VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY
UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING

COMPUTER NETWORKS (CO3093)

Assignment 2

"NETWORK DESIGN AND SIMULATION FOR ACRITICAL LARGE HOSPITAL"

Instructor: Bùi Xuân Giang, *CSE-HCMUT*
Semester: 251
Class: L02
Students: Dương Gia Bảo - 2310207 *(Team MMTers)*
Nguyễn Hồng Minh - 2212059 *(Team MMTers)*
Phạm Thành Trí - 2313621 *(Team MMTers)*
Phan Phúc Thịnh - 2313306 *(Team MMTers)*

HO CHI MINH CITY, NOVEMBER 2025

Mục lục

Danh mục hình vẽ

Danh mục bảng biểu

Danh sách thành viên và nhiệm vụ

STT	Họ và tên	MSSV	Nhiệm vụ	Hoàn thành
1	Dương Gia Bảo	2310207	- Thiết kế khu vực phụ. - Tổng hợp báo cáo và trình bày slide.	100%
2	Phạm Thành Trí	2313621	- Thiết kế khu vực chính. - Thiết kế WAN giữa các Site.	100%
3	Phan Phúc Thịnh	2313306	- Kiểm tra lý thuyết, code và tính liên quan với đề bài. - Hiện thực các mẫu hình P2P, Client-Server. - Thiết kế WebApp và hiện thực các API.	100%
4	Nguyễn Hồng Minh	2212059	- Tổng hợp báo cáo. - Hiện thực cookies, session, đăng nhập. - Kiểm thử và debug backend, proxy.	100%

Bảng 1: Danh sách thành viên và nhiệm vụ

1 Tóm lược dự án

Công Ty CCC muốn thiết kế và mô phỏng hệ thống mạng cho một bệnh viện chuyên khoa lớn, gồm một Trụ sở chính (Main Site) tại Thành phố Hồ Chí Minh (gồm hai tòa A và B) và hai chi nhánh phụ (DBP, BHTQ). Hệ thống được thiết kế nhằm đáp ứng các yêu cầu về kết nối nội bộ giữa các phòng ban, bảo mật cao, độ sẵn sàng cao (HA) và khả năng mở rộng trong 5 năm tới. Mô phỏng sẽ được thực hiện trên Cisco Packet Tracer, bao gồm cấu trúc VLAN, DMZ cho dịch vụ công khai, tường lửa và kết nối WAN giữa các site (SD-WAN/MPLS thay thế trong đề xuất chi phí). Tài liệu này trình bày phương án kiến trúc, sơ đồ mạng, kế hoạch địa chỉ IP, danh sách thiết bị đề xuất, cấu hình mạng cơ bản, kết quả kiểm thử (ping/traceroute) và đánh giá theo các tiêu chí về hiệu năng, bảo mật, khả năng mở rộng.

2 Thiết kế kiến trúc mạng phù hợp với hệ thống

2.1 Phân tích yêu cầu kiến trúc hệ thống

2.1.1 Mạng hệ thống tại trụ sở chính

Địa điểm: Trụ sở chính đặt tại Thành phố Hồ Chí Minh, bao gồm hai tòa nhà **A** và **B**, mỗi tòa có **5 tầng**, mỗi tầng gồm **10 phòng**. Các phòng được trang bị máy tính, thiết bị y tế và hệ thống mạng nội bộ.

Khu kỹ thuật trung tâm: Khu **Data Center**, **phòng IT**, và **Trung tâm cáp (Cabling Central Local)** được bố trí tại một khu vực riêng biệt, cách hai tòa nhà A và B khoảng **50 mét**. Khu này chứa các thiết bị cốt lõi của mạng như **core switch**, **router**, **firewall**, **load balancer**, **patch panels** và **các máy chủ**.

Quy mô hệ thống: Mạng có quy mô trung bình, gồm khoảng **600 máy trạm (workstations)**, **10 máy chủ (servers)**, và **12 thiết bị mạng** (hoặc nhiều hơn nếu tính các thiết bị bảo mật chuyên dụng như firewall, IDS/IPS, VPN gateway...).

Kết nối có dây và không dây: Toàn bộ khu vực trụ sở chính được phủ sóng **Wi-Fi toàn phần**, kết hợp hạ tầng **cáp quang (GPON)** và **Ethernet tốc độ cao**

(**1GbE/10GbE/40GbE**). Các kết nối được tổ chức theo mô hình **VLAN** để phân tách lưu lượng cho các phòng ban khác nhau như: hành chính, bác sĩ, y tá, thiết bị y tế, khách, và khu máy chủ.

Liên kết WAN: Mạng của trụ sở chính được kết nối với hai trụ sở phụ (**Site DBP** và **Site BHTQ**) thông qua **hai đường truyền thuê riêng (leased lines)**. Các liên kết này có thể áp dụng công nghệ **SD-WAN** hoặc **MPLS** để đảm bảo tính ổn định và linh hoạt cho mạng diện rộng (WAN).

Kết nối Internet: Sử dụng **hai đường DSL** (2xDSL) để truy cập Internet, với cơ chế **cân bằng tải (load balancing)** nhằm đảm bảo độ sẵn sàng cao (HA). Tất cả lưu lượng truy cập Internet của các site phụ đều được định tuyến đi qua mạng của trụ sở chính để tập trung quản lý và kiểm soát bảo mật.

Phần mềm và dịch vụ: Bệnh viện sử dụng kết hợp giữa **phần mềm có bản quyền** và **phần mềm mã nguồn mở**, bao gồm các hệ thống chuyên dụng như **HIS**, **RIS/PACS**, **LIS**, **CRM**, cùng các ứng dụng văn phòng, cơ sở dữ liệu, phần mềm client–server, và các ứng dụng đa phương tiện.

Yêu cầu kỹ thuật: Hệ thống phải có khả năng **mở rộng linh hoạt**, **bảo mật cao** (firewall, IDS/IPS, phát hiện phishing), **độ sẵn sàng cao (HA)**, và **khả năng khôi phục nhanh** khi xảy ra sự cố. Đồng thời phải đảm bảo **dễ nâng cấp** và **quản lý tập trung**.

An ninh và kết nối VPN: Mạng cần được cấu hình **VPN site-to-site** giữa các cơ sở, và **VPN truy cập từ xa (teleworker)** cho nhân viên có thể làm việc ngoài bệnh viện nhưng vẫn truy cập vào mạng LAN nội bộ một cách an toàn.

Hệ thống giám sát (Surveillance System): Đề xuất triển khai hệ thống **camera giám sát IP** toàn bệnh viện, kết nối vào VLAN riêng (Camera VLAN), lưu trữ tại **máy chủ NVR** trong Data Center, đảm bảo an ninh vật lý và giám sát 24/7.

2.1.2 Mạng hệ thống tại các trụ sở khác

Cấu trúc: Mỗi trụ sở phụ (DBP và BHTQ) gồm **1 tòa nhà 2 tầng**. Tầng 1 có một **phòng IT** và một **phòng trung tâm cáp (Cabling Central Local)** để kết nối mạng nội bộ.

Quy mô hệ thống: Các site có quy mô nhỏ hơn, gồm khoảng **260 máy trạm**, **2 máy chủ**, và **từ 5 thiết bị mạng trở lên** (bao gồm router, switch, access point, firewall nội bộ).

Kết nối WAN: Hai site này được kết nối trực tiếp với **Main Site** thông qua **đường truyền thuê riêng (leased line)**. Các kết nối này được mã hóa bằng **VPN site-to-site**, giúp dữ liệu trao đổi giữa các cơ sở an toàn, tin cậy và được quản lý tập trung.

Kết nối Internet: Các site phụ không kết nối Internet trực tiếp; toàn bộ lưu lượng Internet được định tuyến qua Main Site để đảm bảo an toàn và giám sát thống nhất.

Bảo mật và vận hành: Các trụ sở phụ vẫn tuân thủ mô hình VLAN tương tự Main Site, sử dụng firewall/router có ACL để phân tách các vùng mạng (Admin, Doctor, Nurse, Guest, Server). Hệ thống DHCP/DNS có thể được cung cấp từ Main Site thông qua VPN, hoặc có server dự phòng cục bộ.

2.1.3 Thông lượng và tải của hệ thống

Hệ thống mạng của bệnh viện được thiết kế để đáp ứng nhu cầu truyền tải dữ liệu lớn và ổn định trong các khung giờ cao điểm. Theo ước tính, khoảng **80% tổng lưu lượng mạng** tập trung vào hai khung giờ **9h00–11h00** và **15h00–16h00**. Lưu lượng này được chia sẻ giữa **trụ sở chính (Main Site)** và **hai trụ sở phụ (DBP, BHTQ)** như sau:

- **Máy chủ (Servers):** Bao gồm các máy chủ cho cập nhật phần mềm, truy cập web, và cơ sở dữ liệu. Tổng lưu lượng ước tính khoảng **1000 MB/ngày tải xuống (download)** và **2000 MB/ngày tải lên (upload)**.
- **Máy trạm (Workstations):** Mỗi máy trạm phục vụ cho các tác vụ như duyệt web, tải tài liệu, và giao dịch với khách hàng hoặc bệnh nhân. Trung bình mỗi máy trạm có lưu lượng khoảng **500 MB/ngày tải xuống** và **100 MB/ngày tải lên**.
- **Thiết bị di động (Wi-Fi):** Các thiết bị của khách hàng truy cập mạng

Wi-Fi của bệnh viện (Guest VLAN) tạo ra lưu lượng khoảng **500 MB/ngày tải xuống**. Với các thông số trên, hệ thống mạng của bệnh viện có thể đáp ứng được nhu cầu truyền dữ liệu y tế (HIS, PACS, LIS), truy cập Internet, và dịch vụ nội bộ mà không xảy ra tắc nghẽn trong giờ cao điểm.

2.1.4 Quy mô phát triển của hệ thống

Hệ thống mạng của bệnh viện được thiết kế với khả năng mở rộng linh hoạt, cho phép bổ sung thiết bị, người dùng và dịch vụ trong tương lai mà không cần thay đổi cấu trúc mạng lõi. Theo dự báo, hệ thống sẽ có tốc độ tăng trưởng trung bình khoảng **20% trong vòng 5 năm**.

2.2 Checklist khảo sát địa điểm

Dùng checklist này khi đi khảo sát địa điểm để thu thập dữ liệu vật lý và kỹ thuật cần thiết trước khi triển khai thiết kế mạng.

- **Thông tin chung**
  - Bản vẽ kiến trúc tòa nhà có kích thước chính xác.
  - Xác định vị trí **Data Center**, **IT Room**, và **Cabling Central Local** (kèm khoảng cách đến tòa A và B).
  - Bản đồ hành lang, phòng kỹ thuật, và lối đi cáp.
- **Về cáp và lắp đặt**
  - Đo khoảng cách từ **IDF** mỗi tầng đến **MDF/Data Center**.
  - Xác định đường đi của cáp ngầm hoặc ống bảo vệ dây, cùng với các điểm đầu và điểm cuối nơi cáp hoặc ống ra - vào.
  - Kiểm tra loại cáp hiện có (Cat5e/Cat6/Fiber) và tình trạng thực tế.
  - Ghi nhận vị trí **patch panels**, **racks**, **PDU**, và **UPS** ở mỗi IDF/MDF.
- **Về nguồn và môi trường**
  - Kiểm tra số lượng ổ cắm điện, mạch điện và khả năng dự phòng **UPS** cho thiết bị mạng.

  - Xác định hệ thống điều hòa (**CRAC**) cho Data Center.
  - Đánh giá khả năng lắp đặt hệ thống làm mát hoặc tản nhiệt cho server.
  - Kiểm tra vị trí lắp đặt **CCTV** và mức độ bảo mật vật lý tại các phòng kỹ thuật.

- **Về thiết bị và yêu cầu hoạt động**
  - Thống kê chính xác số lượng **workstation**, **server**, và **thiết bị y tế** trong từng phòng.
  - Ghi nhận yêu cầu **QoS** cho các dịch vụ như **Voice (VoIP)**, **PACS (DICOM)**, và **thiết bị y tế có truyền dữ liệu (telemetry)**.
  - Xem xét các yêu cầu pháp lý hoặc tiêu chuẩn bảo mật tương tự **HIPAA**.

- **Về wireless và hành vi người dùng**
  - Xác định các khu vực cần phủ sóng Wi-Fi (hành lang, phòng chờ, phòng khám, hội trường...).
  - Ước tính số lượng người dùng tối đa đồng thời trong từng khu vực (đặc biệt sảnh và hội trường).
  - Xác định vị trí dự kiến đặt **Access Points (APs)** và nguồn cấp điện qua **PoE**.

- **Về kết nối WAN và ISP**
  - Thu thập thông tin về kết nối Internet hiện có và nhà cung cấp dịch vụ (ISP) đang sử dụng.
  - Kiểm tra khả năng triển khai **leased line**, **MPLS**, hoặc **SD-WAN**.
  - Xác định vị trí **demarcation point** (điểm bàn giao đường truyền của ISP).

- **Về bảo mật và quản trị**
  - Ghi nhận vị trí khóa và biện pháp kiểm soát truy cập vật lý tới phòng IT hoặc Data Center.
  - Thống kê số lượng nhân viên IT, ca trực và quy trình xử lý sự cố.

- Xác định chính sách **backup**, lưu trữ log (**log retention**) và hệ thống chứng thực (**AD/RADIUS**).

2.3 Xác định khu vực có tải cao và cấu hình thiết bị phù hợp

Trong hệ thống mạng của bệnh viện, lưu lượng (network load) không được phân bố đồng đều giữa các khu vực. Một số khu vực có lưu lượng truy cập, trao đổi dữ liệu và yêu cầu dịch vụ cao hơn bình thường, được xác định là **khu vực tải cao (high-load areas)**. Việc xác định đúng các khu vực này giúp lựa chọn cấu hình thiết bị phù hợp, cũng như xác định vị trí đặt **load balancer** để đảm bảo hiệu suất và độ ổn định cho toàn hệ thống.

- **Trung tâm dữ liệu (Data Center / Server Farm):** Đây là khu vực có tải cao nhất trong toàn hệ thống, nơi đặt các máy chủ HIS, PACS, LIS, Database, và các dịch vụ web nội bộ. Lưu lượng lớn bao gồm truy cập cơ sở dữ liệu, sao lưu dữ liệu (backup), và đồng bộ file ảnh y khoa (DICOM).
  - Thiết bị khuyến nghị: Core Switch 10/40 GbE, Firewall thế hệ mới (NGFW), IDS/IPS, Load Balancer.
  - Tối ưu bằng: cân bằng tải cho dịch vụ web/HIS, VLAN riêng cho Server Farm, uplink 10 Gbps hoặc cao hơn.
- **Khoa Chẩn đoán hình ảnh (Radiology / PACS Room):** Đây là khu vực sinh ra nhiều dữ liệu dung lượng lớn từ thiết bị CT, MRI, X-ray. Cần đường truyền nội bộ tốc độ cao và QoS ưu tiên.
  - Thiết bị khuyến nghị: Distribution Switch 10 GbE, hỗ trợ QoS, buffer lớn.
  - Tối ưu bằng: VLAN riêng cho PACS, QoS mức cao (AF41–42) cho gói tin DICOM.
- **Phòng Xét nghiệm (Laboratories):** Lưu lượng tập trung vào trao đổi kết quả xét nghiệm, đồng bộ mẫu và kết nối thiết bị phân tích tự động.

  - Thiết bị khuyến nghị: Access Switch PoE+ hỗ trợ thiết bị y tế IoT, uplink 1 GbE.
  - Tối ưu bằng: VLAN riêng, ACL hạn chế truy cập ra ngoài Server Farm.

- **Khu hành chính và quản lý (Administrative Area):** Lưu lượng chủ yếu từ dịch vụ văn phòng, mail, web và truy cập hệ thống quản trị nội bộ.
  - Thiết bị khuyến nghị: Access Switch 1 GbE, hỗ trợ segmentation và QoS trung bình.
  - Tối ưu bằng: QoS mức trung bình, NAT và ACL kiểm soát truy cập.

- **Hệ thống giám sát (CCTV / NVR System):** Các camera IP gửi luồng video liên tục về máy chủ NVR trong Data Center, tạo tải mạng cao ổn định.
  - Thiết bị khuyến nghị: Switch PoE+ riêng cho Camera VLAN, uplink 10 GbE đến NVR.
  - Tối ưu bằng: VLAN riêng cho camera, lưu lượng không đi qua core LAN chính.

- **Khu vực Wi-Fi công cộng (Guest / Lobby):** Đây là khu vực có số lượng thiết bị di động truy cập cao và biến động. Cần phân tách VLAN, giới hạn tốc độ (rate-limiting) và cân bằng tải truy cập giữa các AP.
  - Thiết bị khuyến nghị: WLAN Controller + AP 802.11ac/ax, hỗ trợ band steering và load balancing.
  - Tối ưu bằng: VLAN riêng cho khách, chặn truy cập nội bộ, băng thông giới hạn.

Các thiết bị **load balancer** nên được bố trí tại:

- Trước cụm máy chủ HIS/Web (phân tải ứng dụng nội bộ).
- Tại biên mạng (Internet Edge) để chia tải giữa hai đường DSL.
- Giữa các vùng DMZ–LAN nếu có nhiều ứng dụng public-facing.

2.4 Cấu trúc mạng và thiết kế môi trường không dây

Mạng của bệnh viện được thiết kế dựa trên kiến trúc tòa nhà (hai tòa A và B, mỗi tòa 5 tầng, 10 phòng/tầng) với tiêu chí **tiện lợi, thẩm mỹ và khả năng bảo trì dễ dàng**. Hệ thống bao gồm cả **mạng có dây (wired)** và **mạng không dây (wireless)** với hạ tầng tốc độ cao, tuân thủ tiêu chuẩn an ninh mạng hiện đại.

- **Cấu trúc mạng (Network Topology):**
  - Áp dụng mô hình **3 tầng (Three-Tier Architecture)** gồm:
    - **Access Layer:** Switch PoE đặt tại mỗi tầng, kết nối máy trạm, điện thoại IP, camera, và Access Point.
    - **Distribution Layer:** Thiết bị gom uplink từ các tầng, thực hiện định tuyến nội bộ VLAN và lọc lưu lượng (ACL, QoS).
    - **Core Layer:** Đặt tại Data Center, đảm nhiệm chuyển mạch tốc độ cao và định tuyến giữa các VLAN, kết nối WAN/Internet.
  - Liên kết giữa Distribution và Core sử dụng đường truyền **10 Gbps** hoặc **40 Gbps**.
  - Hệ thống cáp chính sử dụng **cáp quang (Fiber)** và **Cat6/Cat6A** trong tòa nhà.
- **Phân vùng và bảo mật mạng (Network Partitioning and Security):**
  - Các VLAN được thiết kế tách biệt theo phòng ban và mục đích sử dụng:
    - **VLAN 10:** Lễ tân.
    - **VLAN 20:** Hành chính và kế toán.
    - **VLAN 30:** An ninh và bảo trì.
    - **VLAN 40:** Quản lý và kỹ thuật.
    - **VLAN 50:** Hội thảo và tập huấn.
    - **VLAN 60:** Quản lý hồ sơ.
    - **VLAN 70:** Kho thuốc.
    - **VLAN 80:** Ban điều hành.

        * **VLAN 90:** Khoa cấp cứu
        * **VLAN 100:** Khoa chẩn đoán hình ảnh.
        * **VLAN 110:** Khoa vật lý trị liệu.
        * **VLAN 120:** Khoa phẫu thuật.
        * **VLAN 130:** Điều trị nội trú.
        * **VLAN 140:** Điều trị đặc biệt.
        * **VLAN 150:** Các phòng nghiên cứu.
        * **VLAN 160:** SERVER_FARM.
        * **VLAN 170:** DMZ SERVER.
        * **VLAN 180:** GUEST.
    - **DMZ Zone:** dành cho máy chủ web, VPN gateway, mail relay.
    - **Firewall:** được đặt tại biên (Edge) giữa Core và Internet để kiểm soát toàn bộ lưu lượng.
    - **IDS/IPS:** hoạt động song song với firewall để phát hiện và ngăn chặn tấn công.
    - **VPN site-to-site:** bảo mật kết nối giữa Main Site và các site phụ (DBP, BHTQ).

- **Mạng không dây (Wireless Network):**
    - Phủ sóng toàn bộ hai tòa nhà A và B bằng các **Access Point** hỗ trợ chuẩn **802.11ac/ax**.
    - Sử dụng mô hình **Controller-based Wi-Fi**, có khả năng quản lý tập trung, cân bằng tải (load balancing) giữa các AP.
    - **SSID phân tách:**
        * **Hospital-Staff:** bảo mật WPA2/WPA3-Enterprise, xác thực 802.1X với RADIUS.
        * **Hospital-Guest:** captive portal, VLAN riêng biệt, giới hạn tốc độ.
    - Các AP được cấp nguồn qua **PoE** từ Access Switch, lắp đặt dọc hành lang để phủ đều sóng.

  - Hỗ trợ **roaming liền mạch** (802.11r/k/v) cho nhân viên di chuyển giữa các tầng.

- **Tiêu chí thẩm mỹ và vận hành:**
  - Phòng kỹ thuật (IDF) bố trí gần thang máy để tối ưu chiều dài cáp.
  - Dây mạng đi trong ống dẫn hoặc máng cáp có dán nhãn theo chuẩn.
  - Dùng **PoE** cho camera và AP để giảm ổ cắm điện, tăng tính thẩm mỹ.
  - Tất cả thiết bị được gắn nhãn rõ ràng (Building–Floor–Room–Port).

Cấu trúc mạng trên giúp đảm bảo hiệu năng, bảo mật, khả năng mở rộng và tính thẩm mỹ của hệ thống, đồng thời đáp ứng yêu cầu vận hành 24/7 của bệnh viện hiện đại.

3 Thiết kế hạ tầng mạng và kết nối WAN

3.1 Danh sách thiết bị

Dựa trên mô hình mạng 3 lớp (Access – Distribution – Core) và yêu cầu kết nối giữa Trụ sở chính và hai chi nhánh (DBP, BHTQ), hệ thống cần các thiết bị mạng có hiệu năng cao, hỗ trợ VLAN, PoE, SD-WAN, tường lửa, và cân bằng tải.

Loại thiết bị	Số lượng	Vị trí triển khai	Chức năng chính	Thông số đề xuất
Core Switch	2	Data Center	Thiết bị chuyển mạch lõi, định tuyến giữa các VLAN, kết nối WAN/Internet	Cisco Catalyst 9500, uplink 40Gbps
Distribution Switch	8	Mỗi tòa nhà A và B (2 switch/tầng)	Gom uplink từ các tầng, thực hiện định tuyến nội bộ	Cisco Catalyst 9300, uplink 10Gbps
Access Switch (PoE+)	20	Mỗi tầng các tòa nhà	Kết nối trực tiếp máy trạm, camera, điện thoại IP và Access Point	Cisco Catalyst 9200, 48 port, PoE+
Router WAN/Edge	3	Main Site và hai chi nhánh	Định tuyến WAN, kết nối leased line/MPLS, hỗ trợ SD-WAN	Cisco ISR 4451-X
Firewall NGFW	2	Main Site (Edge và Internal Zone)	Kiểm soát truy cập, bảo vệ mạng, chống tấn công	FortiGate 100F hoặc Cisco ASA 5506-X

Loại thiết bị	Số lượng	Vị trí triển khai	Chức năng chính	Thông số đề xuất
Load Balancer	2	Data Center	Phân phối tải truy cập giữa các máy chủ HIS/Web	F5 BIG-IP hoặc Cisco ACE
Wireless Controller	1	Data Center	Quản lý tập trung các Access Point và SSID	Cisco 9800-L
Access Point	30	Tòa A và B, hành lang, phòng chờ	Phủ sóng Wi-Fi toàn bộ khu vực	Cisco 2800/3800, chuẩn 802.11ac/ax
Server (HIS, PACS, LIS, CRM, NVR...)	10	Data Center	Chạy các dịch vụ nghiệp vụ và hệ thống y tế	Dell PowerEdge R740
UPS, Rack, Patch Panel	—	IT Room, Cabling Central	Cấp nguồn dự phòng và quản lý cáp mạng	APC 3kVA, Rack 42U
Camera IP	60	Toàn bệnh viện	Giám sát an ninh, lưu trữ tại NVR Server	Hỗ trợ PoE, RTSP, 1080p
Hệ thống cáp mạng	—	Toàn hệ thống	Kết nối LAN/WAN nội bộ, uplink backbone	Cat6A và Fiber OM3 (1/10/40Gbps)

Bảng 2: Danh sách thiết bị đề xuất cùng chức năng và thông số kỹ thuật tiêu biểu

Hệ thống được thiết kế có khả năng mở rộng trong 5 năm, đảm bảo an toàn và dự phòng ở tầng Core và Distribution, hỗ trợ hoạt động 24/7.

3.2 Sơ đồ IP

Hệ thống mạng sử dụng mô hình phân vùng VLAN nhằm tách biệt lưu lượng giữa các phòng ban, nâng cao hiệu năng và bảo mật. Mô hình này đảm bảo việc quản lý IP tập trung, tránh xung đột địa chỉ, đồng thời dễ dàng cấu hình định tuyến (OSPF) giữa các VLAN và các chi nhánh.

3.2.1 Khu vực chính

Sơ đồ VLAN tòa A

VLAN	Tên khu vực	Phòng	Tầng	Số máy	Subnet	Dải địa chỉ
10	Lễ tân	1 - 4	1	24	192.168.1.0/26	192.168.1.1 - 192.168.1.62
20	Hành chính và kế toán	6 - 10	1	36	192.168.1.64/26	192.168.1.65 - 192.168.1.126
30	An ninh và bảo trì	1 - 5	2	30	192.168.2.0/26	192.168.2.1 - 192.168.2.62
40	Quản lý và kỹ thuật	6 - 10	2	30	192.168.2.64/26	192.168.2.65 - 192.168.2.126
50	Hội thảo và tập huấn	1 - 5	3	50	192.168.3.0/26	192.168.3.1 - 192.168.3.62
60	Quản lý hồ sơ	6 - 10	3	10	192.168.3.64/26	192.168.3.65 - 192.168.3.126
70	Kho thuốc	1 - 10	4	60	192.168.4.0/26	192.168.4.1 - 192.168.4.62
80	Ban điều hành	1 - 10	5	60	192.168.5.0/26	192.168.5.1 - 192.168.5.62

Bảng 3: Kế hoạch quy hoạch địa chỉ IP cho tòa A

Sơ đồ VLAN tòa B

VLAN	Tên khu vực	Phòng	Tầng	Số máy	Subnet	Dải địa chỉ
90	Khoa cấp cứu	1 - 5	1	30	192.168.11.0/26	192.168.11.1 - 192.168.11.62
100	Khoa chẩn đoán hình ảnh	6 - 10	1	30	192.168.11.64/26	192.168.11.65 - 192.168.11.126
110	Khoa vật lý trị liệu	1 - 5	2	30	192.168.12.0/26	192.168.12.1 - 192.168.12.62
120	Khoa phẫu thuật	6 - 10	2	30	192.168.12.64/26	192.168.12.65 - 192.168.12.126
130	Điều trị nội trú	1 - 10	3	60	192.168.13.0/26	192.168.13.1 - 192.168.13.62
140	Điều trị đặc biệt	1 - 10	4	60	192.168.14.0/26	192.168.14.1 - 192.168.14.62
150	Các phòng nghiên cứu	1 - 10	5	60	192.168.15.0/26	192.168.15.1 - 192.168.15.62

Bảng 4: Kế hoạch quy hoạch địa chỉ IP cho tòa B

Sơ đồ VLAN khu vực trung tâm dữ liệu

VLAN	Tên khu vực	Số máy	Subnet	Dải địa chỉ
160	SERVER_FARM	5	192.168.16.0/29	192.168.16.1 - 192.168.16.7
170	DMZ SERVER	3	192.168.17.0/29	192.168.17.1 - 192.168.17.7

VLAN	Tên khu vực	Số máy	Subnet	Dải địa chỉ
180	GUEST	—	192.168.96.0/20	192.168.96.1 - 192.168.111.255

Bảng 5: Kế hoạch quy hoạch địa chỉ IP cho khu vực trung tâm dữ liệu

Sơ đồ IP giữa Distribution Layer và Core Layer

Kết nối	Subnet
DS-A ⟷ CORE-SW1	192.168.6.0/30
DS-A ⟷ CORE-SW2	192.168.6.4/30
DS-B ⟷ CORE-SW1	192.168.6.8/30
DS-B ⟷ CORE-SW2	192.168.6.12/30

Bảng 6: Sơ đồ IP giữa Distribution Layer và Core Layer

Sơ đồ IP giữa Core Layer, Server và FireWall

Kết nối	Subnet
DS-DC-1 ⟷ CORE-SW1	192.168.6.0/30
DS-DC-1 ⟷ CORE-SW2	192.168.6.4/30
DS-DC-2 ⟷ FIREWALL-1	192.168.6.24/30
DS-DC-2 ⟷ FIREWALL-2	192.168.6.28/30
CORE-SW1 ⟷ FIREWALL-1	192.168.6.32/30
CORE-SW1 ⟷ FIREWALL-2	192.168.6.36/30
CORE-SW2 ⟷ FIREWALL-1	192.168.6.40/30
CORE-SW2 ⟷ FIREWALL-2	192.168.6.44/30

Bảng 7: Sơ đồ IP giữa Core Layer, Server và Firewall

Sơ đồ IP giữa Firewall và Router

Kết nối	Subnet
FIREWALL-1 ⟷ RTR-MAIN1	192.168.7.0/30
FIREWALL-1 ⟷ RTR-MAIN2	192.168.7.8/30
FIREWALL-1 ⟷ CORE-SW3	192.168.7.16/30
FIREWALL-2 ⟷ RTR-MAIN1	192.168.7.4/30
FIREWALL-2 ⟷ RTR-MAIN2	192.168.7.12/30
FIREWALL-2 ⟷ CORE-SW3	192.168.7.20/30

Bảng 8: Sơ đồ IP giữa Firewall và Router

3.2.2 Khu vực phụ

Sơ đồ VLAN khu vực DBP

VLAN	Tên khu vực	Tầng	Số máy	Subnet	Dải địa chỉ
10	Lễ tân	1	60	192.168.18.0/26	192.168.18.1 - 192.168.18.62
20	Phòng server	1	60	192.168.18.64/26	192.168.18.65 - 192.168.18.126
30	Phòng khám bệnh	2	60	192.168.18.128/26	192.168.18.129 - 192.168.18.190
40	Phòng bệnh	2	60	192.168.18.192/26	192.168.18.193 - 192.168.18.254

Bảng 9: Kế hoạch quy hoạch địa chỉ IP cho khu vực DBP

Sơ đồ VLAN khu vực BHTQ

VLAN	Tên khu vực	Tầng	Số máy	Subnet	Dải địa chỉ
10	Lễ tân	1	60	192.168.19.0/26	192.168.19.1 - 192.168.19.62
20	Phòng server	1	60	192.168.19.64/26	192.168.19.65 - 192.168.19.126
30	Phòng khám bệnh	2	60	192.168.19.128/26	192.168.19.129 - 192.168.19.190
40	Phòng bệnh	2	60	192.168.19.192/26	192.168.19.193 - 192.168.19.254

Bảng 10: Kế hoạch quy hoạch địa chỉ IP cho khu vực BHTQ

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

3.3.1 Lựa chọn công nghệ WAN

Để đảm bảo tính ổn định, bảo mật và khả năng mở rộng cho hệ thống bệnh viện, mô hình WAN được thiết kế theo hướng kết hợp giữa GRE Tunnel VPN và OSPF Dynamic Routing Protocol, cụ thể:

- GRE (Generic Routing Encapsulation) Tunnel VPN:
  - Tạo kênh truyền ảo bảo mật giữa Main Site (trung tâm) và hai Auxiliary Sites (DBP và BHTQ).
  - Cho phép đóng gói (encapsulation) toàn bộ gói tin IP nội bộ để truyền qua môi trường Internet công cộng mà vẫn giữ được cấu trúc mạng LAN.
  - Ưu điểm: Dễ cấu hình, linh hoạt, hỗ trợ nhiều giao thức định tuyến, và hoạt động ổn định ngay cả khi có NAT giữa các router.

- OSPF (Open Shortest Path First):
  - Được triển khai bên trong GRE Tunnel để duy trì bảng định tuyến động giữa các site.
  - Cho phép tự động lựa chọn đường đi ngắn nhất và cập nhật khi có thay đổi về topology mạng.
  - Giúp tối ưu hiệu suất, giảm độ trễ, và đảm bảo khả năng mở rộng khi thêm chi nhánh mới trong tương lai.

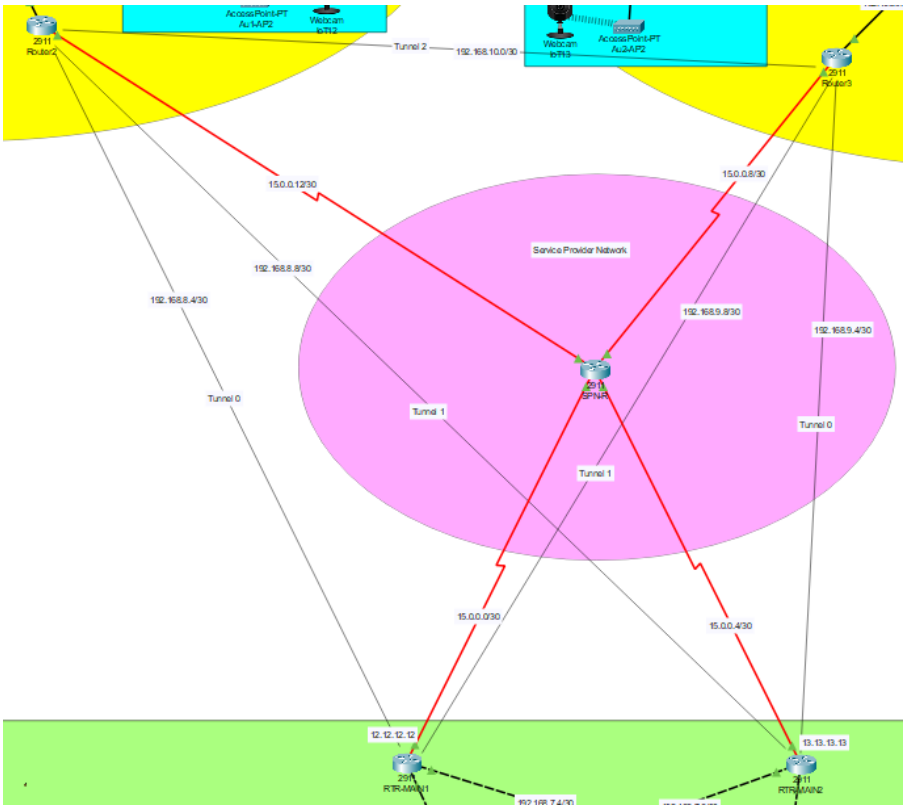
Ngoài ra, bệnh viện có thể xem xét áp dụng MPLS hoặc SD-WAN trong giai đoạn mở rộng, nhằm cải thiện hiệu suất định tuyến, giám sát tập trung, và tăng cường QoS cho các dịch vụ quan trọng như HIS, LIS, PACS,...

3.3.2 Cấu trúc kết nối tổng thể

Kết nối giữa Main Site và hai chi nhánh được xây dựng theo mô hình hub-and-spoke:

- Main Site đóng vai trò hub, nơi đặt các máy chủ chính (HIS, Database, Mail, DNS, Web, File).
- Hai Auxiliary Sites (ĐBP và BHTQ) đóng vai trò spoke, kết nối đến hub qua đường hầm GRE.

Mỗi site phụ có một router cục bộ kết nối với router SPN trung tâm của bệnh viện. Router tại SPN có nhiệm vụ tổng hợp lưu lượng WAN và định tuyến đến router tại Main Site thông qua đường leased line.



Hình 1: Sơ đồ kết nối WAN giữa Main Site và các Auxiliary Sites qua GRE Tunnel VPN

3.3.3 Cấu hình GRE Tunneling

GRE tạo ra một "đường hầm ảo" (virtual tunnel) giữa hai router, giúp mạng ở hai đầu hoạt động như thể đang cùng trong một mạng LAN.

1. Cấu hình GRE Tunnel ở trụ sở chính và hai chi nhánh.

    - Cấu hình ở RTR-MAIN1 router đến Au1-Router router (Tunnel 0): 192.168.8.4/30
    - Cấu hình ở RTR-MAIN1 router đến Au2-Router router (Tunnel 1): 192.168.9.8/30
    - Cấu hình ở RTR-MAIN2 router đến Au2-Router router (Tunnel 0): 192.168.9.4/30
    - Cấu hình ở RTR-MAIN2 router đến Au1-Router router (Tunnel 1): 192.168.8.8/30

2. Cấu hình GRE Tunnel ở chi nhánh DBP với BHTQ.

    - Cấu hình ở Au1-Router router đến Au2-Router router (Tunnel 2): 192.168.10.0/30

3.3.4 Mô tả hoạt động và cơ chế bảo mật

- Khi một máy trạm ở DBP gửi gói tin đến Database Server tại Main Site, gói tin sẽ được router tại DBP đóng gói trong GRE tunnel, mã hóa bởi cơ chế VPN, và gửi đến router tại Main Site.
- Tại Main Site, router giải mã gói tin và chuyển tiếp đến server nội bộ tương ứng.
- Các đường tunnel hoạt động song song, có thể định tuyến dự phòng hoặc cân bằng tải (load balancing) tùy theo chính sách OSPF (Equal-cost multipath routing).
- Bảo mật được tăng cường bằng việc kết hợp IPSec encryption trên tunnel, đảm bảo dữ liệu y tế được bảo vệ tuyệt đối khi truyền qua Internet công cộng.

4 Tính toán lưu lượng

Theo yêu cầu đề bài, ta có:

- Hệ thống đạt cao điểm ở 80% lưu lượng cả ngày vào các khung giờ từ 9 - 11 giờ sáng và từ 15 - 16 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:

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

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

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

Do 80% tổng lưu lượng cả ngày đến trong 3 tiếng cao điểm (9 - 11 giờ sáng, 15 - 16 giờ chiều) nên ta có thể suy ra được bandwidth của server:

$$\frac{(1000 + 2000) \times 10 \times 0.8}{3} \times \frac{8}{3600} \approx 17.78\text{(Mbps)}$$

Throughput của các workstation là:

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

Bandwidth cho các workstation:

$$\frac{600 \times 600 \times 0.8}{3} \times \frac{8}{3600} \approx (213.33\text{Mbps})$$

Throughput của các thiết bị kết nối wifi:

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

Bandwidth của các thiết bị kết nối wifi:

$$\frac{500 \times 0.8 \times 8}{3 \times 3600} \approx 0.30(\text{Mbps})$$

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 cần khoảng $231.41 \times 1.2 = 277.70(\text{Mbps})$.

4.2 Khu vực phụ

Ta có công thức:

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

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

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

Do 80% tổng lưu lượng cả ngày đến trong 3 tiếng cao điểm (9 - 11 giờ sáng, 15 - 16 giờ chiều) nên ta có thể suy ra được bandwidth của server:

$$\frac{(1000 + 2000) \times 2 \times 0.8}{3} \times \frac{8}{3600} \approx 3.56(\text{Mbps})$$

Throughput của các workstation là:

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

Bandwidth cho các workstation:

$$\frac{600 \times 60 \times 0.8}{3} \times \frac{8}{3600} \approx (21.33\text{Mbps})$$

Throughput của các thiết bị kết nối wifi:

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

Bandwidth của các thiết bị kết nối wifi:

$$\frac{500 \times 0.8 \times 8}{3 \times 3600} \approx 0.30(\text{Mbps})$$

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

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

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 cần khoảng $25.19 \times 1.2 = 30.23(\text{Mbps})$.

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 khoảng $277.7 + 30.23 \times 2 \approx 338.16$(Mbps).

4.4 Cấu hình mạng đề xuất

4.4.1 Đề xuất băng thông kết nối

Để đảm bảo hoạt động ổn định và có khả năng mở rộng, trụ sở chính nên sử dụng:

- Đường Internet chính (Primary): 1 Gbps (đối xứng).
- Đường Internet dự phòng (Secondary): 500 Mbps, cấu hình cân bằng tải (load balancing) và tự động chuyển mạch dự phòng (failover).
- Đường WAN (Main $\leftrightarrow$ DBP, BHTQ): tối thiểu 200 Mbps cho mỗi đường thuê riêng (leased line), có thể triển khai SD-WAN hoặc MPLS.

4.4.2 Kết nối WAN

Hệ thống sử dụng công nghệ SD-WAN để đảm bảo băng thông tổng tối thiểu 340 Mbps, hỗ trợ quản lý lưu lượng và tối ưu định tuyến giữa các site.

4.4.3 Mạng nội bộ

Khu vực chính: sử dụng các switch 10 GbE cho các kết nối trong hệ thống nhằm bảo đảm lưu lượng thông suốt giữa các thiết bị.

Khu vực phụ: sử dụng switch 1 GbE, đủ đáp ứng nhu cầu truyền tải nội bộ và kết nối WAN.

4.4.4 Mạng không dây

Hệ thống Wi-Fi được triển khai theo chuẩn Wi-Fi 6 (802.11ax), giúp tăng tốc độ, giảm độ trễ và hỗ trợ chuyển vùng liền mạch (roaming). Đồng thời, áp dụng QoS để ưu tiên băng thông cho các ứng dụng nghiệp vụ quan trọng như HIS, PACS, CRM.

5 Thiết kế sơ đồ mạng với Packet Tracer

Sau khi đã thiết lập và nối dây tất cả thiết bị với nhau, ta tiến hành cấu hình cho từng thiết bị.

5.1 Cấu hình khởi tạo cho thiết bị

Cấu hình này cho các Router, Layer 3 Switch ở các tầng Distribution, Core và các biên của các khu vực.

Listing 1: Cấu hình SSH

```
enable
configure terminal
hostname DS-A
ip domain name AKAZA.net
username admin password
crypto key generate rsa
1024
line vty 0 15
login local
ip ssh version 2
```

5.2 Cấu hình VLAN trunking

5.2.1 Cấu hình cho Layer 2 Switch

Hệ thống một tòa ở khu vực chính bao gồm 5 tầng với khoảng 300 máy trạm, nên trung bình mỗi tầng khoảng 60 máy trạm. Do đó, ở đây ta cần 3 Layer 2 Switch cho mỗi tầng.

Listing 2: Cấu hình Layer 2 Switch

```
enable
configure terminal
hostname SW-A1-01
```

```
vlan 10
name Letan
interface range fa0/1-24
switchport mode access
switchport access vlan 10
```

5.2.2 Cấu hình cho Layer 3 Switch

Ở tầng Distribution, ta dùng hai Layer 3 Switch cho mỗi tòa.

Listing 3: Cấu hình Layer 3 Switch

```
enable
configure terminal
hostname DS-A
vlan 10
name Letan
...
interface range fa0/1-24
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,...,180
```

5.3 Cấu hình Subneting

Ở đường nối các Router với Router, Layer 3 Switch với Layer 3 Switch và Router với Layer 3 Switch, ta gán địa chỉ IP cho các cổng.

Listing 4: Cấu hình địa chỉ IP

```
enable
configure terminal
hostname DS-A
interface gi0/1
ip address 192.168.6.1 255.255.255.252
```

```
no shutdown
```

5.4 Cấu hình OSPF

Ở các Router, Layer 3 Switch ta cần cấu hình để chúng trao đổi thông tin chính xác với nhau.

Listing 5: Cấu hình OSPF cho Layer 3 Switch

```
enable
configure terminal
hostname DS-A
router ospf 1
router-id 3.3.3.3
network 192.168.6.0 0.0.0.3 area 0
network 192.168.6.4 0.0.0.3 area 0
network 192.168.1.0 0.0.0.63 area 0
network 192.168.1.64 0.0.0.63 area 0
network 192.168.2.0 0.0.0.63 area 0
network 192.168.2.64 0.0.0.63 area 0
network 192.168.3.0 0.0.0.63 area 0
network 192.168.3.64 0.0.0.63 area 0
network 192.168.4.0 0.0.0.63 area 0
network 192.168.5.0 0.0.0.63 area 0
network 192.168.96.0 0.0.15.255 area 0
```

Riêng với Firewall, ta cần thay Wild Card Mask thành Subnet Mask.

Listing 6: Cấu hình OSPF cho Firewall

```
enable
configure terminal
hostname FIREWALL-1
router ospf 1
router-id 10.10.10.10
log-adjacency-changes
```

```
network 192.168.7.0 255.255.255.252 area 0
network 192.168.7.8 255.255.255.252 area 0
network 192.168.7.16 255.255.255.252 area 0
network 192.168.6.24 255.255.255.252 area 0
network 192.168.6.32 255.255.255.252 area 0
network 192.168.6.40 255.255.255.252 area 0
```

5.5 Cấu hình DHCP Server

Ta tiến hành cấu hình DHCP để tự động cấp IP cho các thiết bị kết nối.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User
VLAN 180	192.168.96.1	192.168.17.3	192.168.96.2	255.255.240.0	3000
VLAN 150	192.168.15.1	192.168.17.3	192.168.15.2	255.255.255.192	60
VLAN 140	192.168.14.1	192.168.17.3	192.168.14.2	255.255.255.192	60
VLAN 130	192.168.13.1	192.168.17.3	192.168.13.2	255.255.255.192	60
VLAN 120	192.168.12.65	192.168.17.3	192.168.12.66	255.255.255.192	60
VLAN 110	192.168.12.1	192.168.17.3	192.168.12.2	255.255.255.192	60
VLAN 100	192.168.11.65	192.168.17.3	192.168.11.66	255.255.255.192	60
VLAN 90	192.168.11.1	192.168.17.3	192.168.11.2	255.255.255.192	60
VLAN 80	192.168.5.1	192.168.17.3	192.168.5.2	255.255.255.192	60
VLAN 70	192.168.4.1	192.168.17.3	192.168.4.2	255.255.255.192	60
VLAN 60	192.168.3.65	192.168.17.3	192.168.3.66	255.255.255.192	60
VLAN 50	192.168.3.1	192.168.17.3	192.168.3.2	255.255.255.192	60

Hình 2: Cấu hình DHCP cho Main Site

5.6 Cấu hình chuyển tiếp DHCP

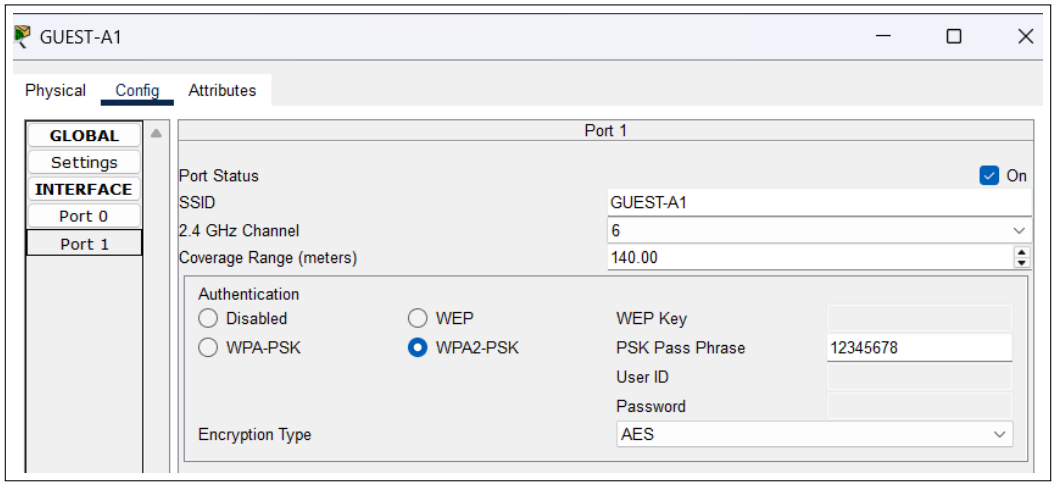
Ta tiến hành cấu hình các Layer 3 Switch ở tầng Distribution để hỗ trợ cấp IP thông qua DHCP.

Listing 7: Cấu hình chuyển tiếp DHCP cho Layer 3 Switch

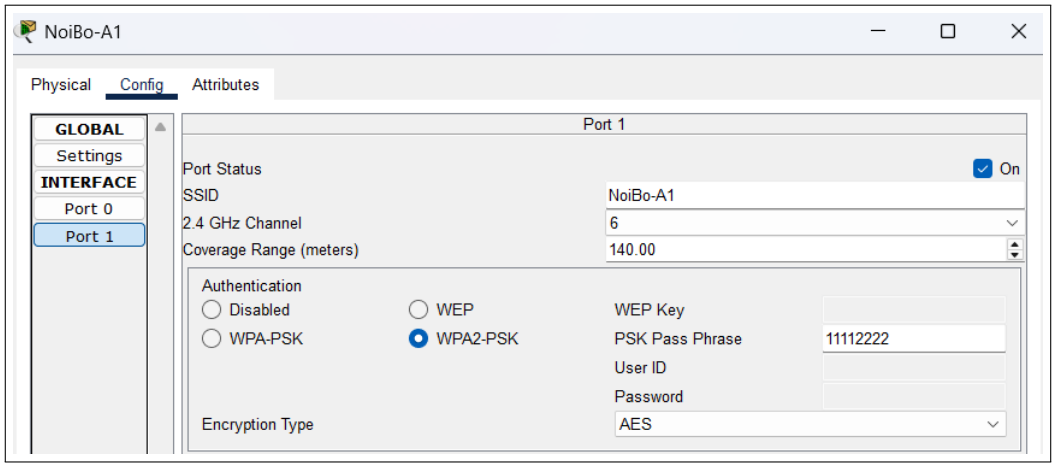
```
enable
configure terminal
hostname DS-A
interface vlan 10
ip address 192.168.1.1 255.255.255.192
ip helper-address 192.168.16.2
...
interface vlan 180
ip address 192.168.96.1 255.255.240.0
ip helper-address 192.168.16.2
```

5.7 Cấu hình Wireless

Ta tiến hành cấu hình wireless cho các Access Point. Ở trụ sở chính, ta thiết lập một Access Point cho khách (GUEST) và một Access Point cho nội bộ sử dụng.



Hình 3: Cấu hình wireless cho khách



Hình 4: Cấu hình wireless cho nội bộ

5.8 Cấu hình ACL

Ta tiến hành cấu hình ACLs (Access-list) cho các Layer 3 Switch ở tầng Distribution để kiểm soát phạm vi truy cập.

Listing 8: Cấu hình ACL cho Layer 3 Switch

```
enable
configure terminal
hostname DS-A
ip access-list extended BLOCK_GUEST
permit udp 192.168.96.0 0.0.15.255 any eq bootpc
permit udp any 192.168.96.0 0.0.15.255 eq bootps
deny ip 192.168.96.0 0.0.15.255 192.168.1.0 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.1.64 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.2.0 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.2.64 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.3.0 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.3.64 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.4.0 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.5.0 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.11.0 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.11.64 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.12.0 0.0.0.63
```

```
deny ip 192.168.96.0 0.0.15.255 192.168.12.64 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.13.0 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.14.0 0.0.0.63
deny ip 192.168.96.0 0.0.15.255 192.168.15.0 0.0.0.63
permit ip 192.168.96.0 0.0.15.255 any
permit ip any any

interface vlan 180
ip access-group BLOCK_GUEST out
```

5.9 Cấu hình Firewall

Ta tiến hành cấu hình Firewall để kiểm soát lưu lượng mạng đi vào và đi ra.

Listing 9: Cấu hình Firewall

```
enable
configure terminal
hostname FIREWALL-1
interface GigabitEthernet1/1
nameif CORE-SW1
security-level 100
ip address 192.168.6.34 255.255.255.252
interface GigabitEthernet1/2
nameif CORE-SW2
security-level 100
ip address 192.168.6.42 255.255.255.252
interface GigabitEthernet1/3
nameif DS-DC-2
security-level 70
ip address 192.168.6.26 255.255.255.252
interface GigabitEthernet1/4
nameif RTR-MAIN1
security-level 70
```

```
ip address 192.168.7.1 255.255.255.252
interface GigabitEthernet1/5
nameif RTR-MAIN2
security-level 70
ip address 192.168.7.9 255.255.255.252
interface GigabitEthernet1/6
nameif CORE-SW3
security-level 0
ip address 192.168.7.17 255.255.255.252
```

5.10 Cấu hình NAT

Ta tiến hành cấu hình NAT cho các router đi ra Internet để chuyển địa chỉ riêng (private IP) thành địa chỉ công (public IP).

Listing 10: Cấu hình NAT cho router

```
enable
configure terminal
hostname RTR-EXTERNAL
interface gi0/0
ip nat inside
interface gi0/1
ip nat outside
interface gi0/2
ip nat outside

ip access-list standard ISP1
permit 192.168.0.0 0.0.255.255
ip access-list standard ISP2
permit 192.168.0.0 0.0.255.255

ip nat inside source list ISP1 interface GigabitEthernet0/1
   overload
```

```
ip nat inside source list ISP2 interface GigabitEthernet0/2
   overload
```

5.11 Cấu hình 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. Cấu hình ở các Layer 2 Switch.

Listing 11: Cấu hình Portfast và BPDU guard

```
enable
configure terminal
hostname SW-A1-01
interface range fa0/1 - 24
spanning-tree portfast
spanning-tree bpduguard enable
```

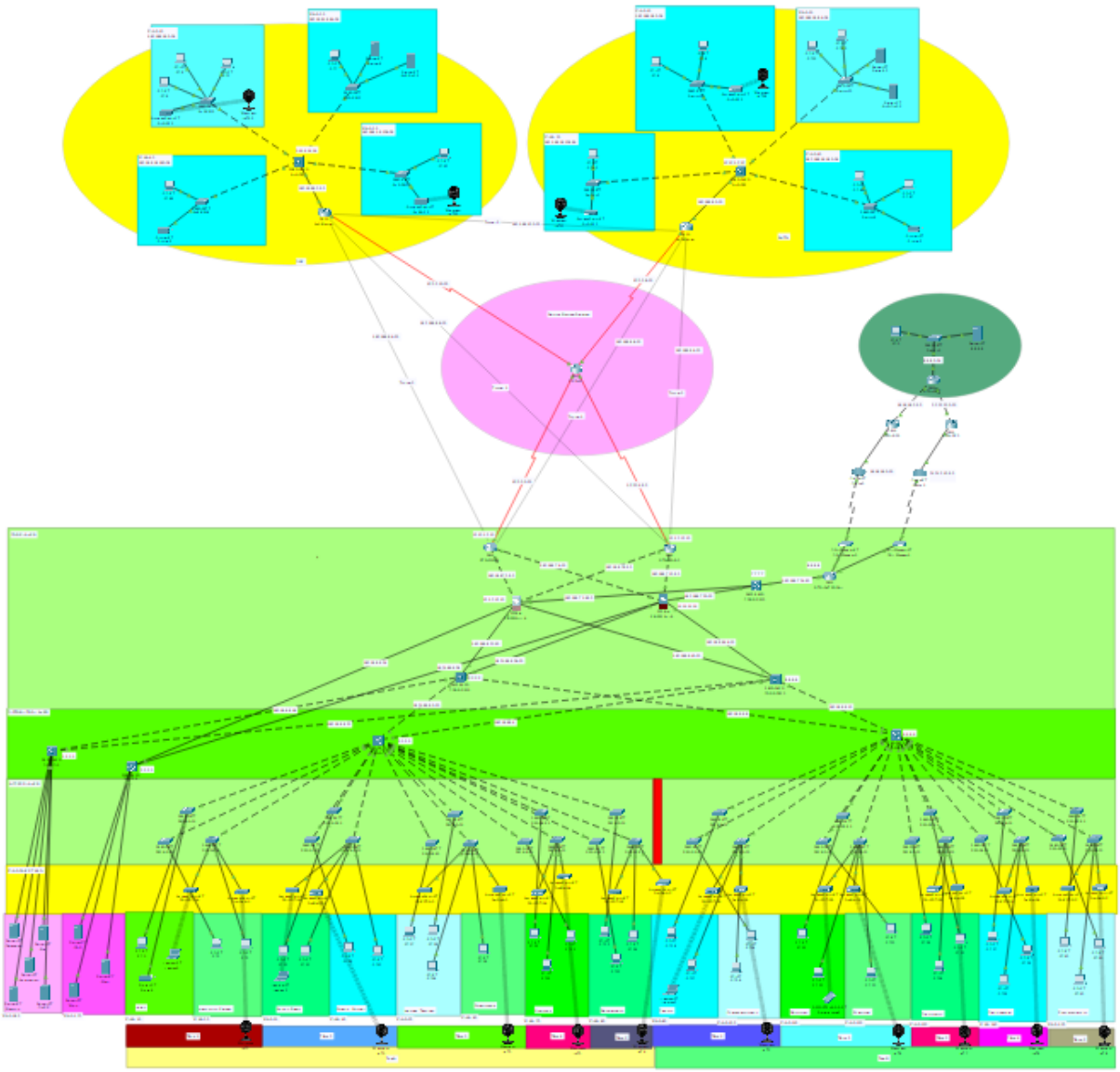
5.12 Cấu hình VPN Tunneling

Ta tiến hành cấu hình VPN cho các router ở biên các khu vực.

Listing 12: Cấu hình VPN cho router

```
enable
configure terminal
hostname RTR-MAIN1
interface Tunnel0
ip address 192.168.8.5 255.255.255.252
tunnel source Serial0/0/0
tunnel destination 15.0.0.13
```

5.13 Tổng quan toàn bộ hệ thống mạng



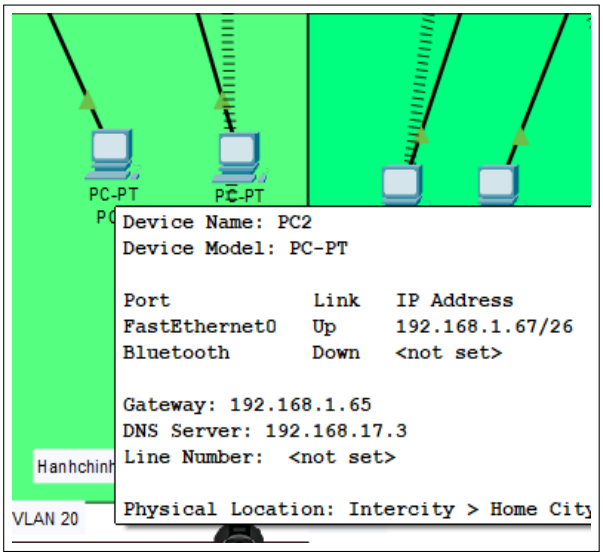
Hình 5: Sơ đồ toàn bộ hệ thống mạng

6 Kiểm thử hệ thống

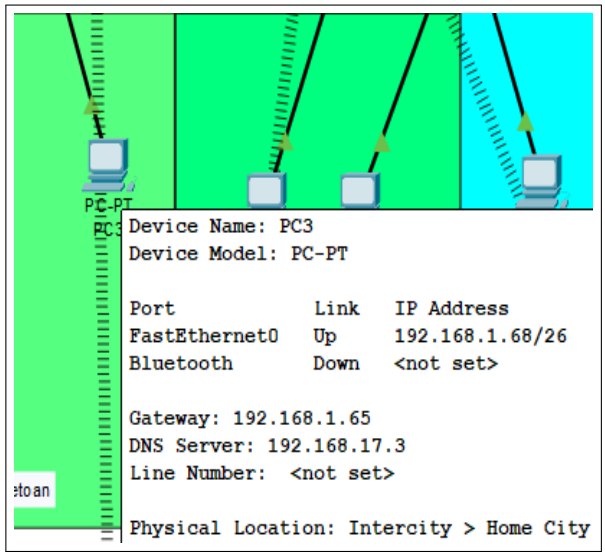
Các địa chỉ ở phần này sẽ không cố định do được cấp tự động bằng DHCP.

6.1 Kết nối giữa các thiết bị trong cùng VLAN

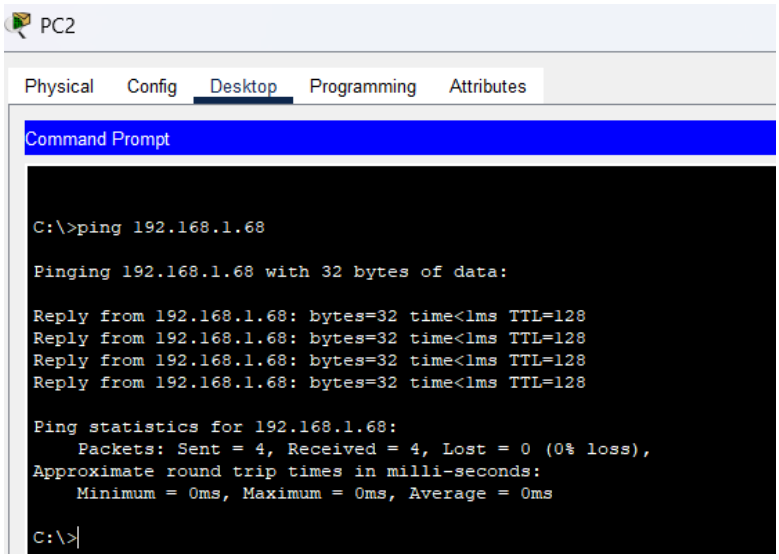
Ở đây ta tiến hành **ping** PC2 (192.168.1.67) và PC3 (192.168.1.68) ở cùng VLAN 20.



Hình 6: Cấu hình địa chỉ IP của PC2 trong VLAN 20



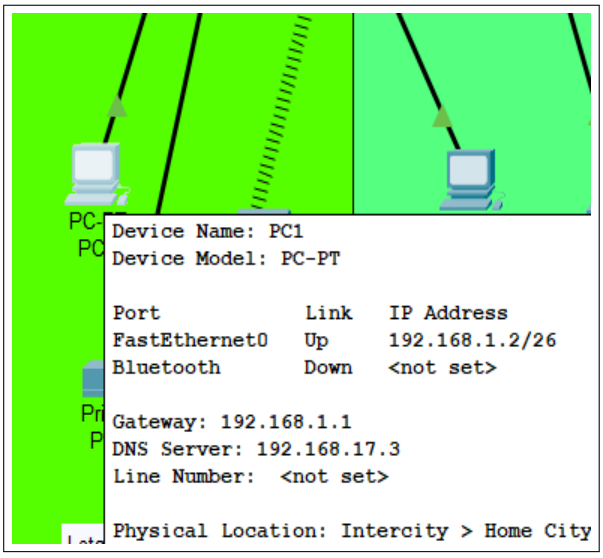
Hình 7: Cấu hình địa chỉ IP của PC3 trong VLAN 20



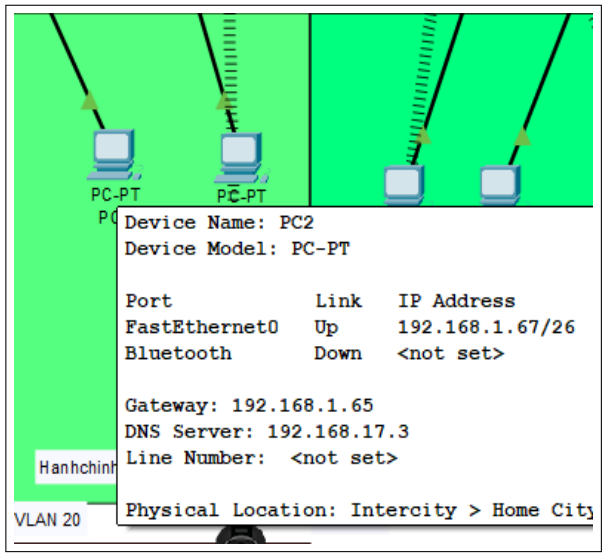
Hình 8: Ping giữa hai PC trong cùng VLAN 20

6.2 Kết nối giữa các thiết bị khác VLAN

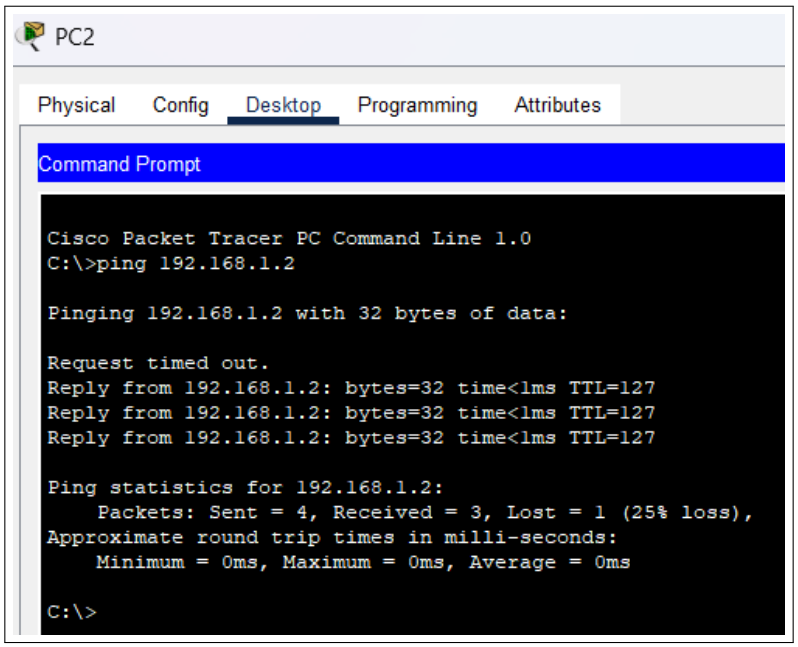
Ở đây ta tiến hành **ping** PC2 (192.168.1.67) ở VLAN 20 và PC1 (192.168.1.2) ở VLAN 10.



Hình 9: Cấu hình địa chỉ IP của PC1 trong VLAN 10



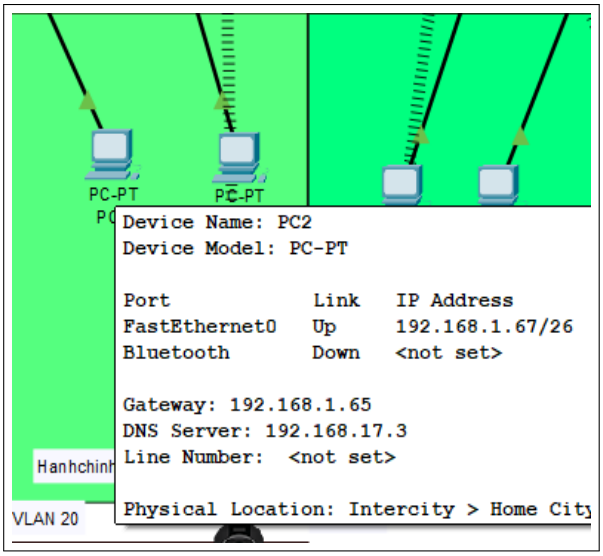
Hình 10: Cấu hình địa chỉ IP của PC2 trong VLAN 20



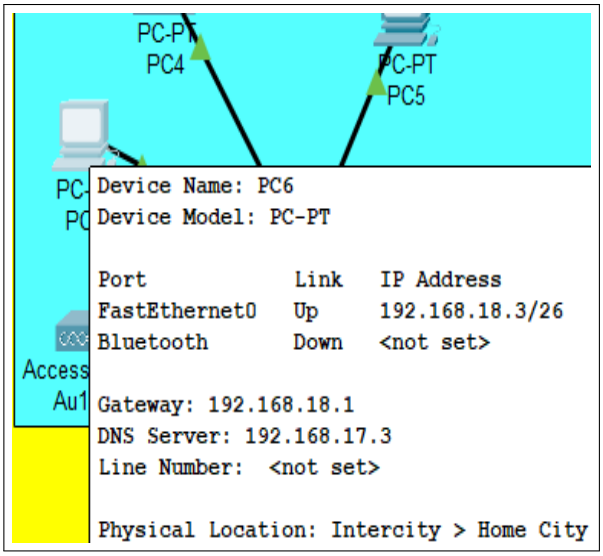
Hình 11: Ping giữa hai PC khác VLAN

6.3 Kết nối giữa các thiết bị thuộc trụ sở chính và hai chính nhánh

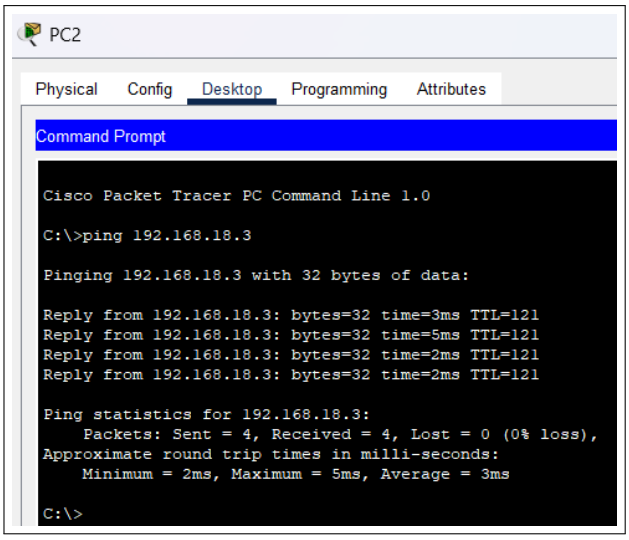
Ở đây ta tiến hành **ping** và **tracert** PC2 (192.168.1.67) ở VLAN 20 thuộc trụ sở chính và PC6 (192.168.18.3) ở VLAN 10 thuộc chi nhánh DBP.



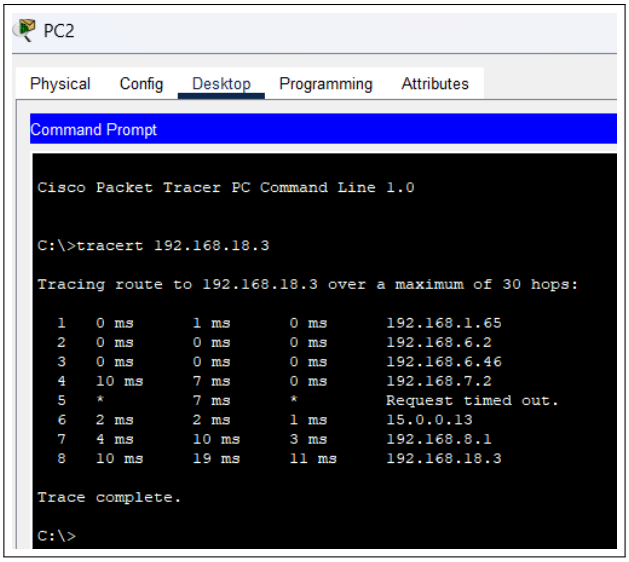
Hình 12: Cấu hình địa chỉ IP của PC2 trong VLAN 20



Hình 13: Cấu hình địa chỉ IP của PC6 trong VLAN 10



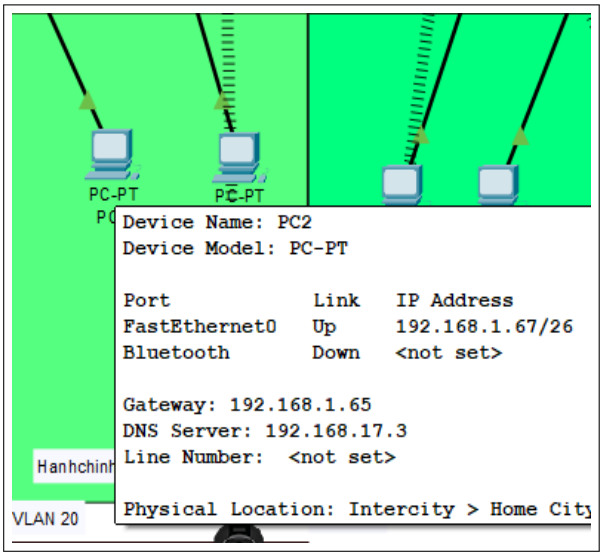
Hình 14: Ping giữa hai PC khác trụ sở



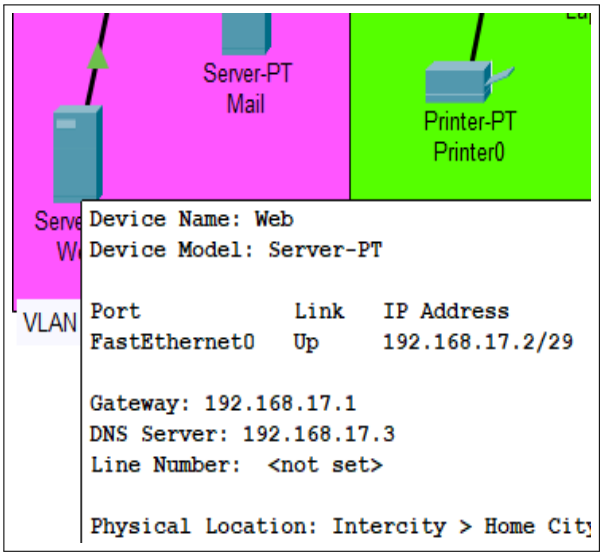
Hình 15: Tracert giữa hai PC khác trụ sở

6.4 Kết nối tới server thuộc DMZ

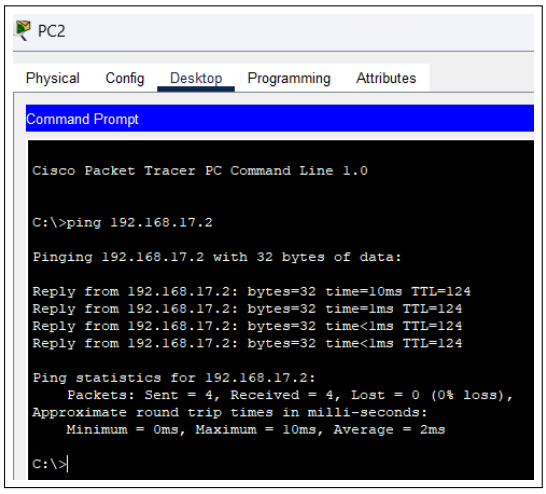
DMZ Server bao gồm Mail, DNS, Web Server, ở đây ta tiến hành **ping** và **tracert** PC2 (192.168.1.67) ở VLAN 20 trụ sở chính tới Web Server (192.168.17.2).



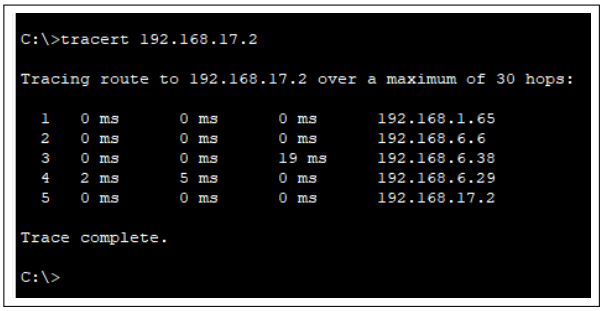
Hình 16: Cấu hình địa chỉ IP của PC2 trong VLAN 20



Hình 17: Cấu hình địa chỉ IP của Web Server trong vùng DMZ



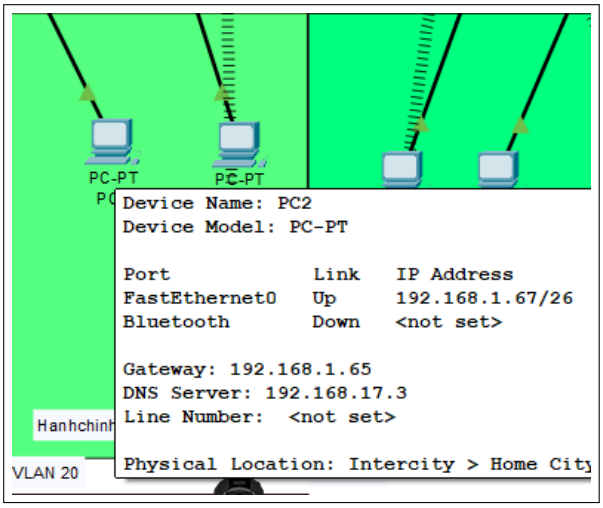
Hình 18: Ping giữa PC và Web Server



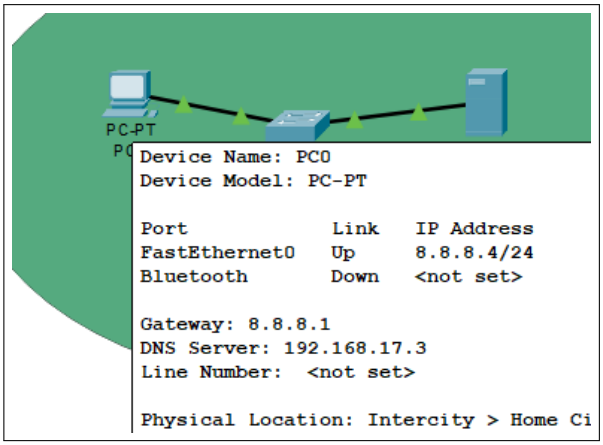
Hình 19: Tracert giữa PC và Web Server

6.5 Kết nối từ Internet đến các máy tính trong mạng LAN

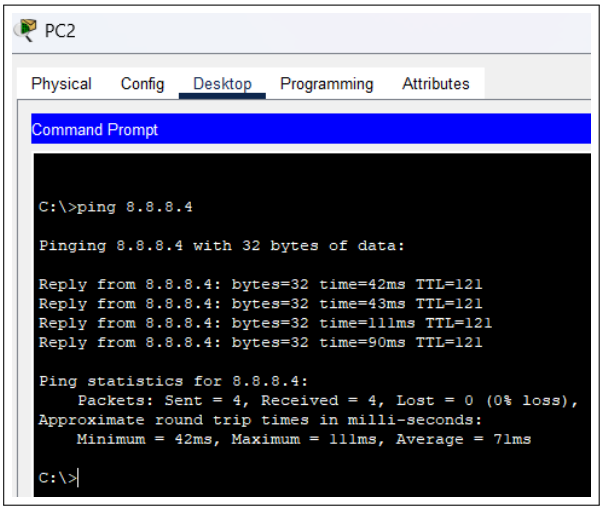
Ở đây ta tiến hành **ping** và **tracert** giữa PC2 (192.168.1.67) và Internet (8.8.8.4).



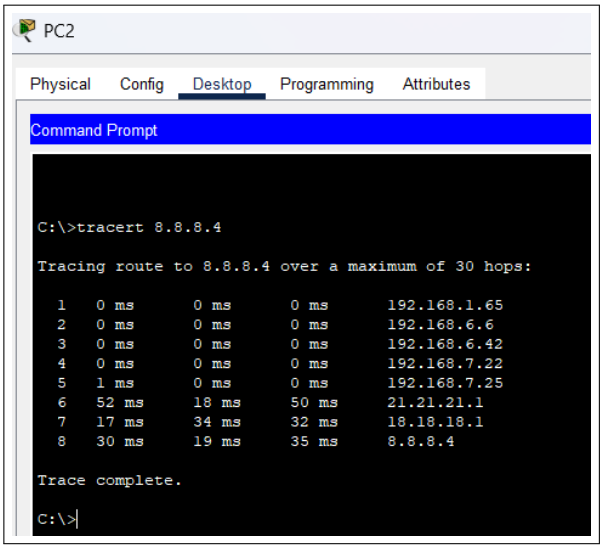
Hình 20: Cấu hình địa chỉ IP của PC2 trong VLAN 20



Hình 21: Cấu hình địa chỉ IP của máy đại diện Internet



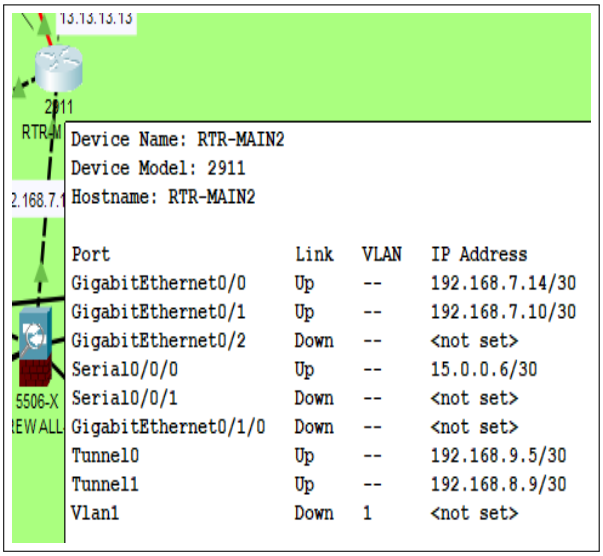
Hình 22: Ping giữa PC và Internet



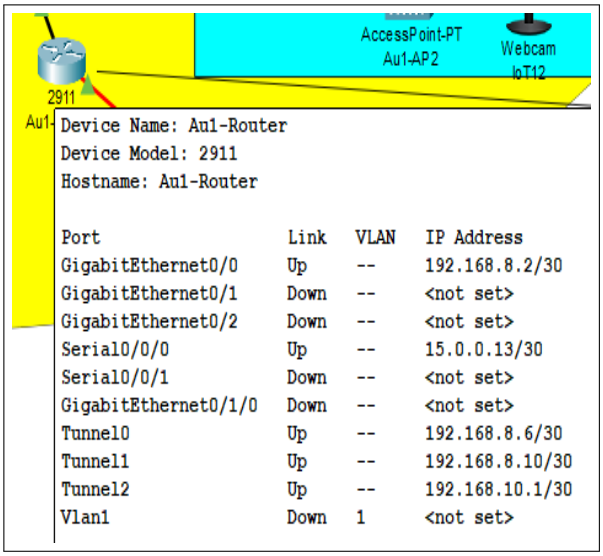
Hình 23: Tracert giữa PC và Internet

6.6 Kết nối VPN giữa các Router biên

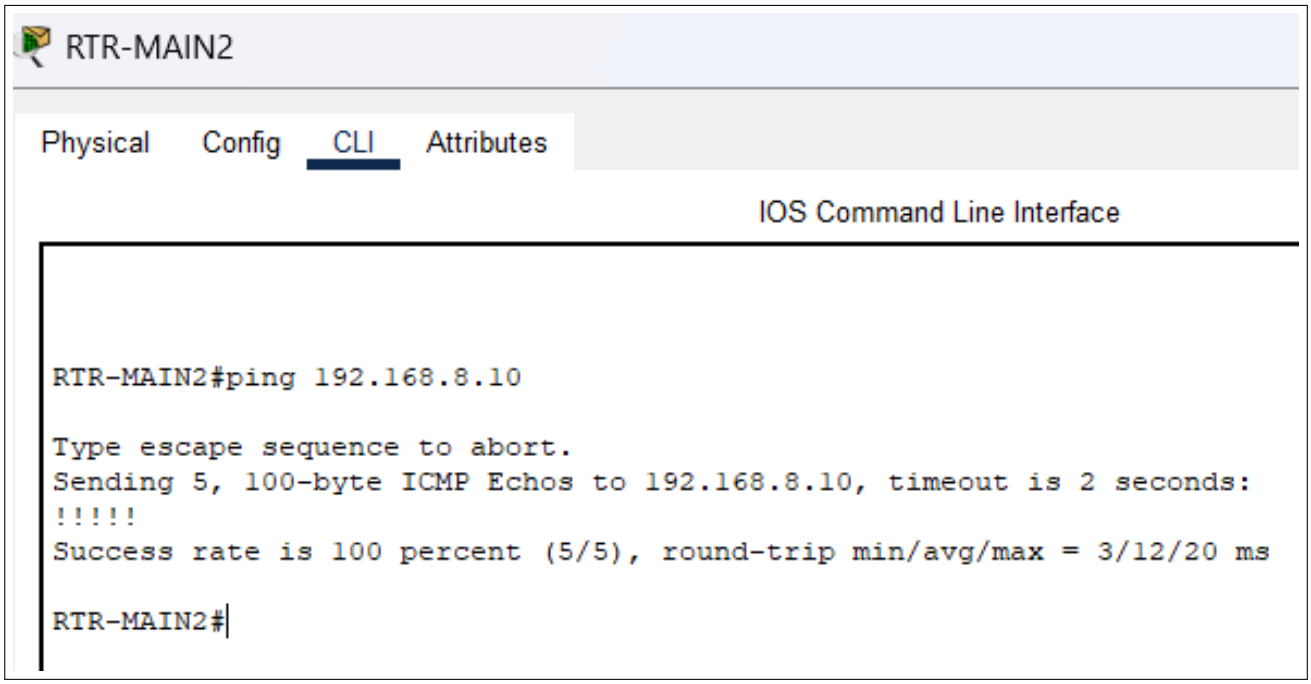
Ở đây ta tiến hành **ping** giữa hai router biên RTR-MAIN2 (192.168.8.9) và Au1-Router (192.168.8.10) thông qua VPN Tunneling đã được thiết lập.



Hình 24: Router RTR-MAIN2



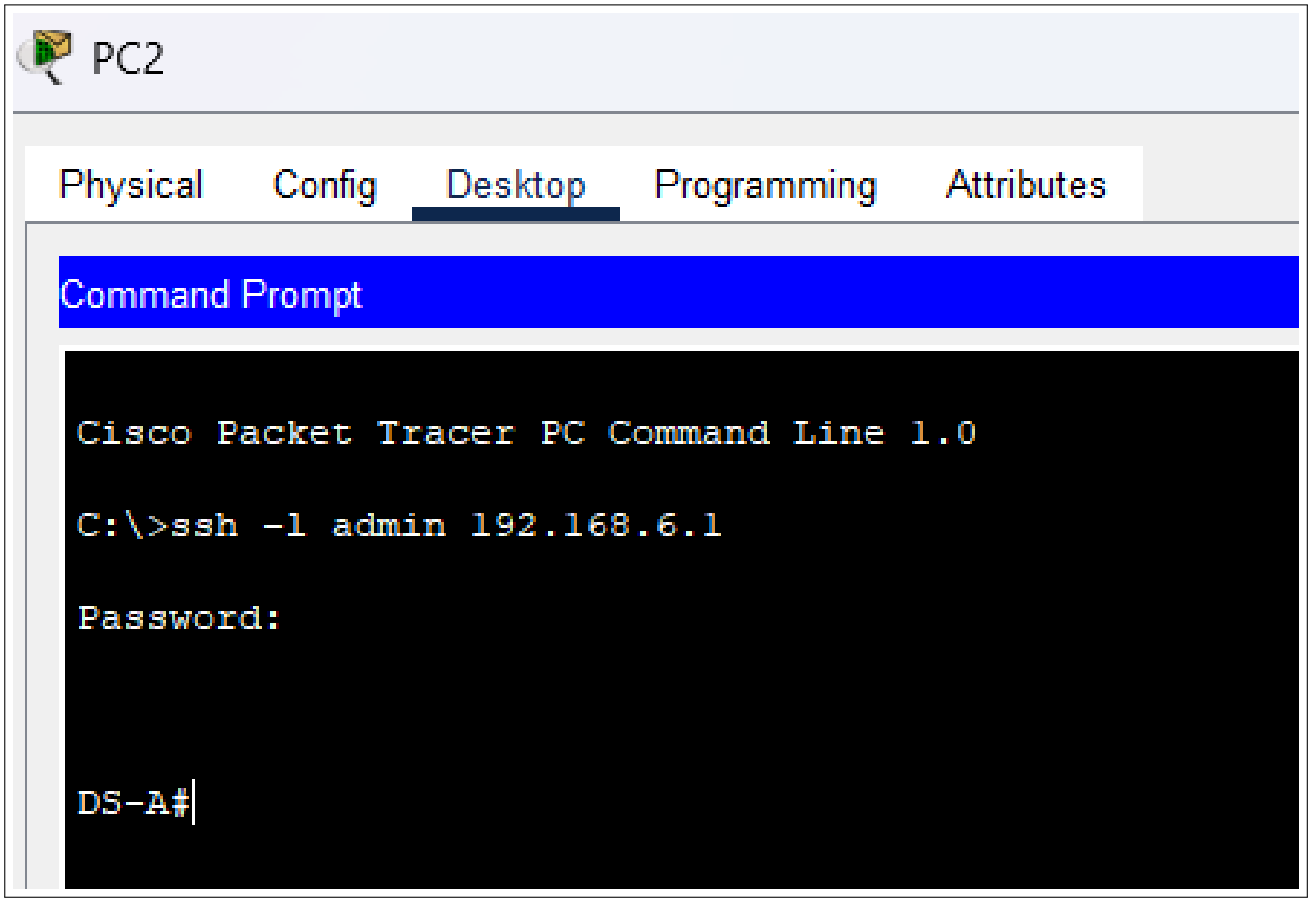
Hình 25: Router Au1-Router



Hình 26: Ping giữa RTR-MAIN2 và Au1-Router

6.7 Kết nối SSH

Kiểm tra kết nối từ PC2 (192.168.1.68) đến cổng GigabitEthernet (192.168.6.1) của Layer 3 Switch (DS-A).



Hình 27: Ping giữa RTR-MAIN2 và Au1-Router

7 Đánh giá hệ thống mạng đã thiết kế

7.1 Độ tin cậy và khả năng duy trì hoạt động

Hệ thống mạng được thiết kế với kiến trúc ba lớp (Access - Distribution - Core) kết hợp cùng cơ chế dự phòng tại tầng Core, đảm bảo độ sẵn sàng cao. Các thiết bị trọng yếu như Core Switch, Firewall, Router WAN đều có cấu hình redundant link và load balancing, cho phép hệ thống tiếp tục hoạt động khi một phần tử gặp sự cố. Ngoài ra, việc triển khai hai đường truyền Internet song song (Primary 1 Gbps và Secondary 500 Mbps) giúp tăng tính ổn định, đảm bảo truy cập Internet liên tục cho toàn bộ bệnh viện.

Cơ chế OSPF dynamic routing trong mạng WAN cho phép tự động cập nhật bảng định tuyến và chuyển hướng lưu lượng khi phát hiện lỗi đường truyền. Điều này giúp giảm thời gian downtime, phù hợp với yêu cầu vận hành 24/7 của hệ thống y tế.

7.2 Khả năng nâng cấp và mở rộng

Hệ thống mạng được xây dựng trên nền tảng hạ tầng quang tốc độ cao (1/10/40 Gbps) và cấu trúc VLAN linh hoạt, cho phép mở rộng số lượng người dùng, phòng ban hoặc chi nhánh trong tương lai mà không cần thay đổi kiến trúc lõi. Các thiết bị được lựa chọn (Cisco Catalyst 9500/9300/9200, ISR 4451-X) đều hỗ trợ nâng cấp phần mềm, module mở rộng cổng quang và PoE+, thuận lợi cho việc tích hợp thêm camera, thiết bị IoT, hoặc Access Point thế hệ mới.

Cấu hình mạng có thể mở rộng để triển khai SD-WAN hoặc MPLS, giúp giám sát tập trung và quản lý linh hoạt giữa các chi nhánh khi bệnh viện mở rộng quy mô hoạt động.

7.3 Sự đa dạng về phần mềm và khả năng hỗ trợ

Hệ thống hỗ trợ đồng thời phần mềm thương mại và mã nguồn mở, bao gồm HIS, PACS, LIS, CRM, cùng các dịch vụ web và email nội bộ. Kiến trúc Client–Server cho

phép triển khai trên nhiều nền tảng, dễ dàng tích hợp với các công cụ quản trị (SNMP, SolarWinds, PRTG) nhằm giám sát hiệu năng thiết bị theo thời gian thực.

Việc triển khai DHCP, DNS và RADIUS tập trung giúp giảm tải cấu hình thủ công và tăng tính đồng bộ trong quản lý người dùng. Các VLAN được cấu hình tách biệt cho từng nhóm dịch vụ, thuận tiện cho việc bảo trì, cập nhật và phân quyền.

7.4 Tính an toàn và bảo mật mạng

Hệ thống bảo mật được thiết kế đa lớp gồm Firewall NGFW, IDS/IPS, VPN site-to-site. Các cơ chế ACL, NAT và DMZ zone được áp dụng nghiêm ngặt nhằm kiểm soát truy cập giữa các vùng mạng, đặc biệt giữa mạng nội bộ và Internet.

Kết hợp IPSec encryption trên GRE tunnel đảm bảo dữ liệu y tế (HIS, PACS) được truyền tải an toàn giữa các chi nhánh. Đồng thời, chính sách QoS được áp dụng cho các ứng dụng quan trọng, giúp giảm thiểu nguy cơ tấn công DoS và đảm bảo lưu lượng ưu tiên cho dịch vụ y tế trọng yếu.

7.5 Các vấn đề còn tồn tại

Mặc dù hệ thống đã đạt tiêu chí kỹ thuật và bảo mật, vẫn còn một số hạn chế:

- Chưa tích hợp giải pháp giám sát tự động log và backup dữ liệu định kỳ giữa các chi nhánh.
- Việc triển khai IDS/IPS và VPN đa lớp yêu cầu chi phí đầu tư cao, có thể ảnh hưởng đến ngân sách ban đầu.
- Hệ thống chưa áp dụng hoàn toàn các chuẩn Zero-Trust hoặc NAC (Network Access Control) cho người dùng không cố định.
- Cần thêm cơ chế cảnh báo sớm (SIEM) để phát hiện các hành vi bất thường trong lưu lượng mạng.

7.6 Định hướng phát triển trong tương lai

Trong giai đoạn mở rộng, hệ thống nên hướng đến:

- Triển khai SD-WAN toàn diện nhằm quản lý tập trung và tối ưu định tuyến động giữa nhiều site.
- Ứng dụng AI/ML trong giám sát an ninh mạng, phát hiện sớm sự cố hoặc lưu lượng bất thường.
- Tích hợp cloud backup và hybrid cloud infrastructure, phục vụ lưu trữ PACS và HIS quy mô lớn.
- Nâng cấp Wi-Fi 6E/7 và bổ sung Access Point tại các khu vực đông người (phòng chờ, khu cấp cứu).

Tài liệu tham khảo

[1] J. F. Kurose and K. W. Ross, "Computer networking: A top-down approach 8th edition," *Pearson*, 2021.