ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC & KỸ THUẬT MÁY TÍNH

COMPUTER NETWORKING (CO3094)

Assignment 2

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE HOSPITAL

Giảng viên hướng dẫn: Bùi Xuân Giang
Sinh viên thực hiện: Nguyễn Huy Hoàng - 2211091
Nguyễn Lê Gia Kiệt - 2211761
Nguyễn Chí Thiết - 2213242

Thành phố Hồ Chí Minh, Tháng 10/2024

Mục lục

1 Phân công nhiệm vụ

Thứ tự	Họ và tên	MSSV	Nhiệm vụ	Hoàn thành
1	Nguyễn Huy Hoàng	2211091	- Thiết kế - Cấu hình hệ thống giả lập trên Packet Tracer - Viết báo cáo	100%
2	Nguyễn Lê Gia Kiệt	2211761	- Thiết kế - Cấu hình hệ thống giả lập trên Packet Tracer - Viết báo cáo	100%

Bảng 1: Danh sách nhiệm vụ và tiến độ hoàn thành

2 Xác định cấu trúc mạng thích hợp cho toà nhà

2.1 Phân tích các yêu cầu hệ thống mạng

CCC (Computer & Construction Concept) được yêu cầu thiết kế một mạng máy tính triển khai ở trụ sở chính (Thành phố Hồ Chí Minh) và 2 chi nhánh (DBPStreet và BHTQ Street) của bệnh viện đang được xây dựng.

2.1.1 Phân tích yêu cầu của trụ sở chính

- Gồm hai tòa nhà A và B (mỗi tòa 5 tầng, mỗi tầng 10 phòng), tầng đầu tiên có một phòng IT và hệ thống cáp trung tâm cục bộ (sử dụng patch panel để quản lý và đấu nối các dây dẫn).
- Quy mô trung bình: 600 máy trạm (workstation), 10 máy chủ (server), 12 thiết bị kết nối mạng (hoặc nhiều hơn với các thiết bị dành riêng cho bảo mật).
- Có trung tâm dữ liệu và phòng cáp trung tâm cách 50m từ hai tòa nhà.
- Sử dụng công nghệ mới cho cơ sở hạ tầng mạng bao gồm các kết nối có dây và không dây, cáp quang (GPON), và GigaEthernet 1GbE/10GbE. Tổ chức mạng theo cấu trúc VLAN cho các phòng ban khác nhau.
- Mạng con trụ sở chính kết nối tới hai mạng con chi nhánh bằng 2 kênh truyền riêng (Leased line) cho kết nối WAN và 2 đường dây thuê bao kỹ thuật số (DSL) cho việc truy cập Internet với cơ chế cân bằng tải (Load Balancing). Tất cả lưu lượng truy cập vào Internet đều đi qua mạng con trụ sở chính.
- Sử dụng kết hợp các phần mềm được cấp phép và các phần mềm có mã nguồn mở, các ứng dụng văn phòng, các ứng dụng client-server, các ứng dụng đa phương tiện và cơ sở dữ liệu.
- Yêu cầu về tính bảo mật cao (firewall, IPS/IDS, phishing detection), tính sẵn sàng cao (High Availability), tính bền vững (Robustness) khi có lỗi xảy ra, dễ dàng nâng cấp hệ thống.
- Đề xuất cấu hình VPN cho kết nối giữa các chi nhánh và cho nhân viên làm việc từ xa kết nối vào mạng LAN của bệnh viện.
- Đề xuất một camera giám sát cho bệnh viện.

2.1.2 Phân tích yêu cầu của các chi nhánh

Các chi nhánh được thiết kế tương tự như trụ sở chính nhưng với quy mô nhỏ hơn:

- Toà nhà chi nhánh có 2 tầng, tầng đầu tiên có một phòng IT và một hệ thống cáp trung tâm cục bộ.
- Quy mô nhỏ: 260 máy trạm (workstation), 2 máy chủ (server), 5 thiết bị kết nối mạng trở lên.

Triển khai việc kết nỗi giữa trụ sở chính và các chi nhánh thông qua các liên kết WAN (có thể chọn một trong cách công nghệ như SD-WAN, MPLS,...)

2.1.3 Phân tích yêu cầu về thông lượng

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) có thể được chia sẻ giữa trụ sở chính và các chi nhánh như sau:

- 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 workstation 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,..).

2.2 Chi tiết hệ thống mạng

Trước khi chuẩn bị bắt tay xây dựng một hệ thống mạng, việc trước hết và quan trọng 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:

- Về địa điểm lắp đặt:
  - Tòa nhà có bao nhiều tầng.
  - Mỗi tầng có bao nhiêu phòng.
  - Mỗi phòng có kích thước như thế nào.
  - Nhà mạng hỗ trợ tốt nhất đối với địa điểm lắp đặt đó.
  - Tòa nhà có đường đi dây riêng hay không, hay phải tự đi dây và thi công đường dây.
- Về tổ chức bệnh viện:
  - Các bố trí phòng ban ở các phòng, các tầng.
  - Quy mô của mỗi phòng ban là bao nhiêu.
  - Các máy chủ được bố trí ở đâu.

Đối với bài tập lớn này, nhóm chúng em giả định đã khảo sát thành công các địa điểm chuẩn bị lắp đặt hệ thống mạng và có được kết quả như sau:

2.2.1 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 như vậy đều có kích cỡ phù hợp cho khoảng 60 người làm việc cùng lúc.
- Đã tìm được nhà mạng hỗ trợ tốt nhất cho địa điểm tòa nhà.
- Tòa nhà có đường đi dây riêng, không cần tự thi công đường dây.
- Mỗi tầng cần cung cấp hệ thống mạng không dây, tối đa không quá 60 thiết bị kết nối cùng lúc cho mỗi tầng. Mỗi phòng không quá 6 workstation. Mạng không dây riêng cho Phòng Lễ tân với tối đa không quá 70 thiết bị kết nối cùng lúc.

1. **Tầng 1:**
    - **Phòng Lễ tân (Reception):** Có 6 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 60). Ngoài ra còn có một camera và một máy cảm biến chuyển động để giám sát an ninh.
2. **Tầng 2:**
    - **Phòng máy chủ (Server farm) và DMZ:** Có 5 servers phục vụ công việc nội bộ bệnh viện và 1 Web server thuộc DMZ.
3. **Tầng 3:**
    - **Phòng ban Quản lí nhân sự (Human Resources):** Có 6 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 60).
4. **Tầng 4:**
    - **Phòng ban Tiếp thị và Bán thuốc (Marketing and Sale):** Có 6 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 60).
    - **Phòng Quản trị (Administration):** Có 6 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 60).
5. **Tầng 5:**
    - **Phòng ban Tài chính và Kế toán (Financial and Accounting):** Có 6 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 60).
    - **Phòng ban Nghiên cứu và Phát triển (Research and Development):** Có 6 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 60).
    - **Phòng lưu trữ thuốc:** Có 6 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 60).

2.2.2 Chi nhánh ở đường ĐBP và BHTQ

- Mỗi chi nhánh có 2 tầng với 260 workstations, 2 servers, 5 networking devices.
- Cả hai toà nhà chi nhánh đều giống nhau và kết quả khảo sát là như nhau ở cả hai chi nhánh này.
- Tòa chi nhánh có 2 tầng:
    - **Tầng 1** được phân thành 3 khu vực, gồm 2 phòng nhỏ và 1 phòng lớn. Phòng nhỏ sẽ được sử dụng làm phòng Lễ tân và phòng Server, phòng lớn sẽ là không gian làm việc của nhân viên.
    - **Tầng 2** được thiết kế theo kiểu studio (phòng thu) nghĩa là không có phân phòng riêng rẻ cho từng tầng. Mỗi tầng như vậy đều có kích cỡ phù hợp cho 40 người làm việc cùng lúc.
- Đã tìm được nhà mạng hỗ trợ tốt nhất cho địa điểm tòa nhà.
- Tòa nhà có đường đi dây riêng, không cần tự thi công đường dây.

- Mỗi tầng cần cung cấp hệ thống mạng không dây, tối đa không quá 130 thiết bị kết nối cùng lúc cho mỗi tầng. Mạng không dây riêng cho Phòng Lễ tân với tối đa không quá 260 thiết bị kết nối cùng lúc.

Chi nhánh ở ĐBP

1. **Tầng 1**
    - **Phòng ban Kĩ thuật thông tin (IT):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác. (tối đa không quá 130).
    - **Phòng ban Quản lí nhân sự (Human Resources):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác. (tối đa không quá 130).
    - **Phòng Lễ tân (Reception):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác. Ngoài ra còn có một camera và một máy cảm biến chuyển động để giám sát an ninh. (tối đa không quá 130).
    - **Phòng máy chủ (Server farm):** Có 2 servers phục vụ công việc nội bộ bệnh viện.
2. **Tầng 2**
    - **Phòng ban Tiếp thị và Bán thuốc (Marketing and Sale):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác(tối đa không quá 130).
    - **Phòng ban Tài chính và Kế toán (Financial and Accounting):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 130).
    - **Phòng ban Nghiên cứu và Phát triển (Research and Development):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác. (tối đa không quá 130).
    - **Phòng Quản trị(Administration):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác. (tối đa không quá 130).

Chi nhánh ở BHTQ

1. **Tầng 1**
    - **Phòng ban Kĩ thuật thông tin (IT):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác.(tối đa không quá 130)
    - **Phòng ban Quản lí nhân sự (Human Resources):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác. (tối đa không quá 130)
    - **Phòng Lễ tân (Reception):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác. Ngoài ra còn có một camera và một máy cảm biến chuyển động để giám sát an ninh. (tối đa không quá 130)
    - **Phòng máy chủ (Server farm):** Có 2 servers phục vụ công việc nội bộ bệnh viện.
2. **Tầng 2**
    - **Phòng ban Tiếp thị và Bán thuốc (Marketing and Sale):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác(tối đa không quá 130)
    - **Phòng ban Nghiên cứu và Phát triển (Research and Development):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác. (tối đa không quá 130)
    - **Phòng Quản trị (Administration):** Có 52 workstations và một số thiết bị kết nối mạng không dây khác. (tối đa không quá 130)

2.3 Xác định vùng có tải trọng lớn trong Bệnh viện

Tất cả lưu lượng truy cập vào Internet của hệ thống đều đi qua mạng Trụ sở chính. Do đó, đường kết nối từ Multi-switch của trụ sở chính lên router trụ sở chính là vùng có tải lớn nhất. Đây là nơi phục vụ hoạt động của một lượng máy lớn, hoạt động trong thời gian dài với cường độ cao. Đồng thời đây còn là nơi tập trung nhiều tác vụ như kết nối tới các server, kết nối với các máy quan trọng khác.

Tầng 2 của trụ sở chính và các chi nhánh là khu vực đặt nhiều PC, các server cùng với đó hệ thống cáp trung tâm nên đây cũng là vùng có lượng tải lớn.

Sau khi thực hiện khảo sát và xem xét các yêu cầu của hệ thống mạng, ta có thể dễ dàng xác định được các vùng có tải trọng lớn trong Bệnh viện bao gồm:

- **Hệ thống Web Server:** Cho phép tất cả người dùng Internet đều có thể tìm kiếm thông tin, trao đổi thông tin với website. Do vậy, cần phải đảm bảo về tốc độ truy cập, tính ổn định.
- **Trung tâm dữ liệu và mạng (Trụ sở chính:)** Trung tâm cho tất cả lưu lượng truy cập, sử dụng máy chủ cao.
- **Tầng 1 (Chi nhánh phụ):** Có phòng IT nơi tổng hợp lưu lượng truy cập cục bộ, xử lý tải máy chủ.
- Đối với các vị trí có tải trọng lớn kể trên, hệ thống sẽ áp dụng các cơ chế cân bằng tải phù hợp.

Cân bằng tải (Load-balancing) là phương thức phân phối lưu lượng truy cập mạng đều nhau trên một vùng tài nguyên hỗ trợ ứng dụng. Các ứng dụng hiện đại phải xử lý đồng thời hàng triệu người dùng và trả về chính xác văn bản, video, hình ảnh và dữ liệu khác cho từng người dùng một cách nhanh chóng và đáng tin cậy. Để xử lý lưu lượng truy cập cao như vậy, hầu hết các ứng dụng sở hữu nhiều máy chủ tài nguyên, trong đó dữ liệu được sao chép giữa các máy chủ với nhau. Bộ cân bằng tải là thiết bị nằm giữa người dùng và nhóm máy chủ, đồng thời đóng vai trò là bộ điều giải, đảm bảo rằng tất cả các máy chủ tài nguyên đều được sử dụng như nhau.

Cân bằng tải có thể được áp dụng bằng cách cho các công việc và dịch vụ nặng như mail, trao đổi file, kết nối với chi nhánh,... đi qua leased line để đảm bảo đường truyền mạnh, tốc độ truyền/nhận dữ liệu nhanh chóng và ổn định; đối với các công việc nhẹ hơn như truy cập web thì được đi trên đường xDSL để giảm thiểu chi phí hệ thống. Hệ thống áp dụng phương pháp cân bằng tải khi kết nối trụ sở chính với các chi nhánh thông qua 2 kênh thuê riêng (leased lises) và 2 xDSL để truy cập Internet với cơ chế cân bằng tải. Các server cũng được chia ra các công việc riêng biệt để tránh tình trạng quá tải khi tập trung các công việc vào một server.

2.4 Lựa chọn kiến trúc mạng

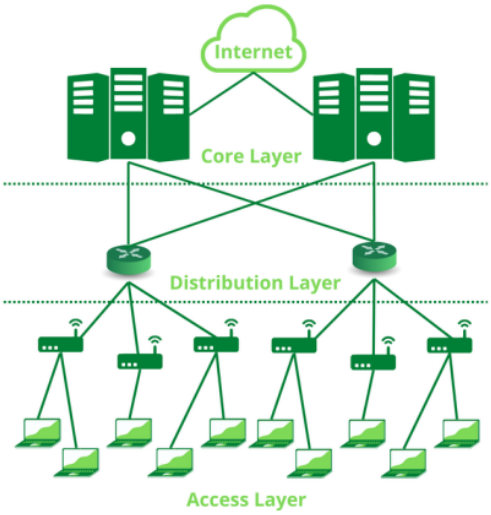
2.4.1 Cấu trúc mạng của hệ thống mạng

Ta thiết kế cấu trúc mạng theo mô hình **Thiết kế mạng phân tầng (Hierarchical Network Design)**. 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.



Hình 1: Mô hình phân tầng với 3 tầng

Lý do lựa chọn

- **Khả năng mở rộng:** Mô hình mạng phân cấp được thiết kế để dễ dàng mở rộng, điều này rất quan trọng khi mạng bệnh viện dự kiến sẽ tăng trưởng 20% trong vòng 5 năm tới.
- **Quản lý đơn giản:** Việc tổ chức mạng thành các lớp giúp việc bảo trì, xử lý sự cố và nâng cấp trở nên hiệu quả hơn.
- **Hỗ trợ VLAN và bảo mật:** Thiết kế này cho phép triển khai VLAN hiệu quả để phân tách lưu lượng giữa các phòng ban, nâng cao bảo mật và cải thiện hiệu suất.
- **Độ sẵn sàng cao:** Mô hình này tích hợp các cơ chế dự phòng và chịu lỗi tại lớp lõi (Core) và lớp phân phối (Distribution), đảm bảo hoạt động không gián đoạn cho các dịch vụ quan trọng của bệnh viện.
- **Tiết kiệm chi phí trong việc mở rộng:** Việc mở rộng trong tương lai, chẳng hạn tích hợp thêm các phòng ban hoặc các cơ sở phụ, có thể thực hiện bằng cách bổ sung thiết bị tại các lớp phù hợp mà không cần thay đổi toàn bộ hệ thống mạng.

Tuy nhiên mô hình này cũng có những **nhược điểm:**

- **Chi phí ban đầu cao:** Việc triển khai mạng phân cấp đòi hỏi mua thêm thiết bị, chẳng hạn như switch lớp lõi và lớp phân phối, làm tăng chi phí ban đầu.
- **Cấu hình phức tạp:** Thiết kế này yêu cầu lên kế hoạch và cấu hình cẩn thận, đặc biệt đối với giao tiếp giữa các lớp, giao thức dự phòng và quản lý VLAN.

- **Sự dư thừa trong thiết kế:** Với các chi nhánh phụ nhỏ hơn, một thiết kế phân cấp đầy đủ có thể không cần thiết do nhu cầu lưu lượng thấp.
- **Thách thức trong bảo trì:** Đảm bảo hệ thống hoạt động tốt và cập nhật thường xuyên cho tất cả các lớp đòi hỏi nhân sự có kỹ năng và giám sát liên tục.

Sau khi xem xét những ưu nhược điểm, nhóm kết luận thiết kế mạng phân cấp là lựa chọn tối ưu cho mạng bệnh viện nhờ vào khả năng mở rộng, bảo mật và quản lý hiệu quả. Mặc dù có thể tăng độ phức tạp và chi phí ban đầu, lợi ích lâu dài vượt trội hơn, đảm bảo hoạt động mạng ổn định và hiệu quả cho các dịch vụ y tế quan trọng.

2.4.2 Thông tin tổng quan về hệ thống mạng

- Kiến trúc mạng được sử dụng bao gồm:
  - Mạng nội bộ LAN: Đây là mạng cục bộ chỉ sử dụng trong toà nhà, dành cho các phòng ban làm việc, ví dụ:
    - VLAN 10: Quản trị viên.
    - VLAN 20: Khoa y tế.
    - VLAN 30: Khách hàng/bệnh nhân.
  - Với mỗi bộ phận, chúng ta sẽ tạo một VLAN riêng cho bộ phận đó. Điều này đáp ứng nhu cầu chia sẻ riêng tư giữa các phòng ban và tăng hiệu suất hệ thống bằng cách giảm chi phí phát sóng, giúp dễ dàng phát hiện lỗi. Một kỹ thuật khác được sử dụng là VLAN Trunking Protocol (VTP). Công nghệ này làm cho việc quản lý các VLAN (thêm / xóa / sửa) đồng bộ và dễ dàng hơn vì chỉ cần thực hiện các thay đổi trên switch ở chế độ VTP server, tất cả các thay đổi sẽ được cập nhật vào switch ở chế độ VTP client.
  - Subinterface: Được sử dụng để định tuyến giữa các VLAN. Nó giúp tiết kiệm cổng vật lý của bộ định tuyến. Với một cổng vật lý chúng ta có thể chia thành nhiều cổng logic (subinterface).
  - Subnet mask: Được dùng phân chia địa chỉ IP. Ở đây ta dùng địa chỉ IP bắt đầu từ 192.168.1.1. Mỗi VLAN sẽ có dải IP khác nhau giúp cho việc lưu trữ tối ưu hóa việc phân bổ địa chỉ IP.
  - Phân hệ mạng DMZ: Gồm hệ thống máy chủ web, dns dành cho khách hàng và nội bộ truy cập. Trên máy chủ web có các hệ thống giao dịch trên mạng của bệnh viện, Internet Hospital, tra cứu các sản phẩm và dịch vụ của bệnh viện, các thông tin quảng cáo,...
  - Sử dụng DHCP: Đây là giao thức cho phép cấp phát địa chỉ IP một cách tự động cùng với các cấu hình liên quan khác như subnet mask và gateway mặc định. Máy tính được cấu hình một cách tự động vì thế sẽ giảm việc can thiệp vào hệ thống mạng phù hợp trong các mô hình quy mô lớn. Nó cung cấp một database trung tâm để theo dõi tất cả các máy tính trong hệ thống mạng. Mục đích quan trọng nhất là tránh trường hợp hai máy tính khác nhau lại có cùng địa chỉ IP.
    - Nếu không có DHCP, các máy có thể cấu hình IP thủ công (cấu hình IP tĩnh). Việc cấu hình IP tĩnh đối với ít máy có thể làm được còn với rất nhiều máy thì sẽ mất thời gian và dễ xảy ra sai xót. DHCP có nhiệm vụ giúp quản lý nhanh, tự động và tập trung việc phân phối địa chỉ IP bên trong một mạng.

    * Cách thức hoạt động của DHCP chính là khi một thiết bị yêu cầu địa chỉ IP từ một router thì ngay sau đó router sẽ gán một địa chỉ IP khả dụng cho phép thiết bị đó có.
    * DHCP mang lại nhiều ưu điểm, song bên cạnh đó cũng còn mặt hạn chế. Chẳng hạn như việc ta không nên sử dụng địa chỉ IP động, địa chỉ IP thay đổi đối với các thiết bị cố định và cần truy cập liên tục.

- Sử dụng cấu trúc liên kết hình sao(star topology) cho mỗi tòa nhà (trụ sở chính và 2 chi nhánh). Ở mỗi tầng, các máy giao tiếp với nhau thông qua mạng bằng cách đẩy các dữ liệu đến switch ở mỗi tầng. Switch này sẽ thực hiện điều hướng tất cả các nguồn dữ liệu ở tầng của mình. Các switch layer 2 sẽ được kết nối với nhau thông qua switch layer 3. Ưu điểm:
    - Có chi phí thấp.
    - Nó cho phép quản lý và khắc phục sự cố mạng dễ dàng hơn, mở rộng mạng bằng cách thêm các thiết bị bổ sung sẽ nhanh hơn và dễ dàng hơn nhiều.
    - Nếu 1 máy gặp sự cố, không ảnh hưởng đến những máy khác.

2.5 Thiết kế mạng không dây

Sử dụng mạng wifi phục vụ cho việc sử dụng laptop và điện thoại của người dùng và khách hàng ở khu vực giao dịch và lễ tân. Ưu điểm:

- Cho phép nhiều người dùng kết nối qua cùng một mạng trong một thời gian rất ngắn mà không có bất kỳ cấu hình nào, các kết nối có thể được thực hiện thông qua bộ định tuyến hoặc công nghệ điểm phát sóng. Tính dễ sử dụng và tiện lợi này không có trong các mạng có dây.
- Việc lắp đặt một điểm truy cập Wifi tương đối dễ dàng so với kết nối mạng có dây. So với kết nối mạng có dây, mạng không dây mang lại lợi thế đáng kể về chi phí và nhân công.

Bên cạnh đó, ta có những nhược điểm:

- Mặc dù mạng không dây đã sử dụng nhiều kỹ thuật mã hóa, nhưng Wifi vẫn dễ bị hack. Do tính chất không dây, nó có khả năng bị tấn công cao, đặc biệt là các mạng wifi công cộng. Vì mạng wifi công cộng được mở cho bất kỳ ai nên tin tặc có thể áp đặt ID mạng giả của họ. Người dùng có thể vô tình kết nối với ID giả mạo này và thuộc nhóm nạn nhân của cuộc tấn công mạng.
- Tốc độ của mạng wifi sẽ giảm khi ta di chuyển ra khỏi điểm truy cập. Ở các tòa nhà nhiều tầng độ mạnh của mạng Wifi có thể thay đổi ở các tầng khác nhau.

Để nâng cao bảo mật của wifi, ta sử dụng tiêu chuẩn bảo mật WPA2/PSK.

3 Chi tiết các thiết bị sử dụng

3.1 Các thiết bị dùng trong hệ thống

3.1.1 Router

- **Router:** Dùng để kết nối giữa các chi nhánh và mạng internet, sử dụng router Cisco 2811

Hình 2: Router2811

- Tổng số cổng: 2.
- Số lượng khe cắm mở rộng: 9.
- Công nghệ Ethernet: FastEthernet.
- Bộ nhớ tiêu chuẩn: 256 MB.
- Bộ nhớ tối đa: 760 MB.
- Bộ nhớ flash: 64MB/256MB.

3.1.2 Switch

- **Switch layer 2:** Dùng để tạo thiết bị kết nối ở cùng 1 tầng, sử dụng switch 2960-24TT.

Hình 3: Switch2960-24TT

- Số cổng: 24 x 10/100 Ethernet Ports.
- Bộ tính năng: LAN Base.
- Chuyển đổi băng thông: 32Gps.
- Bộ nhớ flash: 32MB.
- Băng thông chuyển tiếp: 16Gps.

- **Switch layer 3:** Việc kết nối các VLAN ở các tầng lại với nhau cần đến sự hỗ trợ của switch layer 3, đồng thời đem lại tốc độ cao hơn, bảo mật tốt hơn. Sử dụng Switch layer 3 3560-24PS.

Hình 4: Switch layer 3 3560-24PS

- Số cổng: 24 x 10/100 Ethernet Ports.
- Bộ nhớ flash: 32 MB.
- Bộ tính năng: cơ sở IP.

3.1.3 Access point

- **Access point:** là một thiết bị mạng không dây hoạt động như một cổng để các thiết bị kết nối với mạng cục bộ. Chúng được sử dụng để mở rộng vùng phủ sóng không dây của mạng hiện có để một lượng lớn khách hàng có thể truy cập khi đến ngân hàng. Sử dụng Wireless-G Access Point LINKSYS WAP54G.

Hình 5: Wireless-G Access Point LINKSYS WAP54G

- An ninh mạng không dây: mã hoá 128-bit WPA, lọc địa chỉ MAC
- Tốc độ tối đa đạt 54Mbps theo chuẩn G không dây (802.11g) và 11Mbps theo chuẩn B không dây (802.11b)

3.1.4 Firewall

- **Firewall:** Đảm bảo việc truy cập được bảo mật. Hạn chế các rủi ro từ các dữ liệu độc hại khi truy cập Internet. Sử dụng firewall Cisco 5506.

Hình 6: firewall Cisco 5506

- Thông lượng VPN 3DES / AES tối đa: 250Mbps.
- Kết nối tối đa/giây: 5000.
- Kết nối đồng thời: 50000.
- Tốc độ truyền băng thông: 100 MB/s

3.1.5 Modem

- **Modem:** là một thiết bị phần cứng chuyển đổi dữ liệu từ định dạng kỹ thuật số, dùng để liên lạc trực tiếp giữa các thiết bị có hệ thống dây chuyên dụng, thành một thiết bị phù hợp với phương tiện truyền dẫn như đường dây điện thoại hoặc radio. Có 2 modem phổ biến: DSL và cable.Sử dụng Modem DSL-AX82U, DSL vì chúng có tốc độ ổn định hơn modem cáp.

Hình 7: DSL-AX82U

- Tốc độ truyền dữ liệu WLAN tối đa: 5400 Mbit/s.
- Tốc độ truyền dữ liệu mạng LAN:10/100/1000 Mbit/s.

3.1.6 Thiết bị khác

Ngoài những thiết bị trên còn có các thiết bị khác: các server, máy tính tham gia vào mạng Lan, các thiết bị kết nối không dây,...

3.2 Kế hoạch địa chỉ IP

3.2.1 Trụ sở chính ở TP. Hồ Chí Minh (Tòa A và B)

Tòa A:

Bảng 2: VLAN của Tòa A

VLAN	Tầng	IP range	Subnet Mask	Gateway
VLAN10	Tầng 1	192.168.10.0/24	255.255.255.0	192.168.10.1
VLAN20	Tầng 2	192.168.20.0/24	255.255.255.0	192.168.20.1
VLAN30	Tầng 3	192.168.30.0/24	255.255.255.0	192.168.30.1
VLAN40	Tầng 4	192.168.40.0/24	255.255.255.0	192.168.40.1
VLAN50	Tầng 5	192.168.50.0/24	255.255.255.0	192.168.50.1

Tòa B:

Bảng 3: VLAN của Tòa B

VLAN	Tầng	IP range	Subnet Mask	Gateway
VLAN60	Tầng 1	192.168.60.0/24	255.255.255.0	192.168.60.1
VLAN70	Tầng 2	192.168.70.0/24	255.255.255.0	192.168.70.1
VLAN80	Tầng 3	192.168.80.0/24	255.255.255.0	192.168.80.1
VLAN90	Tầng 4	192.168.90.0/24	255.255.255.0	192.168.90.1
VLAN100	Tầng 5	192.168.100.0/24	255.255.255.0	192.168.100.1

Tất cả đại chỉ IP nội bộ của các workstations phía trên được cấp phát động theo giao thức DHCP. Địa chỉ IP nội bộ mạng của các servers trong Server farm đều được cấp phát tĩnh.

3.2.2 Chi nhánh ở ĐBP

Bảng 4: Địa chỉ mạng của các VLAN

VLAN	Tầng (Thiết bị)	IP range	Subnet Mask	Gateway
VLAN11	Tầng 1	172.16.10.0/24	255.255.255.0	172.16.10.1
VLAN12	Tầng 2	172.16.20.0/24	255.255.255.0	172.16.20.1
VLAN13	Server	172.16.50.0/24	255.255.255.0	172.16.50.1

Bảng 5: Dãy mạng trung gian

IP range	Subnet Mask
172.16.30.0/30	255.255.255.252

IP của các workstations được cấp phát động theo giao thức DHCP. IP của các server đều được cấp phát tĩnh.

3.2.3 Chi nhánh ở BHTQ

VLAN	Tầng (Thiết bị)	IP range	Subnet Mask	Gateway
VLAN21	Tầng 1	10.0.10.0/24	255.255.255.0	10.0.10.1
VLAN22	Tầng 2	10.0.20.0/24	255.255.255.0	10.0.20.1
VLAN23	Server	10.0.50.0/24	255.255.255.0	10.0.50.1

Bảng 6: Cấu hình VLAN

IP range	Subnet Mask
10.0.30.0/30	255.255.255.252

Bảng 7: Dãy mạng trung gian

IP của các workstations được cấp phát động theo giao thức DHCP. IP của các server đều được cấp phát tĩnh.

3.2.4 Sơ đồ IP cho mạng WAN

Tên Subnet	IP range	Subnet Mask
Trụ sở - Chi nhánh DBP	100.100.2.0/24	255.255.255.0
Trụ sở - Chi nhánh BHTQ	100.100.3.0/24	255.255.255.0

Bảng 8: Mạng WAN

3.3 Lược đồ hệ thống

Hệ thống bao gồm 1 router dùng để kết nối các chi nhánh và kết nối với Internet bên ngoài thông qua modem DSL.

Mỗi tầng được trang bị 1 switch để kết nối các máy tính trong tầng. Các switch này sẽ được kết nối đến Multilayer Switch . Riêng tầng 1 ở trụ sở chính và chi nhánh sử dụng 2 switch vì có số lượng máy lớn hơn các tầng còn lại.

Các server được đặt ở một khu vực khác và được kết nối trực tiếp vào Multilayer Switch để tăng tốc độ tải.

- Ngoài ra, trong tầng 1 còn có 1 Access Point để cung cấp wifi cho khách hàng khi đến ngân hàng. Đối với kết nối giữa các chi nhánh với nhau:
  - Trụ sở chính kết nối với các chi nhánh bằng kết nối WAN sử dụng giao thức OSPF.
  - Trụ sở chính dùng 2 đường leased-line trực tiếp đến các router ở phía chi nhánh. Các chi nhánh chỉ cần kết nối đến trụ sở chính mà không cần kết nối đến chi nhánh kia.
  - 2 modem DSL được thiết kế theo cân bằng tải khi truyền dữ liệu ra internet.

4 Thông lượng, băng thông của hệ thống

Thông lượng(Throughput): là lượng thông tin được truyền đi thành công trên mạng trong một đơn vị thời gian.

Băng thông(Bandwidth): là tốc độ tối đa mà trang web có thể truyền tải trong 1s. Hay nói cách khác, nó là dung lượng của liên kết mạng để truyền tải dữ liệu tối đa giữa website với người dùng tính trong 1 đơn vị thời gian.

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,..).

4.1 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 dowload và upload trong 1 ngày:

$$10 \times (1000 + 2000) + 600 \times (500 + 100) + 100 \times 500 = 440000\,\text{MB/ngày} \tag{1}$$

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

$$\frac{440000}{8 \times 3600} = 15.28\,\text{MB/s} = 122.22(Mbps) \tag{2}$$

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

$$\frac{440000 * 0,8}{3 \times 3600} = 32.592\,\text{MB/s} = 260.742(Mbps) \tag{3}$$

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:

$$260.742 \times 1,2 = 312.89(Mbps) \tag{4}$$

4.2 Chi nhánh

Chi nhánh bao gồm 260 workstation, 2 server và giả sử có 50 truy cập mạng không dây.

Tổng lưu lượng dowload và upload trong 1 ngày:

$$2 \times (1000 + 2000) + 260 \times (500 + 100) + 50 \times 500 = 187000\,\text{MB/ngày} \tag{5}$$

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

$$\frac{187000}{8 \times 3600} = 6.493\,\text{MB/s} = 51.943(Mbps) \tag{6}$$

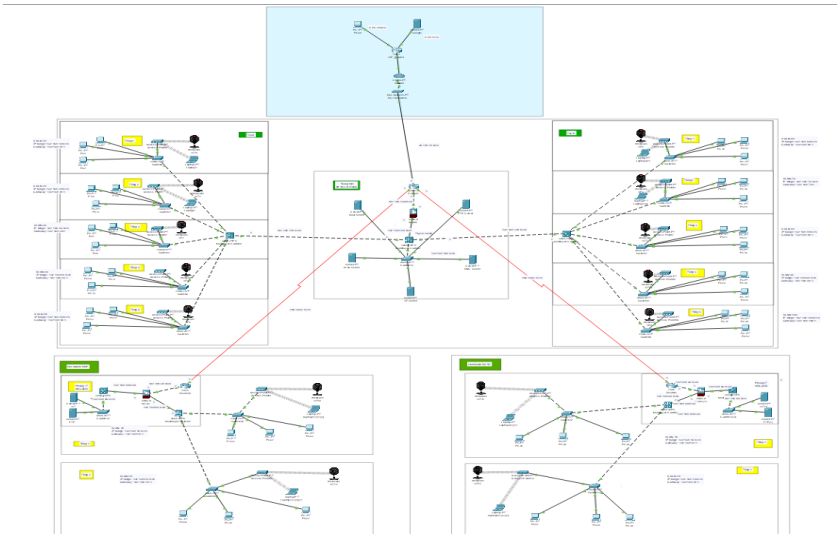
Do 80% lưu lượng mạng tập trung trong 3 giờ cao điểm nên băng thông của hệ thống là:

$$\frac{187000 * 0,8}{3 \times 3600} = 13.851\,\text{MB/s} = 114.4095(Mbps) \tag{7}$$

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:

$$114.4095 \times 1,2 = 137.2914(Mbps) \tag{8}$$

5 Thiết kế hệ thống bằng Packet Tracer

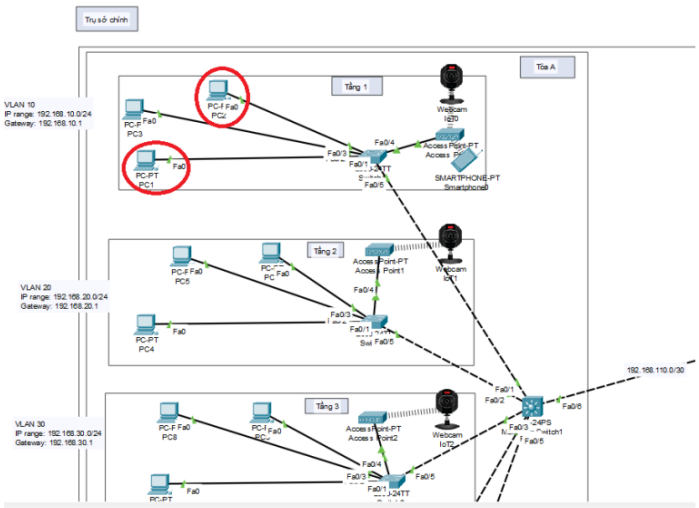


Hình 8: Tổng quan hệ thống

6 Kiểm tra hệ thống sử dụng Ping, Traceroute

6.1 Kiểm tra kết nối của các máy trong cùng VLAN

Ta có 2 PC ở Tòa A của chi nhánh chính nằm trong cùng mạng **VLAN 10**



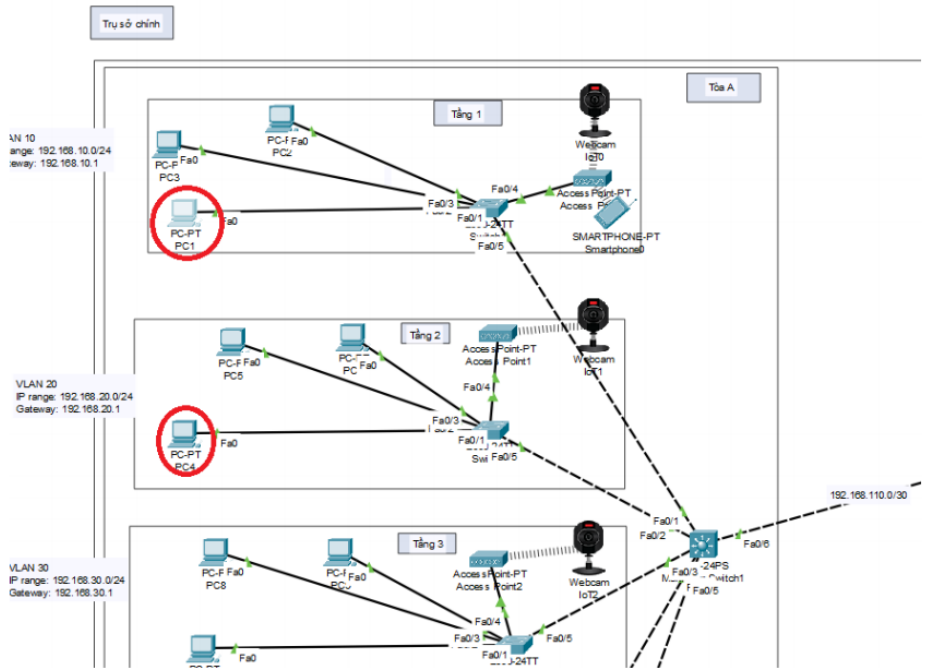
Hình 9: Ping trong cùng VLAN

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Hình 10: Kết quả Ping trong cùng VLAN

6.2 Kiểm tra kết nối các máy khác VLAN

Ta có 2 PC nằm khác mạng **VLAN 10 (Tầng 1)** với **VLAN 20 (Tầng 2)**



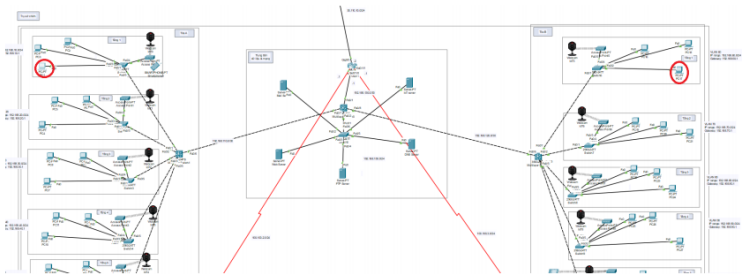
Hình 11: Ping khác VLAN

```
C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time=9ms TTL=127
Reply from 192.168.20.3: bytes=32 time<1ms TTL=127
Reply from 192.168.20.3: bytes=32 time=2ms TTL=127
Reply from 192.168.20.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>
```

Hình 12: Kết quả Ping khác VLAN

6.3 Kiểm tra kết nối giữa các PC ở trụ sở chính

Ta có 2 PC nằm 2 vị trí khác nhau tại Tòa A với Tòa B



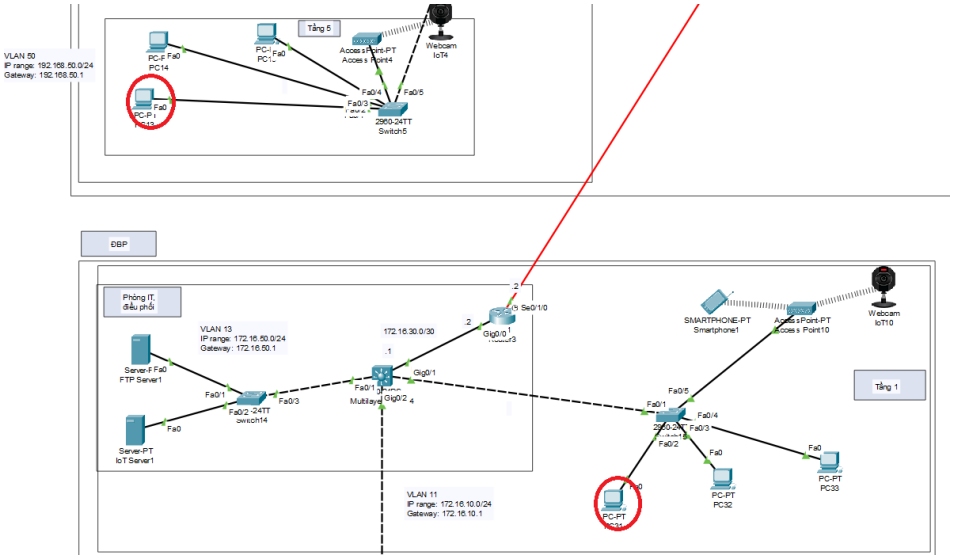
Hình 13: Ping giữa 2 tòa trụ sở chính

```
C:\>ping 192.168.60.4

Pinging 192.168.60.4 with 32 bytes of data:

Reply from 192.168.60.4: bytes=32 time<1ms TTL=125
Reply from 192.168.60.4: bytes=32 time<1ms TTL=125
Reply from 192.168.60.4: bytes=32 time<1ms TTL=125
Reply from 192.168.60.4: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.60.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Hình 14: Kết quả Ping giữa 2 tòa trụ sở chính

6.4 Kiểm tra kết nối giữa các PC ở trụ sở chính và các chi nhánh

Tiến hành ping để kiểm tra kết nối giữa trụ sở chính và trụ sở phụ.



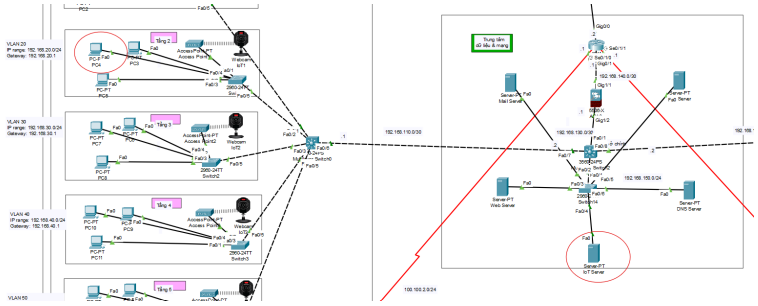
Hình 15: Ping giữa trụ sở chính và trụ sở phụ

```
C:\>ping 172.16.10.3

Pinging 172.16.10.3 with 32 bytes of data:

Reply from 172.16.10.3: bytes=32 time=2ms TTL=123
Reply from 172.16.10.3: bytes=32 time=1ms TTL=123
Reply from 172.16.10.3: bytes=32 time=1ms TTL=123
Reply from 172.16.10.3: bytes=32 time=1ms TTL=123

Ping statistics for 172.16.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Hình 16: Kết quả Ping giữa trụ sở chính và trụ sở phụ

6.5 Kết nối tới server trong vùng DMZ

Tiến hành ping để kiểm tra kết nối server



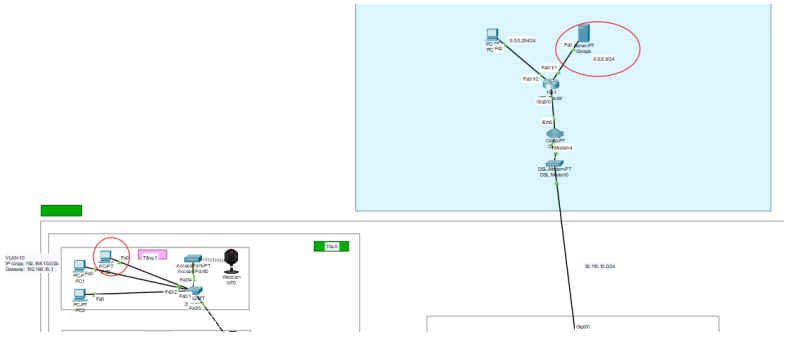
Hình 17: Ping từ máy tính đến server

```
C:\>ping 192.168.150.7

Pinging 192.168.150.7 with 32 bytes of data:

Reply from 192.168.150.7: bytes=32 time<1ms TTL=126
Reply from 192.168.150.7: bytes=32 time<1ms TTL=126
Reply from 192.168.150.7: bytes=32 time<1ms TTL=126
Reply from 192.168.150.7: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.150.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

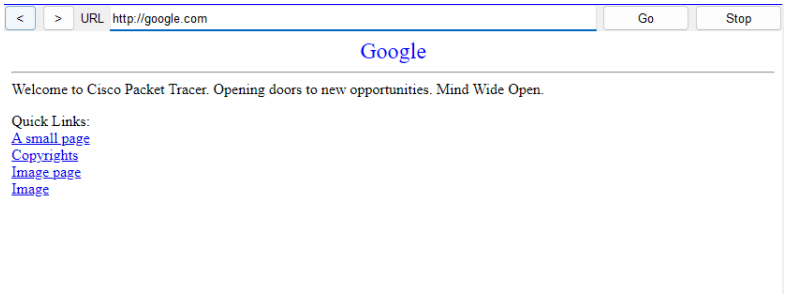
Hình 18: Kết quả Ping từ máy tính đến server

6.6 Kết nối ra ngoài Internet

Kiểm tra kết nối ra ngoài Internet bằng cách cho máy tính truy cập vào google.com (địa chỉ IP là 8.8.8.8).



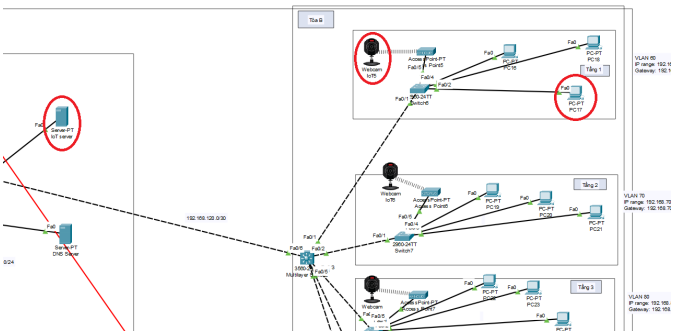
Hình 19: Kết nối ra ngoài Internet



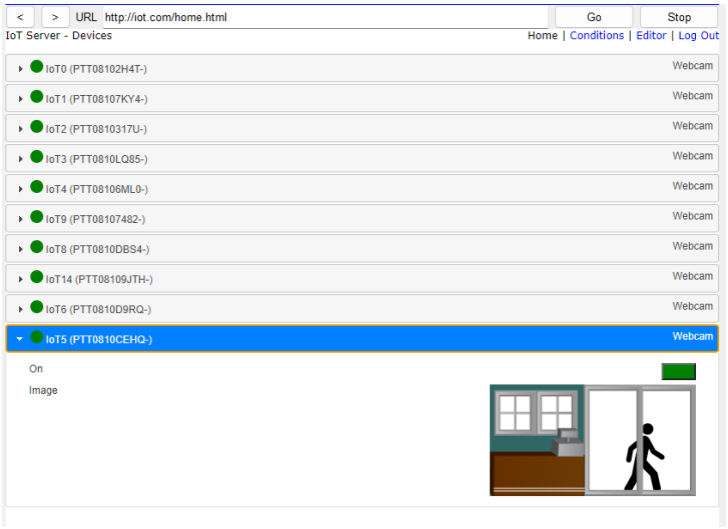
Hình 20: Kết quả kết nối ra ngoài Internet

6.7 Hệ thống quản lý camera giám sát

Truy cập vào hệ thống quản lý camera giám sát (tài khoản và mật khẩu: admin)



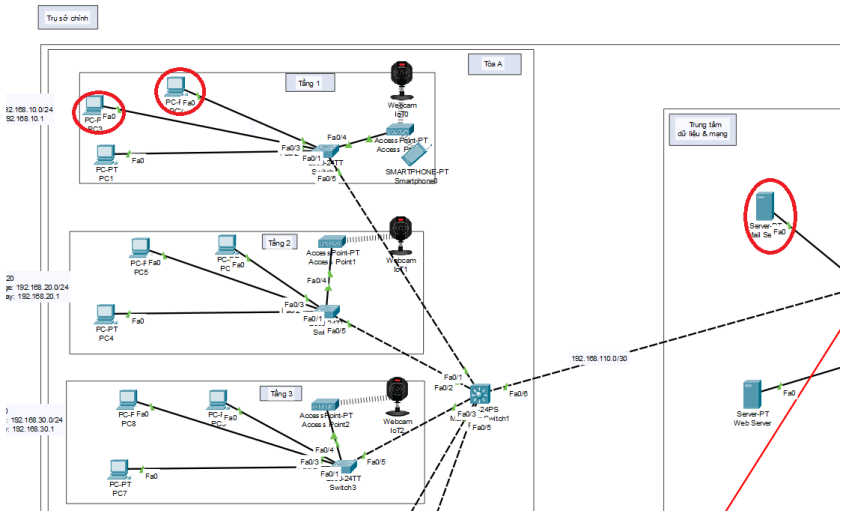
Hình 21: Truy cập hệ thống quản lý camera giám sát



Hình 22: Kết quả khi truy cập vào hệ thống camera giám sát

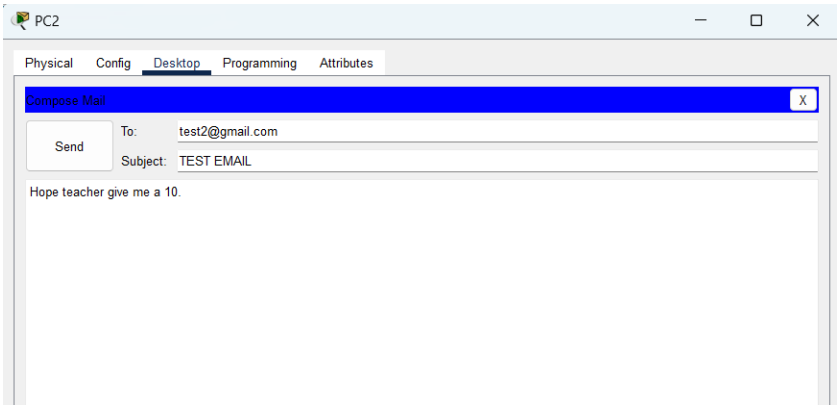
6.8 Hệ thống thư điện tử

Tiến hành gửi và nhận email để kiểm thử chức năng của thư điện tử.



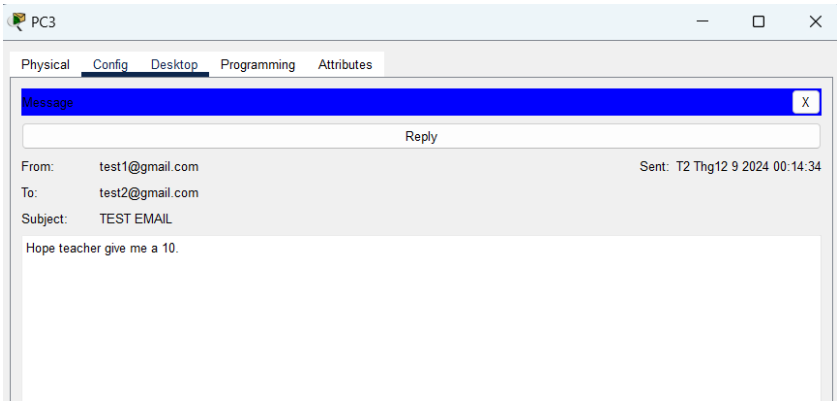
Hình 23: Truy cập hệ thống thư điện tử

PC2 đăng nhập vào tài khoản test1@gmail.com (tài khoản và mật khẩu: test1), sau đó tiến hành gửi email cho test2@gmail.com.



Hình 24: Soạn thư

PC3 đăng nhập vào tài khoản test2@gmail.com (tài khoản và mật khẩu: test2), sau đó tiến hành nhận và xem nội dung thư.



Hình 25: Nhận thư

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. **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.

3. **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.
4. **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: 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 site-to-site và 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 load balancer:** Bổ sung thêm cơ chế cân bằng tải để để phục cho cho hệ thống những lúc cao điểm, hạn chế tình trạng nghẽn hoặc sập server.