đặt cơ bản cho switch
- 1 cổng quản lý Ethernet RJ45 để quản lý và cài đặt cơ bản cho switch
- 1 cổng USB 2.0 để sao lưu/tải lên cấu hình và nâng cấp firmware

### 3.1.4 Router 2911


Hình 9: Router 2911

- **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)

### 3.1.5 Firewall 5506-X

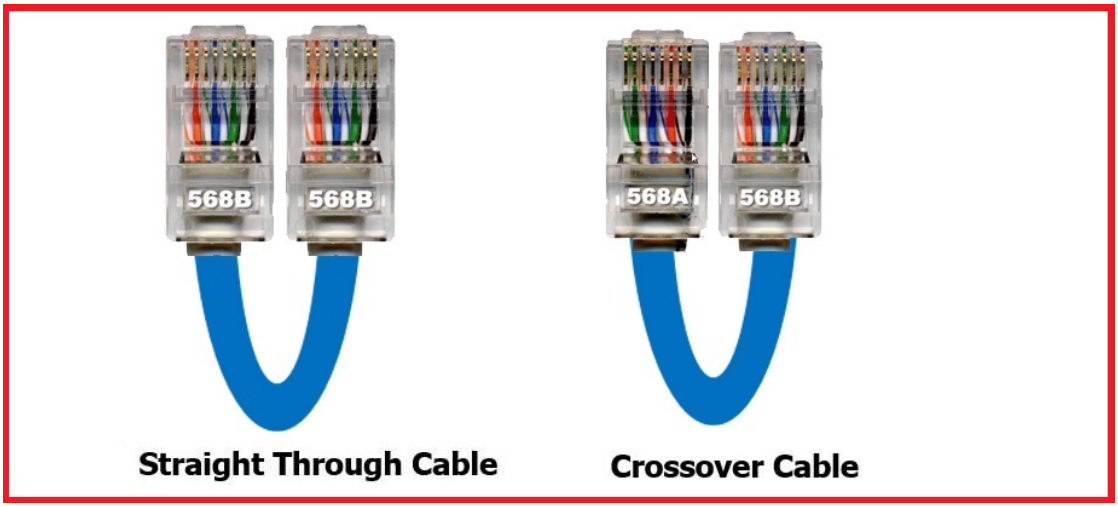

Hình 10: Firewall ASA 5506-X

| | |
|---|---|
| Giao diện | 8 x 1 Gigabit Ethernet interface, 1 management port |
| Thông lượng Firewall | 300 Mbps |
| Thông lượng 3DES/AES VPN tối đa | 100 Mbps |
| IPsec site-to-site VPN peers | 10; 50 with Security Plus license |
| Số VLAN | 5; 30 with Security Plus license |
| Bộ nhớ | 4GB |

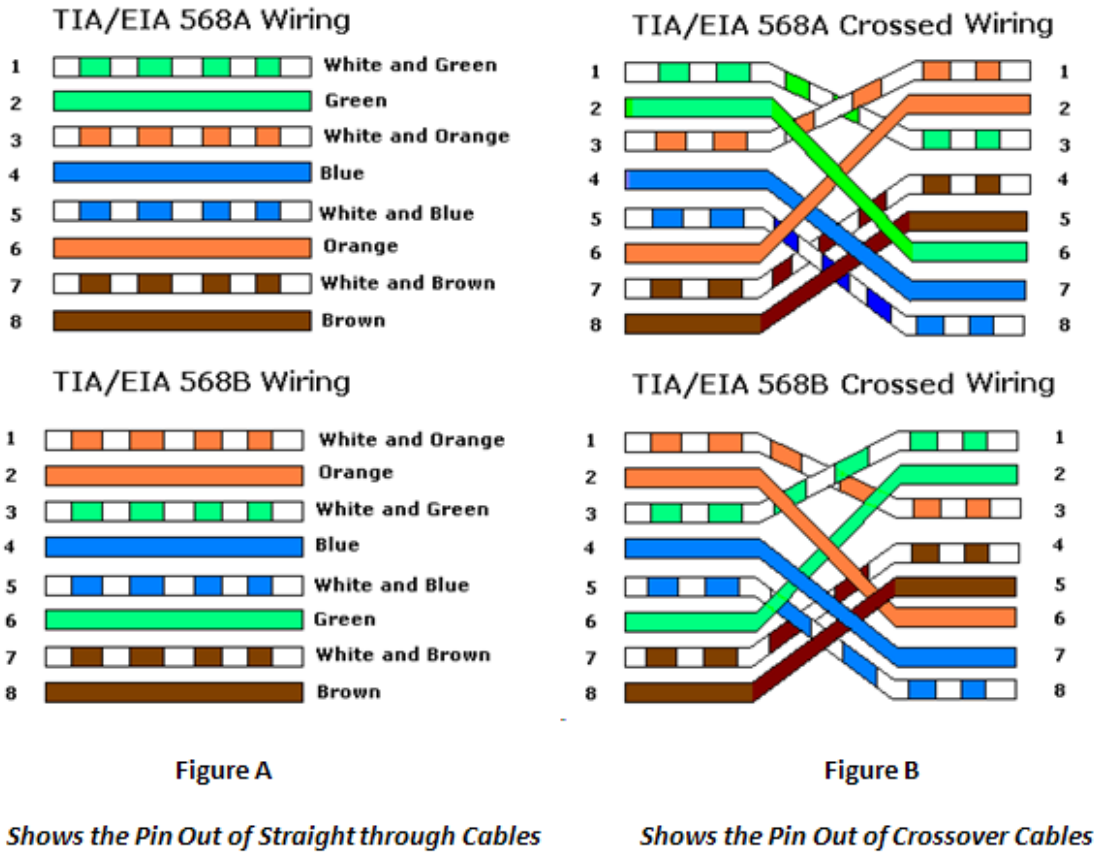
Bảng 2: Thông số cấu hình

### 3.1.6 Các loại dây kết nối sử dụng

- Cáp thẳng: Là cáp Ethernet với 2 đầu kết nối giống nhau, dùng để kết nối các thiết bị khác loại nhau (PC với Switch, Switch với Router,...), dùng cho các kết nối dưới 100m.
- Cáp chéo: Là cáp Ethernet với 2 đầu kết nối khác nhau, dùng để kết nối các thiết bị cùng loại (PC với PC, Switch với Switch,...), dùng cho các kết nối dưới 100m.




Hình 11: So sánh 2 loại cáp




Hình 12: So sánh 2 loại cáp

- Cáp Serial DTE: Dùng để kết nối 2 Router trong mạng WAN, qua cổng serial, dùng cho kết nối có khoảng cách 15-20m.

Hình 13: Cáp Serial DTE

## 3.2 Sơ đồ IP

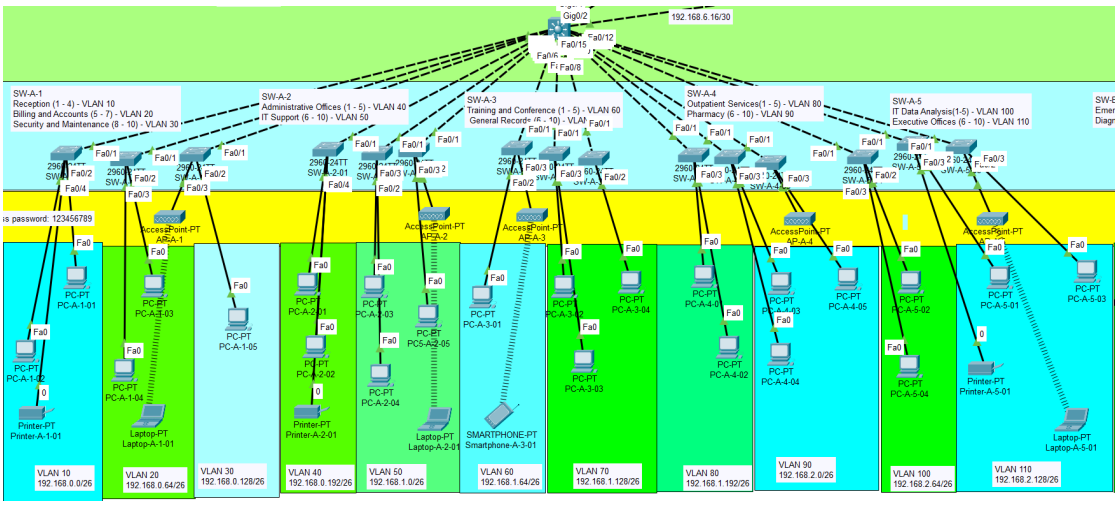
### 3.2.1 Khu vực chính

Sơ đồ VLAN các toà:

- Toà A (Khu hành chính):

| VLAN | Tên khu vực | Phòng | Tầng | Subnet | Usable IP Range |
|---|---|---|---|---|---|
| VLAN 10 | Lễ tân | 1-4 | 1 | 192.168.0.0/26 | 192.168.0.1 - 192.168.0.62 |
| VLAN 20 | Hành chính & kế toán | 5-7 | 1 | 192.168.0.64/26 | 192.168.0.65 - 192.168.0.126 |
| VLAN 30 | An ninh và bảo trì | 8-10 | 1 | 192.168.0.128/26 | 192.168.0.129 - 192.168.0.190 |
| VLAN 40 | Quản lý | 1-5 | 2 | 192.168.0.192/26 | 192.168.0.193 - 192.168.0.254 |
| VLAN 50 | Kỹ thuật | 6-10 | 2 | 192.168.1.0/26 | 192.168.1.1 - 192.168.1.62 |
| VLAN 60 | Hội thảo và tập huấn | 1-5 | 3 | 192.168.1.64/26 | 192.168.1.65 - 192.168.1.126 |
| VLAN 70 | Quản lý và lưu trữ hồ sơ | 6-10 | 3 | 192.168.1.128/64 | 192.168.1.129 - 192.168.1.190 |
| VLAN 80 | Điều trị ngoại trú | 1-5 | 4 | 192.168.1.192/26 | 192.168.1.193 - 192.168.1.254 |
| VLAN 90 | Kho thuốc | 6-10 | 4 | 192.168.2.0/26 | 192.168.2.1 - 192.168.2.62 |
| VLAN 100 | Phân tích dữ liệu | 1-5 | 5 | 192.168.2.64/26 | 192.168.2.65 - 192.168.2.126 |
| VLAN 110 | Hành chính cao cấp/Ban điều hành | 6-10 | 5 | 192.168.2.128/26 | 192.168.2.129 - 192.168.2.190 |

Bảng 3: Sơ đồ VLAN toà A

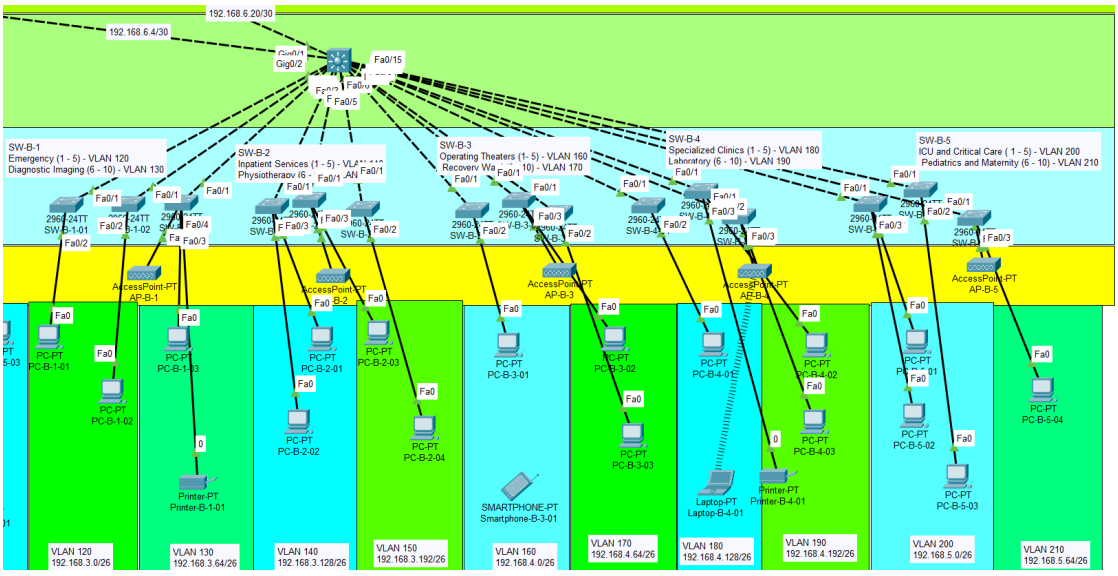



Hình 14: Thiết kế hệ thống mạng toà A

- Toà B (Khu khám chữa bệnh):

| VLAN | Tên khu vực | Phòng | Tầng | Subnet | Usable IP Range |
|---|---|---|---|---|---|
| VLAN 120 | Khoa Cấp cứu | 1-5 | 1 | 192.168.3.0/26 | 192.168.3.1 - 192.168.3.62 |
| VLAN 130 | Khoa Chẩn đoán hình ảnh | 6-10 | 1 | 192.168.3.64/26 | 192.168.3.65 - 192.168.3.126 |
| VLAN 140 | Khu vực Điều trị nội trú | 1-5 | 2 | 192.168.3.128/26 | 192.168.3.129 - 192.168.3.190 |
| VLAN 150 | Khoa Vật lý trị liệu | 6-10 | 2 | 192.168.3.192/26 | 192.168.3.193 - 192.168.3.254 |
| VLAN 160 | Khoa Phẫu thuật | 1-5 | 3 | 192.168.4.0/26 | 192.168.4.1 - 192.168.4.62 |
| VLAN 170 | Khu vực Hồi sức | 6-10 | 3 | 192.168.4.64/26 | 192.168.4.65 - 192.168.4.126 |
| VLAN 180 | Khoa Điều trị đặc biệt | 1-5 | 4 | 192.168.4.128/26 | 192.168.4.129 - 192.168.4.190 |
| VLAN 190 | Các phòng nghiên cứu | 6-10 | 4 | 192.168.4.192/26 | 192.168.4.193 - 192.168.4.254 |
| VLAN 200 | Khoa Hồi sức tích cực và Chống độc | 1-5 | 5 | 192.168.5.0/26 | 192.168.5.1 - 192.168.5.62 |
| VLAN 210 | Khoa Sản Nhi | 6-10 | 5 | 192.168.5.64/26 | 192.168.5.65 - 192.168.5.126 |

Bảng 4: Sơ đồ VLAN toà B

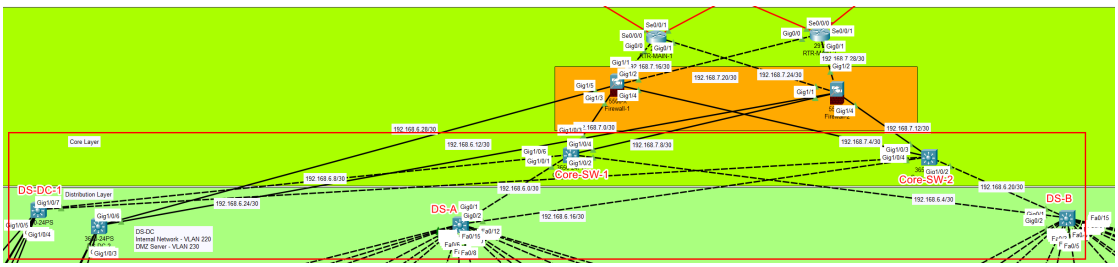



Hình 15: Thiết kế hệ thống mạng toà B

Sơ đồ IP giữa Distribution Layer và Core Layer:

| Kết nối | Subnet |
|---|---|
| Core-SW-1 ⟷ DS-A | 192.168.6.0/30 |
| Core-SW-1 ⟷ DS-B | 192.168.6.4/30 |
| Core-SW-1 ⟷ DS-DC-1 | 192.168.6.8/30 |
| Core-SW-2 ⟷ DS-A | 192.168.6.16/30 |
| Core-SW-2 ⟷ DS-B | 192.168.6.20/30 |
| Core-SW-2 ⟷ DS-DC-1 | 192.168.6.24/30 |

Bảng 5: Sơ đồ IP DS - Core

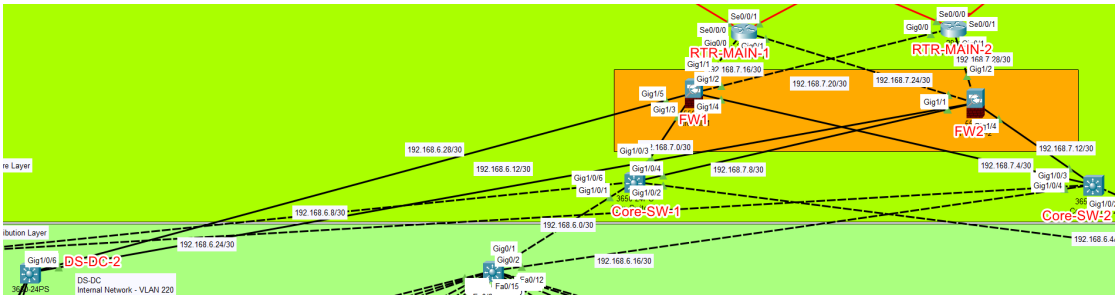



Hình 16: Thiết kế kết nối mạng giữa các Switch Layer 3 ở Distribution Layer và Core Layer

Sơ đồ IP giữa các thiết bị trong Core Layer và từ các DMZ Server:

| Kết nối | Subnet |
|---|---|
| DS-DC-2 ⟷ FW-1 | 192.168.6.28/30 |
| DS-DC-2 ⟷ FW-2 | 192.168.6.24/30 |
| Core-SW1 ⟷ FW-1 | 192.168.7.0/30 |
| Core-SW1 ⟷ FW-2 | 192.168.7.8/30 |
| Core-SW2 ⟷ FW-1 | 192.168.7.4/30 |
| Core-SW2 ⟷ FW-2 | 192.168.7.12/30 |
| Core-SW2 ⟷ Core-SW1 | 192.168.7.48/30 |
| RTR-Main-1 ⟷ FW-1 | 192.168.7.16/30 |
| RTR-Main-1 ⟷ FW-2 | 192.168.7.20/30 |
| RTR-Main-2 ⟷ FW-1 | 192.168.7.24/30 |
| RTR-Main-2 ⟷ FW-2 | 192.168.7.28/30 |

Bảng 6: Sơ đồ IP Core & DMZ Server




Hình 17: Thiết kế kết nối mạng ở tầng Core Layer và DMZ Server

Sơ đồ IP Server:

- Kết nối nội bộ:
  - **Subnet:** 192.168.5.128/29
  - **Usable IP Range:** 192.168.5.129 - 192.168.5.135
  - : Chi tiết:
    - DHCP Server:
- DMZ server:
  - **Subnet:** 192.168.5.136/29
  - **Usable IP Range:** 192.168.5.137 - 192.168.5.143

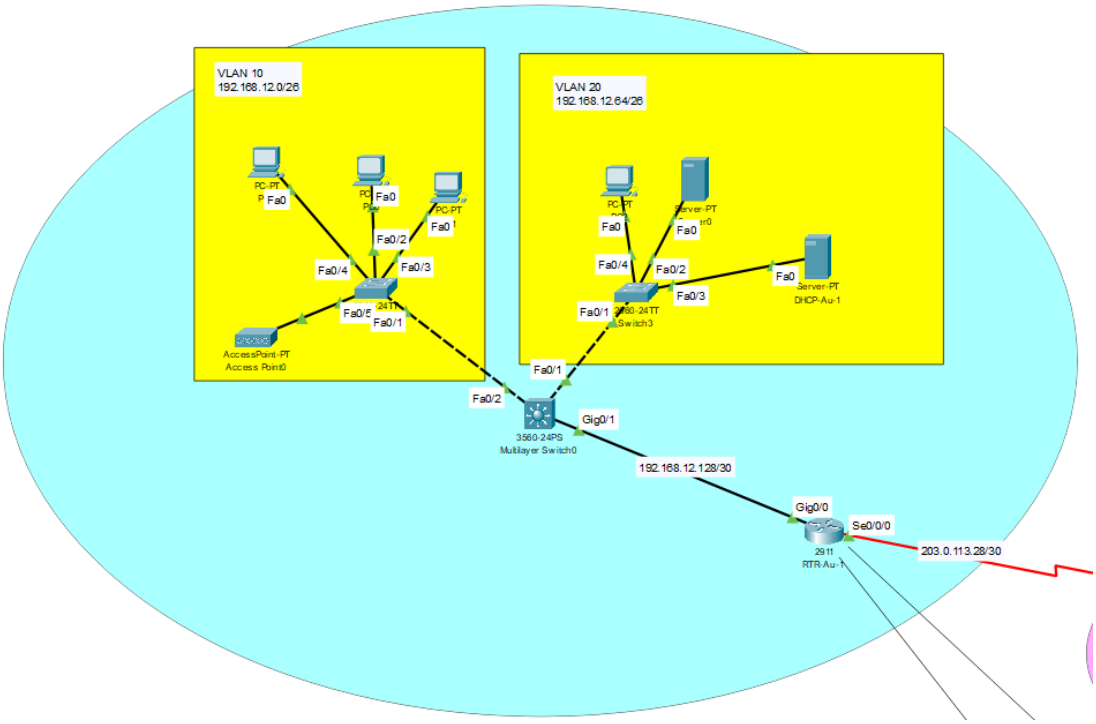
### 3.2.2 Các khu vực phụ

#### 3.2.2.1 Khu vực ĐBP

| Tầng | VLAN | Subnet |
|---|---|---|
| Tầng 1 | VLAN 10 | 192.168.12.0/26 |
| Tầng 2 | VLAN 20 | 192.168.12.64/26 |

Bảng 7: Sơ đồ IP các tầng

Giữa switch layer 3 và router: 192.168.12.128/30
Giữa router và SPN: 203.0.113.28/30



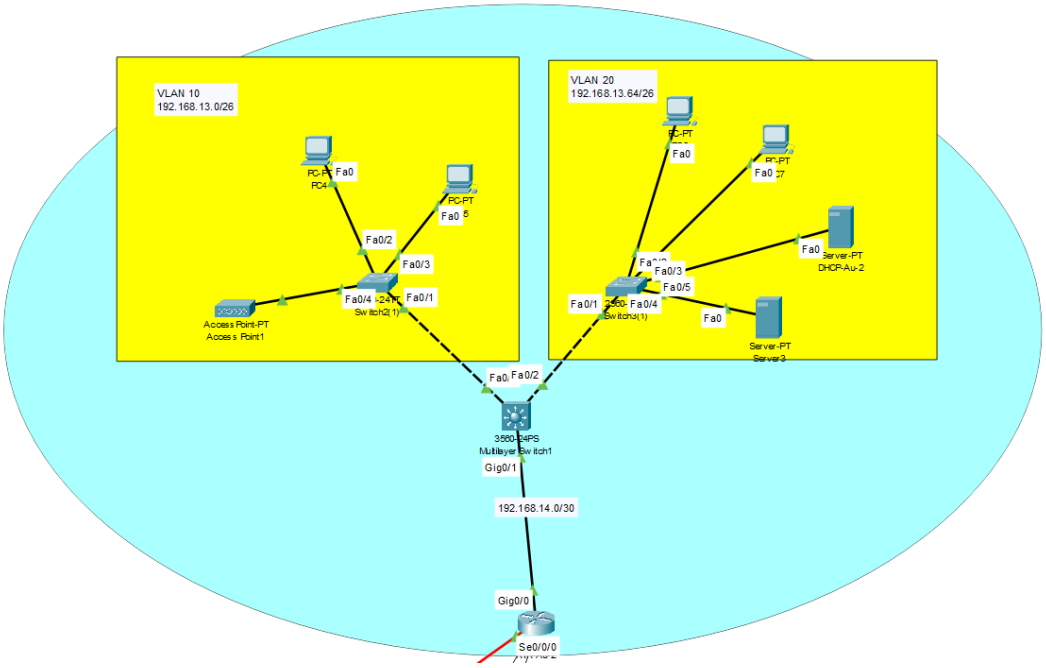

Hình 18: Sơ đồ kết nối khu vực ĐBP

#### 3.2.2.2 Khu vực BHTQ

| Tầng | VLAN | Subnet |
|---|---|---|
| Tầng 1 | VLAN 10 | 192.168.13.0/26 |
| Tầng 2 | VLAN 20 | 192.168.13.64/26 |

Bảng 8: Sơ đồ IP các tầng

Giữa switch layer 3 và router: 192.168.14.0/30
Giữa router và SPN: 203.0.113.24/30



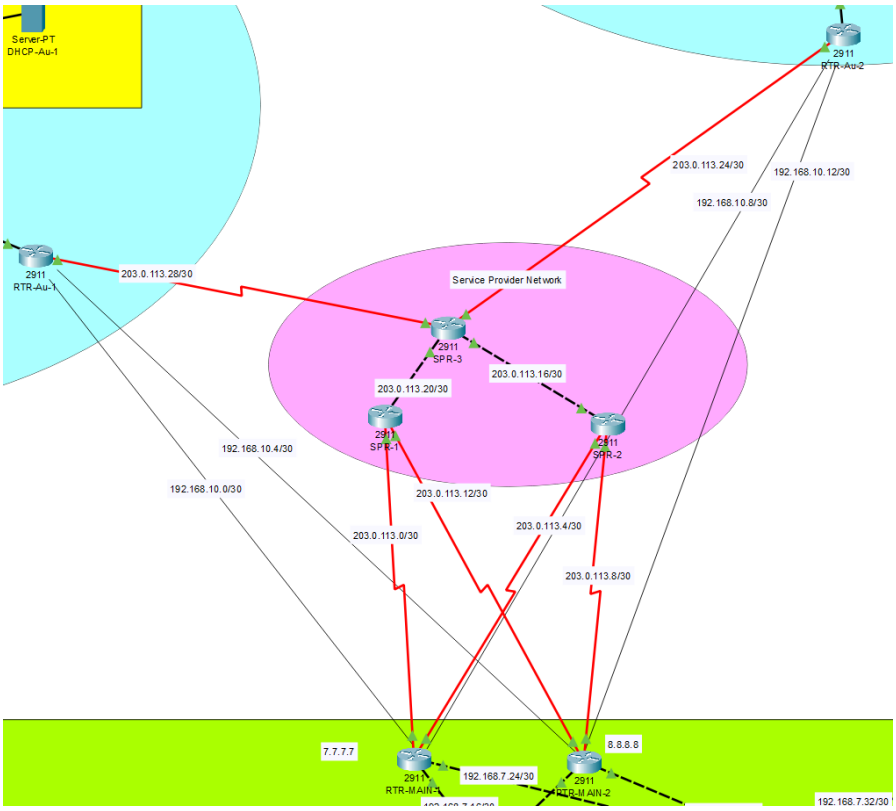

Hình 19: Sơ đồ kết nối khu vực BHTQ

## 3.3 Sơ đồ kết nối WAN giữa Main Site và các Auxiliary Site

### 3.3.1 Công nghệ WAN được sử dụng

- **GRE Tunnel VPN:**
  - Được sử dụng để tạo các kênh kết nối bảo mật giữa Main Site và Auxiliary Sites.
  - Đóng gói các gói dữ liệu để truyền qua mạng công cộng (Internet).
  - Kết hợp với giao thức OSPF để duy trì bảng định tuyến động.
- **OSPF (Open Shortest Path First):**
  - Tự động cập nhật bảng định tuyến giữa các site qua GRE Tunnel.
  - Chọn đường đi tối ưu cho các gói tin.

### 3.3.2 Sơ đồ kết nối WAN




Hình 20: Sơ đồ kết nối WAN giữa Main Site và hai Auxiliary Sites qua GRE Tunnel VPN

### 3.3.3 Chi tiết cấu hình GRE Tunnel

**GRE Tunnel giữa Main Site và Auxiliary Sites:**

- Tunnel được thiết lập giữa các router tại Main Site và mỗi Auxiliary Site.
- Các GRE Tunnel sử dụng địa chỉ IP riêng để giao tiếp:
  - **Tunnel 1 (RTR-MAIN-1 - Auxiliary Site 1):**
    - Tunnel IP: 192.168.10.1/30 (RTR-MAIN-1) và 192.168.10.2/30 (Auxiliary Site 1).
    - Public IP: 203.0.113.1 (RTR-MAIN-1) và 203.0.113.30 (Auxiliary Site 1).
  - **Tunnel 2 (RTR-MAIN-1 - Auxiliary Site 2):**
    - Tunnel IP: 192.168.10.9/30 (RTR-MAIN-1) và 192.168.10.10/30 (Auxiliary Site 2).
    - Public IP: 203.0.113.5 (RTR-MAIN-1) và 203.0.113.26 (Auxiliary Site 2).
  - **Tunnel 3 (RTR-MAIN-2 - Auxiliary Site 1):**
    - Tunnel IP: 192.168.10.5/30 (RTR-MAIN-2) và 192.168.10.6/30 (Auxiliary Site 1).
    - Public IP: 203.0.113.13 (RTR-MAIN-2) và 203.0.113.30 (Auxiliary Site 1).

  - **Tunnel 4 (RTR-MAIN-2 - Auxiliary Site 2):**
    * Tunnel IP: 192.168.10.13/30 (RTR-MAIN-2) và 192.168.10.14/30 (Auxiliary Site 2).
    * Public IP: 203.0.113.9 (RTR-MAIN-2) và 203.0.113.26 (Auxiliary Site 2).

- GRE Tunnel kết hợp với OSPF để định tuyến giữa các site.

#### 3.3.4 Mô tả hoạt động kết nối

- Các GRE Tunnel đảm bảo kết nối bảo mật giữa Main Site và Auxiliary Sites qua Internet.
- OSPF định tuyến động cho phép cập nhật bảng định tuyến và phát hiện thay đổi mạng.
- Các kết nối đảm bảo tính ổn định và giảm độ trễ khi truy cập tài nguyên từ các site.

# 4 Tính toán các thông số

Từ yêu cầu, có được:

- Hệ thống đạt cao điểm ở 80% lưu lượng cả ngày vào các khung giờ từ 9 giờ sáng - 11 giờ trưa và từ 3 - 4 giờ chiều.
- Lưu lượng tải lên cho mỗi server hằng ngày là 2000 MB/ngày, tải xuống là 1000 MB/ngày
- Lưu lượng tải lên cho mỗi máy trạm là 100 MB/ngày, tải xuống là 500 MB/ngày
- Lưu lượng tải xuống của mỗi thiết bị sử dụng wifi là 500 MB/ngày.
- Hệ thống mạng bệnh viện dự kiến sẽ tăng trưởng với tốc độ 20% trong 5 năm, về các khía cạnh như số người sử dụng, tốc độ kết nối, mở rộng các khu vực,...

## 4.1 Khu vực chính

Ta có công thức:

$$\text{Throughput (Mbps)} = \frac{\text{Traffic(MB/hour)} * 8\text{(bits/byte)}}{3600\text{(seconds/hour)}}$$

### 4.1.1 Server

Với việc bệnh viện sẽ hoạt động liên tục cả ngày, throughput của server là:

$$\frac{(1000 + 2000) \times 10}{24} \times \frac{8}{3600} \approx 2.78\text{Mbps}$$

Với việc 80% tổng lưu lượng cả ngày đến trong 3 tiếng cao điểm (9 - 11 giờ sáng, 3 - 4 giờ chiều), thì tính được bandwidth của server:

$$\frac{10 \times 3000 \times 80\%}{3} \times \frac{8}{3600} \approx 17.78\text{Mbps}$$

### 4.1.2 Workstations

Throughput của các workstation là:

$$\frac{(500 + 100) \times 600}{24} \times \frac{8}{3600} \approx 33.33\text{Mbps}$$

Bandwidth cho các workstation:

$$\frac{600 \times 600 \times 80\%}{3} \times \frac{8}{3600} \approx 213.33\text{Mbps}$$

### 4.1.3 Các thiết bị kết nối wifi

Throughput:

$$\frac{500 \times 8}{24 \times 3600} \approx 0.05\text{Mbps}$$

Bandwidth:

$$\frac{500 \times 80\% \times 8}{3 \times 3600} \approx 0.30\text{Mbps}$$

#### 4.1.4 Tất cả

Từ các giá trị đã tính bên trên, ta có tổng throughput của cả khu vực chính:

$$2.78 + 33.33 + 0.05 \approx 36.16\text{Mbps}$$

Và Bandwidth yêu cầu:

$$17.78 + 213.33 + 0.30 \approx 231.41\text{Mbps}$$

Với việc có yêu cầu hệ thống mạng dự kiến tăng trưởng với tốc độ 20% trong 5 năm, để đảm bảo sự ổn định thì:

$$\text{Required Bandwidth} = 231.407 * 1.2 = 277.70\text{Mbps}$$

### 4.2 Khu vực phụ

Tương tự như khu vực chính, với mỗi khu vực phụ, ta có

#### 4.2.1 Server

Với việc bệnh viện sẽ hoạt động liên tục cả ngày, throughput của server là:

$$\frac{(1000 + 2000) \times 2}{24} \times \frac{8}{3600} \approx 0.56\text{Mbps}$$

Với việc 80% tổng lưu lượng cả ngày đến trong 3 tiếng cao điểm (9 - 11 giờ sáng, 3 - 4 giờ chiều), thì tính được bandwidth của server:

$$\frac{2 \times 3000 \times 80\%}{3} \times \frac{8}{3600} \approx 3.56\text{Mbps}$$

#### 4.2.2 Workstations

Throughput của các workstation là:

$$\frac{(500 + 100) \times 60}{24} \times \frac{8}{3600} \approx 3.33\text{Mbps}$$

Bandwidth cho các workstation:

$$\frac{600 \times 60 \times 80\%}{3} \times \frac{8}{3600} \approx 21.33\text{Mbps}$$

#### 4.2.3 Các thiết bị kết nối wifi

Throughput:

$$\frac{500 \times 8}{24 \times 3600} \approx 0.05\text{Mbps}$$

Bandwidth:

$$\frac{500 \times 80\% \times 8}{3 \times 3600} \approx 0.30\text{Mbps}$$

#### 4.2.4 Tất cả

Từ các giá trị đã tính bên trên, ta có tổng throughput của một khu vực phụ:

$$0.56 + 3.33 + 0.05 \approx 0.94\text{Mbps}$$

Và Bandwidth yêu cầu:

$$3.56 + 21.33 + 0.30 \approx 25.19\text{Mbps}$$

Với việc có yêu cầu hệ thống mạng dự kiến tăng trưởng với tốc độ 20% trong 5 năm, để đảm bảo sự ổn định thì:

$$\text{Required Bandwidth} = 25.19 \times 1.2 = 30.23\text{Mbps}$$

### 4.3 Băng thông yêu cầu

Với những giá trị đã tính được bên trên, băng thông cần có từ nhà mạng để cả khu vực chính và 2 khu vực phụ có thể sử dụng ổn định trong 5 năm tới, sẽ là:

$$\text{ISP required bandwidth} = 277.7 + 30.23 \times 2 \approx 338.15\text{Mbps}$$

Có thể làm tròn lên 340 - 350 Mbps để dự phòng các tình huống sau này.

### 4.4 Cấu hình mạng đề xuất

#### 4.4.0.1 Kết nối WAN

SD-WAN có thể đảm bảo lượng băng thông ít nhất là 340 Mbps.

#### 4.4.0.2 Mạng nội bộ

- Khu vực chính: Triển khai sử dụng các switch 10GbE cho các kết nối trong hệ thống, nhằm đảm bảo lưu lượng thông suốt giữa các thiết bị.
- Khu vực phụ: Sử dụng các switch 1GbE là đủ.

#### 4.4.0.3 Mạng không dây

Sử dụng công nghệ Wifi-6 (mới nhất), đảm bảo khả năng chuyển vùng liền mạch và ưu tiên chất lượng dịch vụ (QoS) cho các ứng dụng quan trọng.

**4.4.0.4 Bảo mật** Triển khai tường lửa, hệ thống phát hiện/ngăn chặn xâm nhập trái phép, và có VPN để nhân viên có thể làm việc từ xa (từ khu vực phụ sang khu vực chính và ngược lại).

# 5 Thiết kế

## 5.1 Cấu hình khởi tạo cho thiết bị

Sau khi thiết kế và nối dây cần cấu hình cho các Router và Layer 3 switch hostname, password, SSH.

```
enable
configure terminal
hostname DS-Au-2
banner motd #NO Unauthorised Access!!!#
no ip domain lookup
line console 0
password cisco
login
exit
enable password cisco
service password-encryption
do wr
```

Listing 1: Cấu hình hostname và mật khẩu

```
ip domain name cisco.net
username admin password cisco
crypto key generate rsa
1024
line vty 0 15
transport input ssh
login local
ip ssh version 2
do wr
```

Listing 2: Cấu hình SSH

## 5.2 Cấu hình VLANs trunk

```
int range gi1/0/6-7
switchport mode trunk
exit
vlan 230
name DMZ_Server
exit
int range gi1/0/1-5
switchport mode access
switchport access vlan 230
exit
```

Listing 3: Cấu hình VLANs trunk

## 5.3 Subneting

Ở bước này sẽ đánh địa chỉ IP cho các VLAN, các đường nối giữa Layer 3 switch với Router và Router với Router. Nhóm đã trình bày ở phần trên.

```
int gi0/0
ip address 192.168.0.1 255.255.255.252
no shut
```

Listing 4: Gán địa chỉ IP cho một Interface

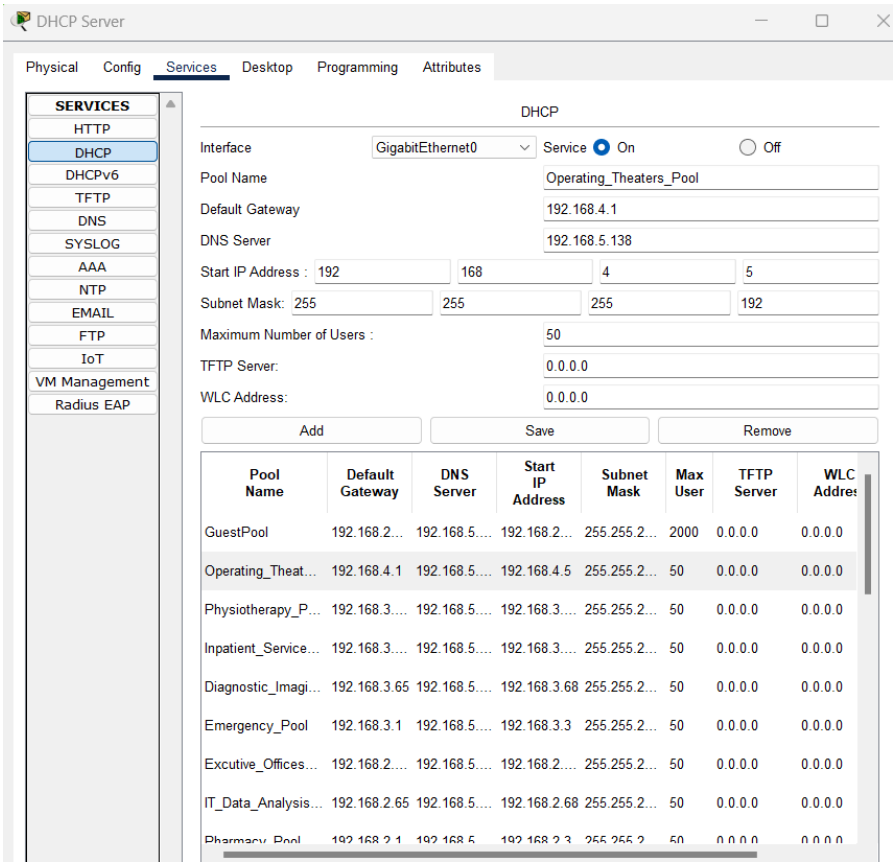
## 5.4 OSPF

```
router ospf 1
router-id 8.8.8.8
network 192.168.7.20 0.0.0.3 area 0
network 192.168.7.28 0.0.0.3 area 0
network 203.0.113.8 0.0.0.3 area 0
network 203.0.113.12 0.0.0.3 area 0
exit
```

Listing 5: Quảng cáo mạng bằng OSPF

## 5.5 DHCP server và các device khác

Được cấu hình trực tiếp trên phần mềm Cisco Packet Tracer như hình bên dưới.




Hình 21: Cấu hình trên server DHCP server

## 5.6 Inter VLAN routing

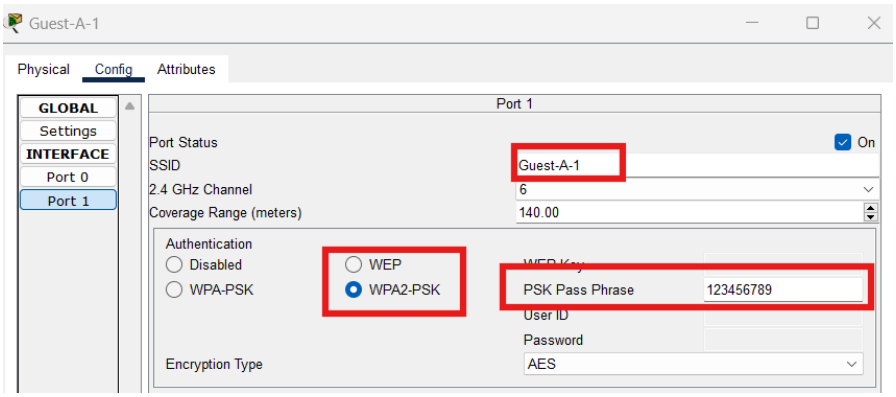
Sau đó cần cấu hình trên Distribution Switch để nhận gói tin địa chỉ từ DHCP.

```
int vlan 10
no sh
ip address 192.168.0.65 255.255.255.192
ip helper-address 192.168.5.130
exit
```

Listing 6: Inter VLAN routing

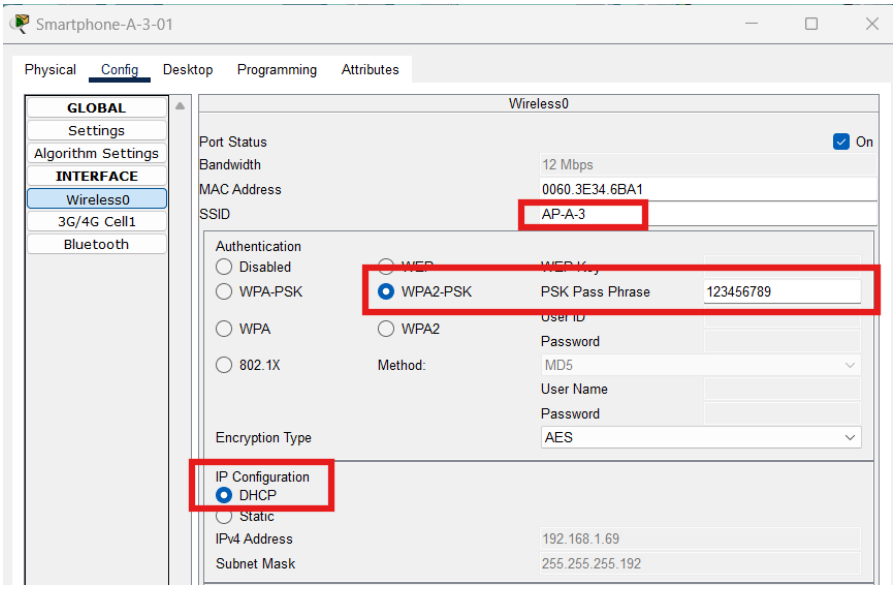
## 5.7 Cấu hình Wireless

Cấu hình một Access point trên Cisco Packet Tracer như hình bên dưới.




Hình 22: Cấu hình wireless

Cấu hình cho một Smart phone kết nối với Access Point.




Hình 23: Cấu hình smart phone kết nối với AP

## 5.8 PAT và ACL

Dưới đây là code cấu hình PAT và ACL cho router để permit các gói tin TCP, ICMP, UDP đến 192.168.5.139 (Web Server).

```
interface GigabitEthernet0/0
ip nat inside
interface GigabitEthernet0/1
ip nat outside
exit

access-list 100 permit tcp 192.168.5.139 0.0.0.255 any
```

```
access-list 100 permit udp 192.168.5.139 0.0.0.255 any
access-list 100 permit icmp 192.168.5.139 0.0.0.255 any

ip nat inside source list 100 interface GigabitEthernet0/1 overload
```

Listing 7: Cấu hình PAT cho router

## 5.9 Firewall

Cấu hình Firewall tương đối giống với Router khác ở chỗ thêm Security level vào mỗi Interface và khi thực hiện routing bằng ospf mặt nạ mạng thay vì dùng wildcard mask sẽ phải dùng subnet mask. Cấu hình ACL tương tự như trên.

```
interface gi0/1
no shutdown
nameif Core-SW-1
ip address <<ip address>> <<subnet mask>>
security-plan <<0-100>>
exit
exit
write memory
```

Listing 8: Cấu hình Firewall

```
router ospf 1
network 192.168.6.28 255.255.255.252 area 0
```

Listing 9: OSPF cho Firewall

## 5.10 Portfast và BPDU guard

Cấu hình Portfast và BPDU guard giúp các thiết bị mới tham gia vào mạng có thể ngay lập tức có được IP mà không phải đợi thực hiện các giao thức STP (sẽ mất khoảng hơn 30s). Cấu hình ở các Access Switch như sau.

```
interface range fa0/2-24
spanning-tree portfast
spanning-tree bpduguard enable
exit
do wr
```

Listing 10: Portfast và BPDU guard

## 5.11 GRE tunnel VPN

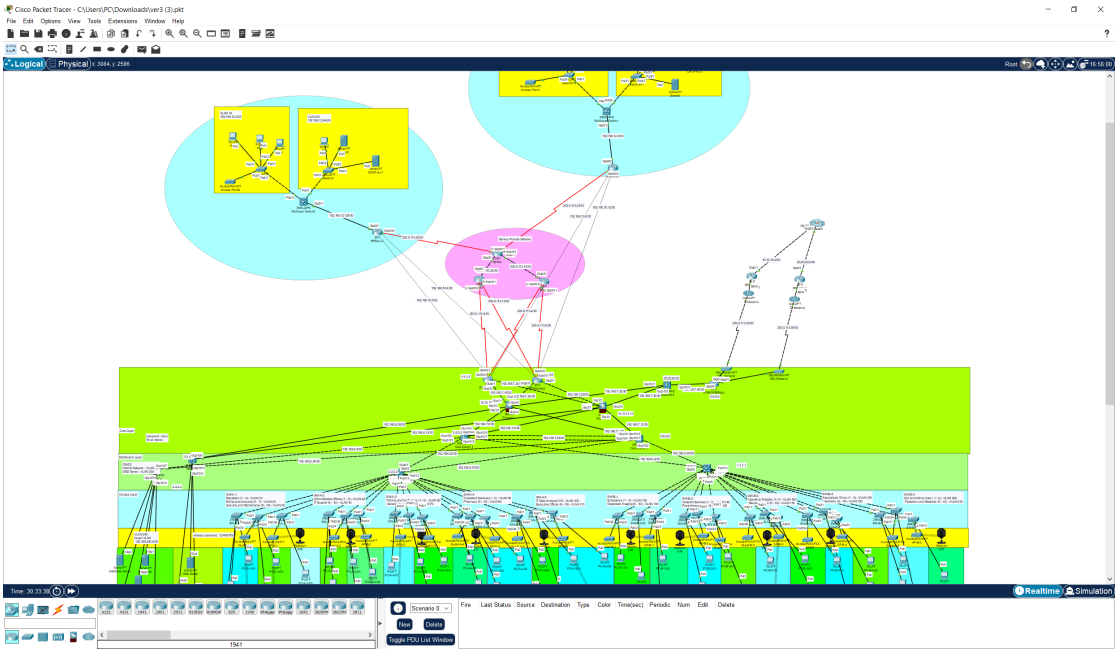
Do Cisco Packet Tracer không hỗ trợ MPLS nên nhóm dùng GRE tunnel (tương tự nhưng kém bảo mật hơn) để sử dụng thay thế. Cấu hình VPN ở các Router biên như sau.

```
int tunnel 0
tunnel source serial 0/0/0
tunnel destination 203.0.113.1
ip address 192.168.10.2 255.255.255.252
```

```
int tunnel 1
tunnel source serial 0/0/0
tunnel destination 203.0.113.13
ip address 192.168.10.6 255.255.255.252
```

Listing 11: GRE tunnel

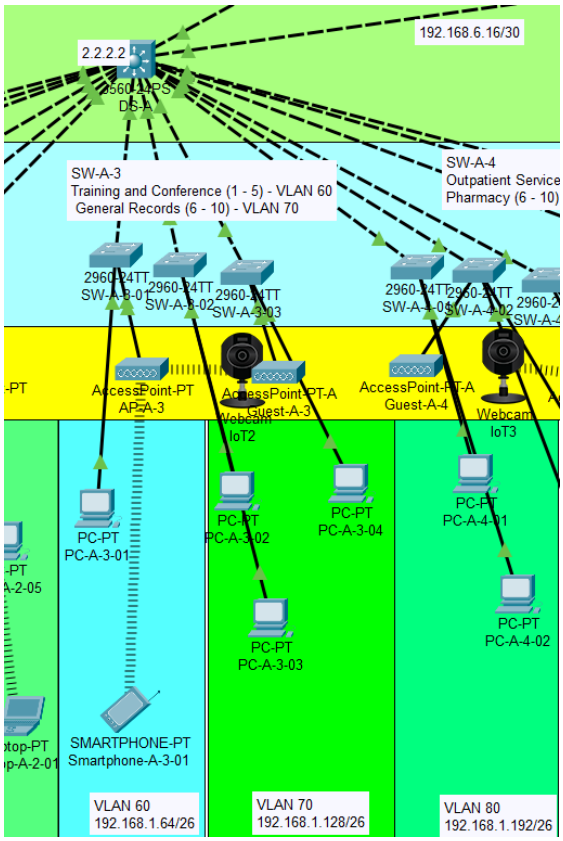
## 5.12 Tổng quan kiến trúc hệ thống



# 6 Kiểm thử hệ thống

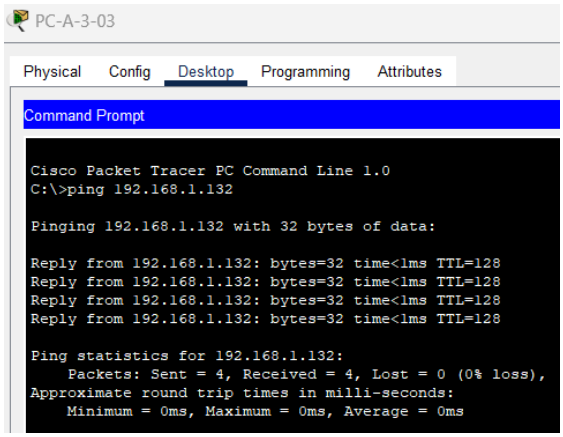
Để thuận tiện cho việc kiểm thử thì nhóm đã cấu hình firewall permit các gói tin ICMP, IP, TCP. Trên thực tế thì firewall sẽ phải chặn việc ping từ Internet vào mạng nội bộ. Các địa chỉ IP được cấp phát tự động bằng DHCP server nên sẽ không cố định.

## 6.1 Kết nối giữa các thiết bị thuộc cùng VLAN




Hình 24: Kết nối giữa hai PC thuộc cùng VLAN 70

Bây giờ hãy chú ý vào PC-A-3-03 và PC-A-3-04 lần lượt có địa chỉ IP là 192.168.1.131 và 192.168.1.132. Chúng ta sẽ thực hiện ping từ PC-A-3-03 tới PC-A-3-04. Dưới đây là kết quả.

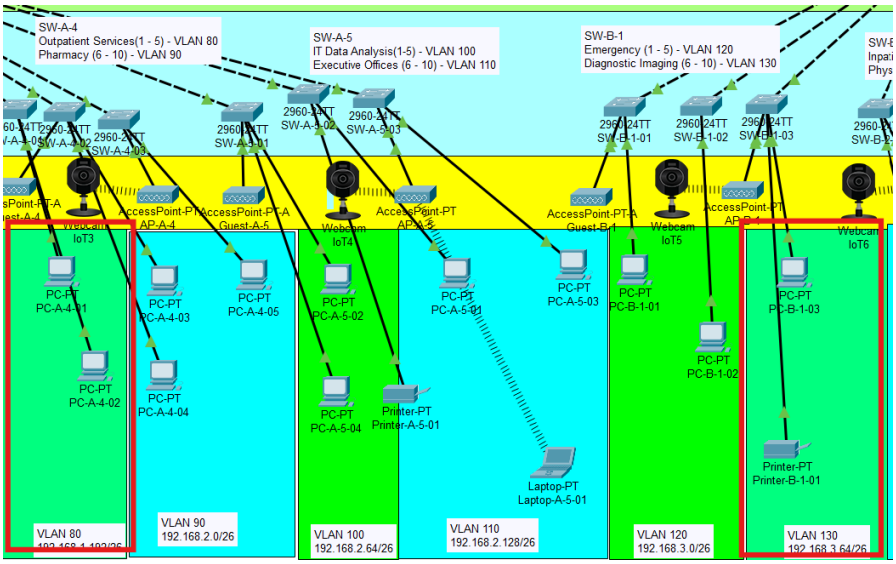



Hình 25: Ping giữa hai PC thuộc cùng VLAN 70

Như vậy kết nối thành công giữa PC thuộc cùng VLAN.

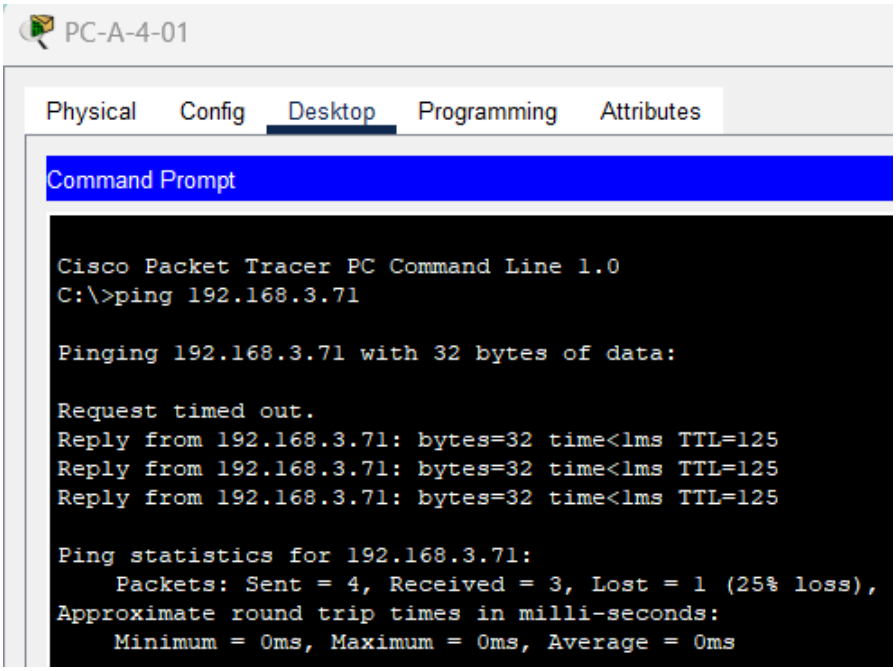
## 6.2 Kết nối giữa các thiết bị khác VLAN

Chúng ta sẽ kiểm tra kết nối giữa PC-A-4-01 và PC-B-1-03 lần lượt thuộc VLAN 80 và VLAN 130. Và có địa chỉ IP là 192.168.1.197 và 192.168.3.71.



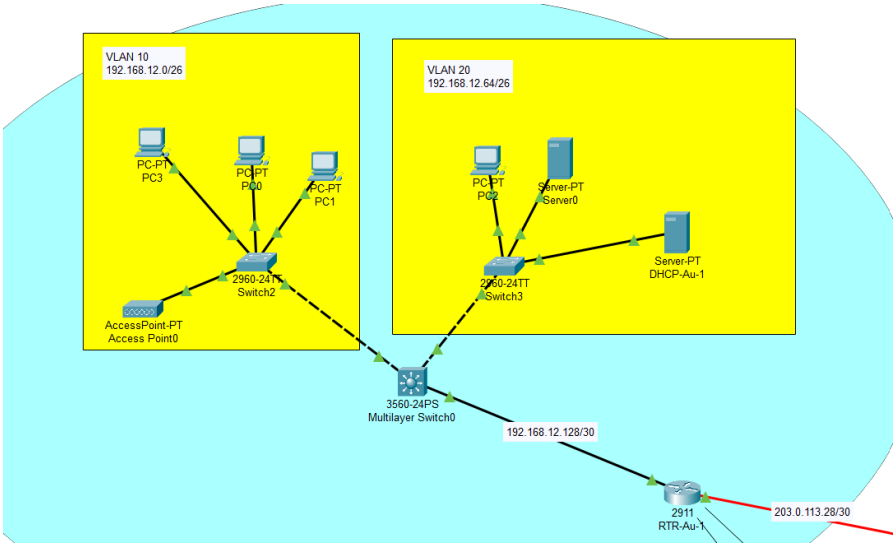

Hình 26: Kết nối giữa hai PC thuộc VLAN 80 và VLAN 130

Vậy là kết nối giữa các thiết bị khác VLAN thành công.




Hình 27: Kết nối giữa hai PC thuộc VLAN 80 và VLAN 130

## 6.3 Kết nối giữa thiết bị thuộc Main site và Auxiliary site




Hình 28: PCs thuộc Auxiliary site 1

Chúng ta sẽ dùng lại PC-A-4-01 có IP là 192.168.1.197. Ở lần kiểm thử này chúng ta sẽ dùng lệnh tracert để tìm đường đi đến PC0 thuộc VLAN 10 của Auxiliary site 1 với IP là 192.168.12.5.

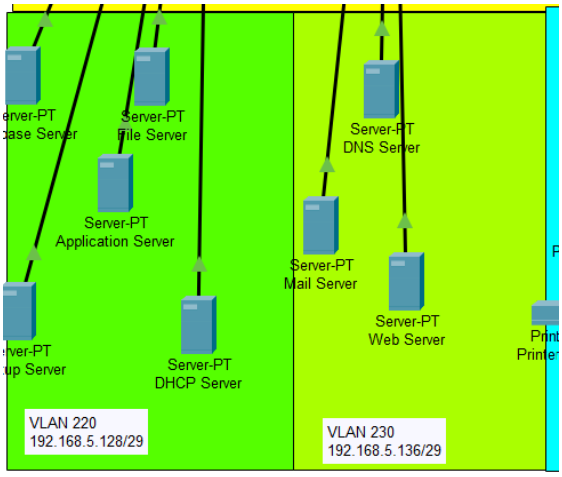
```
C:\>tracert 192.168.12.5

Tracing route to 192.168.12.5 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.193
  2    0 ms      0 ms      0 ms      192.168.6.18
  3    0 ms      7 ms      0 ms      192.168.7.10
  4    0 ms      0 ms      0 ms      192.168.7.30
  5    1 ms      1 ms      1 ms      203.0.113.21
  6    1 ms      0 ms      1 ms      203.0.113.18
  7    2 ms      2 ms      2 ms      203.0.113.30
  8    2 ms      29 ms     1 ms      192.168.12.129
  9    *         1 ms      0 ms      192.168.12.5
```

Hình 29: Tracert từ Main site tới Auxiliary site

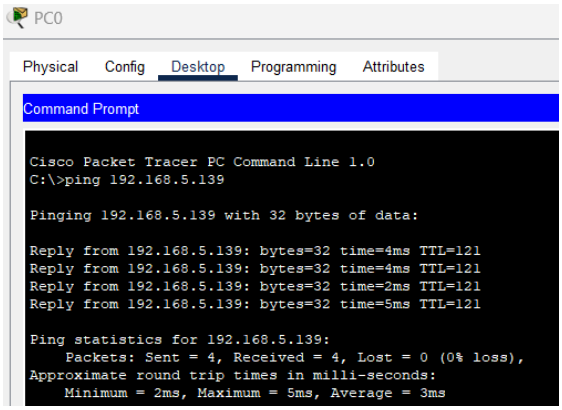
## 6.4 Kết nối tới server thuộc DMZ




Hình 30: Các server ở Main site

VLAN 230 là các server thuộc DMZ gồm Web server, Mail Server và DNS server. Một điều hiển nhiên nếu kết nối được với Web server thì sẽ phải kết nối được tới DNS server để phân giải tên miền. Ở phần này ta sẽ chỉ ping từ PC thuộc VLAN ở Main site tới Web server.

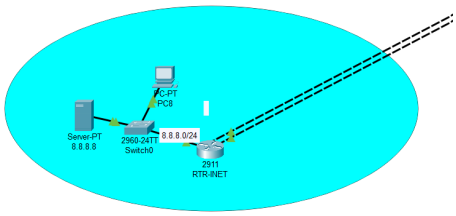
Chúng ta sẽ dùng PC0 thuộc VLAN 10 của Auxiliary site 1 ở phần trước để ping tới web server với IP 192.168.5.139.



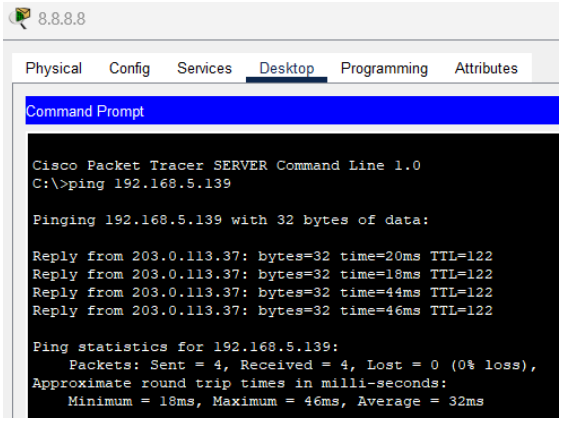

Hình 31: Ping tới Web server

## 6.5 Kết nối từ Internet tới web server

Ta sẽ thực hiện Ping từ server 8.8.8.8 thuộc Internet tới Web server.




Hình 32: Internet




Hình 33: Ping từ Internet tới Web server

# 7 Đánh giá lại hệ thống mạng đã thiết kế

## 7.1 Tổng quan về các công nghệ đã triển khai

Hệ thống mạng được xây dựng dựa trên các công nghệ hiện đại để đảm bảo hiệu suất, tính bảo mật, và khả năng mở rộng. Các công nghệ chủ chốt bao gồm:

- **Cấu hình VLAN và Inter-VLAN Routing:**
  - Phân chia mạng thành các VLAN độc lập, tạo sự cách ly lưu lượng giữa các phòng ban, giúp tăng cường bảo mật và quản lý.
  - Dùng Inter-VLAN Routing để các VLAN có thể giao tiếp hiệu quả qua Layer 3.
- **Giao thức định tuyến OSPF:** Cung cấp khả năng định tuyến động, giúp tối ưu hóa đường truyền giữa các site và tự động khôi phục khi có sự cố.
- **EtherChannel trên Layer 3 Switch:**
  - Sử dụng EtherChannel để gộp nhiều đường truyền vật lý thành một kênh logic, tăng băng thông và cải thiện khả năng dự phòng.
  - Cơ chế load balancing phân phối lưu lượng dựa trên thuật toán như `src-dst-ip` (IP nguồn/đích) hoặc `src-dst-mac` (MAC nguồn/đích).
- **GRE Tunnel VPN:** Sử dụng để kết nối an toàn giữa các site qua mạng WAN, thay thế MPLS, cung cấp sự bảo mật và khả năng mã hóa lưu lượng.
- **Máy chủ DHCP:** Tự động cấp phát địa chỉ IP cho các thiết bị trong mạng, giảm thiểu sai sót khi cấu hình thủ công.
- **PAT và ACL:**
  - **PAT (Port Address Translation):** Sử dụng một địa chỉ IP công cộng để chia sẻ cho nhiều thiết bị nội bộ khi truy cập Internet.
  - **ACL (Access Control List):** Kiểm soát quyền truy cập, giới hạn lưu lượng theo chính sách cụ thể.
- **Tường lửa (Firewall):** Bảo vệ mạng khỏi các mối đe dọa từ bên ngoài, áp dụng các chính sách bảo mật nâng cao.
- **Hệ thống không dây (Wireless):** Sử dụng Access Point hỗ trợ hai băng tần (dual-band) và chuẩn bảo mật WPA3, đảm bảo kết nối ổn định, bảo mật cao.
- **PortFast và BPDU Guard:** Giảm thời gian khởi động cổng truy cập (PortFast), bảo vệ mạng khỏi lỗi do BPDU không mong muốn gây ra (BPDU Guard).

## 7.2 Đánh giá các đặc điểm quan trọng

- **Độ tin cậy:**
  - OSPF và GRE Tunnel cung cấp kết nối ổn định và khả năng tự phục hồi khi có sự cố.
  - EtherChannel giảm thiểu downtime nhờ dự phòng tự động khi một trong các liên kết vật lý gặp lỗi.

- **Khả năng mở rộng:**
  - Thiết kế VLAN linh hoạt, dễ dàng bổ sung thêm người dùng hoặc thiết bị mới.
  - EtherChannel tăng khả năng mở rộng băng thông mà không cần thay đổi cấu trúc mạng vật lý.
  - GRE Tunnel có thể mở rộng để kết nối thêm các site phụ.
- **Bảo mật:**
  - Chuẩn WPA3 trên mạng không dây và ACL giúp quản lý lưu lượng hiệu quả.
  - Firewall áp dụng chính sách Zero Trust Network để giảm thiểu rủi ro từ bên ngoài.
- **Hiệu suất:**
  - EtherChannel tăng tổng băng thông giữa các thiết bị mạng và cải thiện hiệu suất lưu lượng với cơ chế load balancing.
  - Wi-Fi hai băng tần (dual-band) tối ưu hóa hiệu suất kết nối không dây.
  - Định tuyến OSPF tối ưu hóa các kết nối nội bộ và giữa các site.

## 7.3 Các vấn đề còn tồn tại

- **Hiệu suất của GRE Tunnel:** Khi lưu lượng cao hoặc số lượng site tăng, GRE Tunnel có thể giảm hiệu quả, không đáp ứng tốt như SD-WAN hoặc MPLS.
- **Hiệu quả cân bằng tải của EtherChannel:** Cân bằng tải trên EtherChannel phụ thuộc vào thuật toán hash, có thể không đạt hiệu quả tối ưu nếu lưu lượng không đa dạng về nguồn/đích.
- **Khả năng giám sát và phân tích:** Thiếu hệ thống giám sát log và phân tích lưu lượng tập trung.
- **Khó khăn trong bảo trì:** Việc quản lý cấu hình VLAN, EtherChannel, và Inter-VLAN Routing đòi hỏi đội ngũ IT có kỹ năng cao.

## 7.4 Định hướng phát triển trong tương lai

- **Tối ưu hóa công nghệ WAN:**
  - Nâng cấp từ GRE Tunnel lên SD-WAN để tăng hiệu quả, đơn giản hóa quản lý.
  - Tích hợp thêm giao thức bảo mật như IPsec để tăng cường an toàn.
- **Nâng cao bảo mật:**
  - Tích hợp hệ thống giám sát tập trung (SIEM) để theo dõi và phân tích mối đe dọa.
  - Triển khai chính sách Zero Trust Network Access (ZTNA) cho toàn bộ hệ thống.
- **Tự động hóa quản lý mạng:**
  - Sử dụng Software-Defined Networking (SDN) để tự động hóa cấu hình, giảm thiểu lỗi thủ công.
  - Áp dụng công nghệ AI/ML để dự đoán và xử lý sự cố trước khi chúng xảy ra.

- **Phát triển hạ tầng mạng:**
  - Quy hoạch lại subnet để chuẩn bị cho sự mở rộng trong tương lai.
  - Nâng cấp thiết bị mạng để hỗ trợ chuẩn Wi-Fi mới như Wi-Fi 6E và tốc độ cao hơn (10GbE).
  - Xây dựng thêm các liên kết EtherChannel để cải thiện băng thông và dự phòng ở những khu vực chịu tải cao.