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 (TN) (CO3094)

Bài tập lớn

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE COMPANY

Lớp L07 - Nhóm 1

Giảng viên hướng dẫn: Lê Bảo Khánh
Sinh viên: Huỳnh Nguyên Phúc - 2110451
Cao Minh Quân - 2112109
Trần Nguyễn Thái Bình - 2110051
Trương Hoàng Nguyên Vũ - 2112673

Email: phuc.huynhdaihocbk94@hcmut.edu.vn

Thành phố Hồ Chí Minh, tháng 11/2023

Mục lục

1 Danh sách thành viên & Phân công công việc

STT	Họ và tên	MSSV	Công việc	Phần trăm công việc
1	Huỳnh Nguyên Phúc	2110451	Design + Report + Slide	25%
2	Cao Minh Quân	2112109	Design + Report + Slide	25%
3	Trần Nguyễn Thái Bình	2110051	Design + Report + Slide	25%
4	Trương Hoàng Nguyên Vũ	2112673	Design + Report + Slide	25%

2 Cơ sở lý thuyết và công nghệ sử dụng

2.1 Virtual Local Area Network (VLAN)

2.1.1 Định nghĩa

VLAN (Virtual LAN) là một mạng LAN ảo. Về mặt kỹ thuật, VLAN là một miền quảng bá được tạo bởi các switch. Thông thường, router đóng vai trò tạo ra miền quảng bá. Một switch có thể tạo ra VLAN, khi switch có một broadcast (dạng tin nhắn được gửi đi nhưng không có địa chỉ cụ thể) được gửi bởi một thiết bị nằm trong một VLAN sẽ được chuyển đến những thiết bị khác trong cùng VLAN, tuy nhiên broadcast sẽ không được forward (chuyển tiếp) đến các thiết bị trong VLAN khác.

2.1.2 Lý do sử dụng VLAN

- *Tiết kiệm băng thông*: Vì VLAN chia nhỏ mạng LAN thành các đoạn nhỏ hơn nên khi gửi một gói tin, nó sẽ gửi cho một VLAN duy nhất mà không truyền cho các VLAN khác. Do đó, sử dụng VLAN giúp giảm được lưu lượng, tiết kiệm băng thông đường truyền mà không làm giảm tốc độ đường truyền.
- *Tăng khả năng bảo mật*: Các VLAN khác nhau không được truy cập vào nhau. Nếu một VLAN có sự cố cũng không ảnh hưởng đến VLAN khác.
- *Dễ dàng mở rộng*: Trên một switch nhiều cổng, có thể cấu hình VLAN khác nhau cho từng cổng, do đó dễ dàng kết nối thêm các máy tính với các VLAN.
- *Sử dụng VLAN giúp hệ thống mạng có tính linh động cao*: VLAN có thể dễ dàng di chuyển các thiết bị. VLAN có thể được cấu hình tĩnh hay động. Trong cấu hình tĩnh, người quản trị mạng phải cấu hình cho từng cổng của mỗi switch. Sau đó, gán cho nó vào một VLAN nào đó. Trong cấu hình động mỗi cổng của switch có thể tự cấu hình VLAN cho mình dựa vào địa chỉ MAC của thiết bị được kết nối vào.

2.2 De-Militarized Zone (DMZ)

2.2.1 Định nghĩa

De-Militarized Zone (DMZ) được dịch là vùng phi quân sự, hay trong lĩnh vực mạng nói chung, đây là vùng trung lập và có thể được truy cập từ Internet. DMZ thường được sử dụng để đặt các máy chủ như Web server, Mail server,... hoặc các ứng dụng khác có thể được truy cập từ Internet.

2.2.2 Lý do sử dụng DMZ

DMZ đóng vai trò quan trọng trong một hệ thống mạng với những lý do sau đây:

- *Triển khai các dịch vụ trực tuyến*: DMZ cho phép triển khai các dịch vụ trực tuyến như trang web, email, FTP,... mà khôngng ảnh hưởng đến mạng nội bộ. Các dịch vụ này được đặt trong DMZ và chỉ cho phép truy cập từ bên ngoài thông quan Internet, giảm thiểu rủi ro đối với hệ thống mạng nội bộ
- *Bảo vệ hệ thống mạng*: DMZ giúp bảo vệ hệ thống mạng khỏi các cuộc tấn công từ bên ngoài. Tường lửa giúp DMZ kiểm soát lưu lượng mạng truy cập vào các dịch vụ và ứng

dụng được đặt trong DMZ, chỉ cho phép các kết nối được chấp nhận và ngăn chặn các kết nối độc hại

- *Cung cấp dịch vụ cho đối tác và khách hàng*: DMZ cung cấp một môi trường an toàn để cung cấp các dịch vụ cho đối tác và khách hàng từ xa. Các dịch vụ được đặt trong DMZ và được kiểm soát bởi tường lửa để đảm bảo rằng chỉ những kết nối hợp lệ mới được phép truy cập
- *Quản lý truy cập*: DMZ cho phép quản lý truy cập vào các dịch vụ và ứng dụng từ bên ngoài. Quản trị viên có thể cấu hình tường lửa DMZ để kiểm soát truy cập vào các dịch vụ và ứng dụng, chỉ cho phép các kết nối cụ thể và ngăn chặn các kết nối độc hại

2.3 Dynamic Host Configuration Protocol (DHCP)

2.3.1 Định nghĩa

DHCP được viết tắt từ cụm từ Dynamic Host Configuration Protocol (có nghĩa là Giao thức cấu hình động máy chủ). DHCP có nhiệm vụ giúp quản lý nhanh, tự động và tập trung việc phân phối địa chỉ IP bên trong một mạng. Ngoài ra DHCP còn giúp đưa thông tin đến các thiết bị hợp lý hơn cũng như việc cấu hình subnet mask (mặt nạ mạng con) hay default gateway (cổng mặc định).

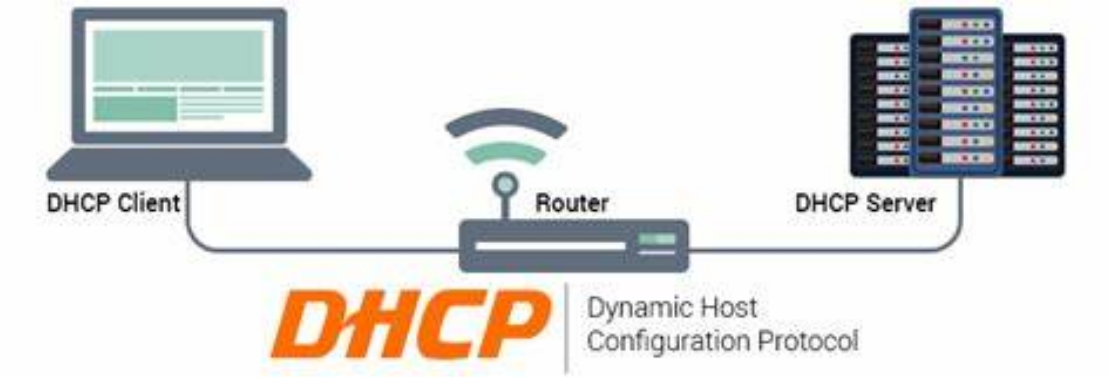
2.3.2 Cách thức hoạt động của DHCP

Khi một thiết bị yêu cầu địa chỉ IP từ một DHCP server (máy chủ) thì ngay sau đó DHCP server sẽ gán một địa chỉ IP khả dụng cho phép thiết bị đó có thể giao tiếp trên mạng.

Như ở các hộ gia đình hay các doanh nghiệp nhỏ thì router sẽ hoạt động như một máy chủ DHCP nhưng ở các mạng lớn hơn thì cần một DHCP server thực thụ.

Cách thức hoạt động của DHCP còn được giải thích ở một cách khác thì khi một thiết bị muốn kết nối với mạng thì nó sẽ gửi một yêu cầu tới máy chủ, yêu cầu này gọi là DHCP DISCOVER. Sau khi yêu cầu này đến máy chủ DHCP thì ngay tại đó máy chủ sẽ tìm một địa chỉ IP có thể sử dụng trên thiết bị đó rồi cung cấp cho thiết bị địa chỉ cùng với gói DHCP OFFER.

Khi nhận được IP thì thiết bị tiếp tục phản hồi lại máy chủ DHCP gói mang tên DHCP REQUEST. Lúc này là lúc chấp nhận yêu cầu thì máy chủ sẽ gửi tin báo nhận (ACK) để xác định thiết bị đó đã có IP, đồng thời xác định rõ thời gian sử dụng IP vừa cấp đến khi có địa chỉ IP mới.



Hình 1: Hình ảnh minh họa cho DHCP

2.3.3 Ưu điểm của DHCP

- *Cấu hình tự động*: Máy tính hay bất cứ thiết bị nào phải cấu hình đúng cách thì mới có thể kết nối với mạng được. DHCP cho phép cấu hình tự động nên dễ dàng cho các thiết bị máy tính, điện thoại, các thiết bị thông minh khác...có thể kết nối mạng nhanh.
- *Không gây ra hiện tượng xung đột trong cấu hình*: Vì DHCP thực hiện theo kiểu gán địa chỉ IP nên sẽ không xảy ra trường hợp trùng địa chỉ IP. Nên so với việc gán theo cách thủ công của IP tĩnh sẽ dễ dàng hơn và giúp hệ thống mạng luôn hoạt động ổn định.
- *Giúp quản lý hệ thống mạng tốt hơn*: DHCP giúp quản lý mạng mạnh hơn vì các cài đặt mặc định và thiết lập tự động lấy địa chỉ sẽ cho mọi thiết bị kết nối mạng đều có thể nhận được địa chỉ IP.
- *Tránh sai lầm đến từ cấu hình thủ công*: Khi đánh tự động nhờ máy chủ DHCP giúp cho người quản lý quản lý có khoa học hơn và không bị nhầm lẫn.
- *Dễ dàng thực hiện các thay đổi*: Ngoài ra người quản lý có thể thay đổi cấu hình và thông số của các địa chỉ IP giúp việc nâng cấp cơ sở hạ tầng được dễ dàng hơn.
- *Dễ dàng mở rộng*: Việc cấu hình động sẽ làm cho việc mở rộng hệ thống trở nên dễ dàng khi mọi thiết bị được kết nối vào hệ thống mạng sẽ được cấu hình một cách tự động.
- *Giúp hệ thống mạng có tính linh động cao*: Một ưu điểm nữa là các thiết bị có thể di chuyển tự do từ mạng này sang mạng khác và nhận địa chỉ IP tự động mới vì các thiết bị này có thể tự nhận IP.

2.3.4 Nhược điểm của DHCP

Mặc dù có rất nhiều lợi ích khi sử dụng DHCP, vẫn có một số hạn chế mà ta cần lưu ý:

- *Không phù hợp với các thiết bị có sự truy cập liên tục*: Không nên sử dụng địa chỉ IP động, địa chỉ IP thay đổi với các thiết bị cố định mà cần truy cập liên tục như server, ...
- *Không phù hợp với các thiết bị phụ thuộc*: Bởi DHCP sử dụng chủ yếu với các hộ gia đình hay văn phòng. Đối với các thiết bị dùng trong văn phòng, như máy in thì việc gán chúng với các địa chỉ IP thay đổi không mang tính thực tiễn. Lúc đó mỗi khi kết nối với máy tính khác thì máy in đó sẽ phải thường xuyên cập nhật cài đặt để máy tính có thể kết nối với máy in.

2.4 Access Control List (ACL)

2.4.1 Định nghĩa

Access Control List (ACL) là danh sách tuần tự các câu lệnh dùng để quản lý quyền truy cập theo chiều đến hoặc đi, xác định cách chuyển tiếp hoặc ngăn chặn một packet (gói tin) trên một thiết bị, được áp dụng trên một interface (giao diện) nào đó, và trên bộ đệm vào hoặc ra, điều khiển router thực hiện các hành động tương ứng là allow (cho phép) hoặc deny (từ chối).

ACL giống như loại stateless firewall (tường lửa không trạng thái); nó chỉ hạn chế, chặn hoặc cho phép các gói tin đang truyền. ACL phổ biến trong các routers hoặc firewall (tường lửa), nhưng chúng cũng có thể được cấu hình trong bất kỳ thiết bị nào chạy trong mạng, từ máy chủ, thiết bị mạng,...

Khi chúng ta xác định ACL trên thiết bị định tuyến cho một interface cụ thể, tất cả packet chạy qua sẽ được xét khớp với nội dung của ACL; sau đó thiết bị sẽ đưa ra quyết định ngăn chặn hay cho phép nó đi qua. Tiêu chí để xác định các quy tắc xét duyệt của ACL có thể là địa chỉ nguồn, địa chỉ đích, một chỉ số port cụ thể, loại gói tin, tính chất gói tin,... Với ACL, chúng ta hoàn toàn có thể lọc các gói tin cho một hoặc một nhóm địa chỉ IP hoặc các giao thức khác, như TCP hoặc UDP, dựa trên thông tin trong IP header hoặc TCP/UDP header.

2.4.2 Lý do sử dụng ACL

- *Kiểm soát lưu lượng ra vào*: Kiểm soát các nguy cơ từ các mạng không đáng tin cậy hoặc từ nguồn phát tin không đáng tin cậy.
- *Hạn chế lưu lượng*: Lưu lượng mạng bị hạn chế để đảm bảo hiệu suất mạng tốt hơn.
- *Mức độ bảo mật cao trong việc truy cập mạng*: ACL giúp chỉ định khu vực nào của máy chủ/mạng/dịch vụ mà người dùng có thể truy cập và khu vực nào không thể.
- *Giám sát chi tiết lưu lượng ra và vào hệ thống*: Mọi gói tin đi vào hay đi ra thiết bị đều phải được duyệt thông qua ACL.

Mục đích chính của việc sử dụng ACL là cung cấp bảo mật cho mạng của bạn. Nếu không có nó, bất kỳ traffic nào cũng được phép đi ra đi vào, làm cho mạng lưới của tổ chức dễ bị tổn thương hơn trước bởi các traffic và truy cập không mong muốn, tiềm ẩn nhiều rủi ro.

2.5 Network Address Translation (NAT)

2.5.1 Định nghĩa

NAT, viết tắt của Network Address Translation, là quá trình một hoặc nhiều địa chỉ IP nội bộ (local IP address) được chuyển đổi thành một hoặc nhiều địa chỉ IP toàn cục (global IP address) và ngược lại nhằm cung cấp khả năng, hỗ trợ quá trình truy cập đến Internet từ thiết bị nội bộ.

2.5.2 Các loại NAT

Có 3 cách để cấu hình NAT bao gồm:

- *Static NAT*: Trong cơ chế này, một địa chỉ IP nội bộ chưa được đăng ký (unregistered private IP address) sẽ được ánh xạ tương ứng với một địa chỉ IP toàn cục hợp lệ duy nhất. Cấu hình này thường được sử dụng trong Web hosting hơn là trong các công ty hoặc doanh

nghiệp do mỗi tổ chức cần nhiều thiết bị nội bộ thực hiện kết nối Internet. Khi đó, việc ánh xạ 1:1 tương ứng sẽ tiêu tốn rất nhiều.

- *Dynamic NAT*: Trong cấu hình này, mỗi địa chỉ IP nội bộ chưa được đăng ký sẽ được ánh xạ thành một địa chỉ IP toàn cục bất kỳ tồn tại trong một IP address pool. Nếu pool không còn global IP address nào, thì các gói tin của private IP address mới sẽ bị bỏ. Cấu hình này cũng rất tiêu tốn khi các tổ chức phải đầu tư một lượng lớn IP address cục bộ cho pool.
- *PAT (Port Address Translation)*: Còn gọi là NAT overload. Trong cấu hình này, nhiều địa chỉ IP nội bộ (local IP address) có thể cùng được ánh xạ vào cùng địa chỉ IP toàn cục. Số port (port number) được dùng để phân biệt kết quả gói tin Internet gửi về thuộc địa chỉ IP nội bộ nào. Phương pháp này thường được dùng vì nó tối ưu chi phí khi nhiều người dùng trong một tổ chức có thể kết nối tới Internet chỉ thông qua một địa chỉ IP toàn cục duy nhất.

2.6 Routing Protocol

Routing Protocol là tập hợp các quy tắc được định nghĩa sẵn để router sử dụng nhằm giao tiếp giữa source và destination, thông qua việc cập nhật bảng routing (routing table).

Có hai loại routing chính: tĩnh (static) và động (dynamic). Trong mạng hệ thống thiết kế trong bài này, nhóm sử dụng static routing và sẽ trình bày cụ thể ý tưởng của static routing.

2.6.1 Static Routing

Static Routing Protocols được sử dụng khi người quản trị thiết lập thủ công đường đi từ điểm bắt đầu (source) tới điểm đích (destination) trong network. Cách thức này tăng được tính bảo mật cao hơn trong hệ thống.

2.7 Throughput (Thông lượng)

Throughput (thông lượng) là tốc độ truyền dữ liệu qua kênh truyền thông hoặc mạng. Đây là số liệu thể hiện lượng dữ liệu có thể truyền được trong một khoảng thời gian nhất định và thường được đo bằng đơn vị bit mỗi giây (bps), byte mỗi giây (Bps) hoặc gói tin mỗi giây (pps). Throughput là một đại lượng quan trọng để đánh giá hiệu suất và hiệu quả của một mạng hoặc một kênh truyền thông. Một throughput cao cho thấy rằng mạng có thể xử lý một lượng lớn lưu lượng mạng một cách hiệu quả, trong khi một throughput thấp cho thấy rằng mạng đang bị tắc nghẽn hoặc có giới hạn băng thông. Công thức tính throughput (T):

$$T = \frac{\text{Tổng dung lượng dữ liệu đã truyền}}{\text{Thời gian truyền}}$$

2.8 Bandwidth (Băng thông)

Bandwidth (băng thông) được định nghĩa là lượng thông lượng truyền tối đa của mạng. Dễ thấy, bandwidth phải có giá trị tối thiểu bằng với throughput tại thời điểm giờ cao điểm để mạng không bị tắt nghẽn. Bandwidth được đo bằng bit, megabit hoặc gigabit trên giây. Công thức tính bandwidth (B) được sử dụng trong thiết kế hệ thống:

$$B = \frac{\text{Tổng dung lượng dữ liệu trong giờ cao điểm}}{\text{Tổng số giờ cao điểm}}$$

2.9 Load Balancing (Cân bằng tải)

Giải pháp cân bằng tải (Network Load Balancing) là một trong những tính năng rất quan trọng với những nhà phát triển, lập trình mạng.Là việc phân bố đồng đều lưu lượng truy cập giữa hai hay nhiều các server có cùng chức năng trong cùng một hệ thống.

Bằng việc sử dụng Network Load Balancing, hệ thống sẽ giảm thiểu tối đa tình trạng một server bị quá tải và ngưng hoạt động. Hoặc khi một server gặp sự cố, cân bằng tải sẽ chỉ đạo phân phối công việc của server đó cho các server còn lại, đẩy thời gian uptime của hệ thống lên cao nhất và cải thiện năng suất hoạt động tổng thể. Điều này đảm bảo tính khả dụng và độ tin cậy của hệ thống và có thể dễ dàng thêm vào hoặc loại bớt các server theo yêu cầu nâng cấp trong tương lai một cách linh hoạt.

2.10 Firewall (Tường lửa)

Firewall (tường lửa) là một thành phần quan trọng trong các hệ thống bảo mật mạng. Nó được thiết kế để ngăn chặn hoặc giảm thiểu các mối đe dọa bảo mật đến từ bên ngoài mạng hoặc từ các máy tính trên mạng nội bộ. Firewall thường được sử dụng để kiểm soát truy cập vào mạng và giám sát lưu lượng mạng.

Cơ chế hoạt động của firewall bao gồm phân tích các giao thức mạng, phát hiện và chặn các gói tin độc hại hoặc có hành vi bất thường. Các chính sách bảo mật của firewall được cấu hình để quyết định liệu các gói tin đó có được phép truy cập vào mạng hay không.

Firewall có thể được triển khai ở nhiều vị trí khác nhau trên mạng, từ cổng vào Internet cho đến các máy tính cá nhân trong mạng nội bộ. Các loại firewall phổ biến bao gồm: firewall phần cứng, firewall phần mềm, firewall ứng dụng, và firewall trung tâm.

3 Yêu cầu hệ thống

3.1 Yêu cầu hệ thống mạng tại trụ sở chính và chi nhánh

Các thiết kế hệ thống mạng sử dụng cho trụ sở chính (TP. Hồ Chí Minh) và hai chi nhánh (Đà Nẵng và Hà Nội) của ngân hàng BB sẽ được miêu tả chi tiết ở các phần tiếp theo.

3.1.1 Trụ sở chính ở TP. Hồ Chí Minh (Ho Chi Minh city Headquarter)

Các thông tin và yêu cầu về hệ thống mạng ở trụ sở chính như sau:

- Tòa nhà trụ sở chính có 7 tầng, tầng 1 bao gồm Phòng ban Kỹ thuật thông tin (IT room) và Phòng tập trung dây mạng & patch panel (Cabling Central Local).
- Quy mô trụ sở chính: 120 workstations (thiết bị làm việc), 5 servers và 12 networking devices (thiết bị mạng).
- Sử dụng các công nghệ mới cho cơ sở hạ tầng mạng bao gồm các kết nối có dây, không dây và cáp sợi (GPON). Mạng được tổ chức theo cấu trúc VLAN và GigaEthernet 1GbE/10GbE.
- Kết nối với hai chi nhánh bằng 2 leased lines (hai đường dây thuê riêng từ các nhà cung cấp) và với Internet bằng 2 DSLs (Digital Subcriber Line hay là đường dây thuê bao số) có sử dụng load balancing (cân bằng tải).

- Sử dụng kết hợp phần mềm được cấp phép và mã nguồn mở, ứng dụng văn phòng, ứng dụng client-server, đa phương tiện và cơ sở dữ liệu.
- Bảo mật cao, an toàn khi xảy ra sự cố, dễ dàng nâng cấp hệ thống.

3.1.2 Chi nhánh ở Đà Nẵng và Hà Nội (Da Nang and Ha Noi Branch)

Trụ sở chính kết nối đến 2 chi nhánh khác ở 2 thành phố lớn là Đà Nẵng và Hà Nội. Mỗi chi nhánh cũng được thiết kế tương tự như trụ sở nhưng ở quy mô nhỏ hơn. Các thông tin và yêu cầu khác đặc thù cho hệ thống mạng ở hai chi nhánh bao gồm:

- Mỗi toà nhà chi nhánh cao 2 tầng, tầng 1 bao gồm Phòng ban Kỹ thuật thông tin và Cabling Central Local.
- Quy mô chi nhánh: 30 workstations, 3 servers và 5 networking devices.

3.1.3 Yêu cầu đặc thù của hệ thống

- Các workstations trong cùng một tầng phòng ban, trừ tầng Lễ Tân (Reception) có thể giao tiếp được với nhau
- Các workstations của cùng tên phòng ban ở trụ sở và chi nhánh có thể giao tiếp được với nhau.
- Các workstations ở tầng Adminstrator mỗi trụ sở hoặc chi nhánh có thế giao tiếp với mọi máy tính của trụ sở hoặc chi nhánh của nó. Riêng workstations tại tầng Admin của trụ sở có thể giao tiếp với toàn bộ workstations của hệ thống.
- Các workstations và laptop ở tầng Lễ tân (Reception) chỉ có thể kết nối tới Internet.
- Các workstations khác tầng nhau (trừ tầng Admin), hay không cùng phòng ban, sẽ không thể kết nối với nhau.

3.1.4 Thông lượng và tải hệ thống

Các thông số về lưu lượng và tải của hệ thống (tập trung khoảng 80% vào giờ cao điểm 9h - 11h và 15h -16h) có thể dùng chung cho trụ sở chính và các chi nhánh như sau:

- Servers dùng cho tác vụ cập nhật, truy cập trang Web, truy cập database (cơ sở dữ liệu)... Tổng dung lượng download (tải xuống) vào khoảng 1000MB/ngày và upload (tải lên) vào khoảng 2000MB/ngày.
- Mỗi workstation dùng cho duyệt Web, tải tài liệu, giao dịch khách hàng... Tổng dung lượng upload vào khoảng 500MB/ngày và download vào khoảng 100MB/ngày.
- Thiết bị kết nối WiFi từ truy cập của khách hàng khoảng 500MB/ngày
- Hệ thống Mạng máy tính của Ngân hàng BB được dự toán cho mức độ phát triển 20% trong 5 năm tiếp theo về nhiều mặt: Về số lượng người sử dụng, tải trọng mạng, mở rộng nhiều chi nhánh,...

3.2 Khảo sát các vị trí cài đặt hệ thống mạng Ngân hàng BB

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:

- *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 công ty:*
  - 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:

Trụ sở chính ở TP. Hồ Chí Minh

- Tòa nhà trụ sở chính có 7 tầng. Tất cả các tầng đều 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 30 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 30 - 40 thiết bị kết nối cùng lúc cho mỗi tầng. Mạng không dây riêng cho Phòng Lễ tân với tối đa không quá 60 thiết bị kết nối cùng lúc
- Cách bố trí các phòng ban:
  - *Phòng ban Kỹ thuật thông tin (IT)*: Nằm ở tầng 1, có 15 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 30)
  - *Phòng ban Quản lý nhân sự (Human Resources)*: Nằm ở tầng 3, có 20 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 40)
  - *Phòng ban Tiếp thị và Bán hàng (Marketing and Sale)*: Nằm ở tầng 4, có 20 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 40)
  - *Phòng ban Tài chính và Kế toán (Financial and Accounting)*: Nằm ở tầng 5, có 20 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 40)
  - *Phòng ban Nghiên cứu và Phát triển (Research and Development)*: Nằm ở tầng 6, có 20 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 40)

- *Phòng Quản trị (Administration)*: Nằm ở tầng 7, có 15 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 30)
- *Phòng Lễ tân (Reception)*: Nằm ở tầng 2, có 20 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 60)
- *Phòng máy chủ (Server farm) và DMZ*: Nằm ở tầng 2, có 4 servers phục vụ công việc nội bộ công ty và 1 Web server thuộc DMZ

Các chi nhánh ở Đà Nẵng và Hà Nội

- Cả hai toà nhà chi nhánh đều giống nhau và kết quả khảo sát là như nhau ở cả hai chi nhánh này
- Tòa nhà chi nhánh có 2 tầng. Tất cả các tầng đều 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 15 thiết bị kết nối cùng lúc cho mỗi tầng. Mạng không dây riêng cho Phòng Lễ tân với tối đa không quá 30 thiết bị kết nối cùng lúc
- Cách bố trí các phòng ban:
  - *Phòng ban Kỹ thuật thông tin (IT)*: Nằm ở tầng 1, có 5 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 15)
  - *Phòng ban Quản lý nhân sự (Human Resources)*: Nằm ở tầng 1, có 5 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 15)
  - *Phòng ban Tiếp thị và Bán hàng (Marketing and Sale)*: Nằm ở tầng 2, có 5 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 15)
  - *Phòng ban Tài chính và Kế toán (Financial and Accounting)*: Nằm ở tầng 2, có 5 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 15)
  - *Phòng ban Nghiên cứu và Phát triển (Research and Development)*: Nằm ở tầng 2, có 5 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 15)
  - *Phòng Quản trị (Administration)*: Nằm ở tầng 2, có 5 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 15)
  - *Phòng Lễ tân (Reception)*: Nằm ở tầng 1, có 5 workstations và một số thiết bị kết nối mạng không dây khác (tối đa không quá 30)
  - *Phòng máy chủ (Server farm)*: Nằm ở tầng 1, có 3 servers phục vụ công việc nội bộ công ty

3.3 Xác định vùng có tải trọng lớn trong Ngân hàng

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 Ngân hàng BB 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 ngân hàng. Do vậy, cần phải đảm bảo về tốc độ truy cập, tính ổn định.
- *Phòng Lễ tân*: Do có sự truy cập của khách hàng nhiều, lượng thông tin ở đây là rất lớn. Do đó cần chú trọng tới cân bằng tải ở nơi đây.
- *Các vị trí tiếp giao*: Các vị trí tiếp giao giữa toàn bộ công ty và mạng Internet cũng như vị trí tiếp giao giữa các chi nhánh và trụ sở chính. Ở vị trí tiếp giao này lượng thông tin di chuyển qua lại là vô cùng lớn, do đó cần chú trọng cân bằng tải.

Đối với các vị trí có tải trọng lớn kể trên, hệ thống sẽ áp dụng các cơ chế cân bằng tải phù hợp.

3.4 Tổng quan thiết kế hệ thống mạng Ngân hàng BB

3.4.1 Cấu trúc mạng của hệ thống mạng

Đối với hệ thống mạng cho Ngân hàng BB với các yêu cầu và các thông tin khảo sát các địa điểm lắp đặt đã có, nhóm lựa chọn cấu trúc *mạng hình sao* cho hệ thống này bởi những ưu điểm sau:

- 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.

3.4.2 Thông tin tổng quan về hệ thống mạng

Thông tin tổng quan về hệ thống mạng mà nhóm sắp thực hiện đươc cho như sau:

- *Phần kết nối Internet và mô phỏng Internet*: Ở phần này, các thiết bị kết nối router riêng được thêm vào để thực hiện kết nối hệ thống với mạng Internet. Nhóm chúng em tạo một vùng mô phỏng Internet bao gồm các ISPs và các vùng mạng khách để người dùng thực hiện kết nối.
- *Phần Server farm và DMZ*: Gồm Server farm chứa hệ thống máy chủ phục vụ các tác vụ như là giao dịch (transaction), thư điện tử (email), cơ sở dữ liệu (database), máy chủ dự phòng (backup), máy chủ Web,.. và DMZ. Các máy chủ thuộc Server farm cần mức độ bảo mật cao, tuy vậy DMZ lại không cần mức độ bảo mật cao; bên cạnh đó DMZ phải đảm bảo được thông lượng cho số lượng truy cập nhiều đến từ Internet, do đó Server farm và DMZ được tách biệt làm hai vùng mạng khác nhau trong hệ thống.
- *Phần mạng máy tính nội bộ* : Gồm các workstation đặt tại các phòng ban của trụ sở chính và chi nhánh ở các tầng mỗi tòa được sử dụng với nhu cầu công việc của các nhân viên trong Ngân hàng. Để đảm bảo được cân bằng tải ở phòng Lễ tân, sẽ có một đường mạng riêng cho phòng này.
- *Phần mạng nội bộ không dây (Wireless LAN)*: Hỗ trợ các kết nối không dây có các thiết bị điện tử có thể kết nối không dây, hỗ trợ kết nối Internet không dây cho nhân viên và khách hàng ở mỗi phòng ban cả ở trụ sở chính hay ở các chi nhánh. Để đảm bảo được cân bằng tải ở phòng Lễ tân, sẽ có một đường mạng riêng cho phòng này.

- *Phần kết nối trụ sở với các chi nhánh khác*: Trụ sở chính của ngân hàng kết nối với các chi nhánh khác của nó theo đường truyền riêng được thuê bởi bên cung cấp kết nối với mạng WAN. Các cơ chế cân bằng tải phù hợp sẽ được áp dụng ở vị trí cổng của hệ thống mạng mỗi tòa nhà.

4 Mô tả cụ thể cho thiết kế mạng

4.1 Các thiết bị mạng sử dụng

4.1.1 Switch

- Switch Layer 2 Cisco WS-C2960-24TT-L: được sử dụng làm Switch chính trong hệ thống, dùng để kết nối với các phòng ban và với switch tổng. Thiết bị có độ bảo mật cao cũng như dễ cấu hình, xử lý. Thông số kỹ thuật:
  - Fast 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 2: Thiết bị chuyển mạch WS-C2960-24TT-L

- Switch Layer 3 Cisco WS-C3650-24PS: Được sử dụng để kết nối các Server trong Server farm hoặc các switch tại phòng ban headquarter và với tường lửa qua 24 cổng Gigabit Ethernet. Thông số kỹ thuật:
  - Gigabit Ethernet: 24 cổng 10/100/1000 PoE+, 4 cổng uplink Gigabit Ethernet with Small Form-Factor Pluggable (SFP).
  - Nguồn điện: 640WAC
  - Available PoE Power: 390 W
  - Memory DRAM: 4 GB

Hình 3: Thiết bị chuyển mạch WS-C3650-24PS

- Multilayer Switch 3560-24PS: Được sử dụng để kết nối với các switch tại các phòng ban của chi nhánh và 2 cổng Gigabit Ethernet để kết nối với tường lửa. Ngoài chức năng chuyển mạch còn có thể định tuyến khi kết nối với các mạng con chi nhánh có nhiều VLAN khác nhau sử dụng Switch Layer 3 là một lựa chọn phù hợp, ngoài ra với yêu cầu chúng ta cũng có thể lựa chọn Router thay thế.

  Thông số kỹ 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 4: Thiết bị chuyển mạch WS-C3560-24PS

4.1.2 Router

Router ISR4331/K9: Được sử dụng để kết nối các chi nhánh với trụ sở, và kết nối mạng công ty với Internet. Thực hiện định tuyến các gói tin giữa các chi nhánh và với bên ngoài công ty. Router có thể được cài đặt các giải thuật hay giao thức định tuyến để truyền các gói tin theo các con đường nhất định. Các giao thức phổ biến là định tuyến tĩnh, RIP (Routing Information Protocol), OSPF (Open Shortest Path First).
Thông số kỹ thuật:

- Gigabit Ethernet: 3 cổng WAN hoặc LAN 10/100/1000
- Serial: 2 cổng RJ45
- NIM slots: 2
- ISC slot: 1
- Tổng thông lượng: 100-300 Mbps
- Memory DRAM: 4 GB (mặc định) / 16 GB (tối đa)
- Bộ nhớ flash: 4 GB (mặc định) / 16 GB (tối đa)

Hình 5: Router ISR4331/K9

4.1.3 Access Point

Access Point (AP) là một thiết bị trong mạng dùng để kết nối các thiết bị không dây như laptop, điện thoại di động vào mạng có dây. AP chủ yếu thực hiện chức năng chuyển đổi từ tín hiệu không dây sang tín hiệu có dây và ngược lại. AP thường được sử dụng để mở rộng phạm vi của một mạng không dây, tạo ra các khu vực sóng không dây mới để cung cấp kết nối Internet và dịch vụ mạng cho các thiết bị không dây. Ngoài ra AP có thể được tích hợp các tính năng bảo mật như mã hóa dữ liệu, xác thực.
Nhóm sử dụng Cisco Business 240AC Access Point. Đây là thiết bị AP cung cấp hiệu suất cao và quản lý dễ dàng cho các mạng nhỏ và vừa. Có thể hỗ trợ tối đa 400 khách hàng cho mỗi điểm truy cập. Thiết bị này được kết nối với switch layer 2 (2) ở mỗi tầng nhằm cung cấp khả năng truy cập không dây cho các máy ở tầng đó bên cạnh các kết nối có dây với workstations.
Thông số kĩ thuật:

- Giao thức liên kết dữ liệu: IEEE 802.11ac
- Bảo mật không dây: Giúp bảo vệ dữ liệu an toàn cao với mã hóa xác thực khi kết nối không dây với bảo mật WPA2.
- Anten: 2 anten bên trong
- Bandwidth: 2.4GHz – 5 GHz
- Ethernet port: 2 x Gigabit (10/100/1000BASE-T autosensing), Power over Ethernet (PoE), xác thực với 802.1X hoặc MAC filtered

Hình 6: Cisco Business 240AC Access Point

4.1.4 Firewall

Một hệ thống an ninh mạng, có thể dựa trên phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát traffic vào, ra khỏi hệ thống. Tường lửa hoạt động như một rào chắn giữa mạng an

toàn và mạng không an toàn. Nhóm lựa chọn tường lửa ASA 5506-X. Cisco ASA 5506-X là một tường lửa đầy đủ tính năng cho các môi trường làm việc từ xa của doanh nghiệp và chi nhánh. Nó cung cấp tường lửa hiệu suất cao, SSL và IPsec VPN và các dịch vụ mạng phong phú trong một thiết bị hoạt động tức thì theo mô-đun. Sử dụng Trình quản lý thiết bị bảo mật thích ứng Cisco (ASDM) đồ họa tích hợp, Cisco ASA 5506-X có thể được triển khai nhanh chóng và dễ dàng quản lý, giúp các doanh nghiệp giảm chi phí hoạt động. Nó có bộ chuyển mạch Gigabit Ethernet, các cổng có thể được nhóm động để tạo ra tối đa ba VLAN riêng biệt cho gia đình, doanh nghiệp và lưu lượng truy cập Internet để cải thiện phân đoạn mạng và bảo mật.

Hình 7: Cisco ASA 5506-X

4.2 Phương án cấp phát địa chỉ IP

Đối với hệ thống mạng này, nhóm sẽ tách hệ thống mạng ở trụ sở chính, hệ thống mạng ở hai chi nhánh thành 3 subnets khác nhau với thông tin cho từng subnet như sau:

- Trụ sở chính ở TP. Hồ Chí Minh: 10.1.0.0/16
- Chi nhánh ở Hà Nội: 10.2.0.0/16
- Chi nhánh ở Đà Nẵng: 10.3.0.0/16

4.2.1 Trụ sở chính ở TP. Hồ Chí Minh

VLAN	Tầng	Phòng ban	Địa chỉ mạng	Địa chỉ khả dụng	Workstations
10	1	Kỹ thuật thông tin	10.1.10.0/24	10.1.10.2 - 10.1.10.254	15 - 30
20	3	Quản lý nhân sự	10.1.20.0/24	10.1.20.2 - 10.1.20.254	20 - 40
30	4	Tiếp thị và Bán hàng	10.1.30.0/24	10.1.30.2 - 10.1.30.254	20 - 40
40	5	Tài chính và Kế toán	10.1.40.0/24	10.1.40.2 - 10.1.40.254	20 - 40
50	6	Nghiên cứu và Phát triển	10.1.50.0/24	10.1.50.2 - 10.1.50.254	20 - 40
200	2	Lễ tân	10.1.150.0/24	10.1.150.2 - 10.1.150.254	20 - 60
500	7	Quản trị	10.1.200.0/24	10.1.200.2 - 10.1.200.254	15 - 30

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

VLAN	Default gateway
10	10.1.10.1
20	10.1.20.1
30	10.1.30.1
40	10.1.40.1
50	10.1.50.1
200	10.1.150.1
500	10.1.200.1

Bảng 2: Bảng VLAN và default gateway cho từng VLAN

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. Dưới đây là địa chỉ Private IP của 4 servers trong Server farm với default gateway là 10.1.250.1:

- Transaction server: 10.1.250.2
- Mail server: 10.1.250.3
- Database server: 10.1.250.4
- Backup server: 10.1.250.5

Tương tự như vậy, địa chỉ IP nội bộ của Web server trong DMZ được cấp phát tĩnh với giá trị là 10.1.251.2 với default gateway là 10.1.251.1

4.2.2 Chi nhánh Hà Nội

VLAN	Tầng	Phòng ban	Địa chỉ mạng	Địa chỉ khả dụng	Workstations
10	1	Kỹ thuật thông tin	10.2.10.0/24	10.2.10.2 - 10.2.10.254	5 - 15
20	1	Quản lý nhân sự	10.2.20.0/24	10.2.20.2 - 10.2.20.254	5 - 15
30	2	Tiếp thị và Bán hàng	10.2.30.0/24	10.2.30.2 - 10.2.30.254	5 - 15
40	2	Tài chính và Kế toán	10.2.40.0/24	10.2.40.2 - 10.2.40.254	5 - 15
50	2	Nghiên cứu và Phát triển	10.2.50.0/24	10.2.50.2 - 10.2.50.254	5 - 15
200	1	Lễ tân	10.2.150.0/24	10.2.150.2 - 10.2.150.254	5 - 30
500	2	Quản trị	10.2.200.0/24	10.2.200.2 - 10.2.200.254	5 - 15

Bảng 3: Bảng VLAN và địa chỉ IP nội bộ khả dụng của chi nhánh Hà Nội

VLAN	Default gateway
10	10.2.10.1
20	10.2.20.1
30	10.2.30.1
40	10.2.40.1
50	10.2.50.1
200	10.2.150.1
500	10.2.200.1

Bảng 4: Bảng VLAN và default gateway cho từng VLAN

IP của các workstations được cấp phát động theo giao thức DHCP. IP của các server đều được cấp phát tĩnh. Dưới đây là địa chỉ Private IP của 3 servers trong Server farm của chi nhánh với default gateway là 10.2.250.1:

- Transaction server: 10.2.250.2
- Database server: 10.2.250.3
- Mail server: 10.2.250.4

4.2.3 Chi nhánh Đà Nẵng

VLAN	Tầng	Phòng ban	Địa chỉ mạng	Địa chỉ khả dụng	Workstations
10	1	Kỹ thuật thông tin	10.3.10.0/24	10.3.10.2 - 10.3.10.254	5 - 15
20	1	Quản lý nhân sự	10.3.20.0/24	10.3.20.2 - 10.3.20.254	5 - 15
30	2	Tiếp thị và Bán hàng	10.3.30.0/24	10.3.30.2 - 10.3.30.254	5 - 15
40	2	Tài chính và Kế toán	10.3.40.0/24	10.3.40.2 - 10.3.40.254	5 - 15
50	2	Nghiên cứu và Phát triển	10.3.50.0/24	10.3.50.2 - 10.3.50.254	5 - 15
200	1	Lễ tân	10.3.150.0/24	10.3.150.2 - 10.3.150.254	5 - 30
500	2	Quản trị	10.3.200.0/24	10.3.200.2 - 10.3.200.254	5 - 15

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

VLAN	Default gateway
10	10.3.10.1
20	10.3.20.1
30	10.3.30.1
40	10.3.40.1
50	10.3.50.1
200	10.3.150.1
500	10.3.200.1

Bảng 6: Bảng VLAN và default gateway cho từng VLAN

IP của các workstations được cấp phát động theo giao thức DHCP. IP của các server đều được cấp phát tĩnh. Dưới đây là địa chỉ Private IP của 3 servers trong Server farm của chi nhánh với default gateway là 10.3.250.1:

- Transaction server: 10.3.250.2
- Database server: 10.3.250.3
- Mail server: 10.3.250.4

4.2.4 Phương án chuyển đổi địa chỉ IP nội bộ thành địa chỉ IP công cộng (public IP) cho giao tiếp Internet

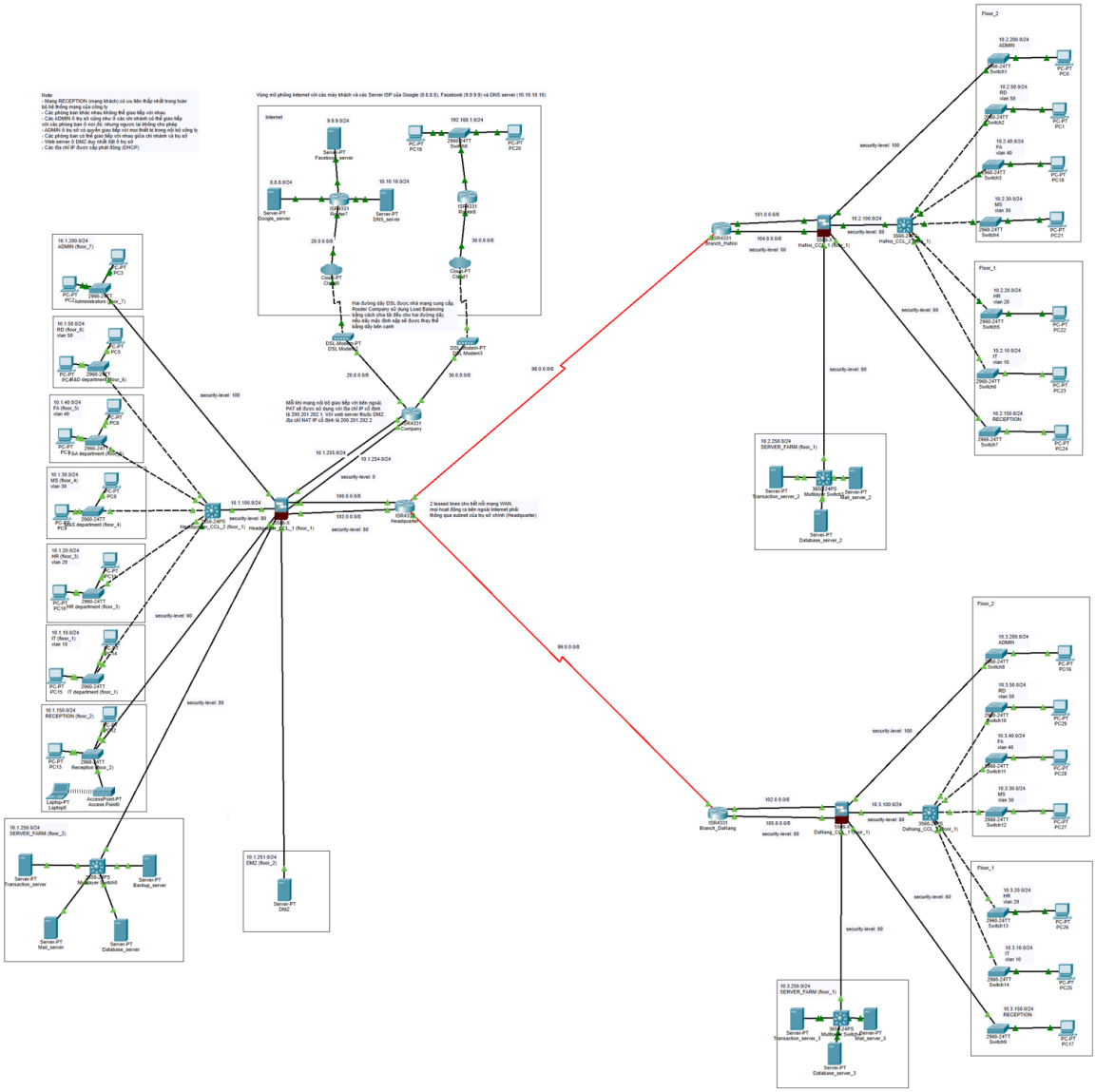
Ở hệ thống mạng này, nhóm sẽ sử dụng PAT như đã được đề cập trong phần cơ sở lý thuyết để ánh xạ toàn bộ địa chỉ IP nội bộ của toàn công ty thành một địa chỉ IP duy nhất khi giao tiếp

với Internet. Bên cạnh đó, vì Web server phục vụ cung cấp dịch vụ cho bên ngoài, thiết bị này sẽ được ánh xạ tĩnh riêng thành một địa chi IP theo cơ chế static NAT.

Địa chỉ sau khi được dịch ra của các thành phần được cung cấp như sau:

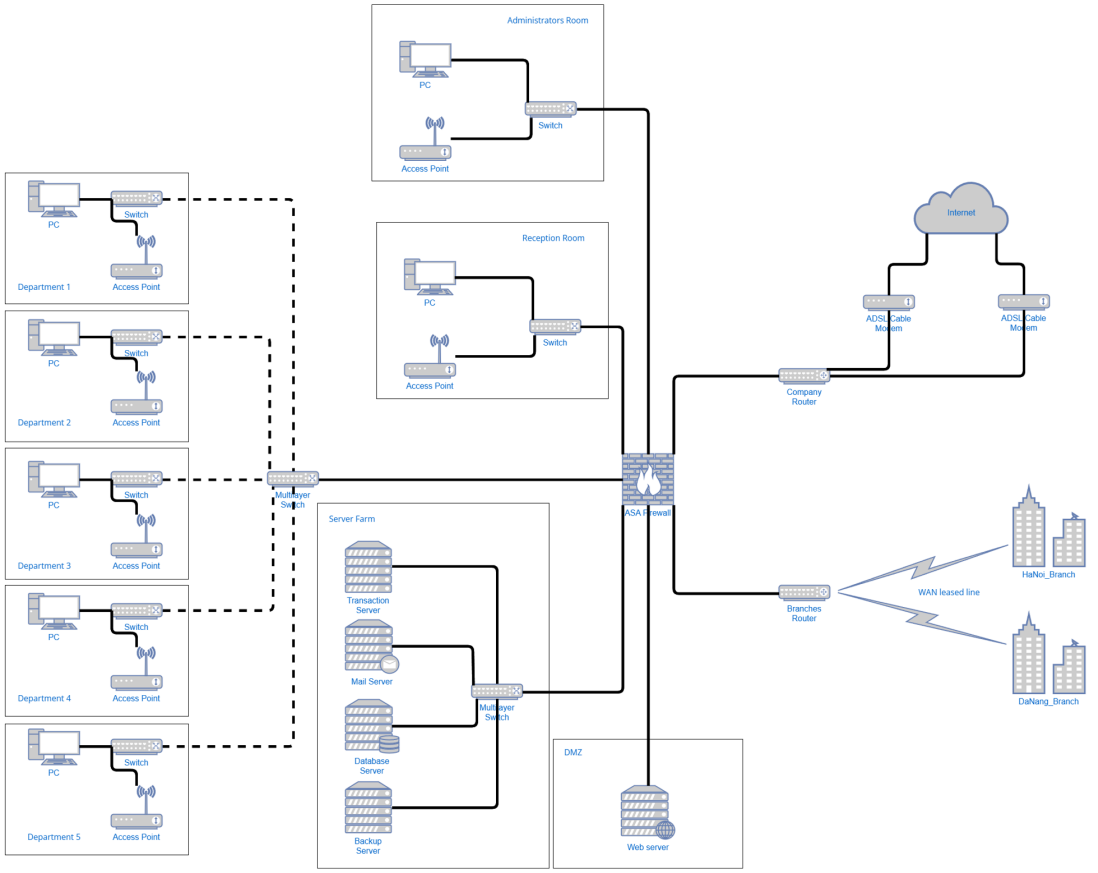
- Toàn bộ thiết bị ở công ty (ngoại trừ DMZ): 200.201.202.1
- Web server ở DMZ: 200.201.202.2

4.3 Thiết kế mạng tại trụ sở chính và ở các chi nhánh



Hình 8: Tổng quan thiết kế mô phỏng hệ thống mạng cho Ngân hàng BB sử dụng phần mềm Packet Tracer

4.3.1 Thiết kế mạng tại trụ sở chính ở TP. Hồ Chí Minh



Hình 9: Sơ đồ đi dây cho trụ sở chính ở TP. Hồ Chí Minh

Sau đây là mô tả chi tiết cho sơ đồ đi dây của trụ sở chính:

- Trong thiết kế này, các thành phần mạng LAN trong trụ sở chính được kết nối với tường lửa trước khi truy cập vào Internet để đảm bảo an toàn cho các servers và các thiết bị nội bộ trong trụ sở. Tường lửa sẽ được kết nối với Internet thông qua một router. Router sẽ kết nối với ADSL Modem và từ ADSL Modem kết nối với Internet qua DSL nhằm cung cấp khả năng truy cập mạng cho hệ thống. Hai đường dây DSLs đó được nhà mạng cung cấp, router Company sử dụng cân bằng tải bằng cách chia tải đều cho hai đường dây, nếu dây mặc định bị sập thì sẽ được thay thế bằng dây bên cạnh.

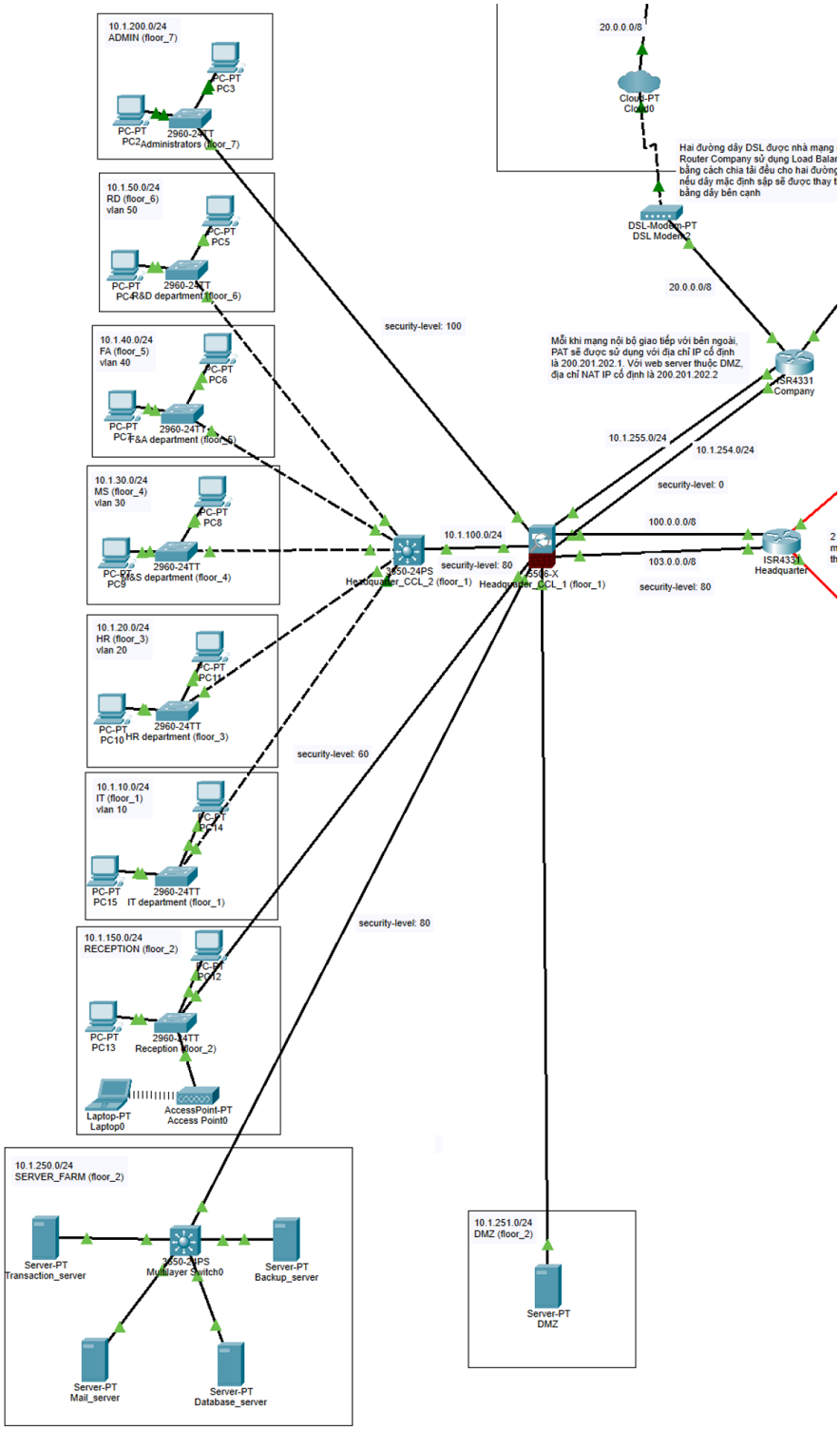
- Các kết nối tới các chi nhánh được nối với tường lửa thông qua một router, từ router sẽ có 2 leased lines kết nối tiếp đến hai chi nhánh ở Hà Nội và Đà Nẵng. Router này sẽ phụ trách công việc luân chuyển dữ liệu từ các chi nhánh ra bên ngoài hoặc đến trụ sở chính và ngược lại.

- Các workstations cùng một phòng ban được liên kết vào cùng một switch layer 2. Khi đó các workstations cùng phòng ban (trong trụ sở chính ở mỗi tầng là mỗi phòng ban khác

nhau) thì được cho vào cùng một VLAN thuận tiện cho việc giao tiếp trong công việc. Bên cạnh đó, mỗi tầng còn có Access Point (AP) phục vụ kết nối không dây để cho phục vụ truy cập Internet của các thiết bị không dây. Các switch tại các phòng ban, trừ Lễ tân và Quản trị, được nối vào một multilayer switch (switch layer 3). Multilayer switch sẽ được nối vào tường lửa. Phòng ban Quản trị, Lễ tân được kết nối trực tiếp vào tường lửa. Thiết kế tách biệt như vậy vì vai trò khác nhau của các thành phần mạng này trong hệ thống mạng.

- Trong Server Farm, các servers được kết nối vào các cổng Giga Ethernets cùng một multilayer switch. Multilayer switch sẽ được nối với tường lửa.
- Kết nối từ Internet chỉ cho phép duy nhất tới Web server ở DMZ bởi tường lửa.

Chi tiết hiện thực trên Cisco Packet Tracer:



Hình 10: Thiết kế mô phỏng hệ thống mạng tại trụ sở chính sử dụng phần mềm Packet Tracer

Đối với mô tả kết nối của thiết kế mô phỏng, ở phần miêu tả sơ đồ đi dây đã nói đầy đủ, bây giờ ta sẽ đi sâu hơn vào cách hoạt động của thiết kế mô phỏng cũng như vai trò của các thiết bị trong thiết kế mô phòng này:

- Để hiện thực tường lửa cho hệ thống, nhóm chúng em sử dụng thiết bị ASA 5506. Vai trò quan trọng nhất của thiết bị này là giúp ngăn chặn các luồng truyền thông tin không được cho phép bởi hệ thống. Thiết bị sử dụng cơ chế phân tầng bảo mật (security-level) cho các kết nối trực tiếp với thiết bị để xác định các luồng truyền thông tin được phép thực thi với nguyên tắc chỉ cho phép truyền thông tin từ bên có bảo mật cao hơn sang bên có bảo mật thấp hơn hoặc tương đương. Ở thiết kế mô phỏng này, kết nối từ các phòng ban trừ Quản trị và Lễ tân đều được đặt security-level = 80. Phòng ban Quản trị được đặt security-level = 100 và là mức độ bảo mật cao nhất. Phòng ban Lễ tân được đặt security-level = 60 là thấp nhất trong mạng nội bộ. Kết nối tới Internet được đặt security-level = 0 giúp ngăn chặn mọi xâm nhập từ bên ngoài vào. Đối với Server Farm và DMZ, cả hai đều được đặt security-level = 80. Để đáp ứng tiếp các yêu cầu của hệ thống về việc giao tiếp giữa các bên, thiết bị còn hỗ trợ ACL bổ trợ cho hệ thống bảo mật phân tầng giúp điều khiển các luồng thông tin linh động hơn. Cuối cùng, thiết bị này còn có thể đóng vai trò như một DHCP server giúp cho việc cấu hình tự động các thiết bị kết nối tới được dễ dàng.

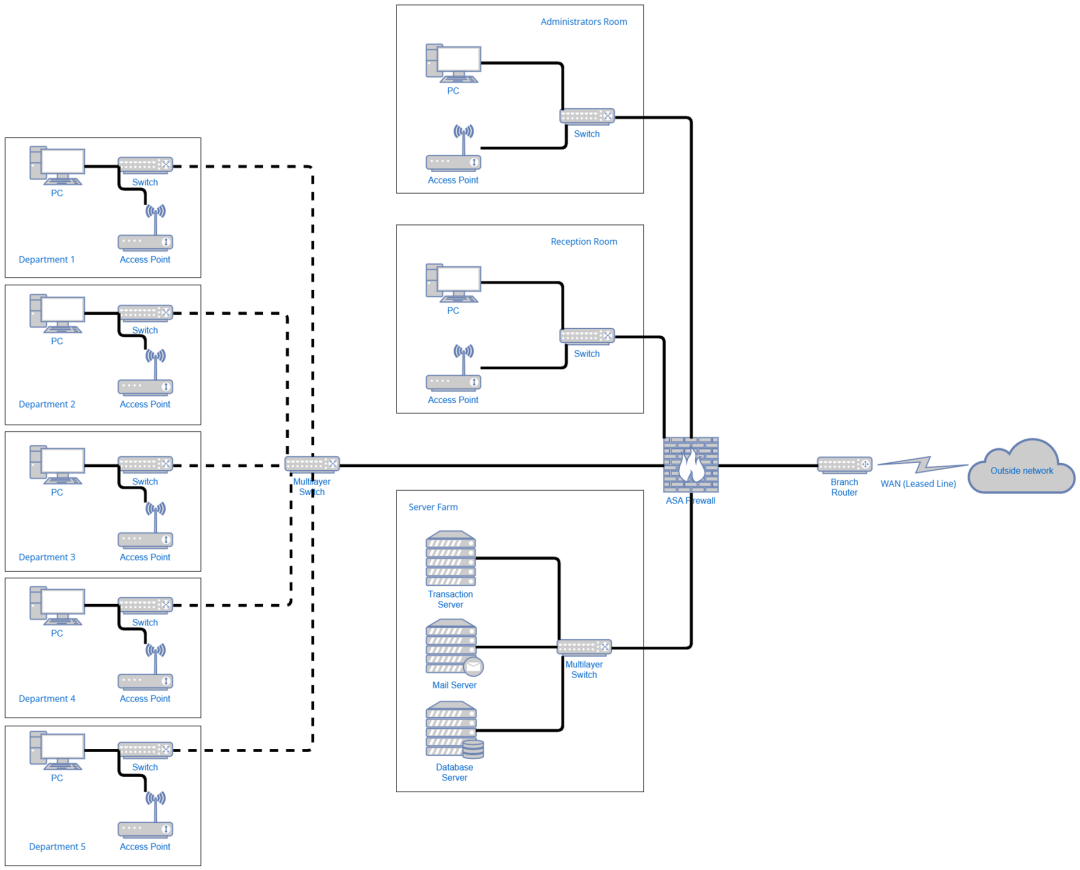
- Các kết nối tới các chi nhánh và Internet được nối với tường lửa thông qua thiết bị router ISR4331. Có thể thấy ở hình trên ở ngay chỗ tiếp giao giữa mạng trụ sở với các chi nhánh và Internet, cân bằng tải được áp dụng khi có hai đường dây phục vụ mang tải. Bên cạnh đó, ở các routers này cũng sẽ thiết lập các ACLs phù hợp với các yêu cầu của hệ thống mạng. Các giao thức định tuyến như định tuyến tĩnh, RIP, OSPF cũng được áp dụng ở các routers này phục vụ tác vụ định tuyến.

- Các workstations cùng một phòng ban được liên kết vào cùng một switch layer 2 WS-C2960-24TT-L. Bên cạnh đó, mỗi tầng còn có Access Point PT (AP-PT) phục vụ kết nối không dây để cho phục vụ truy cập Internet của các thiết bị không dây; có thể thấy để không làm phức tạp thêm thiết kế mô phỏng, phòng ban Lễ tân được cung cấp một Access Point với mục đích thể hiện việc có thể hỗ trợ kết nối không dây cho tất cả các phòng ban.

- Các switch tại các phòng ban, trừ Lễ tân và Quản trị, được nối vào một multilayer switch WS-C3650-24PS. Thiết bị này ngoài nhiệm vụ giúp phân tách các VLAN của mỗi phòng ban còn là hỗ trợ điều khiển luồng thông tin nhờ vào các ACLs và cung cấp DHCP cho các VLAN phòng ban nối vào.

- Trong Server Farm, các servers được kết nối vào các cổng giga ethernets cùng một multilayer switch WS-C3650-24PS.

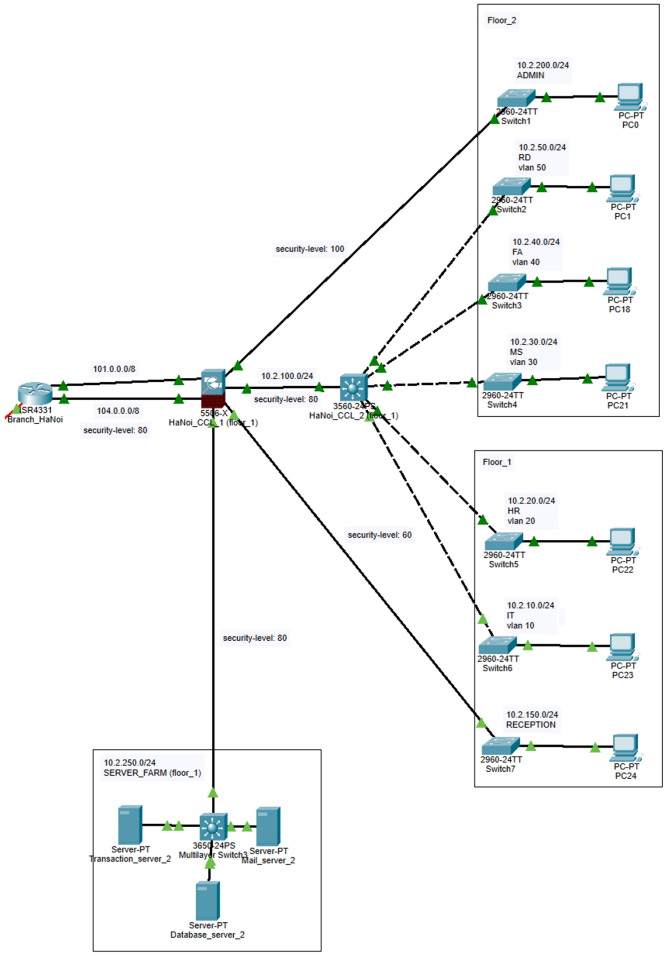
4.3.2 Thiết kế mạng tại các chi nhánh



Hình 11: Sơ đồ đi dây cho các chi nhánh

Sơ đồ đi dây tại các chi nhánh có cấu trúc tương tự giống như tại trụ sở chính. Điểm khác biệt là kết cấu quy mô nhỏ hơn, không có DMZ. Bên cạnh đó, tường lửa không kết nối trực tiếp đến router Company để kết nối tới Internet mà phải thông qua hệ thống mạng ở trụ sở chính.

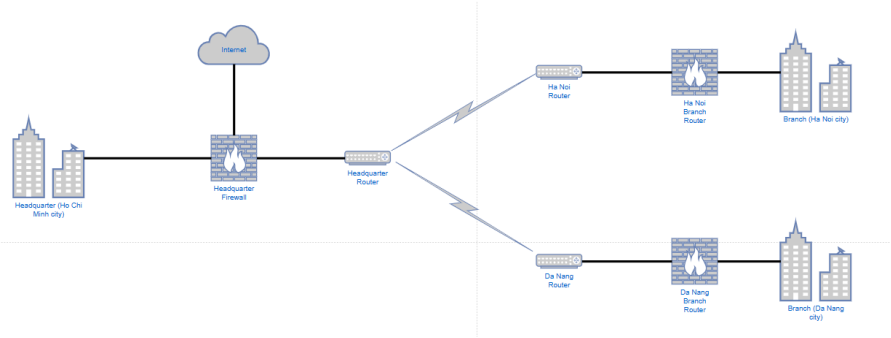
Chi tiết phần hiện thực mạng tại các chi nhánh tại Cisco Packet Tracer:



Hình 12: Thiết kế mô phỏng hệ thống mạng tại các chi nhánh sử dụng phần mềm Packet Tracer

Cũng tương tự như miêu tả thiết kế mô phỏng mạng ở trụ sở chính, thiết kế mô phỏng mạng ở các chi nhánh cũng sử dụng các thiết bị như là ASA 5506 cho tường lửa, router ISR4331 cho kết nối ra bên ngoài, switch layer 2 wS-C2960-24TT-L dành cho mỗi phòng ban,... Tuy vậy quy mô hệ thống mạng ở các chi nhánh sẽ nhỏ hơn so với trụ sở chính. Các ACLs cũng được áp dụng để đáp ứng được các yêu cầu của hệ thống. Ở chỗ tiếp giao giữa hệ thống mạng chi nhánh và bên ngoài, cân bằng tải được áp dụng với hai dây chịu tải kết nối với router.

4.3.3 Thiết kế kết nối giữa các chi nhánh và trụ sở

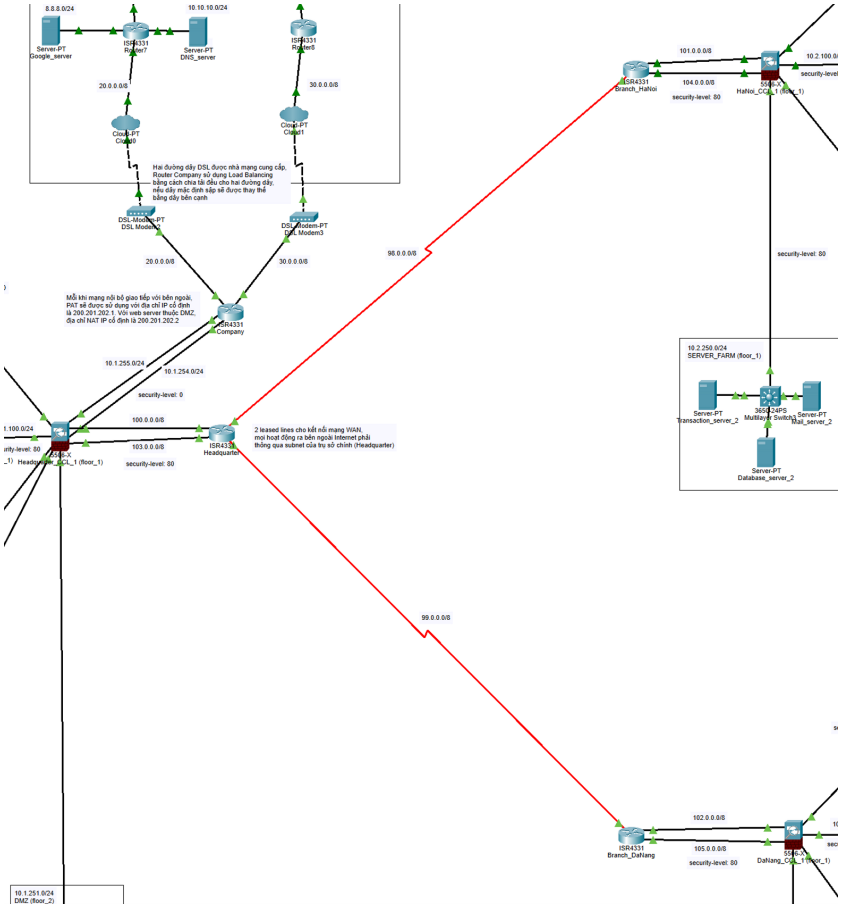


Hình 13: Sơ đồ đi dây cho kết nối giữa trụ sở chính và các chi nhánh

Sau đây là mô tả cho sơ đồ đi dây cho kết nối giữa trụ sở chính và các chi nhánh:

- Tường lửa ở trụ sở chính và các chi nhánh đều được nối với một router cho mỗi nơi để kết nối với mạng bên ngoài.
- Tại router của trụ sở chính cung cấp 2 leased lines cho kết nối mạng WAN kết nối với các router của các chi nhánh.
- Thông qua thiết lập này, mọi hoạt động ra bên ngoài Internet phải thông qua hệ thống mạng của trụ sở chính.

Chi tiết hiện thực phần kết nối giữa trụ sở và hai chi nhánh trong Packet Cisco Tracer:



Hình 14: Hiện thực kết nối giữa trụ sở và các chi nhánh

Ở trong thiết kế mô phỏng này, các hệ thống mạng ở trụ sở chính hay ở các chi nhánh đều được kết nối với bên ngoài bằng router ISR4331.Bên cạnh đó, ở tất cả các điểm tiếp giao đều áp dụng cân bằng tải với hai dây chịu tải cho các vị trí này (giữa trụ sở chính và Internet, giữa trụ sở chính và các chi nhánh).

5 Tính toán throughput, bandwidth và các thông số an toàn cho Mạng máy tính

5.1 Trụ sở chính

Các thông số về lưu lượng và tải của hệ thống tập khoảng 80% vào giờ cao điểm 9h-11h và 15h-16h (3 giờ).

- Lượng upload 1000 MB/ngày và download là 2000 MB/ngày cho mỗi server. Ở trụ sở chính, có tổng cộng 5 server, tổng dung lượng cho download và upload: $5 \times (1000 + 2000) = 15000$ (MB)

- Với mỗi Workstation có dung lượng download khoảng 500 MB/ngày và upload khoảng 100 MB/ngày. Chúng ta có 120 workstations: tổng dung lượng cần đáp ứng cho các workstations: $120 \times (100 + 500) = 72000$ (MB/ngày). Với mạng không dây: Những thiết bị kết nối WiFi từ khách kết nối khoảng 500 MB/ngày.

Tại các giờ cao điểm, đường truyền mạng hoạt động hết công suất, và thông lượng tại các thời điểm này có giá trị cao nhất và đây cũng là giá trị gần với băng thông của mạng nhất, lưu lượng qua mạng tại những thời điểm này chiếm 80% toàn bộ dung lượng qua mạng trong ngày.

- Bandwith: $\frac{(15000 + 72000 + 500) \times 0.8}{3 \times 3600} \approx 6.4815(\text{MB/s}) = 51.8519\ (\text{Mb/s})$.
- Throughput: $\frac{15000 + 72000 + 500}{24 \times 3600} \approx 1.0127\ (\text{MB/s}) = 8.1019\ (\text{Mb/s})$.

5.2 Trụ sở chi nhánh

Các thông số về lưu lượng và tải của hệ thống tập trung khoảng 80% vào giờ cao điểm 9h-11h và 15h-16h (3 giờ).

- Lượng upload là 1000 MB/ngày và download là 2000 MB/ngày cho mỗi Server. Ở trụ sở chi nhánh chúng ta có 3 server, tổng dung lượng upload và download: $3 \times (1000 + 2000) = 9000(MB)$
- Với mỗi Workstation có dung lượng download khoảng 500 MB/ngày và upload khoảng 100 MB/ngày. Chúng ta có 30 Workstations: tổng dung lượng cần đáp ứng cho các Workstations: $30 \times (100 + 500) = 18000$ (MB/ngày). Với mạng không dây: Những thiết bị kết nối WiFi từ khách hàng kết nối khoảng 500 MB/ngày.

Tại các giờ cao điểm, đường truyền mạng hoạt động hết công suất, và thông lượng tại các thời điểm này có giá trị cao nhất và đây cũng là giá trị gần với băng thông của mạng nhất, lưu lượng qua mạng tại những thời điểm này chiếm 80% toàn bộ dung lượng qua mạng trong ngày.

- Bandwith: $\frac{(9000 + 18000 + 5000) \times 0.8}{3 \times 3600} = 2.037\ (\text{MB/s}) = 16.2963\ (\text{Mb/s})$.
- Throughput: $\frac{9000 + 18000 + 500}{24 \times 3600} = 0.3183\ (\text{MB/s}) = 2.5463\ (\text{Mb/s})$.

5.3 Các thông số an toàn

Hệ thống Mạng máy tính của công ty BB được dự đoán cho mức độ phát triển 20% cho nên throughput và bandwidth tối thiểu để hệ thống hoạt động ổn định và có khả năng mở rộng sẽ bằng 120% lượng throughput và bandwidth đã tính ở trụ sở chính và chi nhánh.

5.3.1 Trụ sở chính

$$Bandwith_{safety} = 1.2 \times 51.8519 \approx 62.2229\ (\text{Mb/s})$$
$$Throughput_{safetay} = 1.2 \times 8.1019 \approx 9.7223\ (\text{Mb/s})$$

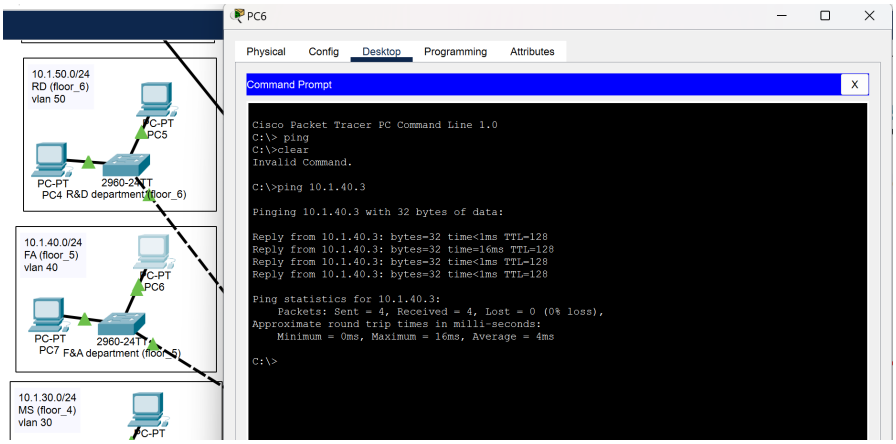
5.3.2 Trụ sở chi nhánh

$$Bandwith_{safety} = 1.2 \times 16.2963 \approx 19.5556\ (\text{Mb/s})$$
$$Throughput_{safetay} = 1.2 \times 2.5463 \approx 3.056\ (\text{Mb/s})$$

6 Mô phỏng hệ thống

Ta mô phỏng hệ thống trong Cisco Packet Tracer:

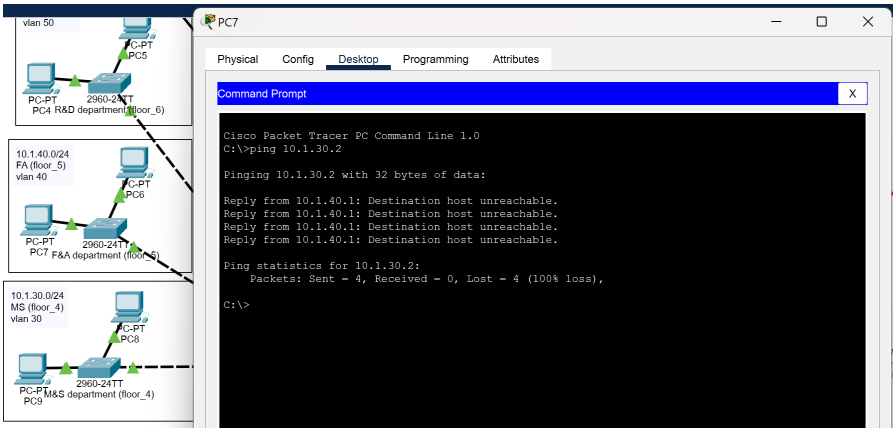
- **Thực hiện ping giữa workstations trong cùng VLAN**: Ta thực hiện ping từ PC6 tới PC7 trong cùng phòng ban Tài chính và Kế toán (tầng 5) của headquarter:



Hình 15: Ping từ PC6 sang PC7 trong cùng VLAN

Từ hình trên ta thấy việc ping thành công với packet loss là 0%.

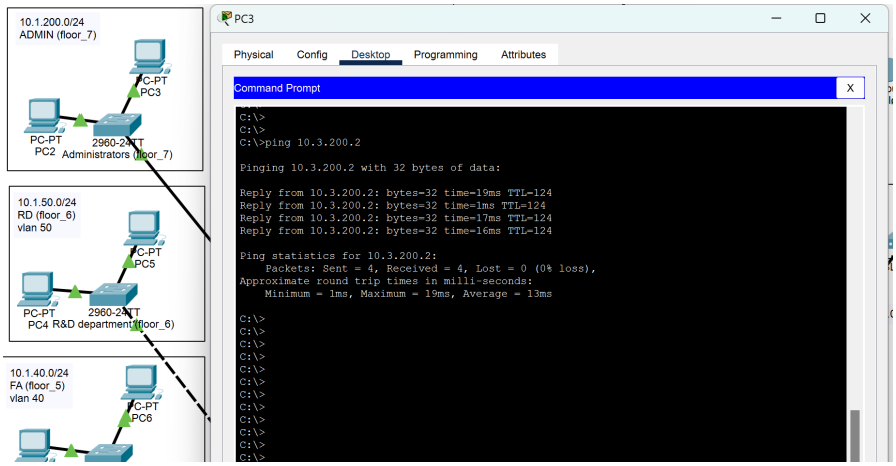
- **Thực hiện ping giữa hai VLAN khác nhau ở cùng trụ sở**: Ta thực hiện Ping từ PC6 tại VLAN 40 (phòng ban FA) sang PC9 tại VLAN 30 (phòng ban HR) tại headquarter:



Hình 16: Ping giữa hai VLAN khác nhau

Từ hình trên, ta thấy hai VLAN khác nhau ở hai phòng ban khác nhau của headquarter không thể ping được tới nhau, packet loss là 100%.

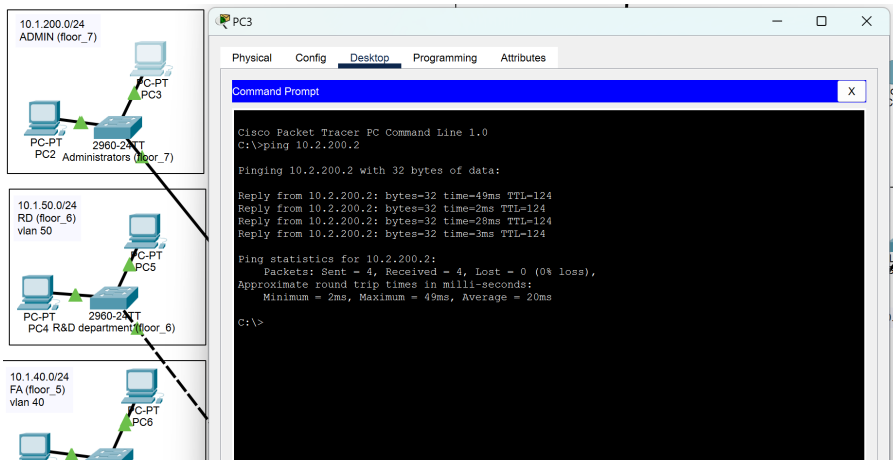
- **Thực hiện ping từ Administrator của Headquarter sang chi nhánh Đà Nẵng**: Ta thực hiện ping từ workstation PC3 của phòng ADMIN tại headquarter sang chi nhánh Đà Nẵng, cụ thể là PC16 của phòng ADMIN chi nhánh Đà Nẵng.



Hình 17: Ping từ ADMIN tại Headquarter sang chi nhánh Đà Nẵng

Từ hình trên, ta thấy ADMIN của headquarter có thể ping được sang chi nhánh Đà Nẵng, packet loss là 0%.

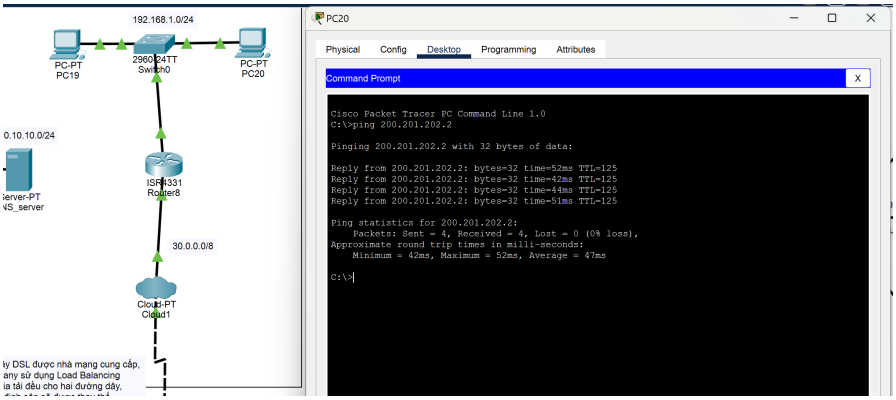
- **Thực hiện ping từ Administrator của Headquarter sang chi nhánh Hà Nội**: Tương tự như việc ping từ Administrator của Headquarter sang chi nhánh Đà Nẵng



Hình 18: Ping từ ADMIN tại Headquarter sang chi nhánh Hà Nội

Từ hình trên, ta thấy ADMIN của headquarter có thể ping được sang chi nhánh Hà Nội, packet loss là 0%.

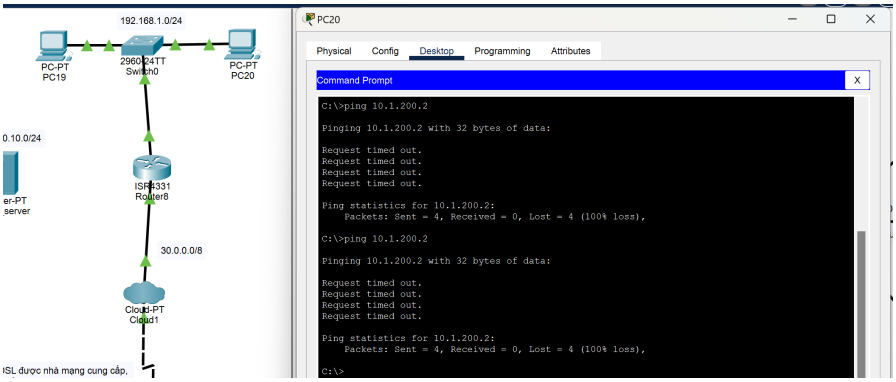
- **Thực hiện ping từ khách hàng internet bên ngoài vào server DMZ dịch vụ của ngân hàng**: Ta thực hiện lệnh ping từ PC20 Internet bên ngoài vào server DMZ của ngân hàng với địa chỉ public là `200.201.202.2`.



Hình 19: Ping khách hàng từ Internet bên ngoài server DMZ

Từ hình trên, ta thấy PC từ Internet bên ngoài có thể kết nối với server DMZ của ngân hàng, packet loss là 0%.

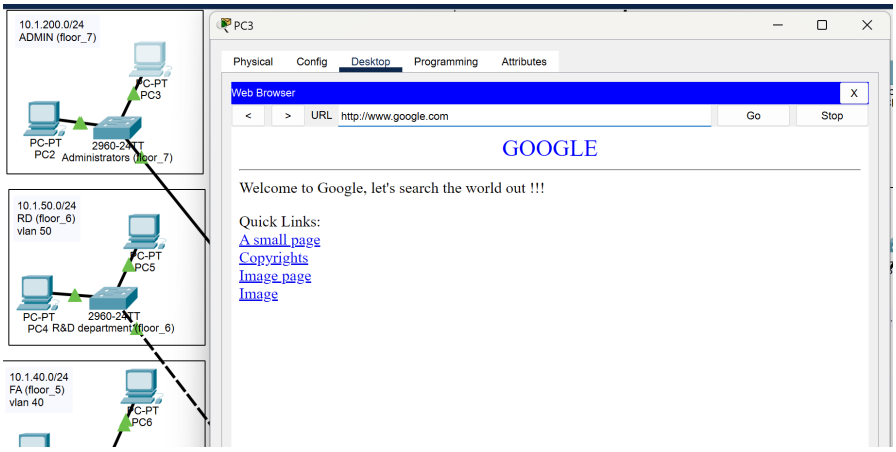
- **Thực hiện ping từ khách hàng Internet bên ngoài vào LAN của công ty**: Ta thực hiện lệnh ping từ PC 20 Internet bên ngoài vào một workstation trong LAN của công ty, cụ thể tại PC2 của công ty.



Hình 20: Ping khách hàng từ Internet bên ngoài vào mạng LAN công ty

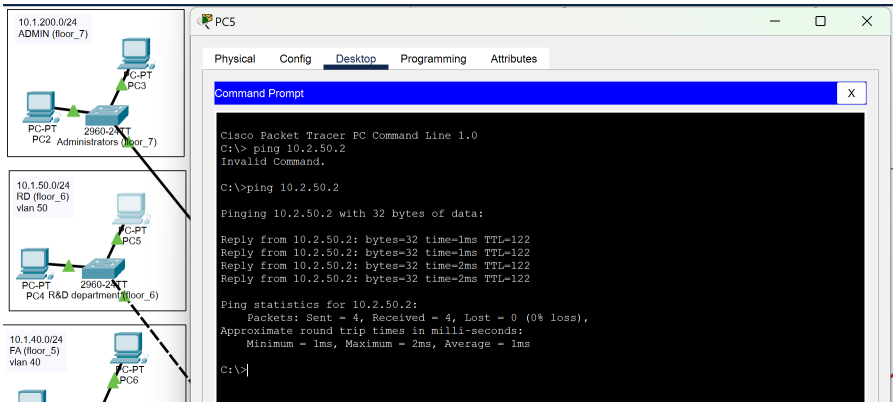
Từ hình trên, ta thấy PC từ Internet bên ngoài không thể kết nối tới mạng LAN của ngân hàng, packet loss là 100%.

- **Thực hiện kết nối từ workstation trong mạng nội bộ ra Google Website**: Ta thực hiện truy cập web browser từ PC3 tại headquarter vào trang web Google nhóm tự thiết kế.



Hình 21: Truy cập trang web Google từ workstation công ty

- **Thực hiện ping giữa các workstation cùng phòng ban giữa chi nhánh và trụ sở**: Ta thực hiện lệnh ping từ PC5 tại phòng ban RD của Headquarter sang PC1 tại phòng ban RD của chi nhánh Hà Nội.



Hình 22: Kết nối giữa workstation cùng phòng ban giữa chi nhánh và trụ sở

Từ hình trên, ta có thể kết nối giữa các workstation cùng phòng ban giữa chi nhánh và trụ sở.

7 Đánh giá hệ thống

7.1 Độ tin cậy

Hệ thống có thể đáp ứng các yêu cầu về lưu lượng dữ liệu mà thống cần đáp ứng. Các thiết bị trong mạng LAN có thể kết nối, giao tiếp với nhau trong mạng cục bộ. Tính bảo mật của hệ thống cũng được đảm bảo khi kết nối ra bên ngoài Internet.

Mỗi chi nhánh và trụ sở khi kết nối ra mạng bên ngoài sử dụng hai đường dây theo cơ chế load-balancing nhằm chia tải khi gặp sự cố hoặc quá tải.

Đường kết nối mạng Internet: Sử dụng hai đường leased-line kết nối chi nhánh với trụ sở, mọi truy cập Internet của hệ thống phải thông qua subnet của trụ sở đảm bảo tính thống nhất. Đường mạng kết nối Internet sử dụng hai đường DSL và ADSL với cơ chế load-balancing nhằm chia tải khi gặp sự cố hoặc quá tải.

Bên cạnh đó, trong Server Farm có backup server cho các server web, mail, database,.. và thường xuyên backup để đảm bảo không bị mất dữ liệu khi gặp sự cố.

7.2 Dễ dàng nâng cấp

Hệ thống mạng thiết kế theo cấu trúc mạng hình sao đảm bảo có thể nâng cấp mở rộng khi cần thiết ví dụ như khi Workstation hoặc server tăng lên. Trong thiết kế hiện tại, nhóm sử dụng **1 switch** cho mỗi phòng ban với **24 port** cho mỗi switch có thể đáp ứng tới **24 hosts**, và tại **switch** của Server Farm có thể hỗ trợ tới **24 servers (vẫn tùy thuộc vào thông lượng)** nên trong trường hợp nhu cầu tăng vẫn có thể đáp ứng.

Nếu trong trường hợp các switch hiện tại không thể đáp ứng được nữa, ta chỉ cần thêm các switch mới và kết nối vào **Switch Layer 3** ở trung tâm (trừ các trường hợp phòng ban Quản trị switch nối thẳng tới ASA). Khi tăng số lượng Server phục vụ cho dịch vụ hệ thống cho bên ngoài mạng nội bộ truy cập, ta chỉ cần thêm việc ánh xạ NAT sang địa chỉ public tĩnh cho server đó. Nhưng nếu chúng ta cần thêm Server với mục đích giảm gánh nặng công việc cho một Server đang có sẵn trong hệ thống do Server hiện tại không còn đáp ứng đủ yêu cầu, thể thực hiện việc thêm này sẽ vất vả hơn so với nhu cầu thêm đặt ra ở trước vì chúng ta cần kết nối các Server có dùng chức năng vào cùng một Switch và sử dụng cần bằng tải để phần chia tải xuống các Server, đảm bảo các Server làm việc đồng đều.

7.3 Phần mềm hỗ trợ

Sử dụng các thiết bị mạng của Cisco - công ty hàng đầu về thiết bị mạng, chúng ta được sử dụng các thiết bị ổn định với kĩ thuật tốt các có tích hợp các phần mềm công nghệ mới nhất, tối ưu nhất, phù hợp với yêu cầu sử dụng và cũng như có nhiều sự lựa chọn khi nâng cấp thiết bị mới.

Tài liệu tham khảo

[1] James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach, 8^{th} Edition

[2] Slide bài giảng môn Mạng máy tính

[3] Cisco, All Products Support, from https://www.cisco.com/c/en/us/support/all-products.html

[4] Configuring DHCP on a Router in Packet Tracer, https://ccnatutorials.in/packet-tracer/configuring-dhcp-on-a-router-in-packet-tracer/