TRƯỜNG ĐẠI HỌC BÁCH KHOA - ĐHQG-HCM

KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

MẠNG MÁY TÍNH (TN) - CO3094

Báo cáo Bài tập lớn 2

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE HOSPITAL

Giảng viên hướng dẫn: BÙI XUÂN GIANG, CSE-HCMUT

Sinh viên: TRẦN HỮU NGUYÊN SƠN - 2312981 - L03
NGUYỄN TĂNG VŨ - 2313962 - L03
PHẠM XUÂN VŨ - 2313966 - L03
NGUYỄN NHÂN THÀNH CHÂU - 2310334 - L03

TP. Hồ Chí Minh, Ngày 13 tháng 11 năm 2025

Mục lục

1 Bảng phân công công việc

Họ và tên	Công việc	Tỷ lệ hoàn thành
Trần Hữu Nguyên Sơn	Thiết kế + Testing + Báo cáo	100%
Nguyễn Tăng Vũ	Thiết kế + Testing + Báo cáo	100%

2 Phân tích cấu trúc mạng phù hợp cho các tòa nhà

2.1 Phân tích yêu cầu hệ thống mạng

2.1.1 Yêu cầu cho trụ sở chính (Main Site)

- Quy mô và cấu trúc vật lý: Gồm 2 tòa nhà A và B, mỗi tòa 5 tầng với 10 phòng/tầng, được trang bị máy tính và thiết bị y tế.
- Vị trí Data Center: Trung tâm dữ liệu, IT và Phòng Cáp Trung tâm đặt trong phòng riêng, cách tòa nhà A và B 50m.
- Quy mô Thiết bị: Cỡ trung bình với 600 máy trạm, 10 máy chủ, 12 thiết bị mạng (hoặc hơn).
- Hạ tầng Mạng: Phải có kết nối có dây và không dây, sử dụng cáp quang (GPON) và GigaEthernet (1GbE/10GbE/40GbE). Mạng được tổ chức theo cấu trúc VLAN cho các phòng ban khác nhau.
- Kết nối WAN: Kết nối với 2 chi nhánh phụ (Site DBP và Site BHTQ) bằng 2 đường truyền thuê riêng (leased lines) cho WAN, có thể áp dụng SD-WAN hoặc MPLS. -
- Internet Access: Sử dụng 2xDSL cho truy cập Internet với cơ chế cân bằng tải (load-balancing), và tất cả lưu lượng Internet phải qua mạng con của trụ sở chính.
- Bảo mật: Yêu cầu bảo mật cao (Firewall, IPS/IDS, phát hiện lừa đảo), tính sẵn sàng cao (HA), khả năng phục hồi và dễ nâng cấp.

2.1.2 Yêu cầu cho các chi nhánh phụ (Auxiliary Sites)

- Tòa nhà 2 tầng, tầng 1 có phòng IT và phòng Cáp Trung tâm.
- 60 máy trạm, 2 máy chủ, 5 thiết bị mạng hoặc hơn.
- Kết nối với trụ sở chính qua WAN (SD-WAN, MPLS,...).

2.1.3 Yêu cầu chung

- Chia sẻ luồng dữ liệu và cân bằng khối lượng công việc giữa các địa điểm chính và phụ.
- Đáp ứng tỷ lệ tăng trưởng 20% của công ty trong 5 năm.
- Bảo mật cao, tính sẵn sàng cao, khả năng phục hồi khi xảy ra sự cố, dễ dàng nâng cấp.
- Tổng lượng tải xuống ước tính khoảng 1000 MB/ngày và tải lên ước tính là 2000 MB/ngày.
- Tổng lượng tải xuống ước tính khoảng 500 MB/ngày và tải lên ước tính là 100 MB/ngày.
- Các thiết bị kết nối WiFi từ khách hàng truy cập để tải xuống khoảng 500 MB/ngày.
- Xây dựng hệ thống camera giám sát tích hợp cho toàn bộ công ty.
- Đề xuất giải pháp VPN để kết nối site-to-site giữa trụ sở chính (Main Site) và hai chi nhánh phụ (Auxiliary Sites) nhằm đảm bảo kết nối bảo mật và ổn định.
- Thiết lập VPN cho các teleworkers (nhân viên làm việc từ xa) để truy cập vào mạng LAN của công ty một cách an toàn.

2.2 Chi tiết hệ thống mạng

Trước khi chuẩn bị xây dựng hệ thống mạng, việc đầu tiên và quan trọng là khảo sát địa điểm lắp đặt. Các nội dung cần khảo sát bao gồm:

2.2.1 Về địa điểm lắp đặt

- Số tầng của tòa nhà.
- Số lượng phòng trên mỗi tầng.
- Kích thước mỗi phòng.
- Nhà mạng hỗ trợ tốt nhất cho địa điểm lắp đặt.
- Tòa nhà có đường đi dây riêng hay phải tự đi dây.

2.2.2 Về tổ chức bệnh viện

- Bố trí phòng ban trên các tầng.
- Quy mô mỗi phòng ban.
- Vị trí các máy chủ.

2.2.3 Trụ sở chính ở TP. Hồ Chí Minh

- Trụ sở chính có 2 tòa (A và B), mỗi tòa có 5 tầng với 600 workstations, 10 servers, 12 networking devices.
- Mỗi tầng phù hợp cho khoảng 60 người làm việc cùng lúc.
- Nhà mạng hỗ trợ tốt nhất đã được xác định.
- Tòa nhà có đường đi dây riêng, không cần thi công thêm.
- Mỗi tầng cần hệ thống mạng không dây, tối đa 60 thiết bị kết nối cùng lúc, riêng Phòng Lễ tân tối đa 70 thiết bị.

2.2.3.1 Chi tiết các tầng

Tầng	Chi tiết phòng ban và thiết bị
1	Phòng Lễ tân: 6 workstations, thiết bị mạng không dây (tối đa 60), 1 camera, 1 cảm biến chuyển động.
2	Phòng máy chủ (Server farm) và DMZ: 5 servers nội bộ, 1 Web server DMZ.
3	Phòng Quản lí nhân sự: 6 workstations, thiết bị mạng không dây (tối đa 60).
4	Phòng Tiếp thị và Bán thuốc: 6 workstations, thiết bị mạng không dây (tối đa 60).
4	Phòng Quản trị: 6 workstations, thiết bị mạng không dây (tối đa 60).
5	Phòng Tài chính và Kế toán: 6 workstations, thiết bị mạng không dây (tối đa 60).
5	Phòng Nghiên cứu và Phát triển: 6 workstations, thiết bị mạng không dây (tối đa 60).
5	Phòng Lưu trữ thuốc: 6 workstations, thiết bị mạng không dây (tối đa 60).

2.2.4 Chi nhánh ở ĐBP và BHTQ

- Mỗi chi nhánh có 2 tầng, 260 workstations, 2 servers, 5 networking devices.
- Nhà mạng hỗ trợ tốt nhất đã được xác định.
- Tòa nhà có đường đi dây riêng.
- Mỗi tầng cần hệ thống mạng không dây tối đa 130 thiết bị, riêng Phòng Lễ tân tối đa 260 thiết bị.

2.2.4.1 Chi nhánh ĐBP

Tầng	Chi tiết phòng ban và thiết bị
1	Phòng IT: 52 workstations, thiết bị mạng không dây (tối đa 130).
1	Phòng Quản lí nhân sự: 52 workstations, thiết bị mạng không dây (tối đa 130).
1	Phòng Lễ tân: 52 workstations, thiết bị mạng không dây (tối đa 130), 1 camera, 1 cảm biến chuyển động.
1	Phòng Server farm: 2 servers.
2	Phòng Tiếp thị và Bán thuốc: 52 workstations, thiết bị mạng không dây (tối đa 130).
2	Phòng Tài chính và Kế toán: 52 workstations, thiết bị mạng không dây (tối đa 130).
2	Phòng Nghiên cứu và Phát triển: 52 workstations, thiết bị mạng không dây (tối đa 130).
2	Phòng Quản trị: 52 workstations, thiết bị mạng không dây (tối đa 130).

2.2.4.2 Chi nhánh BHTQ

Tầng	Chi tiết phòng ban và thiết bị
1	Phòng IT: 52 workstations, thiết bị mạng không dây (tối đa 130).
1	Phòng Quản lí nhân sự: 52 workstations, thiết bị mạng không dây (tối đa 130).
1	Phòng Lễ tân: 52 workstations, thiết bị mạng không dây (tối đa 130), 1 camera, 1 cảm biến chuyển động.
1	Phòng Server farm: 2 servers.
2	Phòng Tiếp thị và Bán thuốc: 52 workstations, thiết bị mạng không dây (tối đa 130).
2	Phòng Nghiên cứu và Phát triển: 52 workstations, thiết bị mạng không dây (tối đa 130).
2	Phòng Quản trị: 52 workstations, thiết bị mạng không dây (tối đa 130).

2.3 Danh sách khảo sát tại địa điểm lắp đặt

Hạng mục	Mục tiêu	Cách thực hiện

Kiến trúc và bố cục tòa nhà	Xác định phạm vi triển khai, vị trí đặt thiết bị mạng chính	• Thu thập bản vẽ mặt bằng 2 tòa (A, B) và các chi nhánh DBP, BHTQ. • Xác định vị trí phòng IT, Data Center, đường đi dây, khu vực hành chính, khu y tế, khu nghiên cứu. • Ghi nhận vật liệu tường, trần (ảnh hưởng sóng Wi-Fi)
Hạ tầng điện - mạng	Kiểm tra khả năng cấp nguồn và kết nối vật lý	Kiểm tra vị trí ổ điện, UPS, tủ rack, nguồn dự phòng. Xác định cáp đồng/cáp quang đã có sẵn, độ dài trung bình từ tủ rack đến phòng xa nhất. Đo điện áp và thử tải ổ cắm (với dụng cụ đo).
Phủ sóng Wi-Fi	Đảm bảo tín hiệu Wi-Fi đủ mạnh	Sử dụng phần mềm khảo sát sóng (Ekahau, NetSpot, hoặc inSSIDer). Đo cường độ sóng tại mỗi tầng (dBm). Ghi nhận điểm "chết sóng" để bố trí thêm Access Point. Kiểm tra can nhiễu giữa các AP (channel overlap).
Lưu lượng mạng dự kiến	Xác định khu vực tải cao	Quan sát và ước tính số thiết bị hoạt động theo phòng. Thống kê số lượng PC, thiết bị y tế kết nối mạng tại từng tầng. Ghi nhận ứng dụng tiêu tốn băng thông lớn (PACS, LIS, Camera IP, Wi-Fi công cộng).
An toàn vật lý	Đảm bảo an ninh thiết bị và khu vực lắp đặt	Kiểm tra khóa cửa phòng server, tủ rack. Xác định vị trí camera giám sát Data Center và hành lang mạng. Đo nhiệt độ phòng IT (nhiệt độ $< 25°C$). Đánh giá lối thoát hiểm, ổn định nhiệt và độ ẩm.

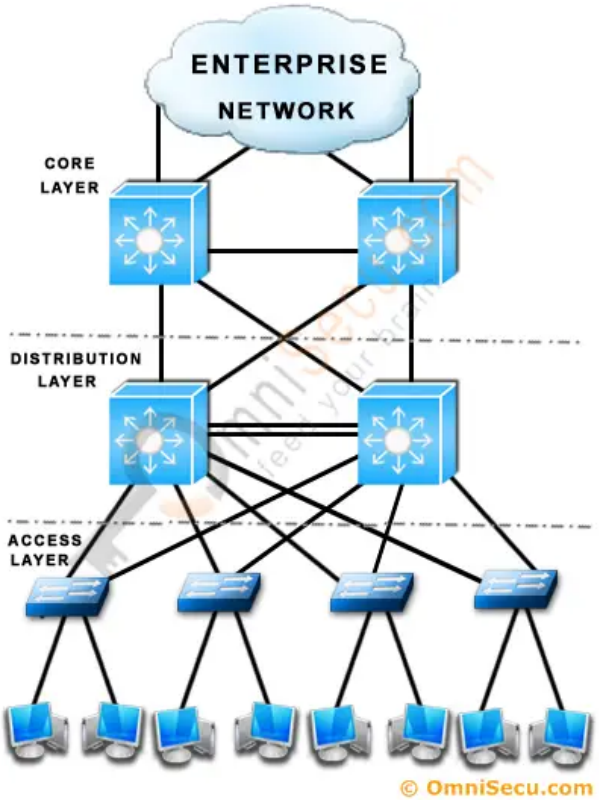
2.4 Xác định khu vực có tải cao

- **Data Center (Trụ sở chính):**
  • Tải cao nhất vì là trung tâm hội tụ toàn bộ lưu lượng mạng.
  • Tất cả lưu lượng từ các ứng dụng quan trọng (HIS, LIS, PACS), Internet, Wi-Fi, và kết nối WAN hội tụ tại Data Center.
  • Đây là nơi đặt toàn bộ server và hệ thống bảo mật (Firewall, IPS/IDS).
  => Đối với các vị trí có tải trọng lớn kể trên, hệ thống sẽ áp dụng các cơ chế cân bằng tải phù hợp

- **Tầng 1 (trụ sở chính):** Đây là nơi tiếp nhận bệnh nhân. Hầu hết các giao dịch được thực hiện qua hệ thống phần mềm HIS (Hospital Information System). Wi-Fi công cộng tại khu vực chờ cho bệnh nhân và người nhà tạo thêm tải mạng đáng kể, đặc biệt trong giờ cao điểm. Tải cao do Wi-Fi công cộng và hoạt động hành chính/phục vụ bệnh nhân.

- **Tầng 2,3 (trụ sở chính)**: Đây vừa là nơi thực hiện thanh toán, vừa là nơi chuẩn đoán hình ảnh (PACS - xử lý và lưu trữ các hình ảnh y khoa, RIS - lịch chụp, theo dõi bệnh nhân, quản lý kết quả báo cáo) yêu cầu băng thông cực lớn, truyền dữ liệu liên tục đến server.
- **Tầng 1 (Chi nhánh phụ):** Có phòng IT nơi tổng hợp lưu lượng truy cập cục bộ, xử lý tải máychủ cùng với đó hệ thống cáp trung tâm nên đây cũng là vùng có lượng tải lớn.

2.5 Cấu trúc mạng



Hình 1: *Sơ đồ cấu trúc của mạng phân tầng*

2.5.1 Cấu trúc mạng phân tầng

Mô hình này hiện nay được coi là phương pháp hiện thực tốt nhất trong toàn ngành để thiết kế hệ thống mạng đáng tin cậy, bền vững, có khả năng mở rộng cũng như tiết kiệm chi phí.

Trong mô hình thiết kệ mạng phân tầng, hệ thống mạng được chia thành nhiều tầng (lớp). Các tầng này được kết nối với nhau theo dạng phân cấp cho phép chia hệ thống mạng thành các khối nhỏ dễ quản lý hơn và các khối này giới hạn lưu lượng cục bộ. Mô hình này có thể được áp dụng cho cả mạng LAN và mạng WAN.

Một mô hình mạng phân tầng thường gặp có 3 tầng: Access Layer, Distribution Layer, Core Layer

Từ đấy, lý do mà nhóm lựa chọn cấu trúc này là vì những ưu thế sau:

- Khả năng mở rộng
- Quản lý đơn giản
- Hỗ trợ VLAN và bảo mật
- Độ sẵn sàng cao
- Tiết kiệm chi phí khi mở rộng

2.6 Phân khu mạng

2.6.1 Vlan cho từng tầng

Mỗi tầng sẽ có một VLAN riêng biệt để đảm bảo việc phân chia lưu lượng và tăng cường bảo mật nhằm giảm thiểu các nguy cơ xâm nhập và đảm bảothông tin nhạy cảm của bệnh viện không bị truy cập trái phép từ các bộ phận khác. Các VLAN này sẽ được cấu hình để phân chia lưu lượng mạng và đảm bảo tính riêng tư trong quá trình giao tiếp giữa các phòng ban.

2.6.2 DMZ và Server Farm

Các dịch vụ công cộng như web server, email server sẽ được đặt trong DMZ (Demilitarized Zone), nơi có mức độ bảo mật thấp hơn để dễ dàng quản lý và hạn chế các mối đe dọa từ bên ngoài. Trong khi đó, các máy chủ quan trọng hơn sẽ được đưa vào Data Center nơi có bảo mật cao hơn và được bảo vệ bằng các biện pháp như tường lửa và IDS/IPS. Mạng DMZ giúp giảm thiểu sự ảnh hưởng khi có một cuộc tấn công từ bên ngoài vào các dịch vụ công cộng, trong khi vẫn đảm bảo bảo mật cho các hệ thống quan trọng.

2.6.3 Mạng nội bộ không dây (Wi-Fi)

Các Access Points (APs) sẽ được bố trí để đảm bảo kết nối Wi-Fi ổn định cho nhân viên và bệnh nhân tại tất cả các khu vực trong bệnh viện. Mạng không dây này sẽ được phân chia thành các VLAN riêng biệt, giúp tách biệt mạng của nhân viên và khách hàng để đảm bảo an toàn và hiệu quả trong việc sử dụng tài nguyên mạng. Mạng Wi-Fi cho nhân viên sẽ được bảo mật nghiêm ngặt hơn với các chính sách mã hóa WPA3, trong khi mạng cho bệnh nhân sẽ được thiết lập với khả năng hạn chế truy cập vào các hệ thống nội bộ của bệnh viện.

2.6.4 Kết nối WAN

Bệnh viện sẽ sử dụng kết nối WAN để liên kết giữa các chi nhánh và trụ sở chính. Kết nối WAN này sẽ giúp chia sẻ dữ liệu và tài nguyên một cách hiệu quả giữa các cơ sở. Để đảm bảo tính bảo mật và bảo vệ thông tin nhạy cảm khi truyền qua Internet, các kết nối WAN sẽ được bảo vệ bằng các kỹ thuật mã hóa VPN. Cùng với đó, các biện pháp cân bằng tải sẽ được áp dụng để tối ưu hóa băng thông và tránh tắc nghẽn khi có nhiều lưu lượng truy cập.

2.7 Mạng bảo mật và cân bằng tải

- Bảo mật mạng: Sử dụng tường lửa, IPS/IDS, và các chính sách bảo mật như VPN để bảo vệ dữ liệu nhạy cảm và đảm bảo chỉ có người dùng hợp lệ truy cập vào các hệ thống quan trọng.

- Cân bằng tải (Load balancing): Các hệ thống như PACS và HIS cần băng thông lớn, vì vậy sử dụng các cơ chế cân bằng tải (load balancing) giữa các server trong Server Farm để đảm bảo hiệu suất cao và tránh tắc nghẽn mạng.
- Giám sát và quản lý mạng: Sử dụng các công cụ giám sát mạng để theo dõi lưu lượng, phát hiện các sự cố và tối ưu hóa hiệu suất hệ thống.

3 Mô tả cụ thể thiết kế mạng

3.1 Các thiết bị sử dụng

3.1.1 Multilayer Switch 3650-24PS

Đây là thiết bị cung cấp đầy đủ các tính năng của chuyển mạch lớp 2 và một số tính năng lớp 3, hỗ trợ truy cập có dây và không dây đồng bộ. WS-C3650-24PS-L mang lại tính bảo mật cao, hiển thị và kiểm soát ứng dụng bằng NetFlow, khả năng phục hồi tốt, dễ dàng triển khai, lý tưởng để sử dụng tại các văn phòng cũng như doanh nghiệp.

Hình 2: *Cisco Multilayer Switch 3650-24PS*

Thông số kỹ thuật:

Đặc tính	**Giá trị**
Ports	24 x 10/100/1000 (PoE+) + 4 x 1G SFP
Network management Interface	RJ-45 Ethernet management port, 4-pair Cat-5 UTP cabling
Management console port	RJ-45-to-DB9 cable for PC connections
Available PoE Power	390W
Switching Capacity	88 Gbps
Maximum stacking number	9
Stack Bandwidth	160 Gbps
Forwarding Performance	41.66 Mpps
FNF entries	24,000
Maximum VLAN IDs	4,094
MAC Address Table Size	32K
CPU	Multicore CPU
RAM	4 GB
Flash Memory	2 GB

3.1.2 Router Cisco 1941

Dùng để kết nối giữa các chi nhánh và mạng Internet. Router chịu trách nhiệm định tuyến lưu lượng giữa các chi nhánh, trung tâm dữ liệu và kết nối bên ngoài. Thiết bị hỗ trợ cài đặt các giao thức định tuyến để lựa chọn đường truyền tối ưu cho các gói tin, đảm bảo hiệu suất và độ tin cậy. Các giao thức phổ biến được hỗ trợ gồm định tuyến tĩnh, RIP, OSPF và EIGRP. Router này cũng tích hợp các tính năng bảo mật và quản lý lưu lượng để hỗ trợ VPN và QoS cho mạng bệnh viện. **Thông số kỹ thuật:**

Hình 3: *Router 1941 Cisco*

Đặc tính	**Giá trị**
Embedded hardware-based crypto acceleration (IPSec)	Yes
Total Onboard Gigabit Ethernet WAN ports	2
RJ-45-Based Ports	2
SFP-Based Ports	0
SM Slots	0
Double-Wide SM Slots	0
EHWIC Slots	2
Double-wide EHWIC Slots	1 (sử dụng 2 khe EHWIC)
ISM Slots	1 (0 trên Cisco 1941W)
Memory (DDR2 ECC DRAM) - Default	512 MB
Memory (DDR2 ECC DRAM) - Maximum	2.0 GB
Compact Flash (external) - Default	Slot 0: 256 MB
Compact Flash (external) - Maximum	Slot 0: 4 GB, Slot 1: 4 GB
External USB flash memory slots (Type A)	2
USB Console Port (Type B)	1 (115.2 kbps)
Serial Console Port	1 (115.2 kbps)
Serial Auxiliary Port	1 (115.2 kbps)
Power Supply Options	AC, PoE
Redundant Power Supply Support	No

3.1.3 Tường lửa ASA 5506-X

Đảm bảo việc truy cập được bảo mật, hạn chế các rủi ro từ dữ liệu độc hại khi truy cập Internet. Sử dụng thiết bị tường lửa Cisco ASA 5506-X.

Hình 4: *Firewall Cisco ASA 5506-X*

Thông số kỹ thuật:

Đặc tính	Giá trị
Thông lượng VPN 3DES/AES tối đa	250 Mbps
Kết nối tối đa mỗi giây	5000
Kết nối đồng thời	50,000
Tốc độ truyền băng thông	100 MB/s

3.1.4 Switch 2960-24TT

Được sử dụng làm switch truy cập chính trong hệ thống mạng bệnh viện, kết nối các máy trạm, thiết bị IoT y tế, và các điểm truy cập Wi-Fi. Thiết bị đảm bảo hiệu suất ổn định, bảo mật cao và dễ cấu hình.

Hình 5: *Cisco Switch 2960-24TT*

Thông số kỹ thuật:

Đặc tính	Giá trị
Feature Set	LAN Base
Uplink Interfaces	2 x 10/100/1000 TX uplinks
Ports	24 x Ethernet 10/100 ports
Throughput	6.5 Mpps
Backplane Capacity	16 Gbps
DRAM	16 MB

3.1.5 Access Point PT

Được triển khai làm điểm truy cập không dây chính trong hệ thống mạng bệnh viện. AP-PT hỗ trợ kết nối các thiết bị di động, máy trạm và thiết bị IoT y tế tại các khu vực

phòng khám, chẩn đoán và hành chính.

Hình 6: *Access Point PT*

Thông số kỹ thuật:

Đặc tính	Giá trị
Chuẩn kết nối	Fast Ethernet
Băng tần	2.4GHz

3.1.6 Thiết bị khác

Ngoài các thiết bị trên, còn có:

- Các máy chủ (server)
- Máy tính trong mạng LAN
- Các thiết bị kết nối không dây khác

3.2 Kế hoạch địa chỉ IP

3.2.1 Tòa A

VLAN	Tầng	IP range	Subnet Mask	Gateway
02	1	192.168.2.0/24	255.255.255.0	192.168.2.1
03	2	192.168.3.0/24	255.255.255.0	192.168.3.1
04	3	192.168.4.0/24	255.255.255.0	192.168.4.1
05	4	192.168.5.0/24	255.255.255.0	192.168.5.1
06	5	192.168.6.0/24	255.255.255.0	192.168.6.1

Tất cả địa chỉ IP nội bộ của các máy trạm được cấp phát động theo giao thức DHCP. Địa chỉ IP nội bộ của các máy chủ trong Server Farm được cấp phát tĩnh.

3.2.2 Tòa B

VLAN	Tầng	IP range	Subnet Mask	Gateway
07	1	192.168.7.0/24	255.255.255.0	192.168.7.1
08	2	192.168.8.0/24	255.255.255.0	192.168.8.1

09	3	192.168.9.0/24	255.255.255.0	192.168.9.1
10	4	192.168.10.0/24	255.255.255.0	192.168.10.1
11	5	192.168.11.0/24	255.255.255.0	192.168.11.1

Tất cả IP nội bộ được cấp phát động bằng DHCP, các máy chủ dùng IP tĩnh.

3.2.3 Chi nhánh ĐBP

VLAN	Tầng	IP range	Subnet Mask	Gateway
12	1	192.168.12.0/24	255.255.255.0	192.168.12.1
13	2	192.168.13.0/24	255.255.255.0	192.168.13.1

Trung gian tại ĐBP: 192.168.21.0/30 Subnet Mask: 255.255.255.252

IP của các máy trạm được cấp phát động qua DHCP. IP của các server được cấp phát tĩnh.

3.2.4 Chi nhánh BHTQ

VLAN	Tầng	IP range	Subnet Mask	Gateway
14	1	192.168.14.0/24	255.255.255.0	192.168.14.1
15	2	192.168.15.0/24	255.255.255.0	192.168.15.1

Trung gian tại BHTQ: 192.168.22.0/30 Subnet Mask: 255.255.255.252

IP của các máy trạm được cấp phát động qua DHCP. IP của các server được cấp phát tĩnh.

3.2.5 Mạng WAN

Tên Subnet	IP range	Subnet Mask
Trụ sở - Chi nhánh DBP	10.0.1.0/24	255.255.255.0
Trụ sở - Chi nhánh BHTQ	10.0.2.0/24	255.255.255.0

4 Tính toán thông lượng và băng thông

4.1 Công thức

$$\text{Throughput} = \frac{\text{Tổng dữ liệu truyền}}{\text{Thời gian}}$$

$$\text{Bandwidth} = \frac{80\% \text{ tải}}{\text{Thời gian giờ cao điểm}}$$

Theo đề:

- Các luồng dữ liệu và tải công việc của hệ thống (khoảng 80% lượng tải trong ngày tập trung vào các khung giờ cao điểm 9 giờ - 11 giờ và 15 giờ - 16 giờ)

- Các server để cập nhật phần mềm, truy cập web và truy cập cơ sở dữ liệu,... Ước tính tổng download là khoảng 1000 MB/ngày và ước tính upload là 2000 MB/ngày.
- Mỗi máy trạm được sử dụng để duyệt Web, tải tài liệu và giao dịch với khách hàng,. . . Ước tính tổng download là khoảng 500 MB/ngày và ước tính upload là 100 MB/ngày.
- Các thiết bị kết nối WiFi của khách hành truy cập để tải về là khoảng 500MB/ngày. Hệ thống mạng của Hospital được ước tính có tốc độ tăng trưởng 20% trong 5 năm (về số lượng người dùng, tải mạng, mở rộng chi nhánh,..).

4.2 Trụ sở chính

Trụ sở chính bao gồm 600 workstation(PC), 10 server và giả sử có 100 lượt truy cập vào mạng không dây. Tổng lưu lượng download và upload trong 1 ngày:

$$10 \times (1000 + 2000) + 600 \times (500 + 100) + 100 \times 500 = 440000 \text{ MB/ngày}$$

Do thời gian làm việc một ngày là 8 tiếng nên thông lượng của hệ thống là:

$$\text{Throughput} = \frac{440000}{8 \times 3600} = 15.28 \text{ MB/s} = 122.22 \text{ Mbps}$$

Do 80% lưu lượng mạng tập trung trong 3 giờ cao điểm nên băng thông của hệ thống là:

$$\text{Bandwidth}_{\text{cao điểm}} = \frac{440000 \times 0.8}{3 \times 3600} = 32.592 \text{ MB/s} = 260.742 \text{ Mbps}$$

Để đáp ứng nhu cầu trong 5 năm tới thì băng thông của hệ thống sẽ tăng thêm 20%.Vì vậy băng thông cần thiết là:

$$\text{Bandwidth}_{5 \text{ năm}} = 260.742 \times 1.2 = 312.89 \text{ Mbps}$$

4.3 Chi nhánh

Chi nhánh bao gồm 260 workstation, 2 server và giả sử có 50 truy cập mạng không dây. Tổng lưu lượng download và upload trong 1 ngày:

$$2 \times (1000 + 2000) + 260 \times (500 + 100) + 50 \times 500 = 187000 \text{ MB/ngày}$$

Do thời gian làm việc một ngày là 8 tiếng nên thông lượng của hệ thống là:

$$\text{Throughput} = \frac{187.000}{8 \times 3600} = 6.493 \text{ MB/s} = 51.943 \text{ Mbps}$$

Do 80% lưu lượng mạng tập trung trong 3 giờ cao điểm nên băng thông của hệ thống là:

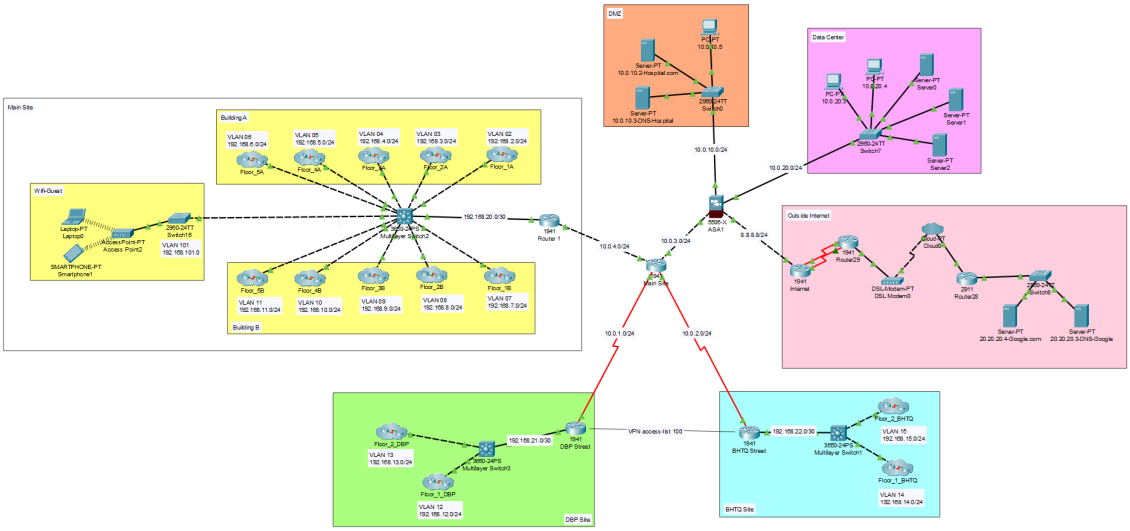
$$\text{Bandwidth}_{\text{cao điểm}} = \frac{187000 \times 0.8}{3 \times 3600} = 13.851 \text{ MB/s} = 114.41 \text{ Mbps}$$

Để đáp ứng nhu cầu trong 5 năm tới thì băng thông của hệ thống sẽ tăng thêm 20%.Vì vậy băng thông cần thiết là:

$$\text{Bandwidth}_{5 \text{ năm}} = 114.41 \times 1.2 = 137.29 \text{ Mbps}$$

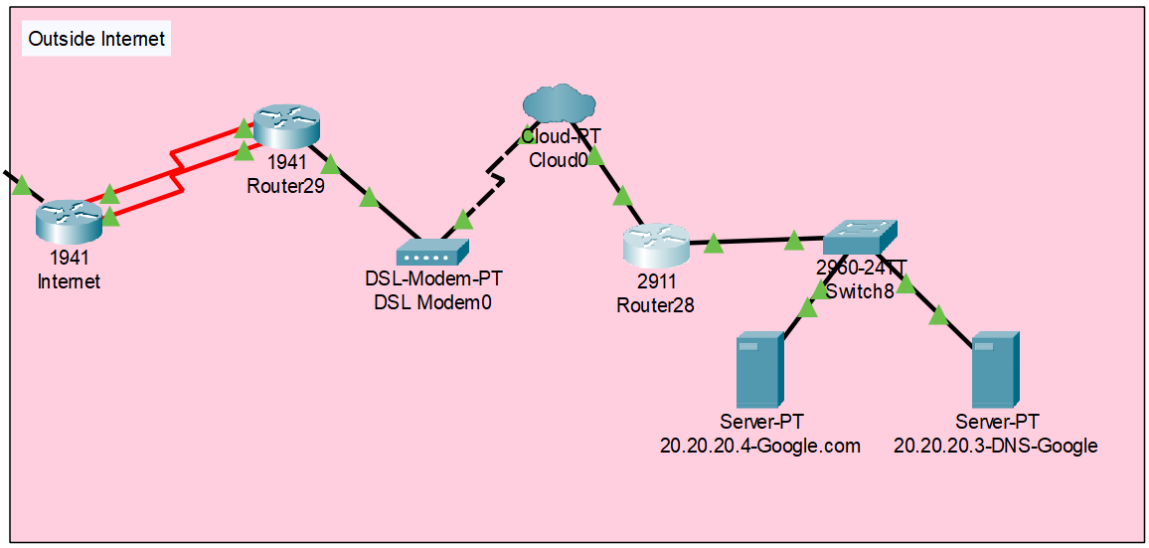
5 Mô phỏng hệ thống bằng Cisco Packet Tracer

5.1 Cấu trúc tổng thể



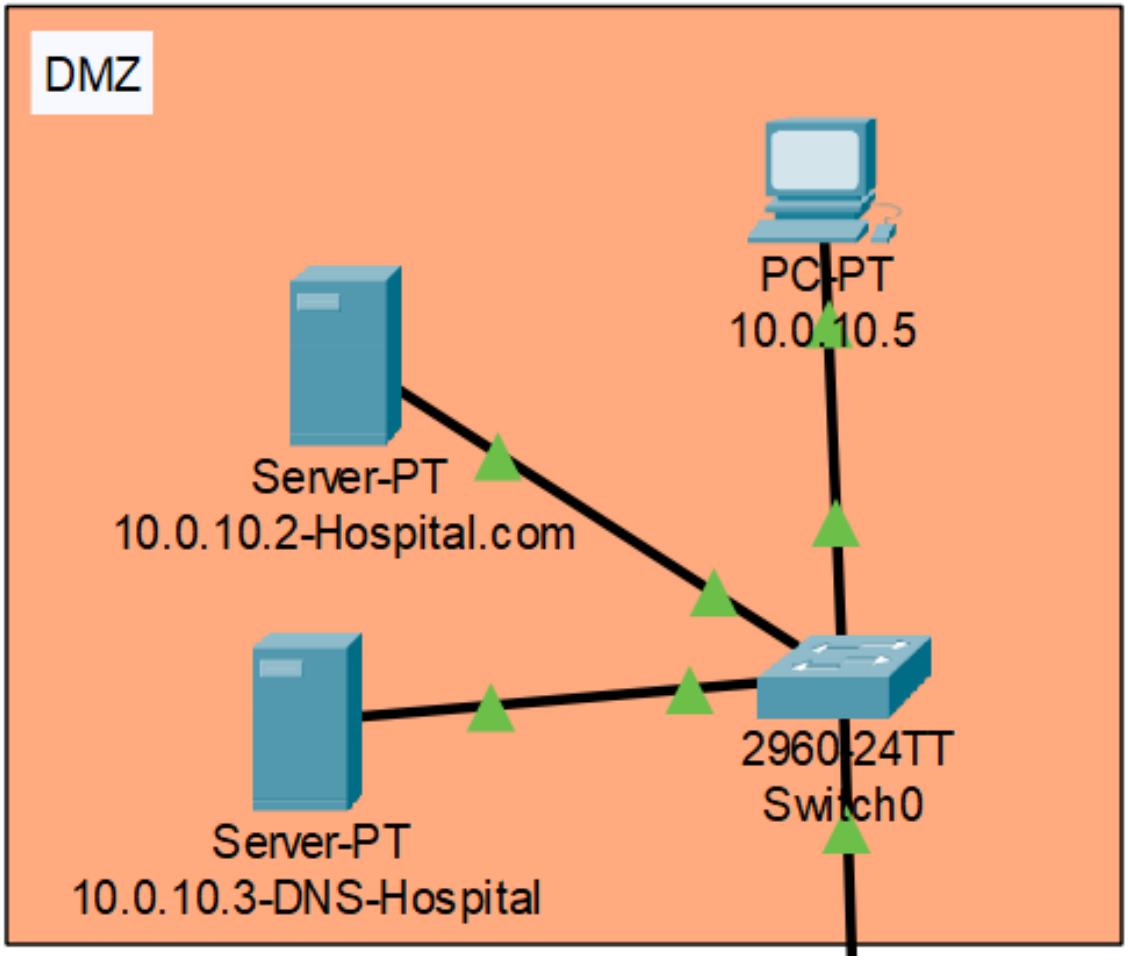
Hình 7: *Tổng thể sơ đồ mạng Bệnh viện*

5.2 Internet



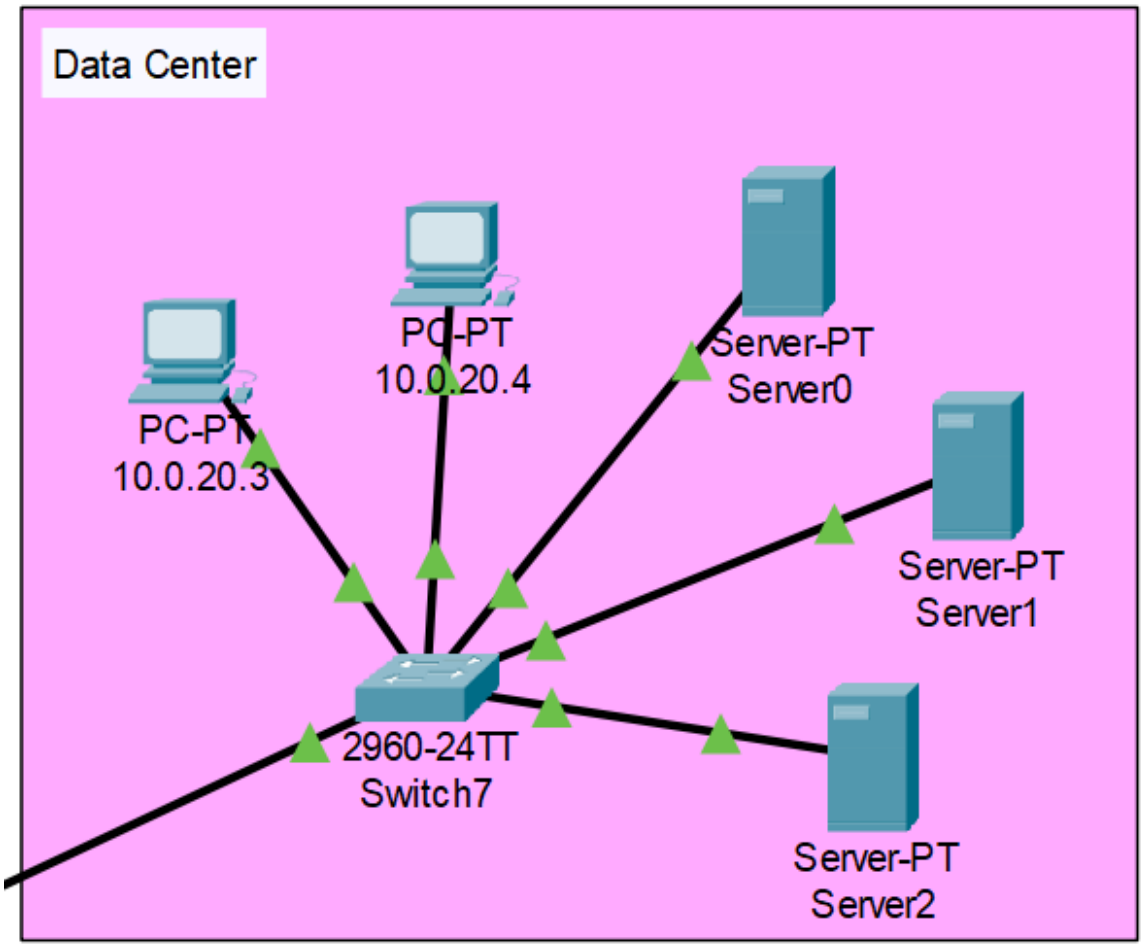
Hình 8: *Cấu trúc Internet*

5.3 DMZ



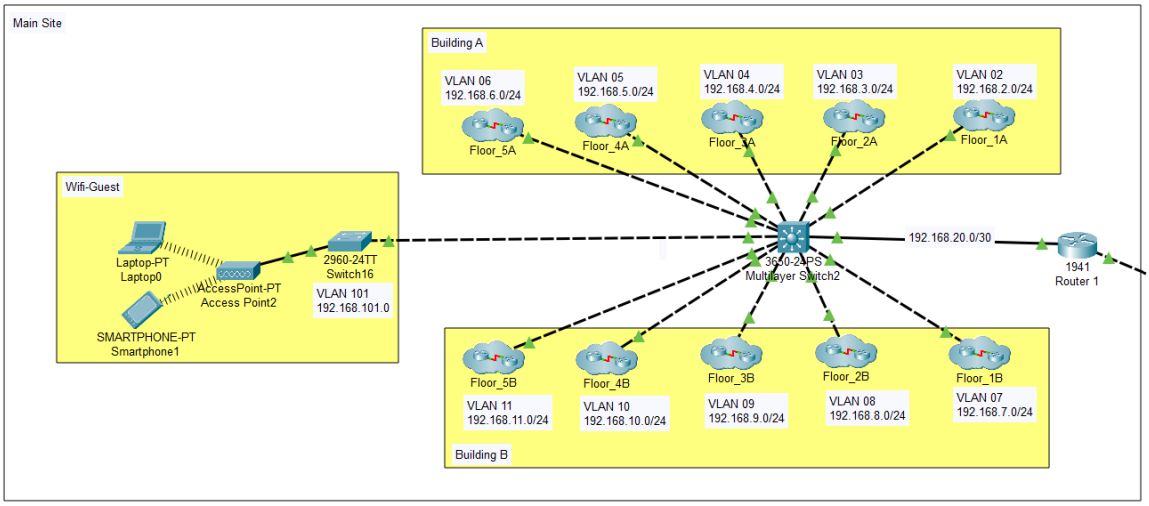
Hình 9: *Cấu trúc DMZ*

5.4 Internet



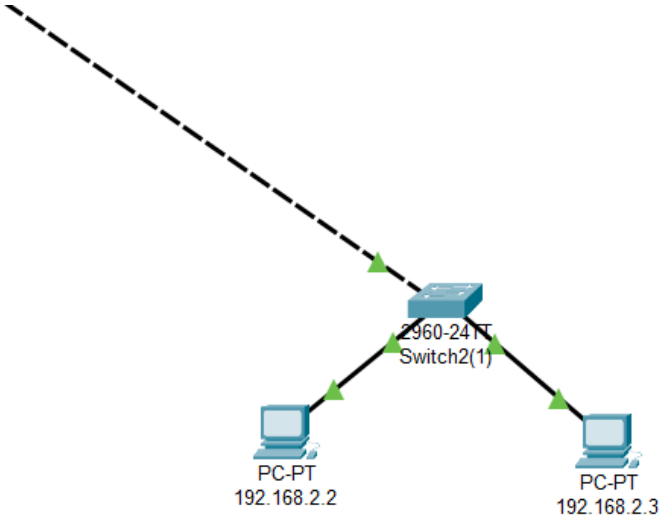
Hình 10: *Cấu trúc Data Center*

5.5 Main site - Cơ sở chính



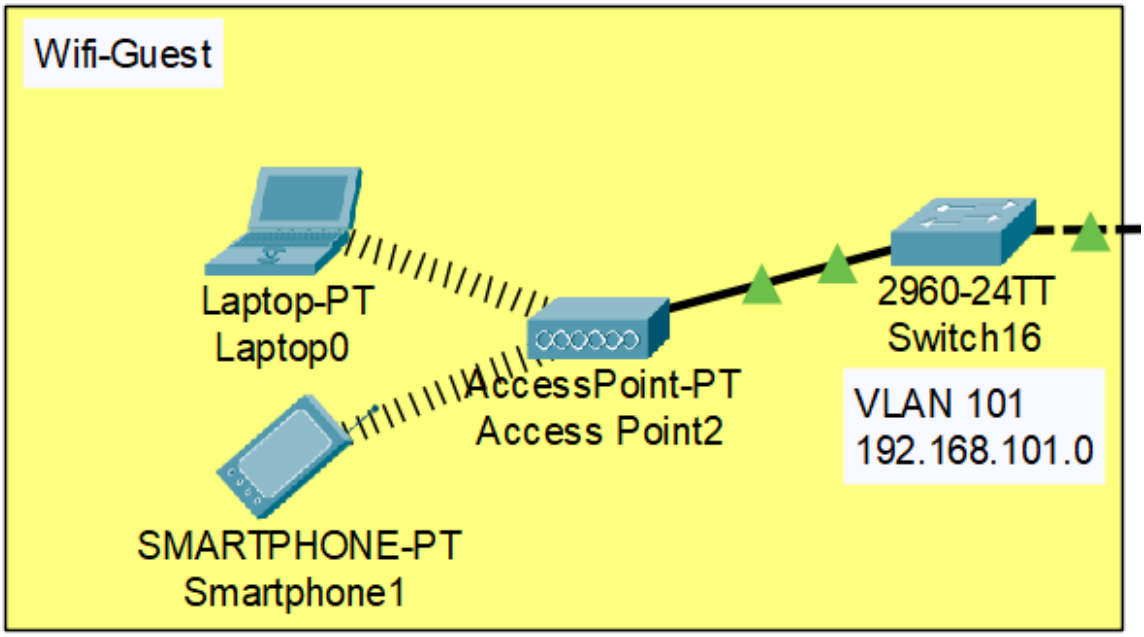
Hình 11: *Cấu trúc cơ sở chính*

- **Cấu trúc các tầng:** Cơ sở chính có 2 tòa nhà, mỗi tòa nhà có 5 tầng với thiết kế giống nhau



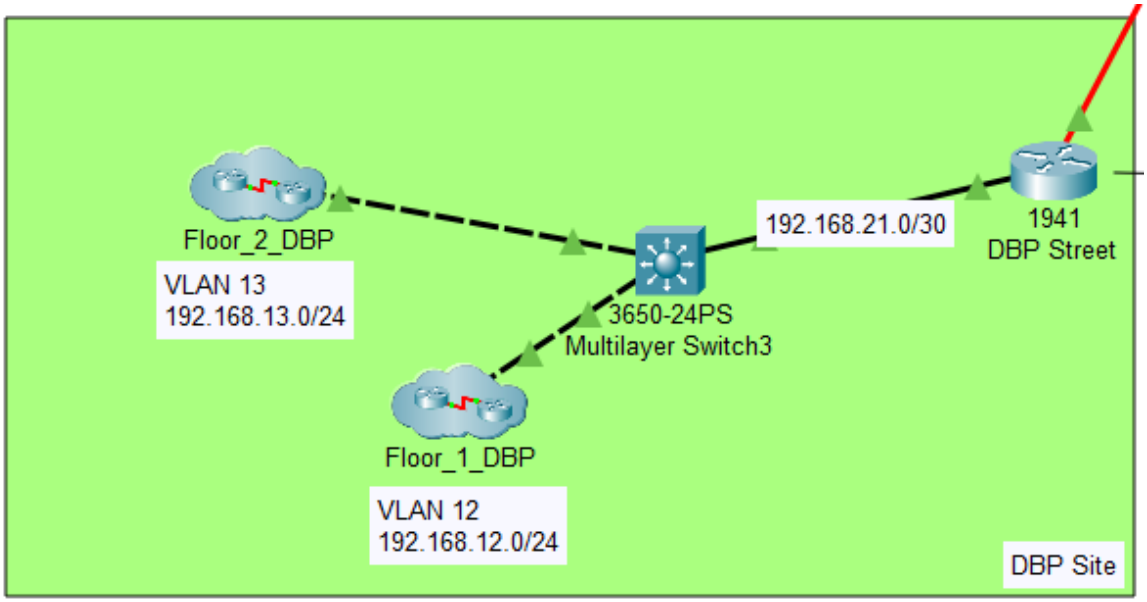
Hình 12: *Cấu trúc mỗi tầng của cơ sở chính*

- **Wifi:** mạng chung của khách hàng sử dụng



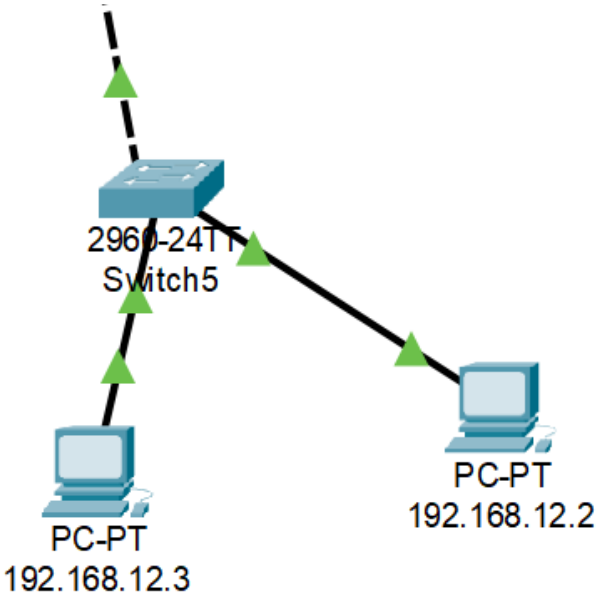
Hình 13: *Cấu trúc Wifi cơ sở chính*

5.6 Cơ sở DBP



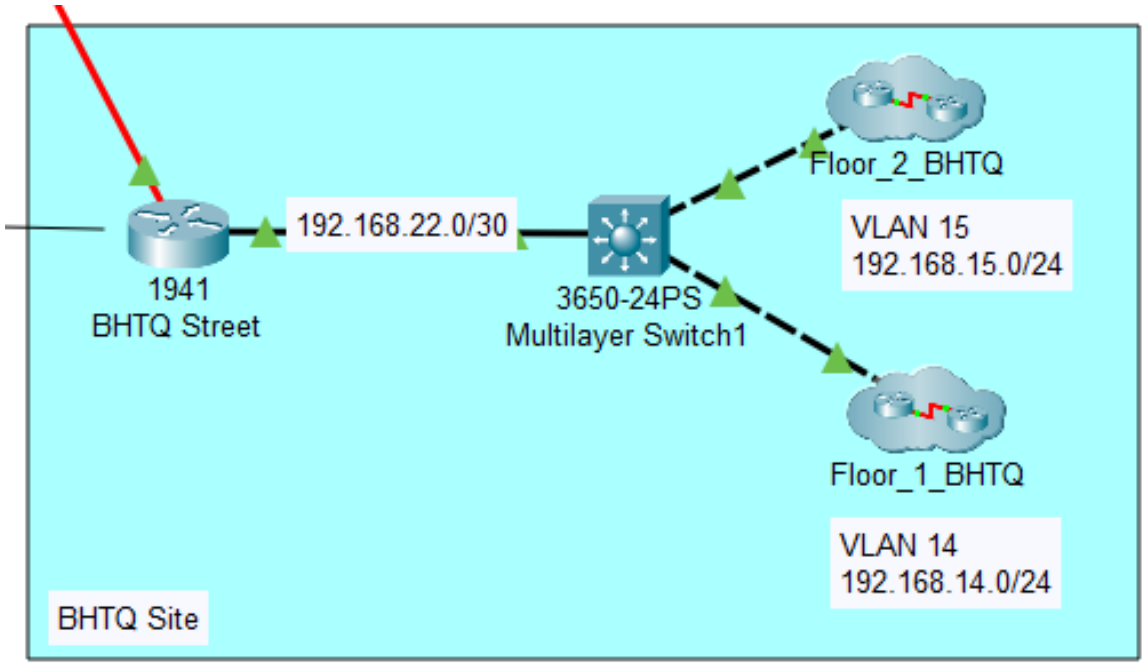
Hình 14: *Cấu trúc cơ sở DBP*

- **Cấu trúc các tầng:** Cơ sở DBP có 2 tầng với thiết kế giống nhau



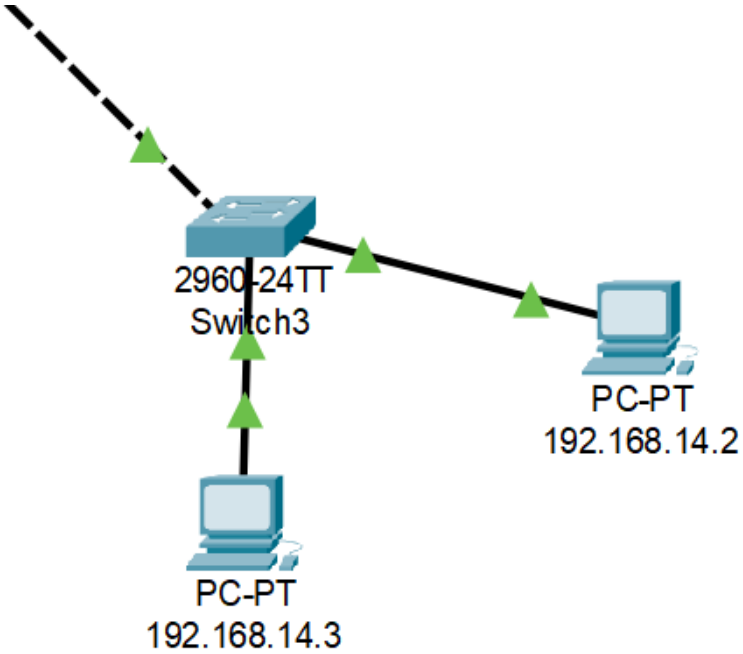
Hình 15: *Cấu trúc mỗi tầng cơ sở DBP*

5.7 Cơ sở BHTQ



Hình 16: *Cấu trúc cơ sở BHTQ*

- **Cấu trúc các tầng:** Cơ sở BHTQ có 2 tầng với thiết kế giống nhau

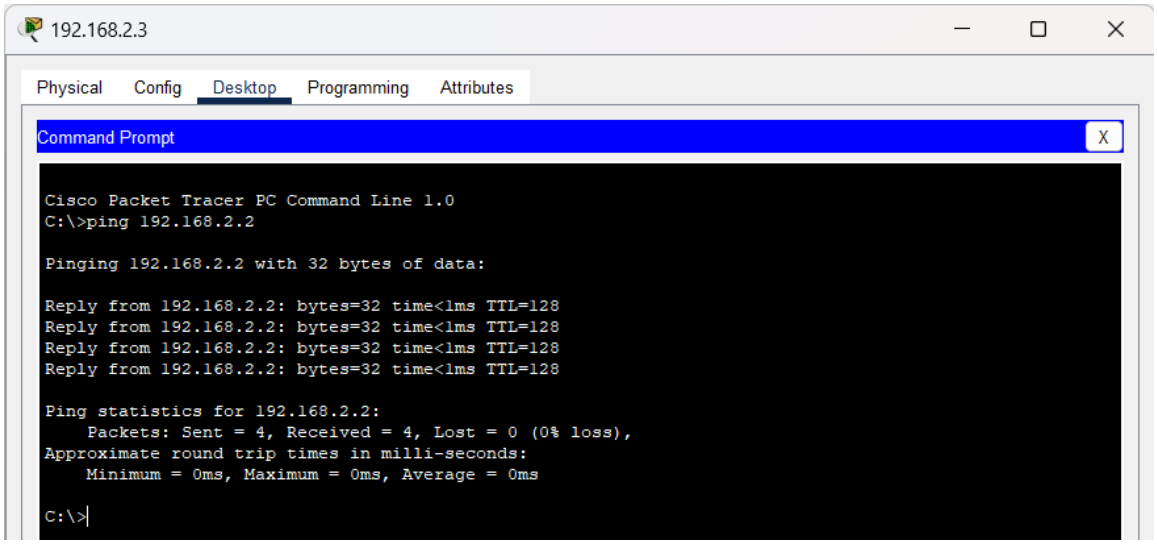


Hình 17: *Cấu trúc mỗi tầng cơ sở BHTQ*

6 Kiểm tra hệ thống

6.1 Kết nối giữa các thiết bị cùng VLAN

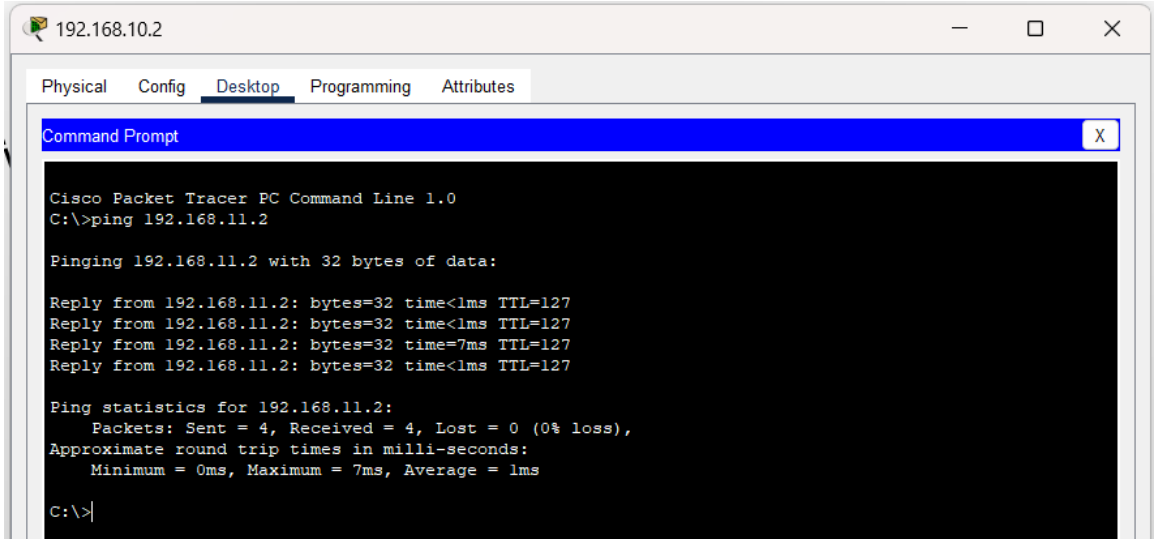
- Thực hiện ping từ PC(192.168.2.3) ở tầng 1 tòa A trụ sở chính (VLAN2) đến PC(192.168.2.2) ở cùng tầng, cùng VLAN2



Hình 18: *Kiểm tra kết nối của các máy cùng VLAN2*

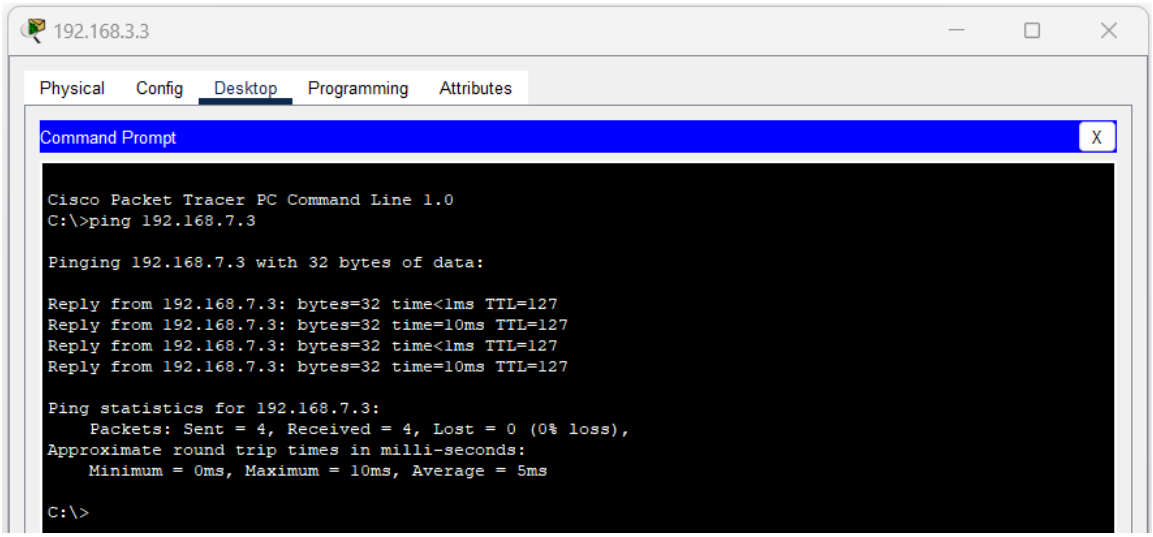
6.2 Kết nối giữa các thiết bị khác VLAN

- Thực hiện ping từ PC(192.168.10.2) ở tầng 4 tòa B trụ sở chính (VLAN10) đến PC(192.168.11.2) ở tầng 5, cùng tòa B (VLAN11)



Hình 19: *Kiểm tra kết nối của các máy khác tầng (khác VLAN) trong một tòa nhà*

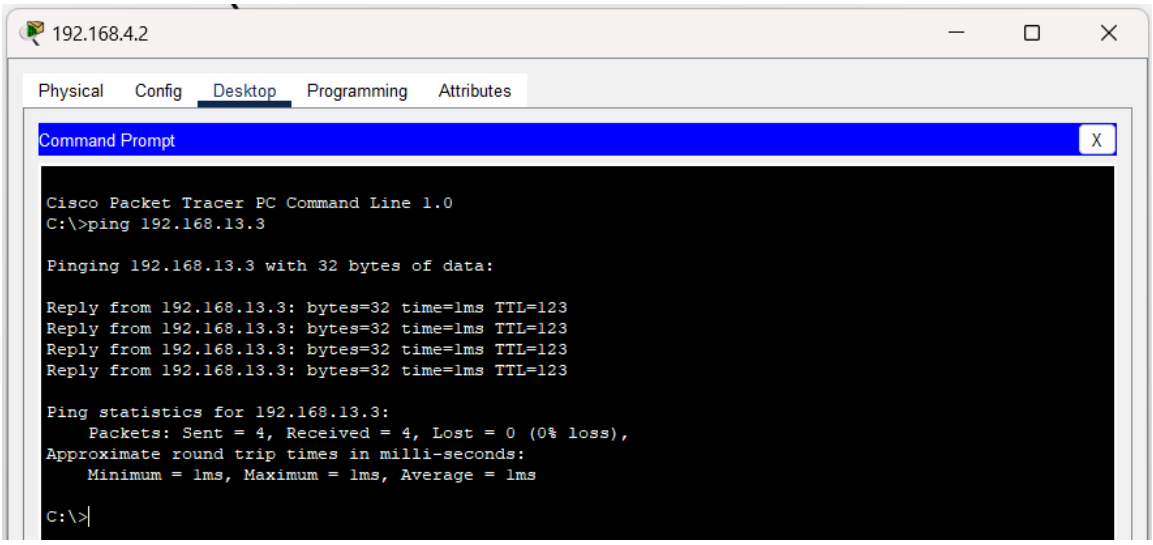
- Thực hiện ping từ PC(192.168.3.3) ở tầng 2 tòa A trụ sở chính (VLAN3) đến PC(192.168.7.3) ở tầng 1 tòa B (VLAN7)



Hình 20: *Kiểm tra kết nối của các máy khác tòa nhà tại trụ sở chính*

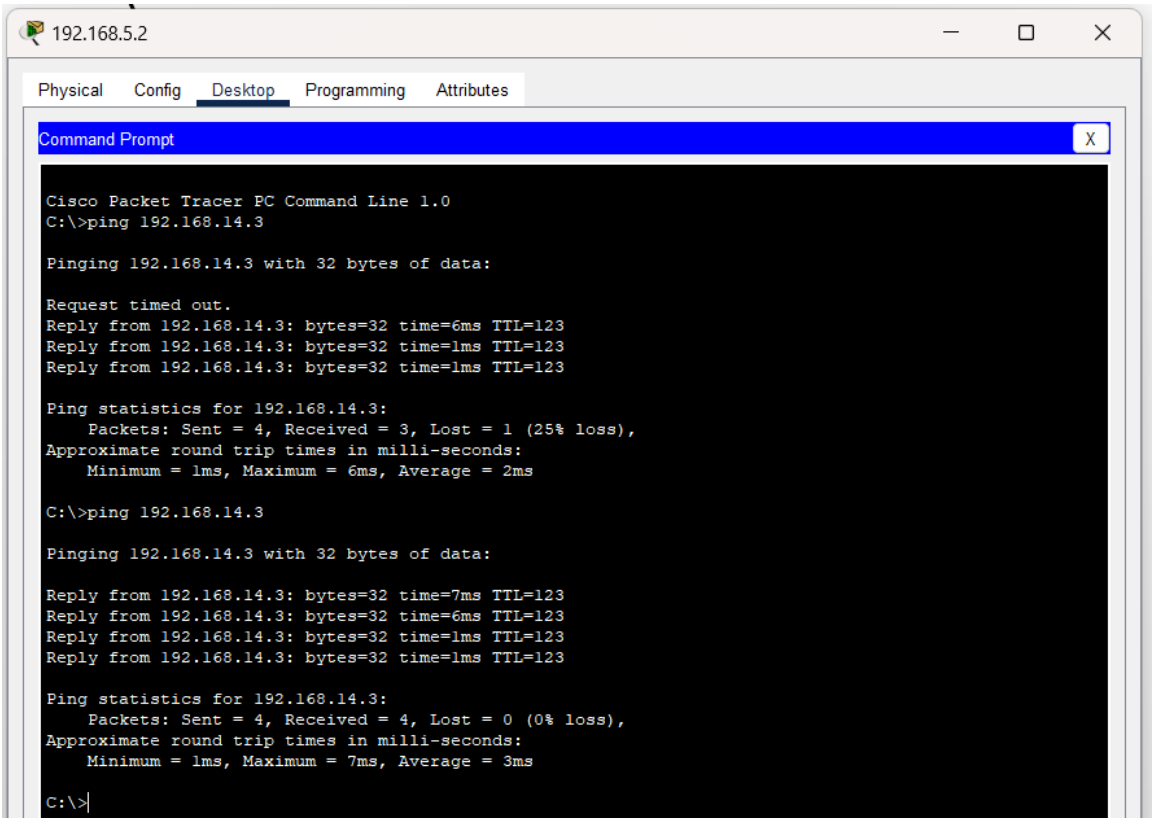
6.3 Kết nối giữa cơ sở

- Thực hiện ping từ PC(192.168.4.2) ở tầng 3 tòa A trụ sở chính (VLAN4) đến PC(192.168.13.3) ở tầng 2 trụ sở DBP (VLAN13)



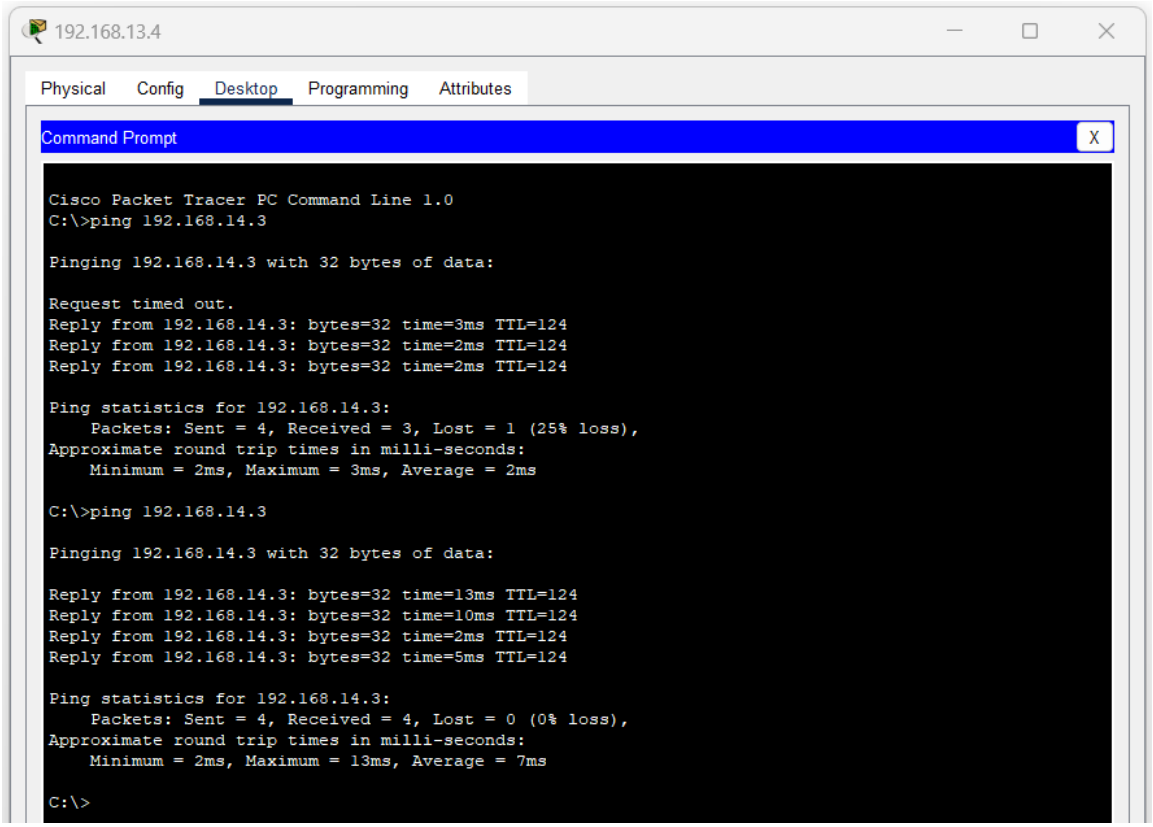
Hình 21: *Kiểm tra kết nối của các máy giữa trụ sở chính và trụ sở DBP*

- Thực hiện ping từ PC(192.168.5.2) ở tầng 4 trụ sở chính (VLAN5) đến PC(192.168.14.3) ở tầng 1 trụ sở BHTQ (VLAN14)



Hình 22: *Kiểm tra kết nối của các máy giữa trụ sở chính và trụ sở BHTQ*

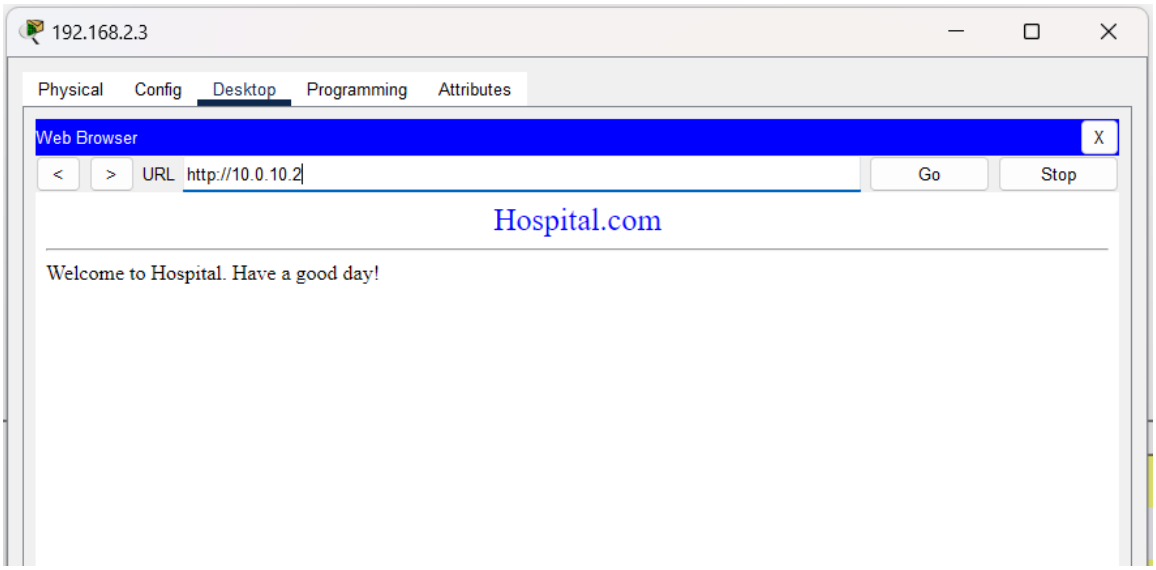
- Thực hiện ping từ PC(192.168.13.4) ở tầng 2 trụ sở DBP (VLAN13) đến PC(192.168.14.3) ở tầng 1 trụ sở BHTQ (VLAN14)



Hình 23: *Kiểm tra kết nối của các máy giữa trụ sở DBP và trụ sở BHTQ*

6.4 Kết nối với web server tại DMZ

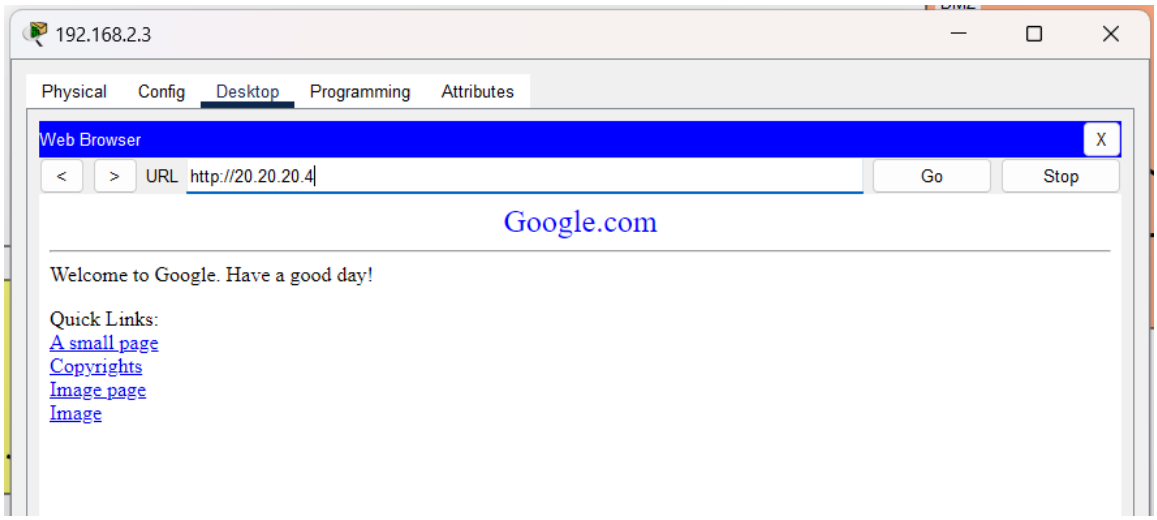
- Thực hiện kết nối từ PC(192.168.2.3) (VLAN2) đến web server Hospital.com đặt tại DMZ



Hình 24: *Kiểm tra kết nối giữa thiết bị nội bộ và web server tại DMZ*

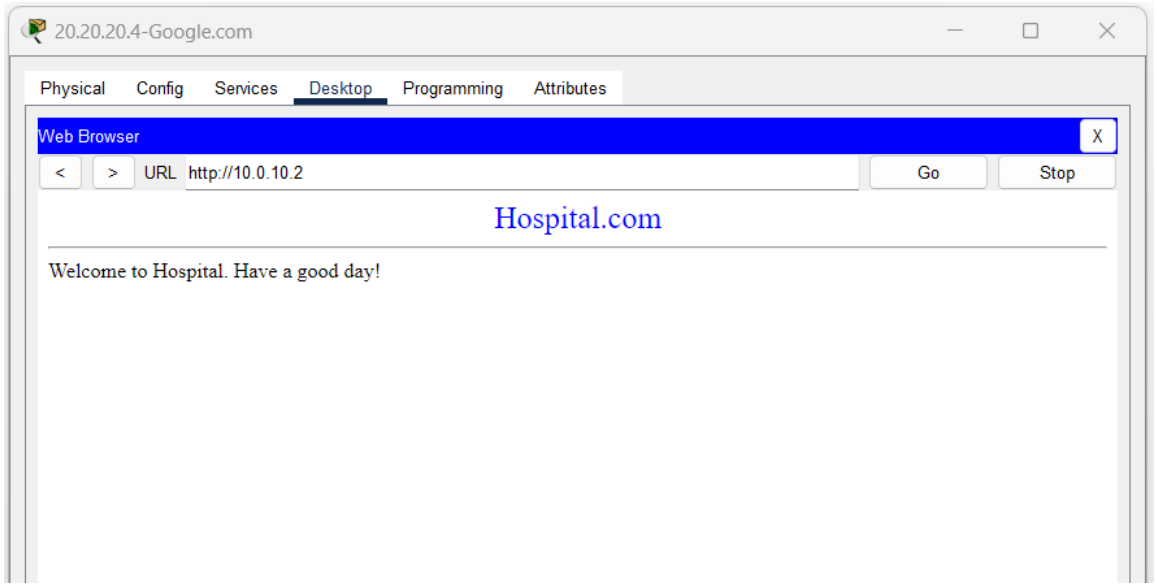
6.5 Kết nối với web server Internet

- Thực hiện kết nối từ PC(192.168.2.3) (VLAN2) đến web server Google.com ở Internet bên ngoài



Hình 25: *Kiểm tra kết nối giữa thiết bị nội bộ và web server ở Internet bên ngoài*

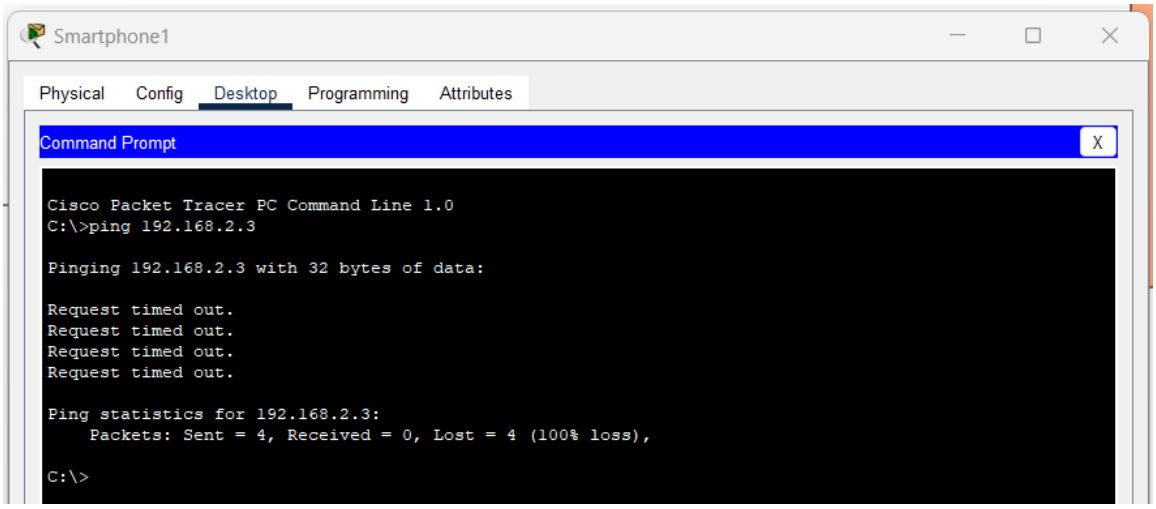
6.6 Kết nối Internet với web server tại DMZ



Hình 26: *Kiểm tra kết nối từ Internet đến web server tại DMZ*

6.7 Kết nối giữa thiết bị khách hàng với thiết bị nội bộ

- Thực hiện kết nối từ thiết bị khác hàng kết nối qua Accesspoint đến thiết bị nội bộ PC(192.168.2.3 thuộc VLAN2)
  => Kết nối thất bại



Hình 27: *Kết nối giữa thiết bị khách hàng với thiết bị nội bộ*

7 Đánh giá hệ thống

7.1 Các công nghệ đã hiện thực được

1. **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 hỗ trợ quản lý.
   - Dùng Inter-VLAN Routing để các VLAN có thể giao tiếp hiệu quả qua Layer 3.
2. **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.
3. **Máy chủ DHCP:** Tự động cấp phát địa chỉ IP cho các thiết bị trong mạng, giảm thiểu sai sót so với cấu hình thủ công.
4. **Hệ thống không dây:** 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.

7.2 Các tiêu chí đánh giá

1. **Độ tin cậy (Reliability):**
   - *Ưu điểm:* Hệ thống sử dụng mô hình mạng phân cấp với các cơ chế dự phòng ở lớp lõi và lớp phân phối giúp đảm bảo độ tin cậy cao, giảm thiểu thời gian chết. Hơn nữa, việc áp dụng các công nghệ như GPON và Ethernet tốc độ cao (1GbE/10GbE/40GbE) cung cấp hiệu suất ổn định.
   - *Nhược điểm:* Hệ thống có thể bị ảnh hưởng nếu các thiết bị cốt lõi hoặc đường truyền WAN gặp sự cố nghiêm trọng mà không được dự phòng đầy đủ.
2. **Hiệu suất (Performance):**
   - Chưa có cân bằng tải tại Gateway dẫn đến việc tải trọng không dược phân phối giữa các địa điểm
   - Tất cả lưu lượng mạng đều đi qua một router tại trụ sở chính (Main site), biến nó thành một điểm tắc nghẽn tiềm năng (congestion point)
3. **Dễ nâng cấp (Ease of Upgrade):**

- *Ưu điểm:* Mô hình phân cấp cho phép bổ sung thiết bị tại từng lớp mà không cần thay đổi toàn bộ hệ thống. Các thiết bị hiện đại với khả năng mở rộng cổng và băng thông giúp dễ dàng nâng cấp khi mạng phát triển theo tốc độ dự kiến 20% trong 5 năm tới.
- *Nhược điểm:* Việc nâng cấp có thể đòi hỏi chi phí cao và yêu cầu nhân viên có kỹ năng để cấu hình các thiết bị mới mà không làm gián đoạn hoạt động của mạng.

4. **Hỗ trợ phần mềm đa dạng (Diverse Support Software):**
   - *Ưu điểm:* Hệ thống hỗ trợ nhiều phần mềm cả mã nguồn mở và có bản quyền như HIS, RIS-PACS, LIS, CRM, cùng với ứng dụng văn phòng, đa phương tiện và cơ sở dữ liệu, đảm bảo đáp ứng đầy đủ các nhu cầu sử dụng của bệnh viện.
   - *Nhược điểm:* Quản lý và duy trì nhiều loại phần mềm đòi hỏi nhân viên IT phải có kỹ năng cao và các tài nguyên quản lý tập trung như máy chủ và cơ sở dữ liệu mạnh.
5. **An toàn mạng (Network Safety):**
   - *Ưu điểm:* Việc sử dụng các VLAN cho từng phòng ban giúp giảm thiểu nguy cơ truy cập trái phép. Các giao thức VPN và SD-WAN tăng cường bảo mật cho việc kết nối giữa các cơ sở.
   - *Nhược điểm:* Hệ thống chưa triển khai hoàn chỉnh các biện pháp phòng chống tấn công như tường lửa, phát hiện phishing hoặc bảo vệ dữ liệu khỏi các lỗ hổng bảo mật nghiêm trọng.

7.3 Định hướng phát triển trong tương lai

1. **Triển khai hệ thống tường lửa mạnh mẽ:** Cấu hình và triển khai hệ thống tường lửa thế hệ mới (Next-Generation Firewall) như Cisco Firepower để bảo vệ toàn bộ hệ thống mạng.
2. **Xây dựng cơ chế VPN bảo mật:**
   - Triển khai VPN cho người làm việc từ xa với giao thức bảo mật cao như IPsec hoặc SSL.
   - Kết hợp xác thực hai yếu tố (2FA) để tăng cường bảo mật truy cập từ xa.
3. **Bổ sung thêm các tính năng hữu ích:** Email, hệ thống camera giám sát
4. **Thiết kế lại hệ thống DNS:** nhằm tối ưu hóa việc phân giải tên miền, giúp người dùng truy cập đến các máy chủ web nội bộ và bên ngoài một cách nhanh chóng và ổn định hơn.
5. **Bổ sung thêm Load Balancer:** Bổ sung cơ chế cân bằng tải để phục vụ hệ thống trong giờ cao điểm, hạn chế tình trạng nghẽn hoặc sập server.