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

Large Assignment 2

MẠNG MÁY TÍNH

Đề tài:

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE COMPANY

GVHD: La Quốc Nhựt Huân
SV thực hiện: Võ Hoàng – 2113422
Dương Phúc Thắng – 2112327
Nguyễn Trần Quang Vũ – 2115325

THÀNH PHỐ HỒ CHÍ MINH, THÁNG 11/2023

Mục lục

1 Danh sách thành viên và phân chia công việc

STT	Họ và tên	MSSV	Công việc	Phần trăm hoàn thành
1	Võ Hoàng	2113422	- Thiết kế hệ thống & viết báo cáo	100%
2	Dương Phúc Thắng	2112327	- Thiết kế hệ thống & trình bày báo cáo	100%
3	Nguyễn Trần Quang Vũ	2115325	- Thiết kế hệ thống & mô phỏng hệ thống	100%

2 Mô tả yêu cầu của hệ thống

CCC (Computer and Construction Concept) đã được yêu cầu thiết kế một mạng máy tính để triển khai tại Trụ sở (tại Thành phố Hồ Chí Minh) và hai Chi nhánh (tại Đà Nẵng và Hà Nội) của Ngân hàng BB đang xây dựng. Các đặc điểm chính của việc sử dụng Công nghệ thông tin trong Công ty này như sau. Trụ sở:

- Toà nhà Trụ sở bao gồm 7 tầng, tầng đầu tiên được trang bị một phòng IT và Trung tâm Cáp Local (sử dụng bảng đấu nối tập hợp dây).
- Quy mô trung bình: 120 máy trạm, 5 máy chủ, 12 thiết bị mạng (hoặc có thể nhiều hơn với các thiết bị đặc biệt về bảo mật).
- Sử dụng công nghệ mới cho cơ sở hạ tầng mạng bao gồm kết nối có dây và không dây, cáp quang (GPON), và GigaEthernet 1GbE/10GbE. Mạng được tổ chức theo cấu trúc VLAN cho các bộ phận khác nhau.
- Mạng phụ Trụ sở kết nối với hai mạng phụ Chi nhánh qua 2 đường thuê để kết nối WAN (có thể áp dụng SD-WAN, MPLS) và 2 xDSL để truy cập Internet với cơ chế cân bằng tải. Tất cả lưu lượng đến Internet đi qua mạng phụ Trụ sở.
- Đối với việc mua phần mềm, công ty sử dụng một kết hợp giữa phần mềm có bản quyền và mã nguồn mở, ứng dụng văn phòng, ứng dụng client-server, đa phương tiện và cơ sở dữ liệu.
- Yêu cầu về bảo mật cao (ví dụ: tường lửa, IPS/IDS, phát hiện lừa đảo), khả năng sẵn có cao (HA), tính ổn định khi gặp sự cố, dễ nâng cấp hệ thống.
- Đề xuất cấu hình VPN cho kết nối site-to-site và cho một nhân viên làm việc từ xa kết nối vào mạng LAN của Công ty.
- Đề xuất hệ thống camera giám sát cho Công ty.

Chi nhánh:

- Toà nhà có 2 tầng, tầng đầu tiên được trang bị 1 phòng IT và 1 Trung tâm Cáp Local.
- Quy mô nhỏ của Chi nhánh BB: 30 máy trạm, 3 máy chủ, 5 hoặc nhiều thiết bị mạng hơn.

Thực hiện kết nối giữa Trụ sở và Chi nhánh thông qua các liên kết WAN, bạn có thể chọn một trong những công nghệ như SD-WAN, MPLS, v.v. sử dụng cho liên kết này tùy thuộc vào chi phí của giải pháp. Liệt kê tất cả các tùy chọn có sẵn.

- Đề xuất các tùy chọn với chi phí.
- Phân tích ưu và nhược điểm của giải pháp được chọn.

Dòng dữ liệu và công việc của hệ thống (khoảng 80% vào giờ cao điểm 9g-11g và 15g-16g) có thể được chia sẻ cho Trụ sở và Chi nhánh như sau:

- Máy chủ cho cập nhật phần mềm, truy cập web và truy cập cơ sở dữ liệu,... Ước lượng tổng cộng tải xuống là khoảng 1000 MB/ngày và tải lên là 2000 MB/ngày.
- Mỗi máy trạm được sử dụng để duyệt web, tải tài liệu và giao dịch với khách hàng,... Ước lượng tổng cộng tải xuống là khoảng 500 MB/ngày và tải lên là 100 MB/ngày.
- Thiết bị kết nối WiFi từ người dùng để tải về khoảng 500 MB/ngày.

Ước tính mạng của Ngân hàng BB có tỷ lệ tăng trưởng 20% trong vòng 5 năm (về số người sử dụng, tải mạng, mở rộng chi nhánh, v.v.).

3 Thiết kế kiến trúc hệ thống

3.1 Khảo sát vị trí cài đặt hệ thống

- Network Load Balancing : Giải pháp cân bằng tải (Load Balancing) là giải pháp phân phối lượng tải trên một thiết bị mạng được truy cập từ nhiều máy tính hoặc một cụm máy tính nhằm tối đa hóa thông lượng và tránh tình trạng quá tải trên thiết bị đó.

- Ta nhận thấy, toàn bộ lượng truy cập ra Internet của 2 chi nhánh đều được chuyển hướng về trụ sở chính tại thành phố Hồ Chí Minh, do đó cơ chế cân bằng tải phải được sử dụng tại đây, đặc biệt là vị trí truyền tải từ mạng nội bộ của tổ chức đến mạng WAN bên ngoài (Internet) để đảm bảo về tốc độ truy cập và tính ổn định.

- Sử dụng cơ chế cân bằng tải (Network Load Balancing) với 2 đường truyền song song sẽ phân tán lượng dữ liệu đồng đều cả 2 đường truyền này. Cả 2 đường truyền hoạt động tốt sẽ cải thiện năng suất tổng thể của hệ thống, hạn chế tắt nghẽn đường truyền cũng như tăng tốc độ phản hồi. Nếu có 1 trong 2 đường truyền xảy ra sự cố, toàn bộ dữ liệu sẽ được đưa đi theo đường truyền còn lại và hệ thống vẫn hoạt động bình thường.

3.2 Thiết kế cấu trúc mạng

- Mạng nội bộ được chia làm 1 trụ sở chính và 2 chi nhánh phụ. Mạng trụ sở chính được xây dựng theo cấu trúc hình sao trong khi 2 chi nhánh được bố trí theo cấu trúc cây.

- Ưu điểm của 2 cấu trúc mạng này là các nút mạng hoạt động độc lập với nhau, nếu một nút mạng bị hư hỏng sẽ không ảnh hưởng đến các nút mạng khác, bên cạnh đó công ty có thể mở rộng hệ thống mạng mà không làm ảnh hưởng quá nhiều đến hệ thống mạng cơ sở. Mạng hình sao cho tốc độ nhanh nhất và dễ sửa chữa.

- Nhược điểm là tốn kém chi phí cho các thiết bị trung gian, khoảng cách từ các máy tính đến trung tâm hạn chế, nếu switch trung tâm bị hỏng, toàn bộ hệ thống mạng sẽ ngưng hoạt động.

- Đối với doanh nghiệp, các máy trong cùng một tòa nhà có khoảng cách không quá xa, các workstation hoạt động trong cùng một tòa nhà nên sử dụng tương đối ít các thiết bị mạng, doanh nghiệp có nhiều phòng ban hoạt động riêng rẽ với nhau, doanh nghiệp cũng muốn giảm thiểu tối đa sự trì trệ hệ thống gây ra bởi sự hư hỏng của một phòng ban cụ thể, do đó áp dụng cấu trúc hình sao và hình cây sẽ đạt được nhiều lợi ích hơn là thiệt hại.

- Chi nhánh kết nối với trụ sở chính bởi đường leased line WAN được thuê bởi bên nhà cung cấp thứ 3 ISP. Chi nhánh sẽ kết nối với router của trụ sở chính trước khi ra Internet để chuyển lượng truy cập về trụ sở.

3.3 Chi tiết hệ thống mạng

Trụ sở chính :

Bao gồm 7 tầng, tầng 1 gồm phòng IT và một phòng tập trung dây mạng, các tầng còn lại từ tầng 2 đến tầng 7, mỗi tầng là một phòng ban riêng của doanh nghiệp. Doanh nghiệp có 120 Workstation được chia cho 7 tầng, từ tầng 2 đến tầng 5 mỗi tầng sẽ có 24 máy và được kết nối bởi 1 switch, bên cạnh đó mỗi tầng còn được trang bị một Accesspoint để phục vụ việc thực hiện công việc trên các thiết bị di động như laptop hoặc máy tính bảng. Hai tầng còn lại là tầng 6 và 7, bởi vì ở khá cao nên sẽ có ít người di chuyển lên 2 tầng này, nên mỗi tầng sẽ được bố trí

ít máy hơn các tầng khác cụ thể là 12 máy, ở mỗi tầng này cũng sẽ được trang bị Accesspoint cho kết nối mạng không dây. Để tối ưu số lượng thiết bị mạng, 2 tầng trên cùng này sẽ sử dụng chung một switch. Tầng 1 sẽ là tầng quản lý của cả trụ sở, phòng IT của tầng 1 sẽ được chia ra làm 2 bộ phận nhỏ bao gồm server và admin.
Bộ phận server bao gồm các máy chủ :

- **Web Server** : là trang web của công ty bao gồm các thông tin như giới thiệu chung về công ty, thông tin liên lạc của công ty, các thông tin quảng cáo, tra cứu sản phẩm, phương thức thanh toán sản phẩm,... . Là ứng dụng cho phép khách hàng từ bên ngoài có thể truy cập.
- **DNS Server (Domain Name System)** : được dùng để phân giải tên miền thành các địa chỉ ip. Đối với khách hàng, việc ghi nhớ tên miền sẽ đơn giản hơn nhiều so với việc ghi nhớ một dãy địa chỉ kỹ thuật.
- **DHCP Server (Dynamic Host Configuration Protocol)**: Vì số lượng workstation trong trụ sở khá lớn nên việc cấp phát địa chỉ tĩnh sẽ tốn thời gian và công sức, do đó chúng ta sử dụng DHCP server để cấp phát địa chỉ động cho mỗi workstation ở các tầng.
- **Mail Server** : là server chịu trách nhiệm về việc chuyển giao thư điện tử được dùng để giao tiếp giữa các tầng, được xây dựng chuyên hóa để trao đổi thông tin giữa giám đốc trụ sở và các quản lý ở các tầng còn lại.
- **IOT Server / Database** : là trung tâm kiểm tra và giám sát kết nối của các thiết bị camera được phân bố trong trụ sở. IOT Server sẽ được quản lý bởi giám đốc và các nhân viên an ninh để đảm bảo tính an toàn của doanh nghiệp. Bên cạnh đó server còn là cơ sở dữ liệu lưu trữ thông tin của khách hàng, do đó server sẽ được bảo mật khỏi các tác nhân bên ngoài.

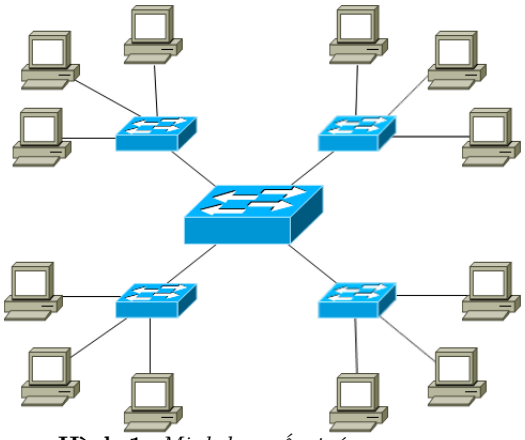
Bộ phận admin bao gồm :

- Một máy tính của giám đốc trụ sở, được toàn quyền truy cập hệ thống, giám sát và đảm bảo tiến độ làm việc của các bộ phận khác ở các tầng thông qua các camera.
- Một máy tính của nhân viên an ninh, được phân quyền giám sát dòng người ra vào trong trụ sở thông qua camera.
- Một máy tính xách tay được kết nối với accesspoint của đội quản trị mạng, có nhiệm vụ kiểm soát hệ thống server cũng như xử lý các trụ trặc về sự cố mạng.

Bên cạnh đó, hệ thống camera sẽ được bố trí khắp tòa nhà, mỗi tầng sẽ có một camera quan sát và phản hồi thông tin liên tục về IOT Server, các camera sẽ hoạt động 24/7 để đảm bảo an ninh trật tự của doanh nghiệp, đặc biệt tín hiệu truyền tải phải ổn định nên ta sẽ lựa chọn kết nối có dây cho các camera và camera ở mỗi tầng sẽ tham gia vào mạng nội bộ của tầng đó thông qua switch.

Với yêu cầu thiết kế mỗi tầng là một Vlan (Virtual Local Area Network) riêng biệt và cấu trúc hình sao đặc trưng, ta cần một switch trung tâm để các tầng có thể giao tiếp với nhau và hỗ trợ điều phối dữ liệu cho các switch ở biên của mạng. Với Switch layer 2 thì việc chuyển đổi giữa các vlan là không thể thực hiện được, nên ta sẽ chọn switch layer 3 vì nó thỏa mãn yêu cầu đề ra.

Cuối cùng, một tường lửa sẽ được sử dụng để tăng cường tính bảo mật của hệ thống mạng nội bộ, tránh sự tấn công của các tin tặc từ bên ngoài, tường lửa sẽ chia mạng thành 3 thành phần bao gồm các workstation trong trụ sở với độ bảo mật cao nhất, vùng DMZ (Demilitarized



Hình 1: *Minh họa cấu trúc mạng sao*

Zone) chứa các server với độ bảo mật cao thứ hai và cuối cùng là vùng mạng bên ngoài WAN không có độ bảo mật. Ngoài ra còn có một router được dùng để truy cập Internet và nhận lượng truy cập từ 2 chi nhánh ở Hà Nội và Đà Nẵng.

Các chi nhánh phụ

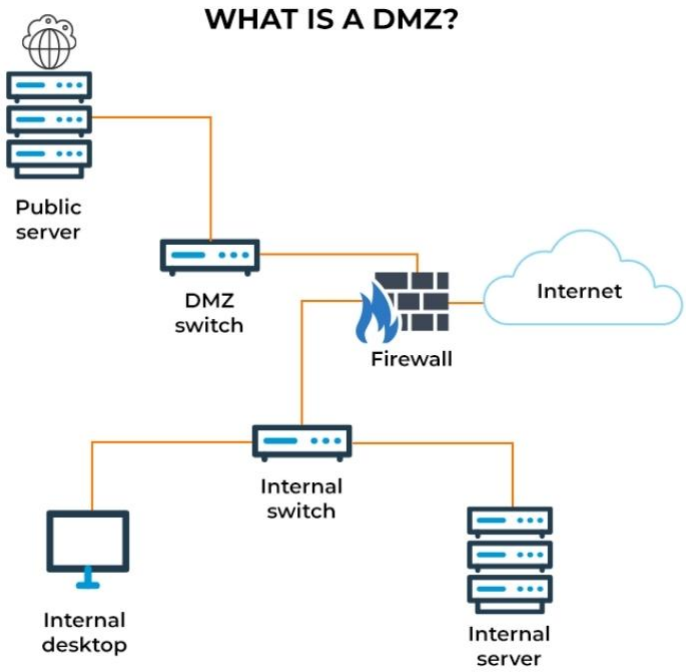
Các chi nhánh phụ với cấu trúc mạng hình cây cũng là một biến thể của cấu trúc mạng hình sao và là một mô hình nhỏ hơn của trụ sở chính. Cả 2 chi nhánh đều được xây dựng giống nhau với 2 tầng, 30 workstation và 3 server. Tương tự như với trụ sở tại Thành phố Hồ Chí Minh, tầng 1 có phòng IT và trung tâm nối cáp, phòng IT cũng sẽ chia được làm 2 bộ phận là server và admin.
Bộ phận server bao gồm :

- **Web Server** : chứa các thông tin về công ty và sản phẩm được bán tại chi nhánh
- **DNS Server** : phân giải tên miền thành địa chỉ IP
- **Mail Server / Database** : trao đổi thư điện tử giữa giám đốc chi nhánh và quản lý tầng 2, server còn là database lưu trữ thông tin quan trọng của khách hàng.

Bộ phận admin gồm : Một máy tính được phân quyền của giám đốc chi nhánh và một máy tính dành cho nhân viên quản trị mạng.

Hệ thống mạng của 2 chi nhánh tương đối nhỏ, và theo yêu cầu của đề thì hai chi nhánh không cần thiết lập hệ thống camera, nên ở đây ta sẽ không sử dụng camera. Với kiến trúc tòa nhà nhỏ chỉ với 2 tầng, ta không cần thiết lập mạng không dây (Wireless) cho từng tầng mà có thể sử dụng chung một mạng không dây cho cả tòa nhà, do đó ta sẽ chọn wireless router làm điểm kết nối wifi. Một Switch layer 2 không thể điều khiển giao tiếp giữa hai tầng nên ta sẽ thay thế bằng một Multilayer Switch để đáp ứng yêu cầu đề ra.

Một tường lửa được dựng lên để bảo vệ hệ thống mạng nội bộ của chi nhánh, tường lửa cũng chia mạng ra làm 3 vùng : **INSIDE** dành cho các máy tính bên trong chi nhánh với độ bảo mật cao nhất, **DMZ** dành cho các server với độ bảo mật thấp hơn và **OUTSIDE** là vùng mạng bên ngoài không có độ bảo mật. Khi mạng của chi nhánh bị tấn công, các server trong



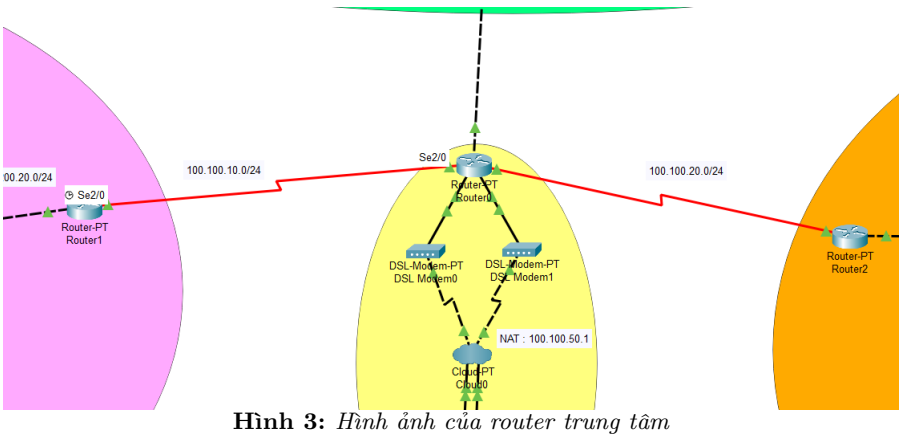
Hình 2: *Mô phỏng phân vùng tường lửa*

vùng DMZ sẽ bị tấn công đầu tiên, lúc này tường lửa sẽ cách ly mạng nội bộ ra khỏi các server và đảm bảo rằng không có cuộc xâm nhập nào của tin tặc có thể truy cập được vào mạng nội bộ.

Bên ngoài tường lửa, chi nhánh sẽ được kết nối đến router của trụ sở chính để chuyển lượng truy cập về trụ sở thay vì được quyền trực tiếp truy cập Internet. Đường truyền kết nối riêng này được cung cấp bởi nhà cung cấp dịch vụ, đường leased line WAN Ethernet có thể đạt tới tốc độ tối đa 10 Gbps hỗ trợ doanh nghiệp có thể liên lạc đường xa và truy cập Internet với tốc độ nhanh, ổn định. Router tại trụ sở ngoài việc giúp tổ chức truy cập Internet còn đảm nhiệm trọng trách truyền gói tin giữa các chi nhánh với nhau. Tại đây có 2 cơ chế được áp dụng :

- **Cơ chế NAT (Network Address Translation) :** được hiểu là cơ chế chuyển đổi từ địa chỉ IP của mạng cục bộ sang địa chỉ public được cung cấp bởi các nhà cung cấp dịch vụ Internet. Cơ chế này là cần thiết vì ta không thể dùng địa chỉ IP của mạng cục bộ để truy cập Internet mà phải thông qua địa chỉ của nhà cung cấp thứ 3. Ngày nay, thiết bị truy cập Internet ngày càng nhiều kéo theo sự thiếu hụt địa chỉ IP, cơ chế NAT giúp giảm thiểu số lượng địa chỉ IPv4 cần có bằng cách cho phép nhiều máy tính sử dụng chung một địa chỉ IP public. Với doanh nghiệp, cơ chế này còn tăng tính bảo mật vì nó che giấu địa chỉ IP của máy tính nội bộ.

- **Cơ chế Network Load-Balancing :** cơ chế được sử dụng nguyên nhân do đây là trọng điểm trung chuyển các gói tin của cả 3 chi nhánh và kết nối 3 chi nhánh với mạng Internet. Thực hiện cơ chế Load-Balancing yêu cầu 2 modem DSL được nối song song và trực tiếp với router trung tâm. Lượng gói tin sẽ được phân phối đồng đều trên 2 modem này để tránh trường hợp dồn toàn bộ áp lực lên một đường truyền duy nhất còn đường truyền khác thì không có hoặc tải thấp làm lãng phí tài nguyên và giảm hiệu suất của hệ thống.



Hình 3: *Hình ảnh của router trung tâm*

4 Danh sách thiết bị và sơ đồ IP

4.1 Sơ đồ địa chỉ IP

Bảng phân chia địa chỉ VLAN và IP Private tại các địa chỉ

4.1.1 Trụ sở chính (Bảng 1)

VLAN	Phòng ban	Địa chỉ mạng	IP Private	Tầng	workstations
20	Lễ Tân	192.168.20.0/24	192.168.20.1 - 192.168.20.254	2	24
30	Marketing	192.168.30.0/24	192.168.30.1 - 192.168.30.254	3	24
40	Quản lý Nhân Sự	192.168.40.0/24	192.168.40.1 - 192.168.40.254	4	24
50	Tài Chính	192.168.50.0/24	192.168.50.1 - 192.168.50.254	5	24
60	Kỹ thuật	192.168.60.0/24	192.168.60.1 - 192.168.60.254	6	12
70	Nghiên cứu thị trường	192.168.70.0/24	192.168.70.1 - 192.168.70.254	7	12
150	ADMIN	192.168.150.0/24	192.168.150.1 - 192.168.150.254	1	3
100	SERVER	192.68.100.0/24	192.168.100.1 - 192.168.100.254	1	5

4.1.2 Chi nhánh Đà Nẵng (Bảng 2)

VLAN	Phòng ban	Địa chỉ mạng	IP Private	Tầng	workstations
21	Lễ Tân Marketing Tài chính Quản lý nhân sự	192.168.21.0/24	192.168.21.1 - 192.168.21.254	2	30
151	ADMIN	192.168.151.0/24	192.168.151.1 - 192.168.151.254	1	2
101	SERVER	192.68.101.0/24	192.168.101.1 - 192.168.101.254	1	3

4.1.3 Chi nhánh Hà Nội (Bảng 3)

VLAN	Phòng ban	Địa chỉ mạng	IP Private	Tầng	workstations
22	Lễ Tân Marketing Tài chính Quản lý nhân sự	192.168.22.0/24	192.168.22.1 - 192.168.22.254	2	30
152	ADMIN	192.168.152.0/24	192.168.152.1 - 192.168.152.254	1	2
102	SERVER	192.68.102.0/24	192.168.102.1 - 192.168.102.254	1	3

4.2 Danh sách thiết bị mạng

4.2.1 Switch layer 2

Ta chọn Cisco Switch WS-C2960-24TC-L

Hình 4: *Cisco Switch WS-C2960-24TC-L*

Thông số kỹ thuật :

Uplink Interface	2 (SFP or 1000BASET)
Ports (Fast Ethernet)	24 x 10/100 Ethernet Ports
Băng thông chuyển tiếp	16 Gbps
Hiệu suất chuyển tiếp	6.5 Gbps
RAM	128 MB
Bộ nhớ Flash	64 MB
Kích thước	4.4cm x 45.0cm x 24.2cm
Trọng lượng	7.73kg
Giá tiền	15.213.000 VND

- WS-C2960-24TC-L cung cấp việc chuyển mạch Ethernet cấp doanh nghiệp hiệu quả, chi phí thấp như các văn phòng chi nhánh, các trang web ở xa và các vị trí bán lẻ, khu vực làm việc thông thường trên máy tính để bàn.
- Thiết bị này cung cấp một loạt các tính năng bảo mật để hạn chế truy cập vào mạng và giảm thiểu các mối đe dọa, bao gồm : kiểm tra ARP động và trình bảo vệ nguồn IP. Cung cấp quản lý lưu lượng thông minh giúp giữ mọi thứ đều trôi chảy, các cơ chế linh hoạt để đánh dấu, phân loại và lập kế hoạch cung cấp hiệu suất cao cho dữ liệu.

4.2.2 Switch layer 3

Ta chọn Cisco Switch WS-C3560-24PS-S

Hình 5: *Ciso Switch WS-C3560-24PS-S*

Thông số kỹ thuật :

Uplink Interface	2 x 10/100/1000 Mbps (GigabitEthernet)
Ports (Fast Ethernet)	24 x 10/100 Mbps (FastEthernet)
Băng thông chuyển tiếp	32 Gbps
Hiệu suất chuyển tiếp	16 Gbps
RAM	128 MB
Bộ nhớ Flash	32 MB
Kích thước	4.4cm x 44.3cm x 29.5cm
Trọng lượng	4.6kg
Giá tiền	32.378.000 VND

- Bộ chuyển mạch Cisco Catalyst 3560V2 WS-C3560V2-24PS-S là thiết bị chuyển mạch Ethernet cấp 3 hiệu quả năng lượng cao cấp. Thiết bị chuyển mạch 3560V2 này hỗ trợ công nghệ Cisco EnergyWise, cho phép các công ty đo lường và quản lý mức tiêu thụ năng lượng của cơ sở hạ tầng mạng và thiết bị kết nối mạng, do đó giảm chi phí năng lượng và lượng khí thải carbon.
- Thiết bị này là một bộ chuyển đổi truy cập lý tưởng cho các môi trường doanh nghiệp, bán lẻ và văn phòng chi nhánh vì nó tối đa hóa năng suất và bảo vệ đầu tư bằng cách cho phép mạng thống nhất dữ liệu, thoại và video.
- Thiết bị hỗ trợ giao diện đồ họa web,giúp dễ dàng cài đặt và cấu hình.

4.2.3 Access Point

Ta chọn access point Linksys WAP54G

- Chuẩn Wifi : Hỗ trợ chuẩn Wifi 802.11g, có tốc độ truyền dữ liệu tối đa lên đến 54Mbps.
- Dải tần số : 2.4 GHz

Hình 6: *Cisco Linksys WAP54G*

- Bảo mật : mã hóa 128-bit WPA, WPA2, WEP, lọc địa chỉ MAC, miễn phí dùng thử các dịch vụ an ninh mạng cao cấp Linksys Wireless Guard WPA-RADIUS
- Vlan : Hỗ trợ chức năng vlan
- Quản lý : Hỗ trợ các giao thức quản lý mạng như SNMP (Simple Network Management Protocol).
- Giá bán : 1.345.000 VND

4.2.4 Router

Ta chọn Router Cisco ISR 4431 / K9

Hình 7: *Cisco ISR 4431 / K9*

Thông số kỹ thuật :

Uplink Interface	2 x 10/100/1000 Mbps (GigabitEthernet)
Ports (Fast Ethernet)	24 x 10/100 Mbps (FastEthernet)
Băng thông chuyển tiếp	500Mbps đến 1Gbps
Cổng WAN/LAN	4
Cổng RJ-45	4
Cổng SFP	4
Bộ nhớ Flash	8GB (mặc định) / 32GB (tối đa)
Kích thước	4.39cm x 43.8cm x 50,7cm
Trọng lượng	20.88kg
Giá tiền	123.881.520 VND

- Thiết bị hỗ trợ nhiều giao diện WAN và có khả năng mở rộng linh hoạt
- ISR 4431/K9 tích hợp nhiều tính năng trong một thiết bị, bao gồm routing, bảo mật, quản lý, VPN, và các dịch vụ khác.
- Nó hỗ trợ nhiều tính năng bảo mật như firewall, VPN, IPS (Intrusion Prevention System), và các tính năng khác để bảo vệ mạng doanh nghiệp.

4.2.5 Tường lửa

Ta chọn Cisco ASA5506H-SP-BUN-K9

Hình 8: *Cisco ASA5506H-SP-BUN-K9*

- Hỗ trợ VPN Site-to-site và remote access VPN, cung cấp khả năng truy cập hiệu suất cao, bảo mật cao và tính sẵn sàng cao để giúp đảm bảo tính liên tục của doanh nghiệp

- Khả năng hiển thị và kiểm soát ứng dụng chi tiết (AVC) hỗ trợ hơn 4.000 lớp ứng dụng và các hoạt động dựa trên các chính sách phát hiện mối đe dọa xâm nhập (IPS) phù hợp để tối ưu hóa hiệu quả bảo mật.
- Lọc URL và danh mục, cung cấp cảnh báo toàn diện và kiểm soát lưu lượng truy cập web và thực thi chính sách trên hàng trăm triệu URL trong hơn 80 danh mục.
- Giá bán : 35.179.000 VND

4.3 Thống kế thiết bị và tổng chi phí

4.3.1 Thống kê thiết bị

Trụ sở chính

STT	Thiết bị	Số lượng
1	Switch layer 2	7
2	Switch layer 3	2
3	Access Point	7
4	Router	1
5	Firewall	1

Chi nhánh Đà Nẵng

STT	Thiết bị	Số lượng
1	Switch layer 2	3
2	Switch layer 3	2
3	Access Point	0
4	Router	1
5	Firewall	1

Chi nhánh Hà Nội

STT	Thiết bị	Số lượng
1	Switch layer 2	3
2	Switch layer 3	2
3	Access Point	0
4	Router	1
5	Firewall	1

4.3.2 Tổng chi phí

STT	Thiết bị	Số lượng	Giá tiền	Thành tiền
1	Switch layer 2	13	15.213.000	197.769.000
2	Switch layer 3	6	32.378.000	194.268.000
3	Access Point	7	1.345.000	9.415.000
4	Router	3	123.881.520	371.644.560
5	Firewall	3	35.179.000	105.537.000
Tổng				878.633.560

5 Tính toán throughput, bandwidth của hệ thống

5.1 Trụ sở chính

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).

- Với mỗi server, lượng upload và download mỗi ngày lần lượt là 2000MB/ngày và 1000MB/ngày, tổng cộng là 3000MB/ngày cho mỗi server. Trụ sở chính có 5 server nên tổng lượng upload và download sẽ là: 5 * 3000 = 15000 (MB/ngày).
- Với mỗi workstation, lượng upload và download mỗi ngày lần lượt là 100MB/ngày và 500MB/ngày, tổng cộng là 600MB/ngày cho mỗi server. Trụ sở chính có 120 workstations nên tổng lượng upload và download sẽ là: 120 * 600 = 72000 (MB/ngày).
- Với wifi, mỗi thiết bị kết nối khoảng 500MB/ngày. Tại trụ sở chính, giả sử mỗi ngày có khoảng 200 lượt truy cập vào wifi thì tổng dung lượng cho wifi là: 200 * 500 = 100000 (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. 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. Do đó:

- Bandwidth:

$$\frac{(15000 + 72000 + 100000) * 0.8}{3 * 3600} = 13.851(MB/s) = 110.814(Mb/s) \quad (1)$$

- Throughput:

$$\frac{(15000 + 72000 + 100000)}{24 * 3600} = 2.164(MB/s) = 17.315(Mb/s) \quad (2)$$

5.2 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).

- Với mỗi server, lượng upload và download mỗi ngày lần lượt là 2000MB/ngày và 1000MB/ngày, tổng cộng là 3000MB/ngày cho mỗi server. Chi nhánh có 3 server nên tổng lượng upload và download sẽ là: 3 * 3000 = 9000 (MB/ngày).
- Với mỗi workstation, lượng upload và download mỗi ngày lần lượt là 100MB/ngày và 500MB/ngày, tổng cộng là 600MB/ngày cho mỗi server. Chi nhánh có 30 workstations nên tổng lượng upload và download sẽ là: 30 * 600 = 18000 (MB/ngày).
- Với wifi, mỗi thiết bị kết nối khoảng 500MB/ngày. Tại chi nhánh, giả sử mỗi ngày có khoảng 100 lượt truy cập vào wifi thì tổng dung lượng cho wifi là: 100 * 500 = 50000 (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. 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. Do đó:

- Bandwidth:

$$\frac{(9000 + 18000 + 50000) * 0.8}{3 * 3600} = 5.704(MB/s) = 45.630(Mb/s) \tag{3}$$

- Throughput:

$$\frac{(9000 + 18000 + 50000)}{24 * 3600} = 0.891(MB/s) = 7.130(Mb/s) \tag{4}$$

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. Do đó:

- Tại trụ sở chính:
  - $Bandwidth_{safety} = 110.814 * 1.2 = 132.978(Mb/s)$
  - $Throughput_{safety} = 17.315 * 1.2 = 20.778(Mb/s)$
- Tại chi nhánh:
  - $Bandwidth_{safety} = 45.630 * 1.2 = 54.756(Mb/s)$
  - $Throughput_{safety} = 7.130 * 1.2 = 8.556(Mb/s)$

6 Đánh giá hệ thống

6.1 Độ tin cậy

Hệ thống có thể đáp ứng các yêu cầu về lưu lượng dữ liệu mà hệ thống cần đáp ứng. Các thiết bị trong mạng LAN có thể kết nối, giao tiếp với nhau trong mạng cục bộ.

6.2 Nâng cấp hệ thống

Với sự tăng trưởng 20% trong vòng 5 năm, đòi hỏi hệ thống phải có sự nâng cấp và bảo trì hợp lí để đáp ứng được sự tăng trưởng này. Có nhiều cách để nâng cấp và bảo trì hệ thống như tăng thêm số lượng thiết bị mạng, đổi mới các thiết bị theo thời gian, sử dụng các thiết bị hiện đại cho hiệu suất cao hơn, ... nhằm tăng bandwith, throughput, tăng các chỉ số an toàn để người dùng hoặc các nhân viên trong tổ chức có thể sử dụng hiệu quả. Ngoài việc tăng cường phần cứng, chúng ta cũng có thể sử dụng các phần mềm, các công nghệ mới để duy trì và phát triển hệ thống mạng.

6.3 An toàn và bảo mật

- Yêu cầu mà hệ thông cần đáp ứng: đối với hệ thống ngân hàng, hệ thống hoạt động với nhu cầu xử lý thông tin dữ liệu nghiệp vụ quan trọng. Nhưng yêu cầu bảo mật mà hệ thống cần đáp ứng: Không cho phép đối tượng bên ngoài truy cập và nhưng hoạt động nghiệp vụ cũng như dữ liệu trong hệ thống, kiểm soát truy cập của người sử dụng, đảm bảo dữ liệu vào và ra an toàn.

- Các tài nguyên cần bảo vệ trong hệ thống: Phân hệ Server là một phần quan trọng của hệ thống và cần được bảo vệ an toàn vì nó chứa những dữ liệu quan trọng của khách hàng cũng như các thông tin giao dịch cần được bảo mật. Khi phân hệ này bị tấn công với mục đích xấu nó có thể ảnh hưởng nghiêm trọng đến khách hàng của ngân hàng và các hoạt động của ngân hàng.

- Những mối đe dọa mà hệ thống có thể gặp phải: Hacker sử dụng các công cụ, phần mềm mã độc tấn hệ thống lấy cắp thông tin khách hàng, kiểm soát các máy tính trong ngân hàng. Ngoài những nguy cơ tìm ẩn ở bên ngoài, những người sử dụng các thiết bị trong mạng LAN cũng là một mối đe dọa lớn khi họ có ý định tấn công hệ thống, đây là một nguy cơ có thể gây ra thiệt hại rất lớn cho ngân hàng bởi nó rất khó để kiểm soát.

- Các biện pháp khắc phục: Sử dụng tường lửa kiểm soát các gói tin được phép vào và ra khỏi hệ thống, mạng LAN các workstations và mạng Server được kết nối tường lửa theo hai đường khác nhau, nó góp phần kiểm soát các yêu cầu mà nhân viên trong hệ thống gửi đến cho Server. Sử dụng tường lửa phần nào ngăn chặn nhưng mỗi nguy cơ bên ngoài và bên trong của hệ thống. Ngoài ra, hệ điều hành và những ứng dụng mà hệ thống sử dụng cũng cần được sao lưu, bảo trì cập nhật thường xuyên để phát hiện ra các lỗi, lỗ hổng cũng như nâng cấp phần mềm công nghệ trong hệ thống, tiếp cận với những công nghệ mới an toàn hơn tối ưu hơn. Bảo trì hệ thống thường xuyên cùng mà một giải pháp tốt cho vấn đề này và đây cũng là một yêu cầu bắt buộc đối với một hệ thống ngân hàng, bảo trì hệ thống thường xuyên giúp kịp thời phát hiện các lỗ hổng về bảo mật, cập nhật, thay mới các phần mềm cũng như phần cứng, an toàn hơn, hiện đại hơn, tối ưu hơn,...

- Các yêu cầu khi gặp sự cố: Cần ngắt toàn bộ kết nối Internet của hệ thống để chặn các kết nối trái phép ở bên ngoài, sử dụng backup Server để sao lưu dữ liệu trong các Server, việc

sao lưu cần được tiến hành thường xuyên, có phòng ban riêng quản lý, giám sát hệ thống mạng xử lý sự cố kịp thời. Ngoài ra cần xây dựng các biện pháp dự phòng, sẵn sàng đối mặt với rủi ro nếu chúng xảy ra.

6.4 Những hạn chế còn tồn tại của dự án

- Các vấn đề bảo mật, an toàn của hệ thống có thể chưa được đảm bảo hoàn toàn.
- Lựa chọn các thiết bị, công nghệ sao cho phù hợp với sự phát triển của dự án.
- Vấn đề bảo trì và phát triển hệ thống trong tương lai cần được thực hiện dễ dàng hơn.

6.5 Định hướng tương lai

Trong tương lai, khi mà công nghệ ngày càng phát triển, quy mô của ngân hàng cũng sẽ được mở rộng, yêu cầu về thiết bị và hệ thống ngày càng cao, thì việc nâng cấp và bảo trì toàn bộ hệ thống trở nên vô cùng quan trọng và phải thực hiện thường xuyên, định kì. Mặt khác, công nghệ càng phát triển thì các mối nguy cơ về an ninh mạng trở nên ngày càng cao, vì vậy chú trọng thực hiện các biện pháp an toàn thông tin cũng là một nhiệm vụ tất yếu trong tương lai.

7 Mô phỏng hệ thống

Sử dụng phần mềm mô phỏng Cisco Packet Tracer
Mô phỏng các yêu cầu sau :

1. Kết nối các PC trong cùng VLAN
2. Kết nối các PC khác VLAN với nhau
3. Kết nối các PC giữa trụ sở chính và các chi nhánh
4. Kết nối đến các máy chủ trong vùng DMZ
5. Ngăn chặn các kết nối từ khách hàng đến các PC nội bộ của tổ chức
6. Kết nối Internet