

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



Mạng máy tính - CO3094

Báo cáo

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE COMPANY

Giảng viên hướng dẫn: Nguyễn Phương Duy

Sinh viên thực hiện: 2110527 - Nguyễn Hoàng Duy Tân
2112594 - Trần Nguyễn Minh Tuệ
2110342 - Nguyễn Minh Lộc

Mục lục

1. Đặc tả đề tài	3
1.1. Phân tích hệ thống mạng	3
1.2. Danh sách thiết bị kiểm tra để khảo sát tại điểm lắp đặt	5
1.3. Lựa chọn cấu trúc mạng phù hợp	5
1.4. Thiết kế mô hình mạng	5
1.5. Các kỹ thuật, công nghệ và mô hình sử dụng trong mạng	9
2. Mô hình CPT xây dựng cho hệ thống	11

Danh mục hình vẽ

Hình 1: Phòng IT	3
Hình 2: Mô hình toàn bộ thiết kế	6
Hình 3: Thiết kế trụ sở chính TP. Hồ Chí Minh	7
Hình 4: Thiết kế chi nhánh Hà Nội	8
Hình 5: Thiết kế chi nhánh Đà Nẵng	8
Hình 6: Web Server	9

Danh mục bảng biểu

1. Đặc tả đề tài

1.1. Phân tích hệ thống mạng

Sử dụng phần mềm Cisco Packet Tracer để thiết kế và mô phỏng một hệ thống cấu trúc liên kết mạng máy tính trong đó các phòng ban khác nhau có một số máy tính ở các tòa khác nhau. Hệ thống được phát triển ở cơ sở chính (Thành phố Hồ Chí Minh) và hai nhánh (Đà Nẵng và Hà Nội) của kiến trúc ngân hàng BB. Những đặc điểm chính của việc sử dụng IT trong công ty được mô tả như sau:

- **Trụ sở chính:**

- Trụ sở chính bao gồm 7 tầng, tầng 1 bao gồm 1 phòng IT và trung tâm tập trung đường dây kết nối mạng (chi tiết hình bên dưới)



Hình 1: Phòng IT

- Quy mô: 120 máy trạm (những máy bàn được đặt sẵn trong công ty để cho nhân viên làm việc), 5 máy chủ, 12 thiết bị mạng (router, switch, repeater,...).
- Cơ sở hạ tầng mạng sử dụng các công nghệ mới: kết nối có dây và không dây, cáp quang GPON, và GigaEthernet 1GbE/10GbE. Mạng được tổ chức dựa theo cấu trúc VLAN (chia nhỏ mạng con) cho các phòng ban khác nhau.
- Mạng con của trụ sở chính kết nối với 2 mạng con của 2 chi nhánh còn lại (Đà Nẵng và Hà

Nội) bằng 2 đường dây riêng (SD-WAN, MPLS) và 2 xDSL để truy cập vào Internet với cơ chế cân bằng tải. Tất cả thiết bị truy cập vào Internet đều đi qua mạng con của Trụ sở chính.

- Để mua lại phần mềm, công ty sử dụng kết hợp phần mềm trả phí và mã nguồn mở, ứng dụng văn phòng, mô hình client-server, đa phương tiện và cơ sở dữ liệu.
- Yêu cầu bảo mật (tường lửa, IPS/IDS,...), tính sẵn sàng cao, bền vững khi xảy ra sự cố, dễ dàng bảo trì và nâng cấp hệ thống
- Đề xuất cấu hình VPN site-to-site (remote) và cho nhân viên làm việc từ xa kết nối với mạng LAN của công ty.
- Đề xuất hệ thống camera bảo mật cho hệ thống.

• **Các chi nhánh còn lại:**

- Tòa nhà có 2 tầng, tầng 1 được trang bị một phòng IT và trung tâm kết nối dây mạng.
- Quy mô: 30 máy trạm, 3 máy chủ và 5 thiết bị mạng

Thực hiện kết nối giữa trụ sở chính và các chi nhánh được thực hiện thông qua WAN links như SD-WAN, MPLS,... được chọn theo giá cả.

- Đề ra những giải pháp với giá cả cụ thể.
- Phân tích thuận lợi và khó khăn của phương án được lựa chọn.

Các luồng dữ liệu và khối lượng công việc của hệ thống (khoảng 80% vào giờ cao điểm từ 9h đến 11h và từ 15h đến 16h) có thể được chia sẻ cho Trụ sở chính và các chi nhánh phụ như sau:

- Những máy chủ cho việc cập nhật phần mềm, truy cập web, và truy cập cơ sở dữ liệu,... Tổng ước tính tải xuống khoảng 1000MB/ngày và ước tính tải lên là 2000MB/ngày.
- Mỗi máy trạm được dùng để duyệt web, tải tài liệu và giao dịch với khách hàng,... Tổng ước tính tải xuống khoảng 500MB/ngày và ước tính tải lên là 100MB/ngày.
- Các thiết bị kết nối Wifi từ truy cập của người dùng cho việc tải tài liệu xuống là khoảng 500 MB/ngày
- Phân tích thuận lợi và khó khăn của phương án được lựa chọn.

Ngân hàng BB ước tính sẽ gia tăng sự phát triển 20% trong vòng 5 năm về số lượng người dùng, tải mạng, mở rộng chi nhánh,....

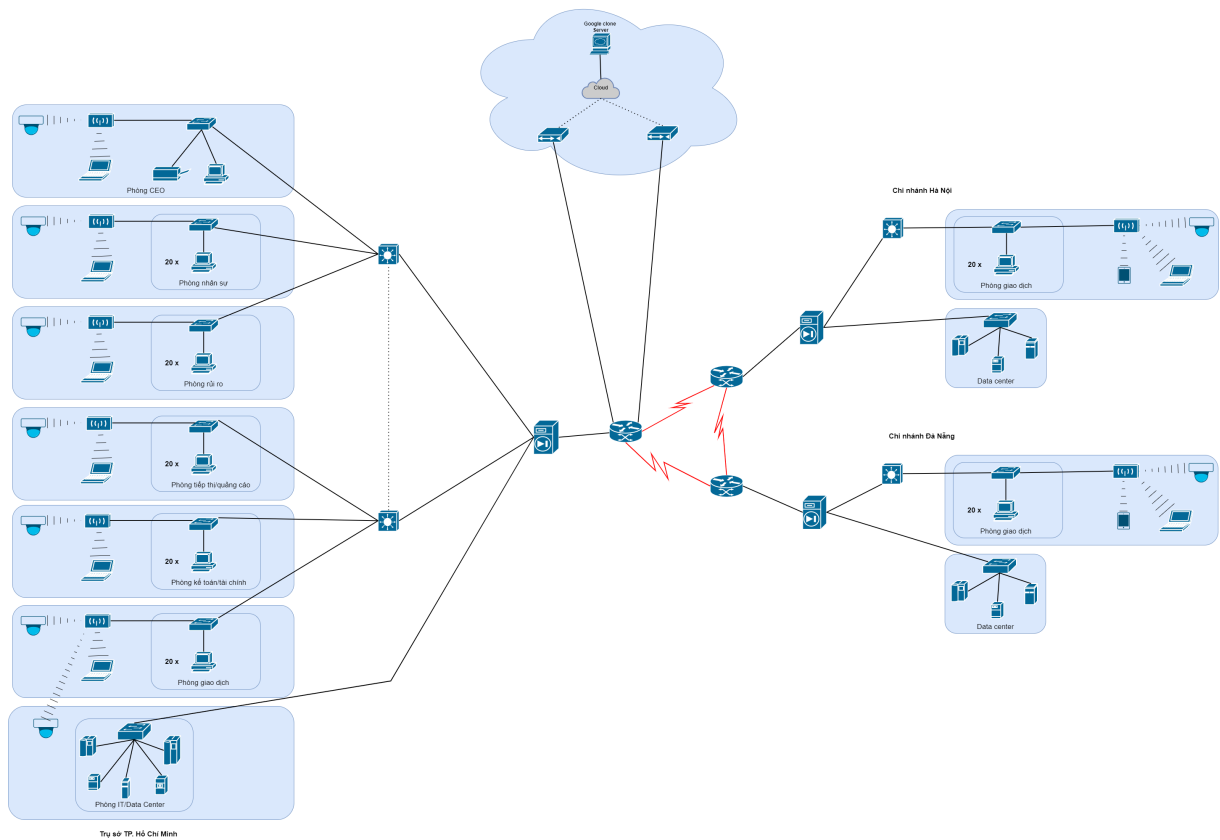
1.2. Danh sách thiết bị kiểm tra đề khảo sát tại điểm lắp đặt

- Firewall 5506-X.
- Router-PT, Server PT.
- Multilayer Switch 3650-24PS, 1 Access Point - PT, các Switch 2960-24TT (ứng với các VLAN của mỗi phòng ban), các workstation (PC, Laptop, Smartphone, printer...
- Vùng có tải lớn tại các khu vực làm việc của các phòng ban trong công ty.

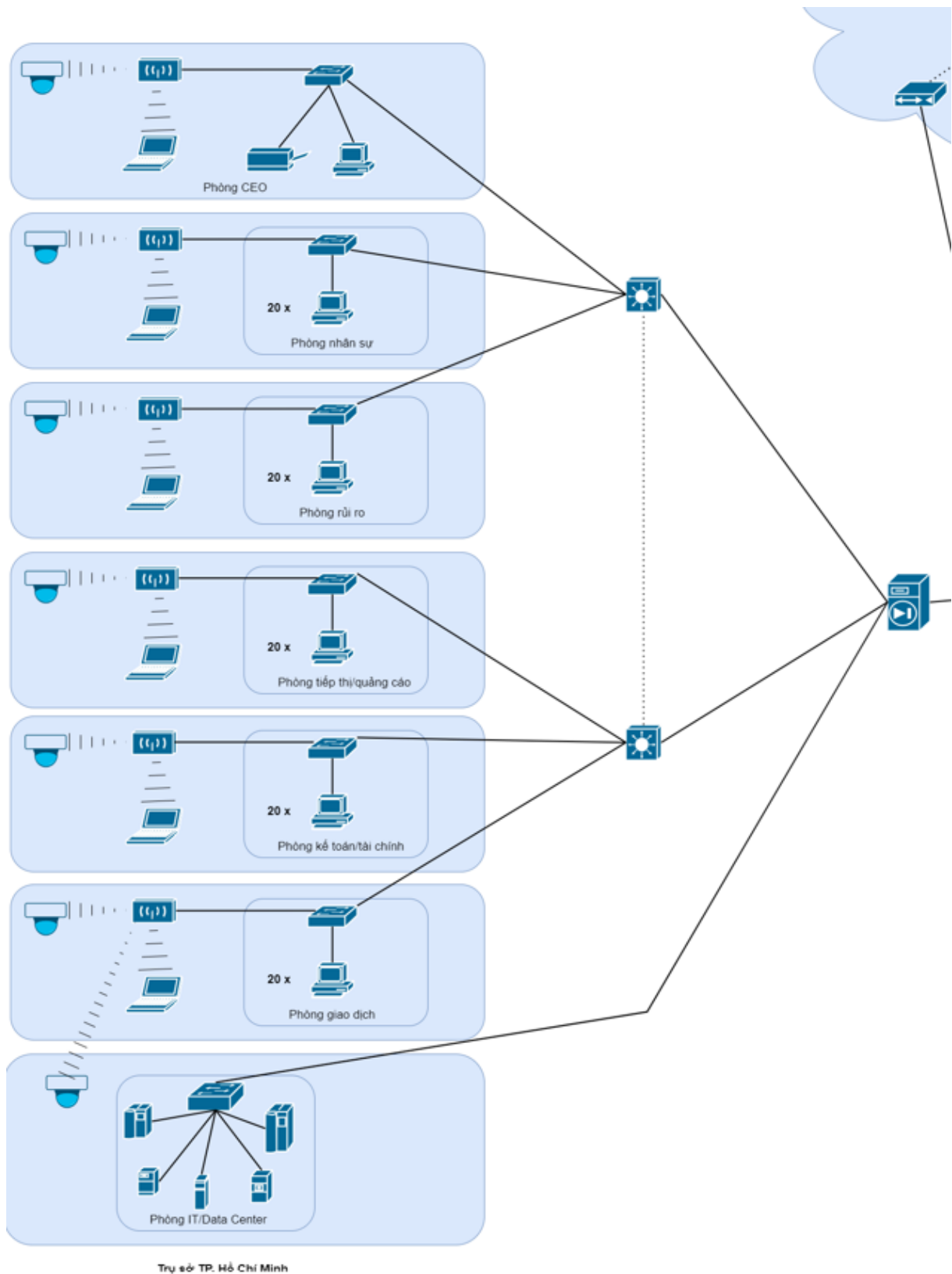
1.3. Lựa chọn cấu trúc mạng phù hợp

- **Trụ sở tại TP. Hồ Chí Minh**
 - Tầng 1 của trụ sở chính có phòng data center, tập trung các server (Web, DNS, FTP, eMail và IoT) kết nối với cùng một switch.
 - Tầng 2 sẽ gồm phòng giao dịch, là nơi thực hiện các giao dịch với khách hàng, cũng như hỗ trợ khách hàng đối với các vấn đề phát sinh. Các máy trạm của phòng này sẽ kết nối với chung 1 switch.
 - Cấu trúc của các tầng từ tầng 3 tới tầng 6 là tương tự nhau, đều gồm 1 phòng ban chức năng (kế toán/tài chính, tiếp thị/quảng cáo, rủi ro, nhân sự) với 1 switch kết nối các máy trạm.
 - Tầng 7 là tầng dành cho phòng CEO, với 1 switch dùng cho các thiết bị trong phòng.
 - Đồng thời, từ tầng 2 đến tầng 7 cũng đều có các điểm truy cập không dây cho các thiết bị khác.
- **Các chi nhánh:** Cũng tương tự với Trụ sở chính, các chi nhánh trong hệ thống đều sẽ lắp đặt phòng kỹ thuật và các thiết bị mạng. Có 3 server sẽ được trang bị tại chi nhánh.

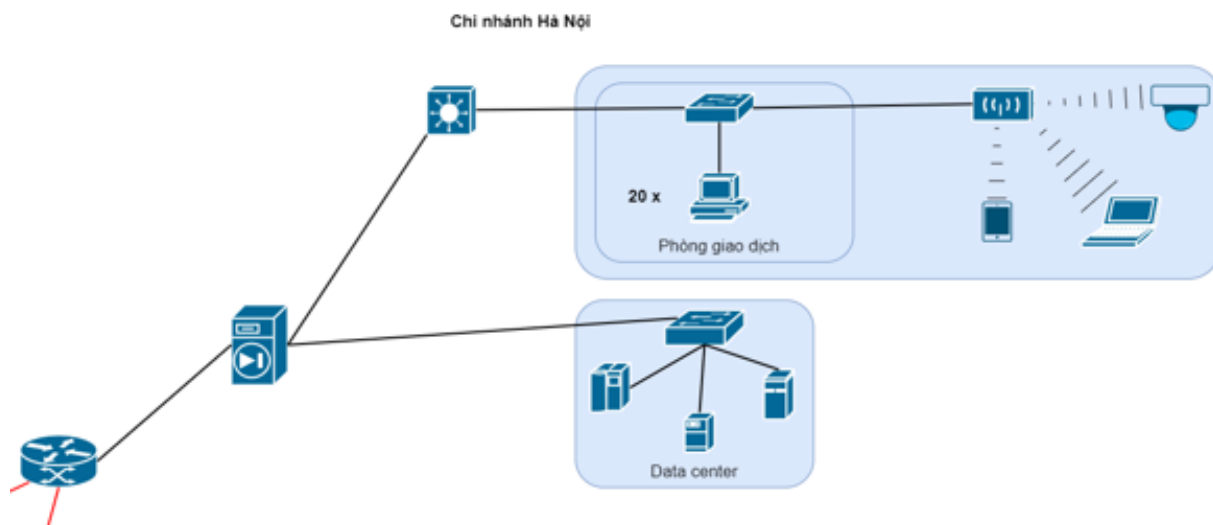
1.4. Thiết kế mô hình mạng



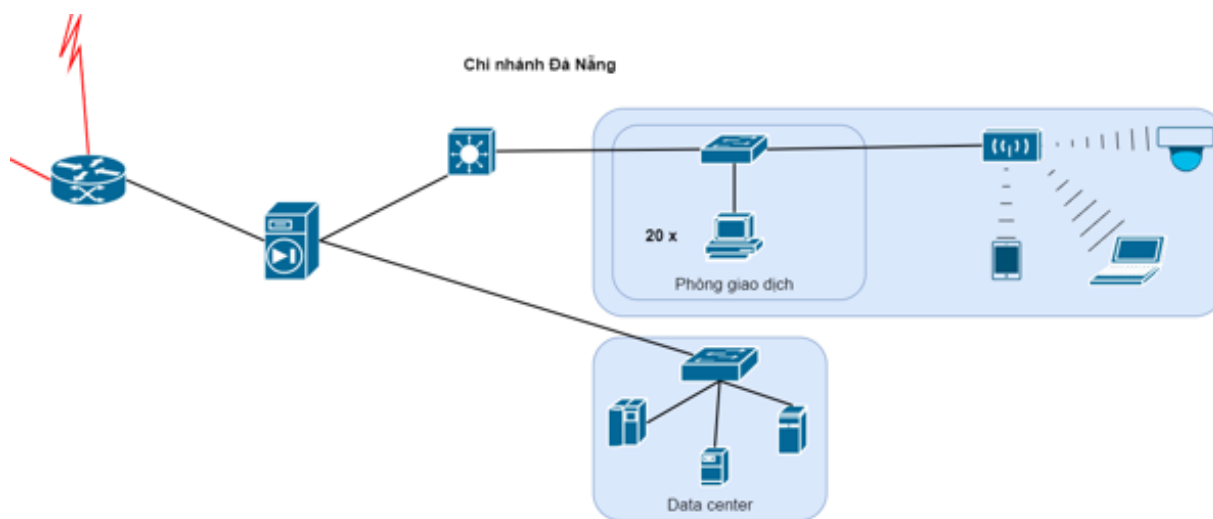
Hình 2: Mô hình toàn bộ thiết kế



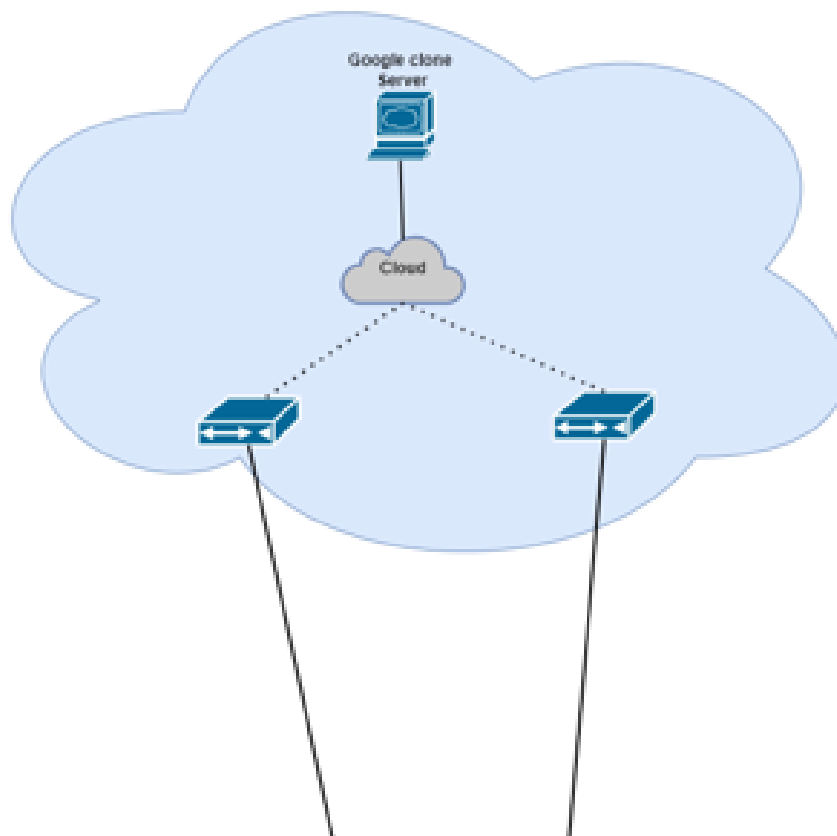
Hình 3: Thiết kế trụ sở chính TP. Hồ Chí Minh



Hình 4: Thiết kế chi nhánh Hà Nội



Hình 5: Thiết kế chi nhánh Đà Nẵng



Hình 6: Web Server

Cấu trúc mạng của BB Bank sẽ được thiết kế theo mô hình phân lớp. Vì mô hình của ngân hàng là quy mô nhỏ do đó Lớp Core và Distribution sẽ được gộp thành một, cùng với đó là lớp Access gồm có các thiết bị switch layer 2 ở mỗi phòng ban.

- Distribution layer: Quảng bá VLAN cấp IP qua bản tin discovery của DHCP Server.
- Access layer: Nhiệm vụ kết nối tới các thiết bị vào từng VLAN.

Ưu điểm mô hình này: sẽ có khả năng chịu lỗi cao, dự phòng và nâng cấp sau này. Tổng quan thì mô hình mạng sẽ được 3 ra làm 3 vùng nhờ việc sử dụng thiết bị tường lửa ASA của Cisco:

- Vùng INSIDE: gồm có các thiết bị mạng bên trong như PC, laptop của nhân viên. Và đây được cho là có mức độ bảo mật cao nhất.
- Vùng DMZ: Gồm các máy chủ.
- Vùng OUTSIDE: được coi như vùng ở bên ngoài Internet, có mức độ bảo mật thấp nhất.

1.5. Các kỹ thuật, công nghệ và mô hình sử dụng trong mạng

IP routing:

Cho phép giao tiếp giữa các VLAN. Bộ định tuyến của mỗi mạng duy trì một bảng các địa chỉ IP và thông tin chi tiết của router hoặc các mạng khác mà nó trước đây đã được kết nối.

OSPF:

Mỗi router khi chạy giao thức sẽ gửi các trạng thái đường link của nó cho tất cả các router trong vùng (area). Sau một thời gian trao đổi, các router sẽ đồng nhất được bảng cơ sở dữ liệu trạng thái đường link với nhau, mỗi router đều có được bản đồ mạng của cả vùng. Từ đó mỗi router sẽ chạy giải thuật Dijkstra tính toán ra một cây đường đi ngắn nhất (Shortest Path Tree) và dựa vào cây này để xây dựng nên bảng định tuyến.

DHCP:

Kỹ thuật này được dùng để cấp phát IP động cho các máy ở các phòng ban. Giảm thiểu lượng công việc cho hệ thống quản trị mạng.

Subnet Mask:

Chúng ta chia Subnet mask cho trụ sở và chi nhánh với private network là 192.168.0.0/23. Mỗi VLAN có một khoảng IP khác nhau. Sử dụng kỹ thuật này, chúng ta sẽ bảo vệ, tối ưu việc cấp phát IP và tối ưu, cải thiện hiệu năng cho toàn mạng.

Mạng DMZ:

DMZ giúp chúng ta bảo vệ servers trong mạng nội bộ. Nếu một server công khai bị tấn công, hacker vẫn không tác động được đến các servers được đặt bên trong DMZ chứa các thông tin quan trọng. Những server được đặt trong DMZ bao gồm: Web, Mail, FTP, IOT, DNS,...



2. Mô hình CPT xây dựng cho hệ thống

Tài liệu tham khảo