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

MẠNG MÁY TÍNH (CO3094)

BÀI TẬP LỚN 2

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE HOSPITAL

Giảng viên hướng dẫn:	TS. Nguyễn Lê Duy Lai	
Sinh viên thực hiện:	Nguyễn Tuấn Huy	2211253
	Võ Hoàng Huy	2211298
	Nguyễn Văn Nhật Huy	2211254

TP. HỒ CHÍ MINH, THÁNG 11/2024

Mục lục

1 Bảng phân công công việc

No.	Họ và tên	Nhiệm vụ	Phần trăm công việc
1	Nguyễn Tuấn Huy	Thiết kế + Report + Slide	100%
2	Võ Hoàng Huy	Thiết kế + Report + Slide	100%
3	Nguyễn Văn Nhật Huy	Thiết kế + Report + Slide	100%

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

2.1 Yêu cầu cho hệ thống mạng

2.1.1 Yêu cầu cho trụ sở chính

- 2 tòa nhà A và B (5 tầng với 10 phòng/tầng) được trang bị máy tính và các thiết bị y tế.
- Trung tâm dữ liệu, IT và Phòng Cáp Trung tâm (sử dụng các bảng kết nối dây cáp) được đặt trong một phòng riêng, cách tòa nhà A và B 50m.
- Quy mô trung bình: 600 máy trạm, 10 máy chủ, 12 thiết bị mạng (hoặc có thể nhiều hơn với các thiết bị chuyên biệt về bảo mật).
- Kết nối không dây phải bao phủ 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 GigaEthernet 1GbE/10GbE/40GbE.
- Mạng con tại trụ sở chính kết nối với hai địa điểm khác (Site DBP và Site BHTQ) bằng 2 đường truyền thuê riêng cho kết nối WAN với cơ chế cân bằng tải.
- Sử dụng kết hợp phần mềm có bản quyền và mã nguồn mở.

2.1.2 Yêu cầu cho các trụ sở chi nhánh

- Tòa nhà có 2 tầng, tầng 1 được trang bị 1 phòng IT và 1 phòng Cáp Trung tâm.
- Quy mô nhỏ: 60 máy trạm, 2 máy chủ, 5 thiết bị mạng hoặc hơn.

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 Checklist khảo sát tại địa điểm lắp đặt

Trước khi chuẩn bị bắt tay xây dựng một hệ thống mạng, việc trước hết và quan trong nhất phải làm là khảo sát trước địa điểm cần cài đặt hệ thống mạng đó, các nội dung cần được khảo sát bao gồm:

Check	Nội dung	Chi tiết thông số
☐	Đánh giá tổng quan	• Đánh giá kiến trúc tòa nhà, cơ sở hạ tầng mạng sẵn có • Dự đoán các vùng gây khó khăn: lắp đặt, kết nối • Lựa chọn mô hình khảo sát phù hợp: Data, Voice, Location
☐	Đặc điểm triển khai	• Mức độ dày đặc, phủ sóng kết nối các thiết bị • Tính di động trang thiết bị kết nối • Đặc điểm khí hậu, môi trường lắp đặt • Khoảng cách giữa các chi nhánh với trụ sở • Vị trí các giám sát đặc biệt, góc quay và lắp đặt cho camera
☐	Công cụ khảo sát	• Xây dựng bản đồ khảo sát: tòa nhà, các phòng, lối đi chuyển • Công cụ: phân tích tầm phủ sóng, đo đạc diện tích, khoảng cách • Vị trí các thiết bị kiểm thử
☐	Số lượng thiết bị	• Số lượng, vị trí các phòng ban, thiết bị kết nối • Số lượng các nhân viên làm việc từ xa • Mục đích sử dụng, lưu lượng các server hệ thống
☐	Yêu cầu vật lý	• Điện năng tiêu thụ • Vị trí các đường dẫn kết nối điện, mạng • Cân nhắc loại giá đỡ, dây buộc, đường nối dây

2.3 Xác định khu vực có tải cao

2.3.1 Cách bố trí các tầng của các tòa

Trụ sở chính

- **Tòa A**: Khu vực khám và điều trị
  - Tầng 1: Khu vực tiếp nhận bệnh nhân
    - Phòng lễ tân & tiếp đón: 15 workstations (đăng ký bệnh nhân).
    - Phòng chờ bệnh nhân: 5 workstations (Wi-Fi công cộng, hỗ trợ).
    - Phòng thông tin: 5 workstations (hỗ trợ, hướng dẫn).
    - Phòng kế toán: 10 workstations (thanh toán hóa đơn).
    - 5-10 phòng trống dành cho mở rộng hoặc lưu trữ vật tư.
  - Tầng 2: Khu khám ngoại trú
    - Mỗi phòng là một phòng khám chuyên khoa: 1-9, mỗi phòng có 2 workstations cho bác sĩ (tổng 18)
    - 10, phòng hỗ trợ y khoa: 5 workstations.
  - Tầng 3-4: Phòng điều trị và chẩn đoán
    - Mỗi tầng chia thành 10 phòng, mỗi phòng có 4 workstations:
      1-9. Phòng chẩn đoán hình ảnh, xét nghiệm (HIS, LIS).
    - 10. Phòng PACS: lưu trữ và xử lý hình ảnh chẩn đoán.
  - Tầng 5: Văn phòng quản lý
    - 1-3. Phòng quản lý hành chính: 15 workstations.
    - 4. Phòng họp: 5 workstations + thiết bị trình chiếu.
    - 5-6. Phòng nhân sự: 10 workstations.
    - 7-10. Kho tài liệu và phòng hỗ trợ khác.
- **Tòa B**: Khu hỗ trợ và nghiên cứu
  - Tầng 1: Phòng công vụ và kho vật tư
    - 1-2. Phòng vận hành thiết bị: 10 workstations.
    - 3-6. Phòng kho và hậu cần.
    - 7-10. Phòng trống cho mở rộng.
  - Tầng 2: Phòng nghiên cứu
    - Mỗi phòng 3 workstations: 1-8, phòng nghiên cứu y học, công nghệ (24 workstations).
    - 9. Phòng họp nghiên cứu: 5 workstations.
    - 10. Phòng dữ liệu nghiên cứu: 10 workstations.
  - Tầng 3-4: Hỗ trợ công nghệ và tài chính
    - Chia thành 10 phòng mỗi tầng:
      1-4. Phòng IT hỗ trợ: 15 workstations (kỹ thuật viên).
      5-10. Phòng kế toán và tài chính: 20 workstations.
  - Tầng 5: Hội đồng quản trị và ban giám đốc
    - 1-3. Phòng giám đốc: 5 workstations.
    - 4-5. Phòng họp cao cấp: 5 workstations + thiết bị trình chiếu.
    - 6-10. Phòng lưu trữ và quản lý dự án.

2.3.2 Xác định khu vực có tải cao

Tòa A

- Tầng 1 (Tiếp nhận bệnh nhân và hành chính): Đây là nơi tiếp nhận bệnh nhân, thực hiện thanh toán, và xử lý thông tin hành chính. 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 3-4 (Chẩn đoán hình ảnh và PACS): PACS (Picture Archiving and Communication System) xử lý và lưu trữ các hình ảnh y khoa (CT, MRI, X-ray), yêu cầu băng thông cực lớn. LIS (Laboratory Information System) kết nối các thiết bị xét nghiệm để truyền dữ liệu sinh học liên tục đến các server. Tải cao từ dữ liệu hình ảnh PACS và xét nghiệm LIS.

Tòa B

- Tầng 2 (Phòng nghiên cứu): Các phòng nghiên cứu cần truy cập dữ liệu từ PACS, LIS và HIS để phân tích, báo cáo. Một số ứng dụng nghiên cứu có thể yêu cầu tải xuống và tải lên dữ liệu lớn từ các server hoặc Internet. Tải cao do các tác vụ nghiên cứu.

Data Center (Trung tâm dữ liệu)

- 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.

2.4 Tổng quan thiết kế mạng

2.4.1 Cấu trúc mạng tổng quan

Cấu trúc mạng: hình sao (Star Topology)

- Với cấu trúc này, các nút mạng ở biên hoạt động độc lập với nhau nên khi một nút mạng bị lỗi, các nút mạng khác vẫn có thể hoạt động bình thường, trừ trường hợp thiết bị mạng trung tâm bị lỗi.
- Cấu trúc này cho phép người thiết kế có thể thêm các thiết bị mà không ảnh hưởng quá nhiều đến mạng có sẵn, hoạt động tốt với tải nặng.

Tích hợp không dây

- Mạng Lưới Wi-Fi (Wireless Mesh Network): Sử dụng AP hỗ trợ Wi-Fi 6, đảm bảo vùng phủ sóng mạnh mẽ và băng thông cao.
- Vị Trí Đặt AP: Phân bổ chiến lược để tránh vùng chết, đặc biệt tại khu vực đông người như sảnh, phòng thí nghiệm, và trung tâm chẩn đoán.

2.4.2 Phân khu mạng

- **VLAN cho từng tầng**: Mỗi tầng sẽ được gán vào một VLAN riêng biệt để đảm bảo việc phân chia lưu lượng và tăng cường bảo mật. Ví dụ, các phòng y tế (HIS, PACS) sẽ có VLAN riêng biệt với các khu vực hành chính. Điều này giúp giảm thiểu các nguy cơ xâm nhập và đảm bảo rằng thông 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.
- **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 như HIS, PACS, LIS sẽ được đưa vào Server Farm, 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.
- **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.
- **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 SSL/TLS và 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.

2.4.3 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 cho thiết kế mạng

3.1 Các thiết bị mạng sử dụng

3.1.1 Router

Router 1941/K9: Được sử dụng để kết nối mạng nội bộ của bệnh viện với các cơ sở phụ và 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 bao gồm định tuyến tĩnh, RIP (Routing Information Protocol), OSPF (Open Shortest Path First), và EIGRP (Enhanced Interior Gateway Routing Protocol). 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 kĩ thuật:

- Gigabit Ethernet: 2 cổng WAN hoặc LAN 10/100/1000
- Serial: 2 cổng RJ45
- Memory DRAM: 512 MB (mặc định) / 2 GB (tối đa)
- Bộ nhớ flash: 256 MB (mặc định) / 8 GB (tối đa)

Hình 1: Router ISR4331/K9

3.1.2 Multilevel Switch

Multilayer Switch 3560-24PS: Được sử dụng để kết nối các switch tại các tầng và phòng ban trong bệnh viện. Với 2 cổng Gigabit Ethernet, thiết bị này kết nối trực tiếp với tường lửa và lớp Core để quản lý lưu lượng giữa các khu vực. Ngoài chức năng chuyển mạch (Layer 2), thiết bị còn hỗ trợ định tuyến (Layer 3) giữa các VLAN của các bộ phận như hành chính, chẩn đoán hình ảnh (PACS), nghiên cứu, và tài chính. Điều này đảm bảo các mạng con trong bệnh viện có thể giao tiếp hiệu quả mà không cần hoàn toàn phụ thuộc vào router. Đây là lựa chọn lý tưởng để triển khai hệ thống mạng nội bộ phức tạp, đảm bảo hiệu suất cao và giảm độ trễ trong xử lý dữ liệu quan trọng.

Thông số kĩ thuật:

- Fast Ethernet: 24 Ethernet 10/100 ports
- Gigabit Ethernet: 2 SFP-based Gigabit Ethernet ports
- IEEE 802.3af and Cisco prestandard Power over Ethernet
- 1 Rack Unit (RU) fixed configuration, multilayer switch
- Standard Multilayer Software Image (SMI) or Enhanced Image (EMI) installed
- Basic RIP and static routing, upgradable to full dynamic IP routing (SMI).
- Advanced IP routing (EMI).

Hình 2: Multilayer Switch 3560-24PS

3.1.3 Switch

Switch Cisco WS-C2960-24TT-L: Được sử dụng làm switch truy cập chính trong hệ thống mạng bệnh viện, kết nối các máy trạm (workstations), thiết bị y tế IoT, và các điểm truy cập Wi-Fi (Access Point) trong từng phòng ban. Thiết bị này hỗ trợ truyền tải dữ liệu từ các khu vực như tiếp nhận bệnh nhân, điều trị, chẩn đoán hình ảnh (PACS), nghiên cứu, và khu hành chính. Với khả năng bảo mật cao, hiệu suất ổn định và dễ dàng cấu hình, thiết bị đảm bảo đáp ứng tốt nhu cầu mạng tại các khu vực trọng yếu của bệnh viện. Thông số kĩ thuật:

- Ethernet: 24 cổng Ethernet 10/100
- Gigabit Ethernet: 2 cổng uplink Ethernet 10/100/1000
- Memory DRAM: 64 MB
- Bộ nhớ flash: 32 MB

Hình 3: Switch Cisco WS-C2960-24TT-L

3.1.4 Access Point

Access Point PT: Được triển khai làm điểm truy cập không dây chính trong hệ thống mạng của bệnh viện, AP-PT hỗ trợ kết nối các thiết bị di động, máy trạm (workstations), và thiết bị IoT y tế tại các khu vực như phòng khám, phòng chẩn đoán, khu vực hành chính và phòng nghiên cứu. Với khả năng hỗ trợ băng tần 2.4GHz, AP-PT cung cấp mạng không dây ổn định và có độ phủ sóng rộng cho các khu vực lớn trong bệnh viện, từ phòng tiếp nhận bệnh nhân cho đến các khu phòng điều trị và nghiên cứu. Dữ liệu được truyền tải từ các phòng ban và thiết bị đầu cuối qua AP-PT về các switch truy cập, đảm bảo thông suốt và an toàn cho các hoạt động y tế quan trọng. Việc triển khai AP-PT giúp bệnh viện duy trì kết nối mạng ổn định và liên tục cho mọi hoạt động, từ chăm sóc bệnh nhân đến nghiên cứu y học. Thông số kĩ thuật:

- Hỗ trợ Fast Ethernet
- Bandwidth: 2.4GHz

Hình 4: Access Point AP-PTs

3.1.5 Firewall

Cisco ASA 5506-X: Là thiết bị bảo mật mạnh mẽ, được triển khai trong hệ thống mạng bệnh viện để kiểm soát lưu lượng mạng vào và ra giữa các khu vực mạng nội bộ của bệnh viện và các kết nối từ bên ngoài, như kết nối Internet hoặc mạng chi nhánh. Cisco ASA 5506-X cung cấp một lớp bảo mật mạnh mẽ, giúp bảo vệ hệ thống mạng khỏi các tấn công từ bên ngoài và đảm bảo rằng chỉ các kết nối hợp lệ được phép đi qua.

Thông số kĩ thuật:

- Cổng: 8 cổng Gigabit Ethernet.
- Hỗ trợ các VLAN: Tạo và quản lý tối đa ba VLAN riêng biệt.
- Tốc độ cổng: Tất cả các cổng Gigabit Ethernet.
- VPN: Hỗ trợ SSL VPN và IPsec VPN cho kết nối từ xa.
- Quản lý: Cung cấp giao diện quản lý đồ họa (ASDM) giúp quản lý và cấu hình thiết bị dễ dàng và hiệu quả.

- Bảo mật: Hỗ trợ các tính năng bảo mật nâng cao như tường lửa, bảo vệ từ các tấn công DDoS, và kiểm soát lưu lượng mạng.

Hình 5: Cisco ASA 5506-X

3.2 Cách bố trí các thiết bị mạng

3.2.1 Data Center và DMZ Zone

- Data Center là nơi tập trung các hệ thống quan trọng của bệnh viện, bao gồm các máy chủ HIS (Hospital Information System), PACS (Picture Archiving and Communication System), LIS (Laboratory Information System), và các dịch vụ mạng như email server hoặc web server.
- DMZ Zone (Demilitarized Zone) là khu vực bảo mật dành riêng cho các dịch vụ công cộng hoặc các dịch vụ cần tiếp cận từ bên ngoài, ví dụ như website bệnh viện hoặc email server. Các máy chủ trong DMZ không được truy cập trực tiếp từ mạng nội bộ để tránh rủi ro bảo mật.
- Kết nối giữa Data Center và DMZ Zone: Việc kết nối các máy chủ trong Data Center và DMZ Zone qua một Switch trung tâm giúp chia sẻ lưu lượng mạng đồng thời dễ dàng quản lý và bảo mật. DMZ giúp tách biệt các dịch vụ công cộng khỏi các hệ thống nội bộ quan trọng.

3.2.2 Kết nối Máy Chủ ISP và Cloud

- ISP (Internet Service Provider) cung cấp kết nối internet cho bệnh viện. Các máy chủ của ISP sẽ được kết nối với Router chính của hệ thống mạng bệnh viện.
- Router chính sẽ kết nối với Cloud, nơi dữ liệu được lưu trữ và các dịch vụ từ bên ngoài sẽ được xử lý.
- DSL-modem sẽ kết nối đến internet, nơi mọi dữ liệu từ bệnh viện sẽ ra ngoài và ngược lại. Dữ liệu này phải được bảo vệ trước khi đi vào mạng bệnh viện thông qua một Firewall. Firewall sẽ kiểm soát các truy cập và bảo vệ hệ thống trước các mối đe dọa từ bên ngoài.

3.2.3 Kết Nối Mạng Ngoài

- Các thiết bị từ bên ngoài như người dùng từ các văn phòng, đối tác hoặc các dịch vụ sẽ kết nối vào mạng bệnh viện qua một Switch. Tất cả các kết nối từ bên ngoài này sẽ được bảo vệ bằng Firewall 1, giúp ngăn ngừa các mối đe dọa và đảm bảo an toàn cho hệ thống.
- Các kết nối này sau đó sẽ được phân phối qua Cloud và kết nối internet qua DSL-modem.

3.2.4 Mạng Trong Bệnh Viện

- Tòa A và Tòa B sẽ được kết nối với Multilayer Switch. Multilayer Switch có thể xử lý và phân phối lưu lượng mạng không chỉ ở Layer 2 (Data Link) mà còn ở Layer 3 (Network Layer), giúp chia sẻ và tối ưu hóa băng thông giữa các tầng, các phòng ban và giữa các tòa nhà trong bệnh viện.
- Mỗi tòa nhà có 5 tầng, mỗi tầng sẽ có một Switch riêng biệt để phân phối mạng cho các phòng ban. Các Switch tầng giúp quản lý lưu lượng mạng hiệu quả giữa các phòng, từ phòng khám, phòng điều trị, đến phòng nghiên cứu.
- Access Points (AP) sẽ được phân phối ở những khu vực cần kết nối Wi-Fi, chẳng hạn như phòng chờ bệnh nhân, phòng khám, và các khu vực văn phòng. Mỗi AP sẽ kết nối với mạng nội bộ của bệnh viện qua các VLAN được cấu hình riêng biệt, giúp phân tách mạng của nhân viên và bệnh nhân. Điều này giúp tăng cường bảo mật mạng bệnh viện và tránh các nguy cơ bị truy cập trái phép từ mạng của bệnh nhân.

3.2.5 Kết nối với các phân điểm phụ

- Phân điểm phụ sẽ được kết nối qua một Router chính, sau đó kết nối tiếp với các Router phụ ở các phân điểm phụ. Điều này giúp việc quản lý lưu lượng mạng giữa các khu vực và phân điểm phụ được hiệu quả.

3.3 Phương án cấp phát IP

Tòa A

VLAN	Tầng	Khu vực	Địa chỉ mạng	Địa chỉ khả dụng
2	1	Khu vực tiếp nhận bệnh nhân	192.168.2.0/24	192.168.2.1 - 192.168.2.254
3	2	Khu khám ngoại trú	192.168.3.0/24	192.168.3.1 - 192.168.3.254
4	3	Phòng điều trị và chẩn đoán	192.168.4.0/24	192.168.4.1 - 192.168.4.254
5	4	Phòng điều trị và chẩn đoán	192.168.5.0/24	192.168.5.1 - 192.168.5.254
6	5	Văn phòng quản lý	192.168.6.0/24	192.168.6.1 - 192.168.6.254

Bảng 1: Bảng VLAN và địa chỉ IP nội bộ khả dụng của tòa A trụ sở chính

VLAN	Default Gateway
2	192.168.2.1
3	192.168.3.1
4	192.168.4.1
5	192.168.5.1
6	192.168.6.1

Bảng 2: Bảng VLAN và default gateway cho từng VLAN ở tòa A

Tòa B

VLAN	Tầng	Khu vực	Địa chỉ mạng	Địa chỉ khả dụng
7	1	Phòng công vụ và kho vật tư	192.168.7.0/24	192.168.7.1 - 192.168.7.254
8	2	Phòng nghiên cứu	192.168.8.0/24	192.168.8.1 - 192.168.8.254
9	3	Hỗ trợ công nghệ và tài chính	192.168.9.0/24	192.168.9.1 - 192.168.9.254
10	4	Hỗ trợ công nghệ và tài chính	192.168.10.0/24	192.168.10.1 - 192.168.10.254
11	5	Hội đồng quản trị và ban giám đốc	192.168.11.0/24	192.168.11.1 - 192.168.11.254

Bảng 3: Bảng VLAN và địa chỉ IP nội bộ khả dụng của tòa B trụ sở chính

VLAN	Default Gateway
7	192.168.7.1
8	192.168.8.1
9	192.168.9.1
10	192.168.10.1
11	192.168.11.1

Bảng 4: Bảng VLAN và default gateway cho từng VLAN ở tòa B

Tất cả địa chỉ IP nội bộ của các workstations phía trên được cấp phát động theo giao thức DHCP. Địa chỉ IP nội bộ mạng của PC và các server trong phòng IT-DMZ đều được cấp phát tĩnh với địa chỉ mạng là 10.0.10.0/24 và default gateway là 10.0.10.1/24.

Tại phân điểm phụ trợ DBP

VLAN	Tầng	Khu vực	Địa chỉ mạng	Địa chỉ khả dụng
12	1	IT & Cabling Central Local	172.168.12.0/24	172.168.12.2 - 172.168.12.254
13	2	Phòng nghiên cứu	172.168.13.0/24	172.168.13.2 - 172.168.13.254

Bảng 5: Bảng VLAN và địa chỉ IP nội bộ khả dụng của chi nhánh DBP

VLAN	Default Gateway
12	192.168.12.1
13	192.168.13.1

Bảng 6: Bảng VLAN và default gateway cho từng VLAN ở chi nhánh DBP

Địa chỉ IP nội bộ của các workstations ở tầng 2 được cấp phát động theo giao thức DHCP. Địa chỉ IP nội bộ mạng của PC và các server ở tầng 1 đều được cấp phát tĩnh.

Tại phân điểm phụ trợ BHTQ

VLAN	Tầng	Khu vực	Địa chỉ mạng	Địa chỉ khả dụng
12	1	IT & Cabling Central Local	172.168.12.0/24	172.168.12.2 - 172.168.12.254
13	2	Phòng nghiên cứu	172.168.13.0/24	172.168.13.2 - 172.168.13.254

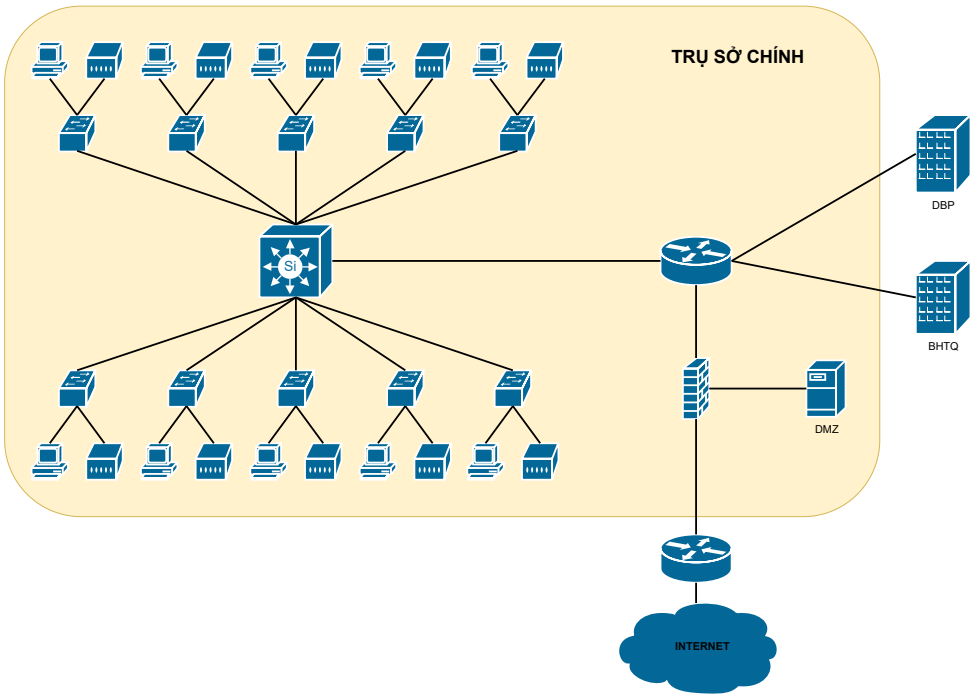
Bảng 7: Bảng VLAN và địa chỉ IP nội bộ khả dụng của chi nhánh BHTQ

VLAN	Default Gateway
14	192.168.14.1
15	192.168.15.1

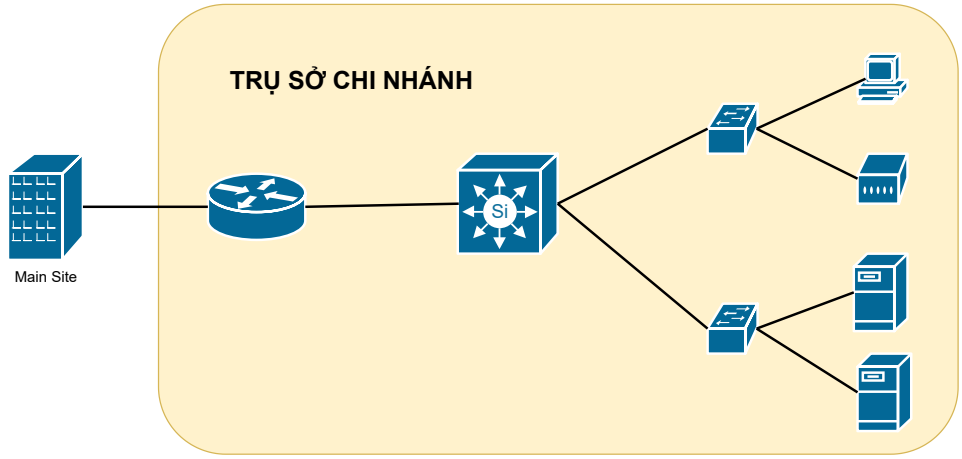
Bảng 8: Bảng VLAN và default gateway cho từng VLAN ở chi nhánh BHTQ

Địa chỉ IP nội bộ của các workstations ở tầng 2 được cấp phát động theo giao thức DHCP. Địa chỉ IP nội bộ mạng của PC và các server ở tầng 1 đều được cấp phát tĩnh.

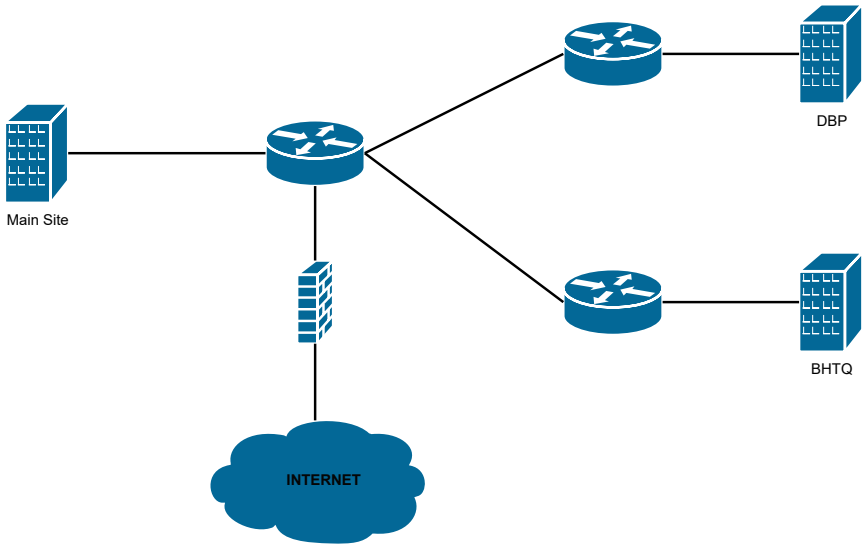
3.4 Thiết kế mạng cho trụ sở chính và 2 phân điểm phụ trợ



Hình 6: Sơ đồ đi dây cho trụ sở chính



Hình 7: Sơ đồ đi dây cho các chi nhánh



Hình 8: Sơ đồ đi dây cho kết nối giữa trụ sở chính và các chi nhánh

4 Tính toán throughput, bandwidth và các thông số an toàn cho hệ thống mạng bệnh viện

Lưu lượng dữ liệu ước tính và khối lượng công việc của hệ thống:

- Tổng dữ liệu tải xuống mỗi máy chủ: $D_s = 1000\,\text{MB/day}$
- Tổng dữ liệu tải lên mỗi máy chủ: $U_s = 2000\,\text{MB/day}$

- Tổng dữ liệu tải xuống mỗi máy trạm: $D_w = 500\,\text{MB/day}$
- Tổng dữ liệu tải lên mỗi máy trạm: $U_w = 100\,\text{MB/day}$
- Tổng dữ liệu tải xuống từ các thiết bị kết nối WiFi: $\text{Data}_{\text{wifi}} = 500\,\text{MB/day}$
- Thời gian cao điểm: 3 giờ
- Tốc độ mạng tại giờ cao điểm đạt 80% công suất tối đa
- Tỷ lệ tăng trưởng của bệnh viện: 20% trong 5 năm

Công thức mạng:

- $1\,\text{MBps} = \frac{8*2^{20}}{10^6}\,\text{Mbps}$
- Tổng lượng dữ liệu truyền tải:

$$\text{Data} = \text{Number} * (\text{Upload} + \text{Download})$$

- Thông lượng giờ cao điểm (PHT):

$$\text{Throughput} = \text{Data} * \frac{\text{PeakRate}}{\text{PeakTime}} = \text{Data} * \frac{0.8}{3*60*60} = \frac{\text{Data}}{13500}$$

- Băng thông tối thiểu trong 5 năm tới:

$$\text{Bandwidth} = \text{Throughput} * \text{GrowthRate} = \text{Throughput} * 1.2$$

Trụ sở chính:

- Trong mạng có dây, có:
  - Số lượng máy chủ: $N_s = 10$
  - Số lượng máy trạm: $N_w = 600$
- Tổng lượng dữ liệu truyền tải của máy chủ:

$$\sum \text{Data}_{\text{server}} = N_s(D_s + U_s) = 10 * (1000 + 2000) = 30000\,\text{MB/day}$$

- Tổng lượng dữ liệu truyền tải của máy trạm:

$$\sum \text{Data}_{\text{workstation}} = N_w(D_w + U_w) = 600 * (500 + 100) = 360000\,\text{MB/day}$$

- Tổng lượng dữ liệu truyền tải trong trụ sở chính:

$$\begin{aligned}\sum \text{Data}_{\text{Main\_Site}} &= \sum \text{Data}_{\text{server}} + \sum \text{Data}_{\text{workstation}} + \sum \text{Data}_{\text{wifi}} \\ &= 30000 + 360000 + 500 = 390500\,\text{MB/day}\end{aligned}$$

- Thông lượng tại giờ cao điểm trong trụ sở chính:

$$\text{Throughput}_{\text{Main\_Site}} = \frac{\sum \text{Data}_{\text{Main\_Site}}}{13500} = \frac{390500}{13500} = 28.9259\,\text{MBps}$$

- Băng thông tối thiểu tại trụ sở chính:

$$\text{Bandwidth}_{\text{Main\_Site}} = \text{Throughput}_{\text{Main\_Site}} * 1.2 = 28.9259 * 1.2 = 34.7111\,\text{MBps}$$

Trụ sở chi nhánh:

- Trong mạng có dây, có:
  - Số lượng máy chủ: $N_s = 2$
  - Số lượng máy trạm: $N_w = 60$
- Tổng lượng dữ liệu truyền tải của máy chủ:

$$\sum \text{Data}_{\text{server}} = N_s(D_s + U_s) = 2 * (1000 + 2000) = 6000\,\text{MB/day}$$

- Tổng lượng dữ liệu truyền tải của máy trạm:

$$\sum \text{Data}_{\text{workstation}} = N_w(D_w + U_w) = 60 * (500 + 100) = 36000\,\text{MB/day}$$

- Tổng lượng dữ liệu truyền tải trong trụ sở chi nhánh:

$$\sum \text{Data}_{\text{Auxiliary\_Site}} = \sum \text{Data}_{\text{server}} + \sum \text{Data}_{\text{workstation}} + \sum \text{Data}_{\text{wifi}}$$

$$= 6000 + 36000 + 500 = 42500\,\text{MB/day}$$

- Thông lượng tại giờ cao điểm trong trụ sở chi nhánh:

$$\text{Throughput}_{\text{Auxiliary\_Site}} = \frac{\sum \text{Data}_{\text{Auxiliary\_Site}}}{13500} = \frac{42500}{13500} = 3.1481\,\text{MBps}$$

- Băng thông tối thiểu tại trụ sở chi nhánh:

$$\text{Bandwidth}_{\text{Auxiliary\_Site}} = \text{Throughput}_{\text{Auxiliary\_Site}} * 1.2 = 3.1481 * 1.2 = 3.7777\,\text{MBps}$$

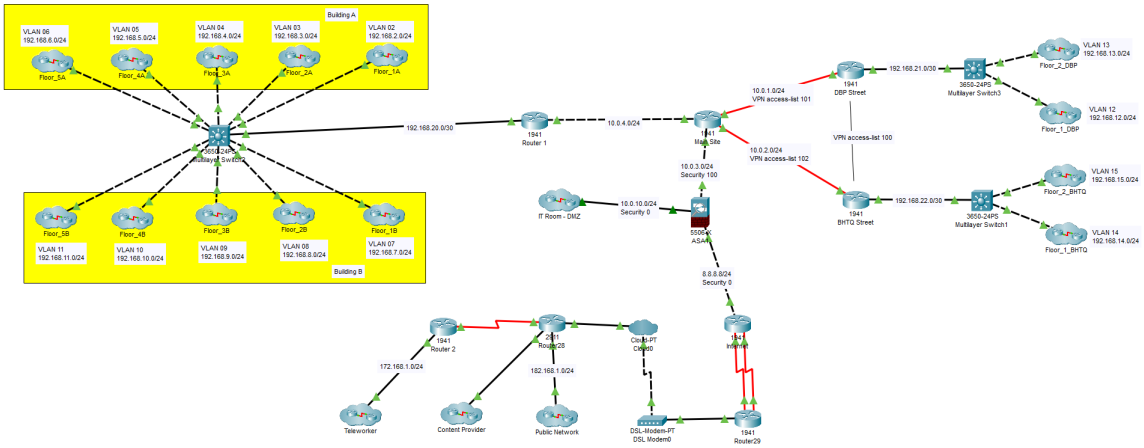
$$= 30.2218\,\text{Mbps}$$

Đề xuất cấu hình cho mạng của bệnh viện:

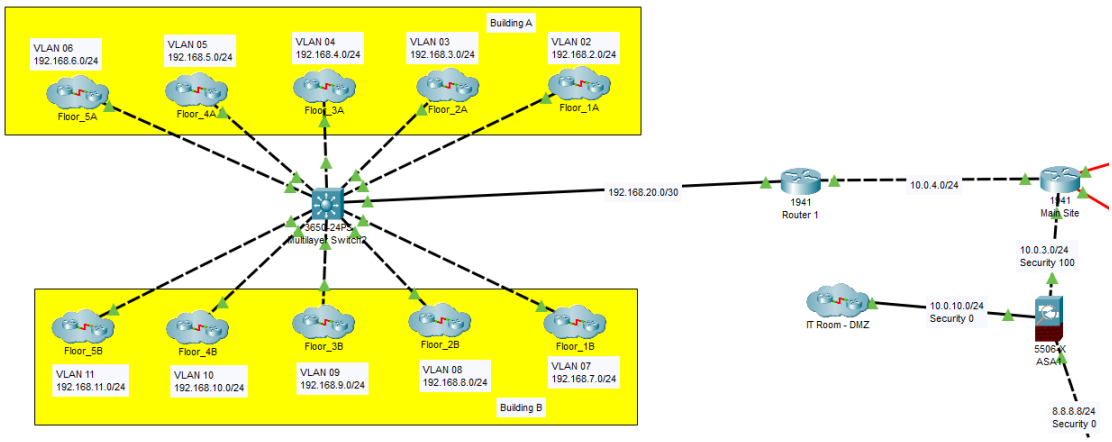
- Dựa trên băng thông dự kiến, đường truyền thuê từ ISP cho mỗi chi nhánh nên có tốc độ **40 Mbps**, phù hợp với sự phát triển của công ty trong 10 năm tới.

5 Thiết kế bản đồ mạng bằng phần mềm mô phỏng Packet Tracer

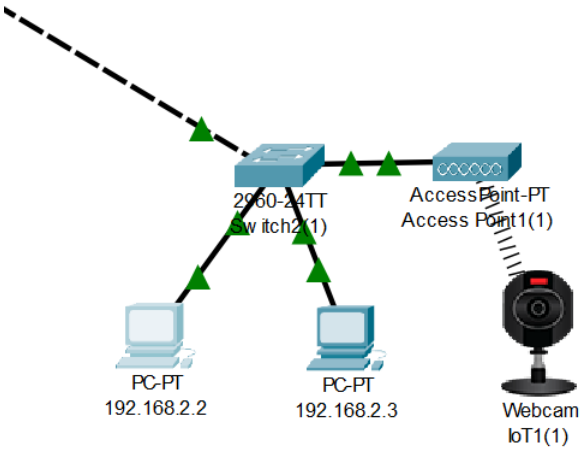
5.1 Cấu trúc tổng thể bản đồ mạng



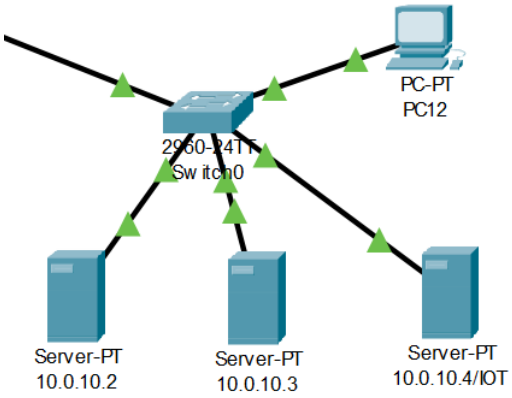
5.2 Trụ sở chính



Hình 9: Cấu trúc tổng thể trụ sở chính

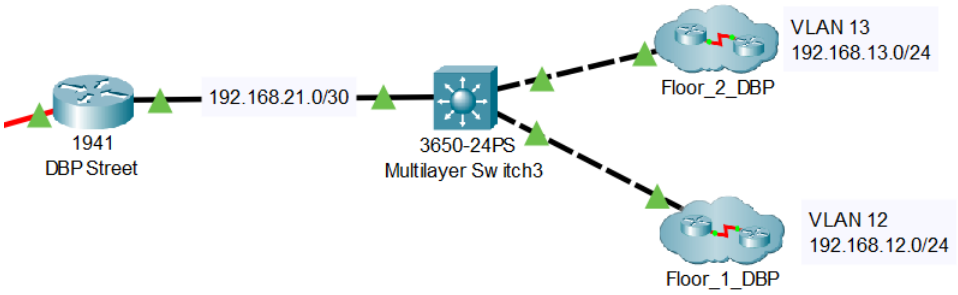


Hình 10: Cấu trúc mạng của tầng 1 trong tòa A (giống nhau ở các tầng)

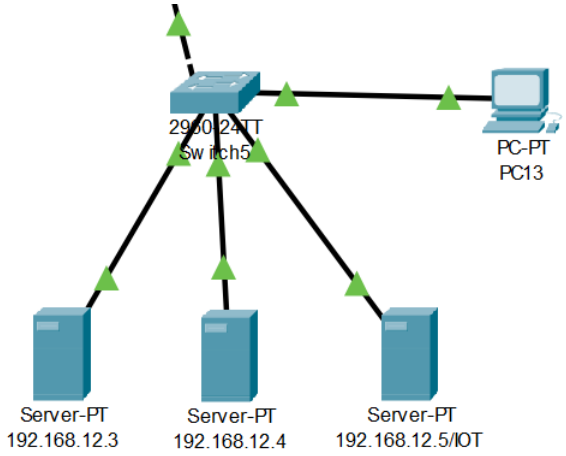


Hình 11: Cấu trúc mạng của phòng IT - DMZ

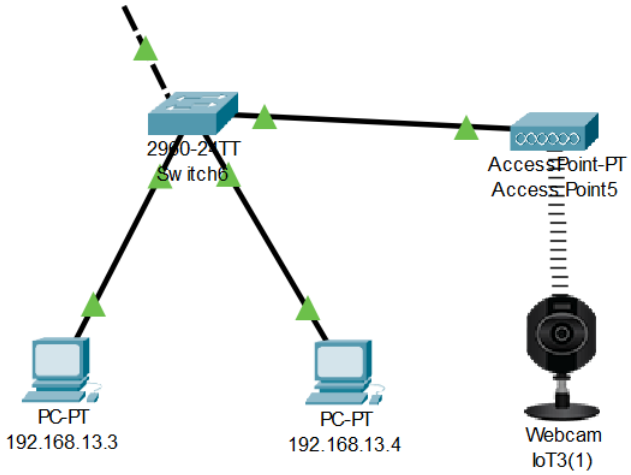
5.3 Trụ sở chi nhánh DBP



Hình 12: Cấu trúc tổng thể chi nhánh DBP

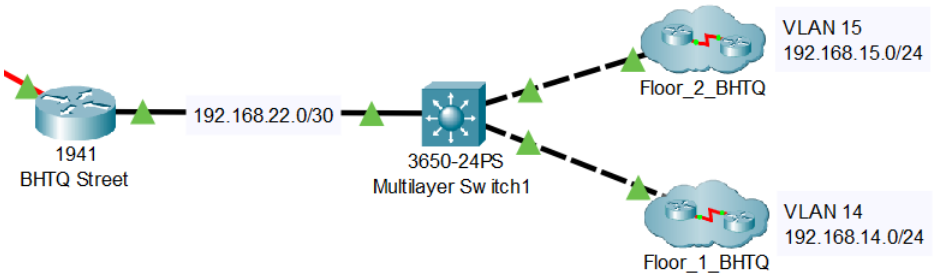


Hình 13: Cấu trúc mạng tầng 1 chi nhánh DBP

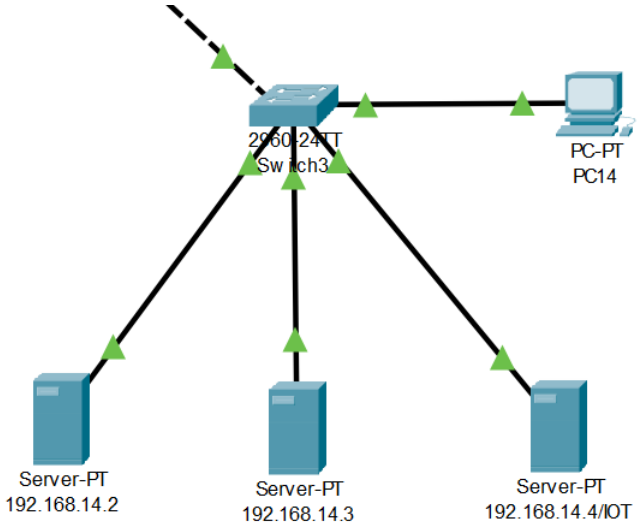


Hình 14: Cấu trúc mạng tầng 2 của chi nhánh DBP

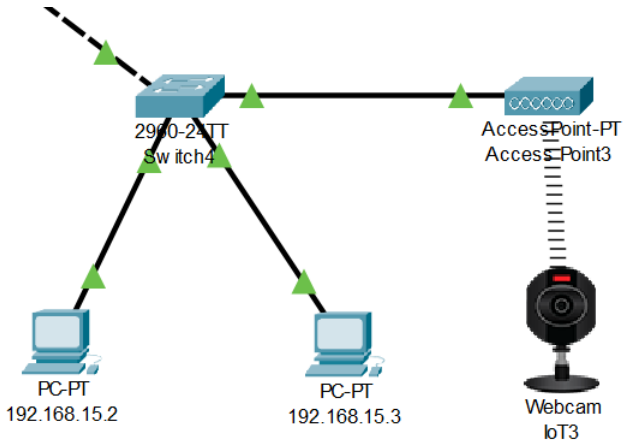
5.4 Trụ sở chi nhánh BHTQ



Hình 15: Cấu trúc tổng thể chi nhánh BHTQ

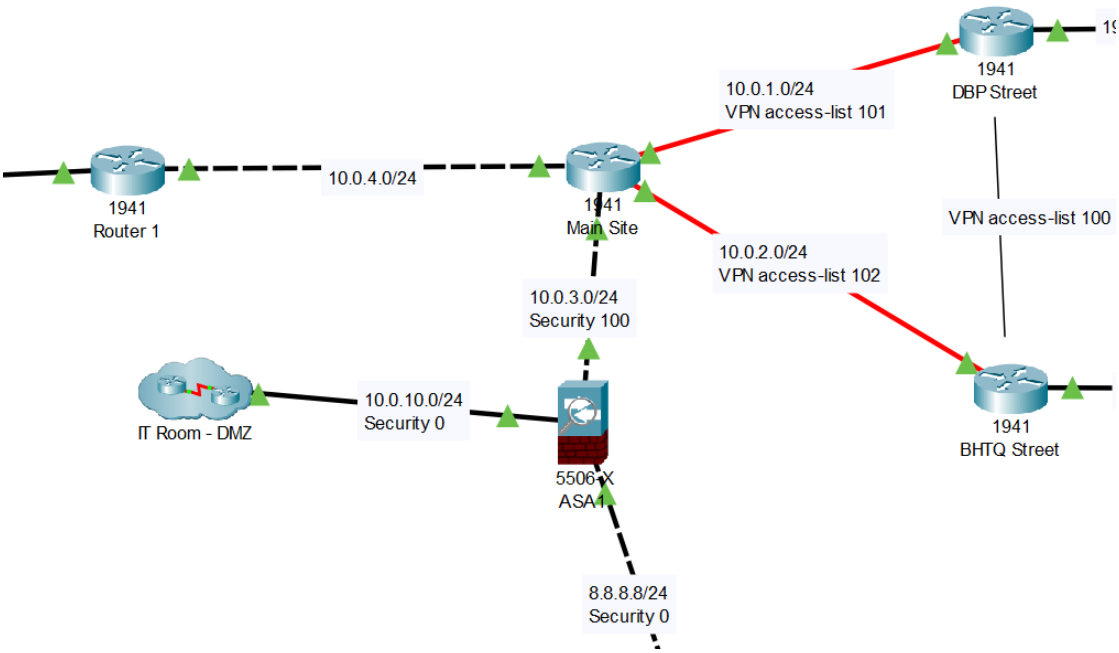


Hình 16: Cấu trúc mạng tầng 1 chi nhánh BHTQ

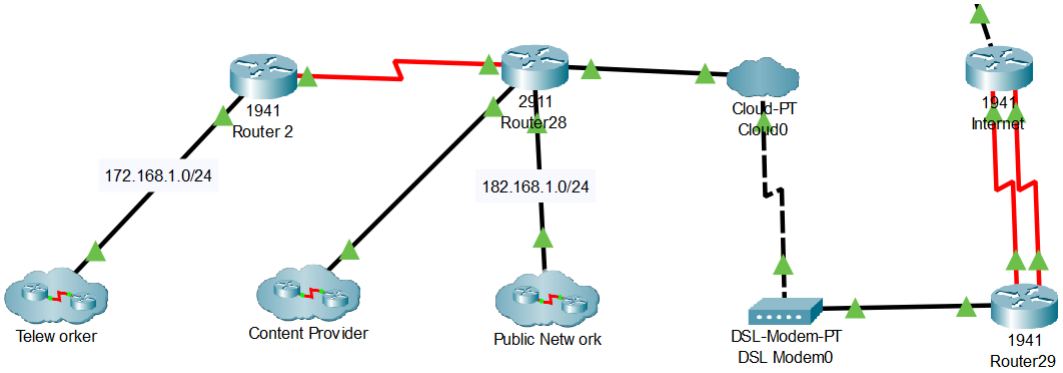


Hình 17: Cấu trúc mạng tầng 2 của chi nhánh BHTQ

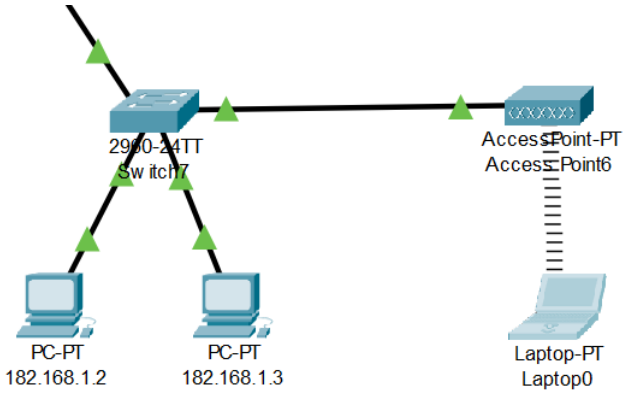
5.5 Kết nối giữa các trụ sở



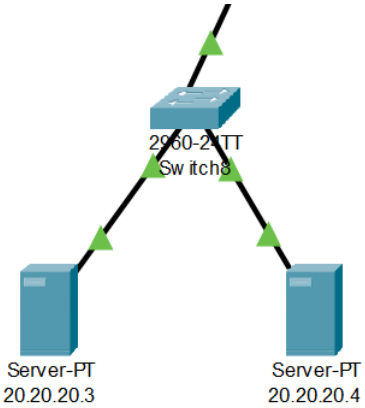
5.6 Internet



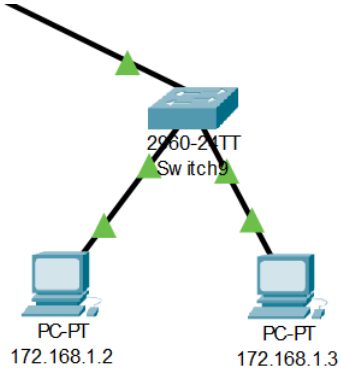
Hình 18: Cấu trúc tổng thể của Internet



Hình 19: Cấu trúc mạng của Public Network



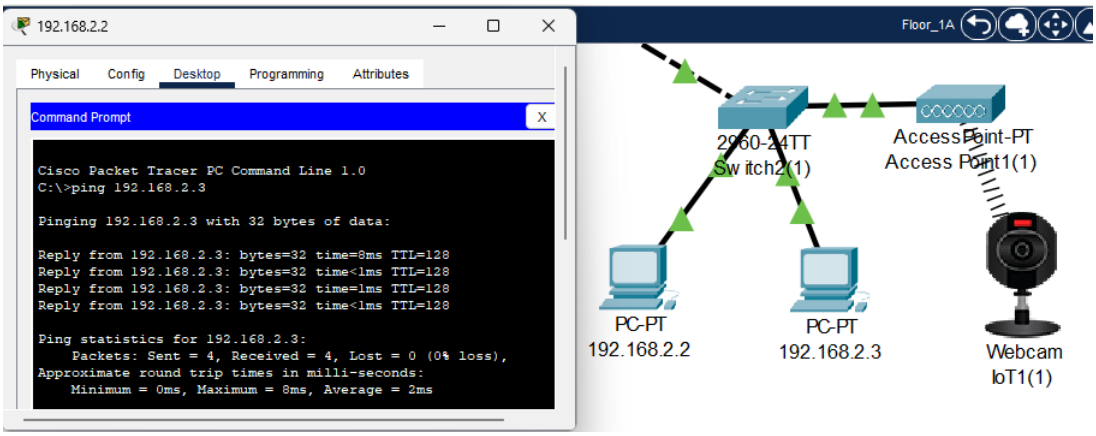
Hình 20: Cấu trúc mạng của Content Provider



Hình 21: Cấu trúc mạng của Teleworker

6 Kiểm thử hệ thống bằng các công cụ phổ biến như ping, traceroute,... trên hệ thống mô phỏng.

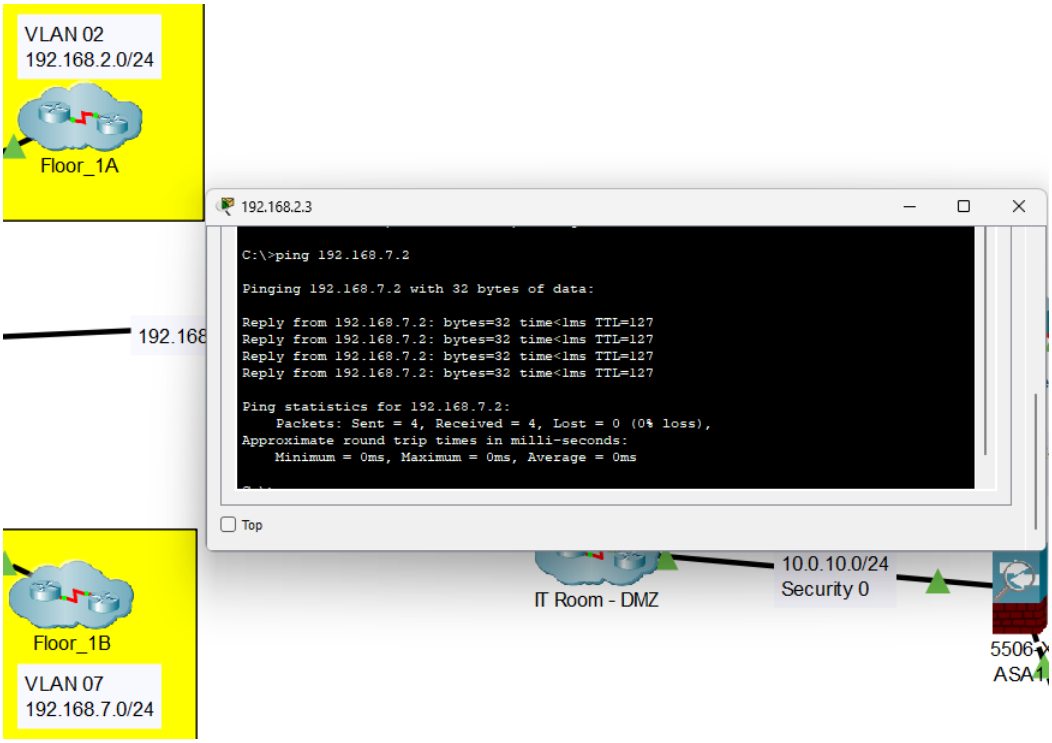
6.1 Kết nối giữa các PC trong cùng một VLAN



Hình 22: Ping giữa 2 PC trong cùng tầng 1 tòa A (VLAN 2)

Thực hiện ping từ PC (192.168.2.2/24) tới PC (192.168.2.3/24). Từ hình trên ta thấy việc ping thành công với packet loss là 0%.

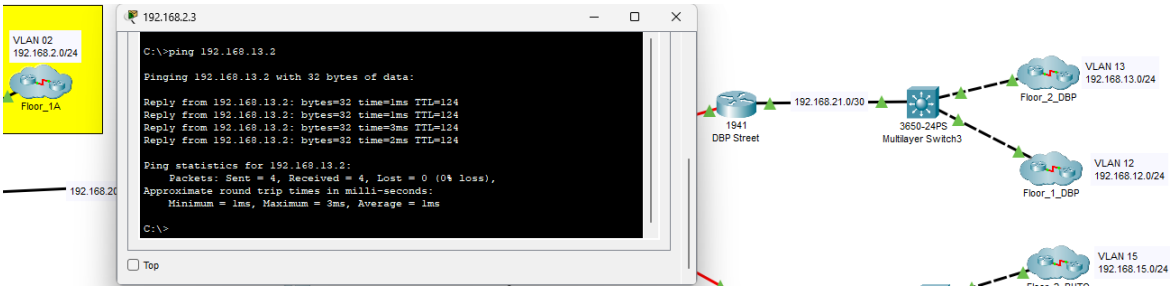
6.2 Kết nối PC giữa các VLAN



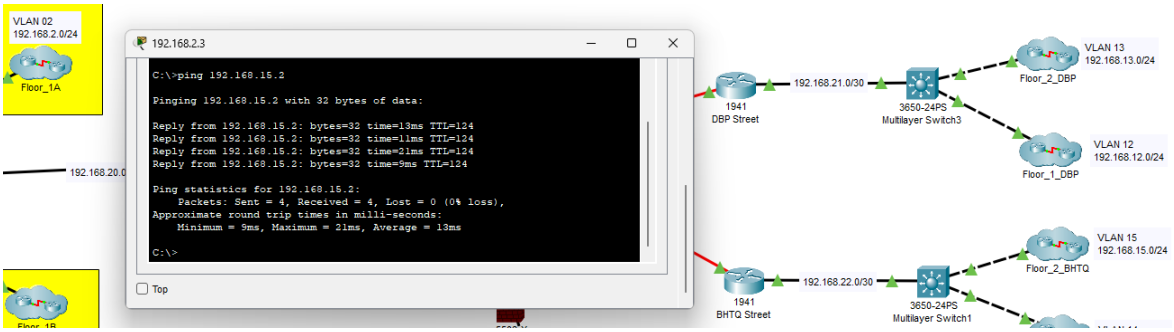
Hình 23: Ping giữa 2 PC ở tầng 1 tòa A (VLAN 2) và tầng 1 tòa B (VLAN 7)

Thực hiện ping từ PC (192.168.2.3/24) tới PC (192.168.7.2/24). Từ hình trên ta thấy việc ping thành công với packet loss là 0%.

6.3 Kết nối các PC giữa trụ sở chính và hai trụ sở chi nhánh



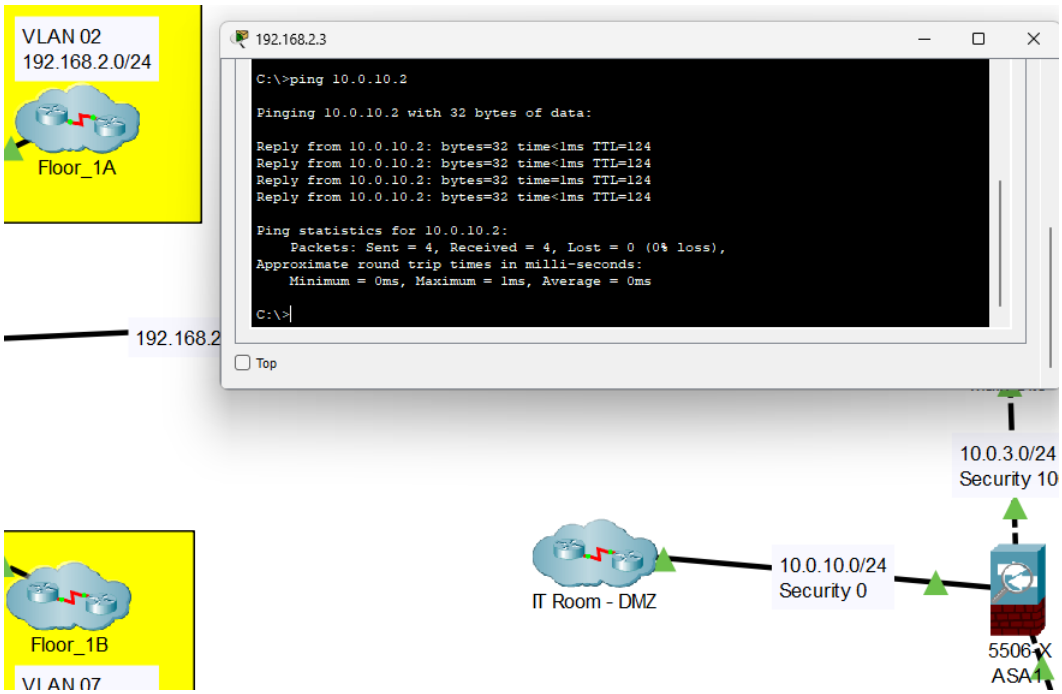
Hình 24: Ping giữa 2 PC ở tầng 1 tòa A ở trụ sở chính (VLAN 2) và tầng 2 ở trụ sở chi nhánh DBP (VLAN 13)



Hình 25: Ping giữa 2 PC ở tầng 1 tòa A ở trụ sở chính (VLAN 2) và tầng 2 ở trụ sở chi nhánh BHTQ (VLAN 15)

Thực hiện ping từ PC (192.168.2.3/24) ở trụ sở chính tới PC (192.168.13.2/24) ở chi nhánh DBP và tới PC (192.168.15.2/24) ở chi nhánh BHTQ. Từ hình trên ta thấy việc ping thành công với packet loss là 0%.

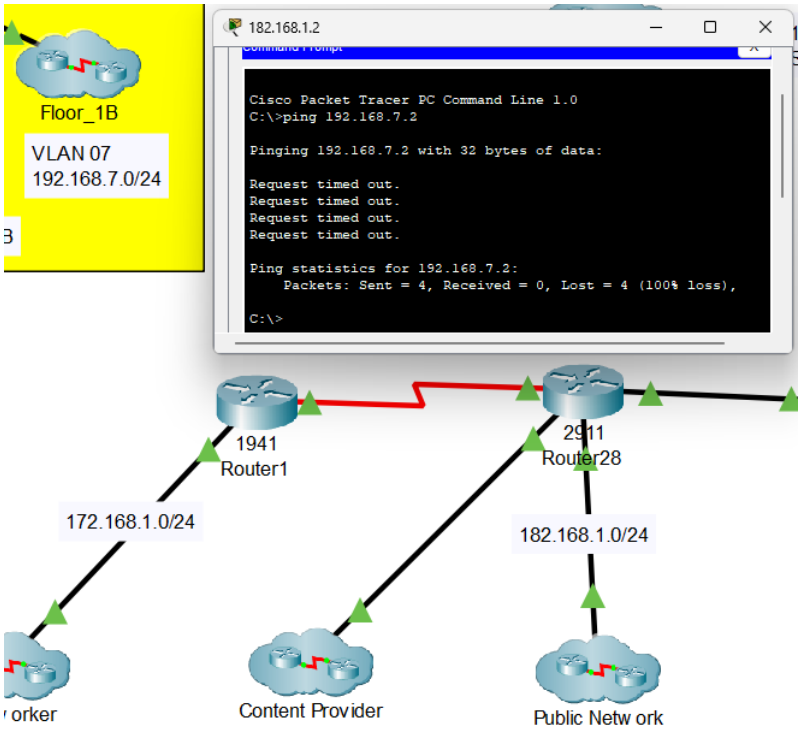
6.4 Kết nối với máy chủ trong DMZ



Hình 26: Ping giữa PC ở tầng 1 tòa A (VLAN 2) và Server ở phòng IT-DMZ

Thực hiện ping từ PC (192.168.2.3/24) tới Server (10.0.10.2/24). Từ hình trên ta thấy việc ping thành công với packet loss là 0%.

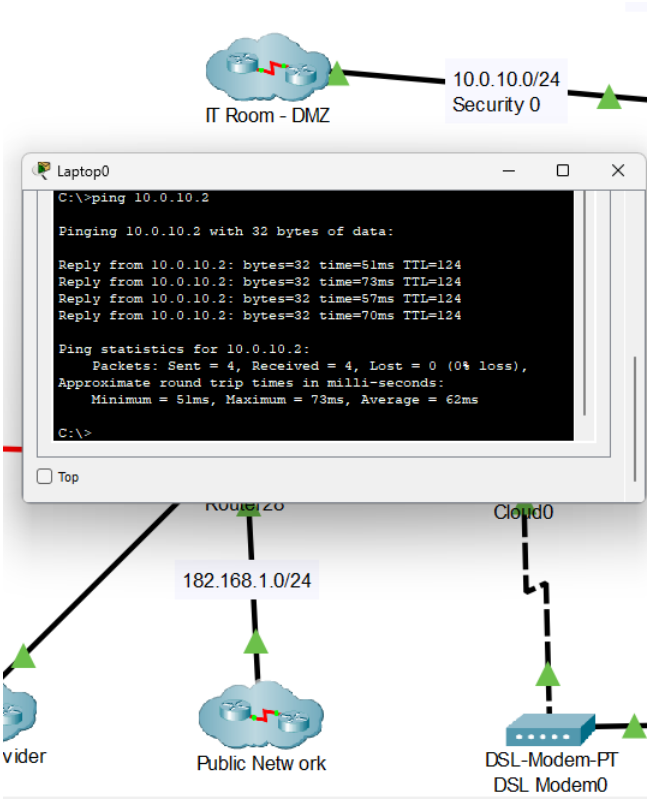
6.5 Không có kết nối từ thiết bị của Khách hàng đến PC trong mạng LAN



Hình 27: Ping giữa PC ở Public Network và PC ở tầng 1 tòa B

Thực hiện ping từ Laptop (182.168.1.2/24) tới PC (192.168.7.2/24). Từ hình trên ta thấy việc ping thất bại với packet loss là 100%.

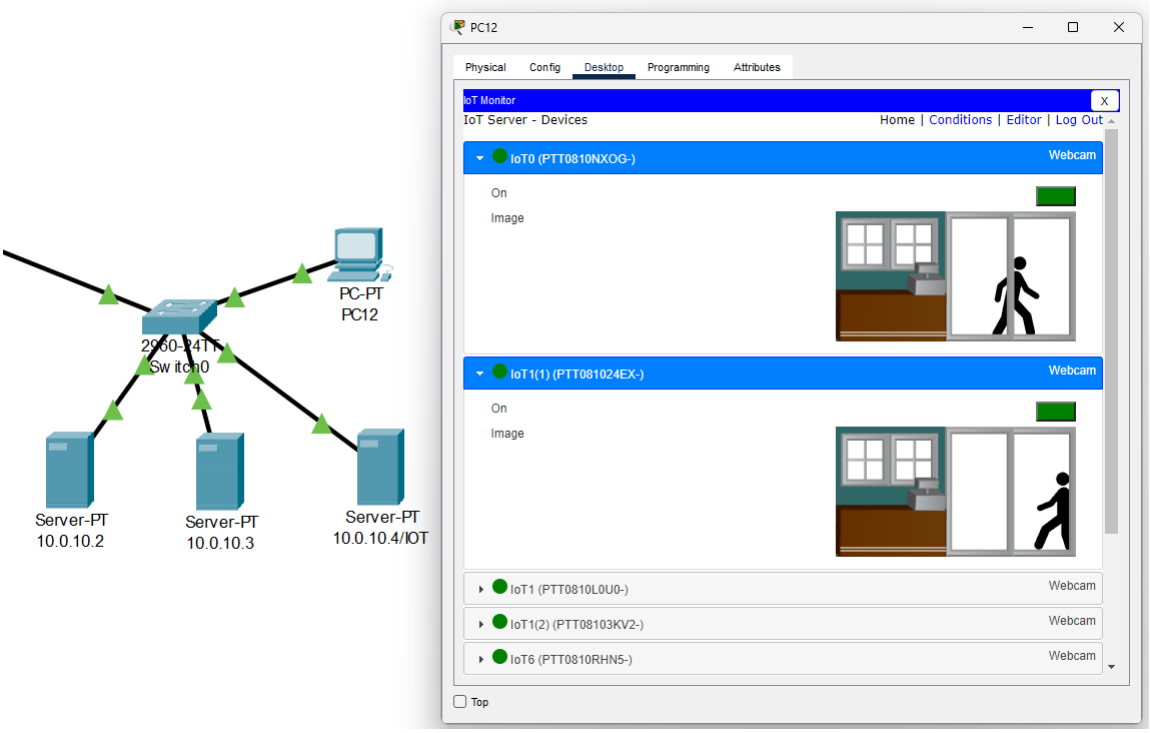
6.6 Kết nối Internet với máy chủ Web



Hình 28: Ping giữa Laptop ở Public Network và Server ở phòng IT-DMZ

Thực hiện ping từ PC (182.168.1.4/24) tới Server (10.0.10.2/24). Từ hình trên ta thấy việc ping thất bại với packet loss là 0%.

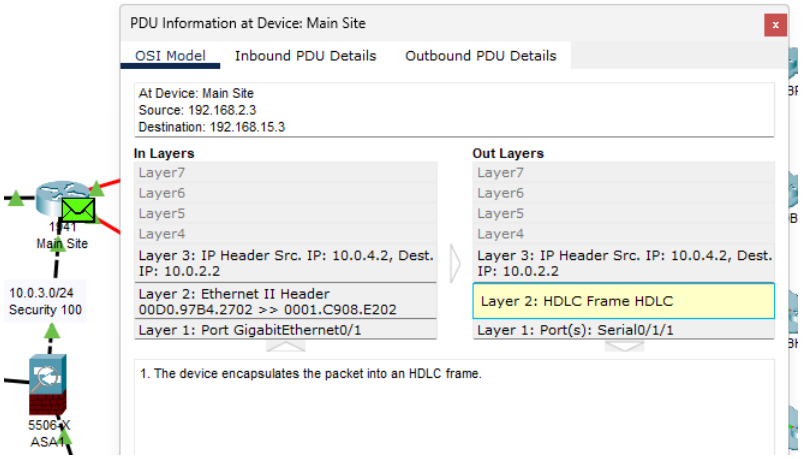
6.7 Hệ thống camera



Hình 29: Server ở phòng IT-DMZ quản lí tất cả các camera ở trụ sở chính

Tại phòng IT của trụ sở chính và tầng một của mỗi chi nhánh, có một máy chủ IoT dành riêng cho việc quản lý tất cả các camera giám sát tại mỗi địa điểm. Bằng cách nhập đúng tên đăng nhập và mật khẩu *(admin, admin)*, từ đó ta có thể truy cập vào hệ thống IoT bằng PC để xem những gì từng camera đang ghi hình và bật/tắt các camera.

6.8 VPN Site to Site



Hình 30: Ping giữa 2 PC ở tầng 1 tòa A (VLAN 2) và ở tầng 2 chi nhánh BHTQ (VLAN 15)

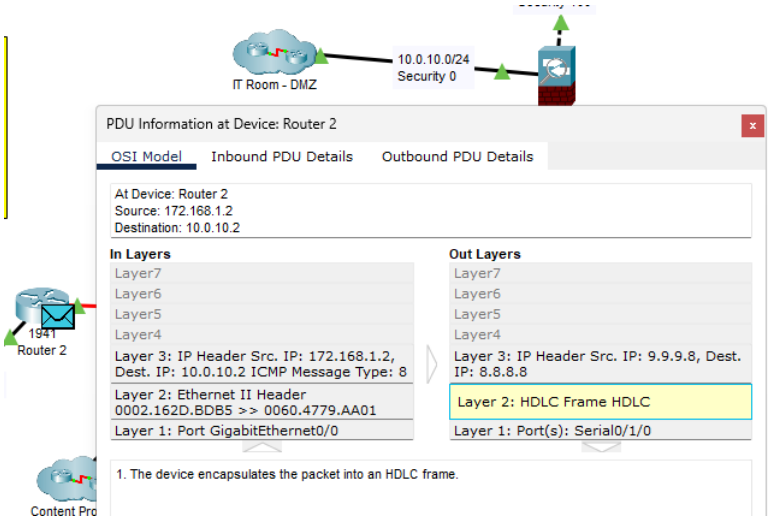
VPN này được triển khai giữa PC (192.168.2.3/24) và PC (192.168.15.3/24) với cấu hình VPN được thiết lập tại Router 1, Router BHTQ_Street và Router DBP_Street .

Trong VPN này, ta sử dụng giao thức IPSec (Internet Protocol Security) VPN, một bộ giao thức mạnh mẽ được thiết kế để tạo các đường hầm mã hóa giữa các thiết bị qua các mạng không tin cậy, chẳng hạn như Internet. IPSec đảm bảo giao tiếp an toàn bằng cách cung cấp tính bảo mật (confidentiality), tính toàn vẹn (integrity), và xác thực (authentication), từ đó bảo vệ quá trình truyền dữ liệu khỏi truy cập trái phép hoặc bị sửa đổi.

Trong cấu hình này, VPN sẽ đóng gói (encapsulate) và mã hóa các gói tin dữ liệu, đồng thời thay đổi địa chỉ IP nguồn trong quá trình truyền giữa các địa điểm. Quá trình đóng gói này đảm bảo rằng các thông tin nhạy cảm sẽ được ẩn đi, không cho phép bất kỳ bên không được phép nào có thể xem hoặc chặn các dữ liệu được truyền.

Bằng cách triển khai IPSec, quá trình giao tiếp giữa các địa điểm trở nên an toàn và được bảo vệ khỏi các mối đe dọa như nghe lén (eavesdropping) hoặc sửa đổi dữ liệu (data manipulation).

6.9 VPN Teleworker



Hình 31: Ping giữa PC ở Teleworker và Server ở DMZ

VPN này được triển khai giữa các nhân viên làm việc từ xa với địa chỉ IP 172.168.1.2/24 và vùng DMZ. Cấu hình VPN được thiết lập trên Router 2 và firewall ASA.

Tương tự như VPN Site-to-Site, giao thức IPSec VPN được sử dụng để bảo vệ các tệp dữ liệu được truyền từ các nhân viên làm việc từ xa đến DMZ và ngược lại. Điều này đảm bảo rằng mạng công cộng không thể truy cập hoặc sửa đổi dữ liệu trong quá trình truyền.

7 Đánh giá hệ thống

7.1 Độ tin cậy (Reliability)

- Mạng có điểm lỗi duy nhất (single point of failure) tại các switch và router do sử dụng topology hình sao (Star Topology).
- Mạng không có cơ chế sao lưu gói tin, dẫn đến nguy cơ mất gói tin cao. Định tuyến VLANs phụ thuộc rất nhiều vào các router một tay (one-armed routers).

7.2 Hiệu suất (Performance)

- Không có cân bằng tải (load balancer) được triển khai tại Gateway, dẫn đến việc tải công việc không được 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).

7.3 Dễ dàng nâng cấp (Ease of Upgrade)

- Mạng chứa một số thiết bị Cisco cũ (legacy devices) không còn được Cisco hỗ trợ, điều này gây khó khăn trong việc nâng cấp mạng để áp dụng các công nghệ mới hiện nay.

7.4 Bảo mật (Security)

- Chỉ có DMZ tại trụ sở chính (Main Site) được mô phỏng; các máy chủ tại các chi nhánh được đặt sau tường lửa và không thuộc DMZ, vì vậy khối lượng công việc không thể được chia sẻ.
- Tường lửa chỉ lọc lưu lượng IP, điều này làm cho mạng dễ bị tổn thương trước các cuộc tấn công giả mạo IP (IP spoofing).

7.5 Tính năng (Features)

- Cân bằng tải (Load balancing) chưa được triển khai do sử dụng cơ chế tường lửa đơn lẻ.
- Mỗi địa điểm có hệ thống camera riêng và không chia sẻ hệ thống camera với các địa điểm khác.