

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



MẠNG MÁY TÍNH

Bài tập lớn

Thiết kế mạng máy tính cho building của ngân hàng

GVHD: Nguyễn Quang Sang

SV thực hiện:	Đào Xuân Đạt	1911000
	Nguyễn Thế Huy	1812404
	Lê Bảo Khánh	1911363
	Vũ Quang Trung	1912330

Tp. Hồ Chí Minh, Tháng 11/2021



Mục lục

1	Danh sách thành viên	2
2	Yêu cầu kiến trúc hệ thống	2
3	Thiết kế hệ thống mạng ngân hàng B Bank Building	3
4	Mô tả cụ thể cho thiết kế mạng	3
4.1	Sơ đồ địa chỉ IP:	6
4.1.1	Trụ sở chính (Bảng 1)	6
4.1.2	Chi nhánh (Bảng 2)	6
4.2	Các Host trong hệ thống mạng	6
4.3	Các thiết bị mạng	7
5	Tính toán throughput, bandwidth và các thông số an toàn cho Mạng máy tính	8
5.1	Trụ sở chính.	8
5.2	Trụ sở chi nhánh.	9
6	Đánh giá hệ thống.	9
6.1	Độ tin cậy.	9
6.2	Dễ dàng nâng cấp.	9
6.3	Phần mềm hỗ trợ.	9
6.4	Tính an toàn vào bảo mật của hệ thống.	10
6.5	Những hạn chế còn vướng mắc trong dự án.	10
6.6	Định hướng tương lai.	11
7	Mô phỏng trên phần mềm	11

1 Danh sách thành viên

No.	Tên	MSSV	Công việc	Phần trăm hoàn thành
1	Đào Xuân Đạt	1911000	- Thiết kế hệ thống - Mô phỏng hệ thống	100%
2	Nguyễn Thế Huy	1812404	- Thiết kế hệ thống - Viết báo cáo	100%
2	Lê Bảo Khánh	1911363	- Thiết kế hệ thống - Mô phỏng hệ thống	100%
3	Vũ Quang Trung	1912330	- Thiết kế hệ thống - Viết báo cáo	100%

2 Yêu cầu kiến trúc hệ thống

Xây dựng hệ thống mạng cho ngân hàng BBB (B Banking Building) chuẩn bị xây mới tại TP.HCM với những thông số quan trọng như sau:

- Tòa building tại trụ sở cao 7 tầng, tầng 1 được trang bị 1 phòng kỹ thuật mạng và Cabling Central Local (Phòng tập trung dây mạng và patch panel);
- BBB dạng SMB Enterprise: 100 workstations, 5 Servers, 10 Network Equipments;
- Dùng công nghệ mới (new technology) về hạ tầng mạng, 100/1000 Mbps, Wireless;
- Dùng kết hợp giữa Licensed và Open Source Softwares;
- Kết nối với bên ngoài bằng 2 Leased Line và 2 ADSL, Load Balancing;
- Ứng dụng văn phòng, Client - Server, đa phương tiện, Database;
- Bảo mật cao, an toàn khi xảy ra sự cố, dễ dàng nâng cấp hệ thống.

Ngân hàng có nhu cầu kết nối đến 2 chi nhánh khác ở 2 thành phố lớn là Nha Trang và Đà Nẵng. Mỗi chi nhánh cũng được thiết kế tương tự như trụ sở nhưng ở quy mô nhỏ hơn:

- Toà nhà cao 2 tầng, tầng 1 được trang bị 1 phòng kỹ thuật Mạng và Cabling Central Local (Phòng tập trung dây mạng và patch panel);
- BBB dạng chi nhánh: 50 workstations, 3 Servers, 5 Network Equipments.

Việc thực hiện kết nối giữa trụ sở và chi nhánh thông qua đường links WAN, chúng ta có thể chọn một trong các công nghệ dùng cho đường links này theo tính kinh tế của giải pháp.

Phân tích ưu nhược điểm của giải pháp được chọn.

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

- Servers dùng cho updates, web access, database access,... Tổng dung lượng upload và download vào khoảng 500 MB/ngày.
- Mỗi workstation dùng cho duyệt Web, tải tài liệu, giao dịch khách hàng,... Tổng dung lượng upload và download vào khoảng 100 MB/ngày.
- Máy laptop kết nối WIFI cho khách hàng truy xuất khoảng 50 MB/ngày.
- Hệ thống Mạng máy tính của Ngân hàng BBB được dự toán cho mức độ phát triển 20% trong 5 năm (về số lượng người sử dụng, tải trọng mạng, mở rộng nhiều chi nhánh,...).

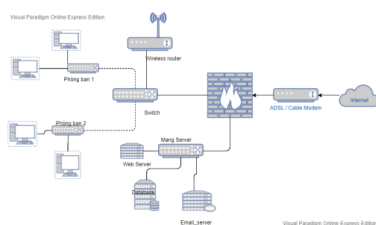
3 Thiết kế hệ thống mạng ngân hàng B Bank Building

Các yêu cầu về kiến trúc cần có cho hệ thống

- Phân hệ kết nối internet: Phần này được trang bị các thiết bị kết nối Gateway Cisco Router riêng kết nối với mạng Internet, cho phép mở rộng và nâng cấp tốc độ cổng kết nối Internet tùy theo nhu cầu phát triển. Người dùng truy nhập vào mạng được xác thực tùy theo quyền truy nhập để vào mạng nội bộ hoặc Internet và CSDL dùng để xác thực được quản lý tập trung trên máy chủ ACS đặt ở vùng quản trị hệ thống
- Phân hệ Server DMZ: Gồm hệ thống máy chủ Web, E-mail, máy chủ ứng dụng dành cho khách hàng, nội bộ truy nhập, trên máy chủ Web gồm có các hệ thống giao dịch trên WEB của Ngân hàng , Internet Banking , homeBanking, các thông tin quảng cáo, tra cứu các sản phẩm của ngân hàng. Ngoài ra còn các máy chủ CSDL lưu trữ các dữ liệu quan trọng của khách hàng, máy chủ này rất quan trọng đối với hệ thống ngân hàng vì nó chứa toàn bộ thông tin khách hàng, các thông tin giao dịch quan trọng của khách hàng, đảm bảo sự an toàn cho chúng mà một yêu cầu quan trọng cần đặt ra khi thiết kế hệ thống mạng này.
- Phân hệ mạng máy tính nội bộ : Gồm các workstations đặt tại các phòng ban của tòa nhà được sử dụng với nhu cầu công việc của các nhân viên của ngân hàng.
- Phân hệ 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.
- Phân hệ kết nối với các chi nhánh khác của ngân hàng: Ngân hàng trung tâm kết nối với các chi nhánh của nó theo đường truyền riêng được thuê bởi bên thứ ba (ISP) kết nối với mạng WAN.

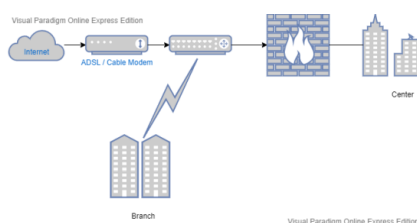
4 Mô tả cụ thể cho thiết kế mạng

Đối với kết nối các workstations và các server ở ngân hàng trung tâm và chi nhánh, nhóm lựa chọn cho cấu trúc hình sao cho mạng lan này bởi những ưu điểm sau: với cấu trúc sao các nút mạng ở biên hoạt động độc lập với nhau nên khi một nút mạng bị lỗi thì các nút mạng khác vẫn hoạt động bình thường, trừ khi switch trung tâm bị lỗi. Ngoài ra với cấu trúc này, chúng ta có thể thêm các thiết bị mà không ảnh hưởng quá nhiều đến mạng có sẵn, hoạt động tốt với tải nặng. Mô hình cụ thể được minh họa ở Hình 1. Cả hai thành phần mạng LAN con được kết nối đến tường lửa trước khi truy cập internet để đảm bảo an toàn cho hệ thống Server và các thiết bị trong nội bộ ngân hàng.



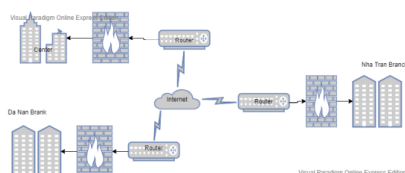
Hình 1: Mô hình mạng LAN minh họa cho từng địa điểm

Tường lửa sẽ được kết nối với internet thông qua một Router, Router sẽ kết nối Modem bằng ADSL nhằm cung cấp internet cho hệ thống và cũng ở Router này nhóm sử dụng phương thức NAT để ánh xạ các địa chỉ cục bộ của mạng LAN sang địa chỉ public để có thể truy cập internet bởi với địa chỉ cục bộ các máy không thể truy cập internet. Với phương thức NAT, chúng ta có thể giảm thiểu sức nặng của các địa chỉ IP Public với chúng là có hạn khi mà số lượng thiết bị truy cập internet này càng tăng, bảo mật thông tin địa chỉ IP Private - địa chỉ mà các thiết bị cục bộ trong mạng LAN sử dụng để giao tiếp với nhau. Sử dụng phương thức NAT tăng tính bảo mật cho hệ thống. Ngoài liên kết với Modem và tường lửa Router này được sử dụng để liên kết với các chi nhánh qua mạng WAN với đường truyền riêng được cung cấp bởi ISP mà ngân hàng lựa chọn hợp tác. Với các chi nhánh được thiết kết tương tự. Hình 2 minh họa cho cho thiết kế.



Hình 2: Kết nối với mạng WAN và các chi nhánh.

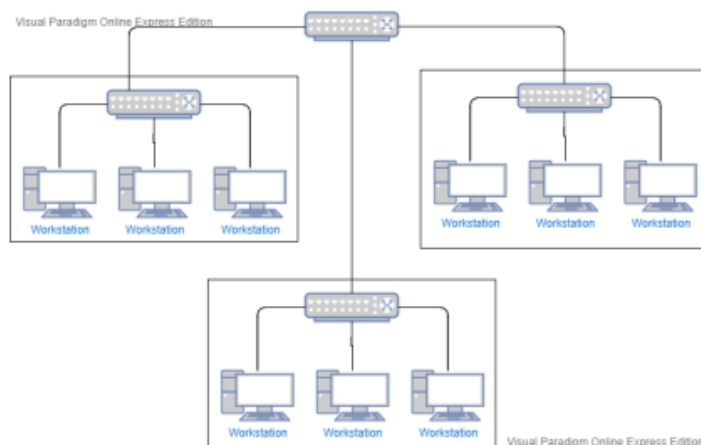
Các chi nhánh và đơn vị trung tâm liên kết với bởi mạng WAN với đường truyền riêng của được cung cấp bởi nhà cung cấp dịch vụ. Liên kết được thực hiện tại Router mà mỗi đơn vị kết nối với internet. Hình 3 minh họa cho liên kết này. Tại các Router liên kết này được thiết lập 3 đường truyền để liên kết ra mạng WAN: đường ADSL liên kết với Modem, và hai đường truyền riêng dùng để liên kết với các chi nhánh. Tại Router chúng ta có thể sử dụng các giải thuật định tuyến nhằm 'Load Balancing' giảm tải trên các đường truyền và tránh các trường hợp dồn toàn bộ áp lực tải lên một đường truyền còn các đường truyền khác thì không có, hoặc tải thấp, rất lãng phí và giảm hiệu suất truy xuất thông tin của hệ thống. Các giải thuật Routing Load Balancing như là RIP, OSPF (là một phiên bản kế thừa của phương thức định tuyến RIP),... Với yêu cầu của hệ thống này, OSPF là một lựa chọn khả thi.



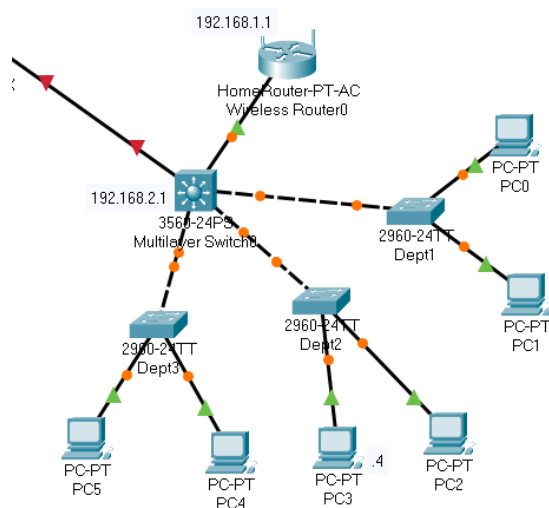
Hình 3: Liên kết các chi nhánh với đơn vị trung tâm.

Như đã giới thiệu ở trên nhóm lựa chọn cấu trúc mạng hình sao để hiện thực mạng các workstations và wireless. Cụ thể như sau: Các workstations của cùng một tầng hoặc có thể với hai tầng cạnh nhau được liên kết vào cùng một switch layer 2 với các workstations của cùng một phòng ban thì được accept vào cùng một Vlan thuận tiện cho việc trao đổi thông tin trong công việc. Các Switch tại các tầng được tổng hợp lại tại một Switch layer 3 và kết nối đến tường lửa nhằm phục vụ các nhu cầu kết nối khác ngoài mạng bộ như kết nối internet, hay kết nối đến các server phục vụ cho các ứng dụng nội bộ của ngân hàng. Tại sao chúng tôi lại sử dụng switch layer 3 ở node tổng hợp các Switch giữa các tầng? Bởi vì các phòng ban được accept vào

các Vlan (10-60) khác nhau nên với switch layer 2 thì việc chuyển đổi giữa các vlan là không thể thực hiện được, nên chúng tôi cần lựa chọn một thiết bị mạng có chức năng định tuyến để chuyển đổi giữa các mạng VLAN và Switch layer 3 thỏa mãn yêu cầu này. Truy cập mạng không dây Wireless cũng được yêu cầu trong hệ thống này, nhóm lựa chọn wireless router để cung cấp phục vụ nhu cầu này và nó được liên kết vào Switch layer 3 tổng hợp ở trên. Hình 3 minh họa cho cấu trúc mạng hình sao nhóm lựa chọn sử dụng, Hình 4 minh họa cho phần thiết kết này ở các chi nhánh.



Hình 4: : Minh họa cấu trúc mạng sao.



Hình 5: : Mạng workstations và wireless.



4.1 Sơ đồ địa chỉ IP:

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

4.1.1 Trụ sở chính (Bảng 1)

VLAN	Phòng ban	Địa chỉ mạng	Phân vùng IP Private	Tầng	workstations
10	Phòng kỹ thuật	192.168.10.0/24	192.168.10.1-192.168.10.255	Tầng 2	20
20	Lễ tân và CSKH	192.168.20.0/24	192.168.20.1-192.168.20.255	Tầng 1	15
30	Phòng Marketing	192.168.30.0/24	192.168.10.1-192.168.30.255	Tầng 3	15
40	Phòng Nhân Sự	192.168.40.0/24	192.168.10.1-192.168.40.255	Tầng 4	15
50	Phòng Tài Chính	192.168.50.0/24	192.168.10.1-192.168.50.255	Tầng 5	20
60	Phòng Quản Lý	192.168.60.0/24	192.168.10.1-192.168.60.255	Tầng 7	15
70	Wireless LAN	192.168.70.0/24	192.168.10.1-192.168.70.200	Tầng 1-7	No
	Server LAN	10.10.1.0/24	10.10.1.1-10.10.1.255	Tầng 6	No

Bảng 1: Bảng VLAN và phân vùng IP Private của trụ sở chính

4.1.2 Chi nhánh (Bảng 2)

VLAN	Phòng ban	Địa chỉ mạng	Phân vùng IP Private	Tầng	workstations
10	Phòng kỹ thuật	192.168.10.0/24	192.168.10.1-192.168.10.255	Tầng 1	10
20	Lễ tân và CSKH	192.168.20.0/24	192.168.20.1-192.168.20.255	Tầng 1	10
30	Phòng Marketing	192.168.30.0/24	192.168.10.1-192.168.30.255	Tầng 2	5
40	Phòng Nhân Sự	192.168.40.0/24	192.168.10.1-192.168.40.255	Tầng 2	10
50	Phòng Tài Chính	192.168.50.0/24	192.168.10.1-192.168.50.255	Tầng 2	10
60	Phòng Quản Lý	192.168.60.0/24	192.168.10.1-192.168.60.255	Tầng 2	5
70	Wireless LAN	192.168.70.0/24	192.168.10.1-192.168.70.200	Tầng 1-2	No
	Server LAN	10.10.1.0/24	10.10.1.1-10.10.1.255	Tầng 6	No

Bảng 2: Bảng VLAN và phân vùng IP Private của trụ sở chính

4.2 Các Host trong hệ thống mạng

1. Workstations: các máy tính văn phòng được cung cấp cho các nhân viên trong công ty sử dụng phục vụ nhu cầu trong công việc, gửi mail, sử dụng các ứng dụng văn phòng và các ứng dụng nội bộ của ngân hàng và các nhu cầu cơ bản khi sử dụng Internet.
2. Các máy khác kết nối mạng Wireless của ngân hàng như laptop, điện thoại thông minh của khách hàng hay nhân viên, liên kết sẽ cung cấp cung cấp một IP Private động cho các thiết bị kết nối và cung cấp liên kết Internet cho các thiết bị này.
3. Server: Các server cần thiết cho một hệ thống ngân hàng:
 - WebServer: Lưu trữ thông tin, xử lý các yêu cầu của khách hàng khi khách hàng sử dụng ứng dụng của ngân hàng.
 - Mail Server: Lưu trữ thông tin các email giao dịch.

- Database server: Lưu trữ các thông tin khách hàng, thông tin giao dịch, thông tin nhân viên và các dữ liệu khác trong hệ thống ngân hàng. Đây cũng là bộ phận quan trọng của một ngân hàng vì nó chứa các thông tin các nhân quan trọng của khách hàng cần được đảm bảo an toàn trước những kẻ tấn công
- Với server có cùng một mục đích được thiết lập thêm để giảm thiểu sức nặng công việc trên 1 server chúng ta cần có cân bằng tải để điều hướng giữa hai Server này nhằm chia sẻ công việc trên mỗi Server và phản hồi yêu cầu kịp thời.

4.3 Các thiết bị mạng

1. **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. Chúng tôi lựa chọn tường lửa ASA 5506. Cisco ASA 5506 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** 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.
2. **Switch**
 - Switch **layer 2 2690-24TT** : Đây là một thiết bị chuyển mạch của Cisco với 24 cổng FastEthernet 10/100 ports đây là cổng mà ta sẽ kết nối các host và kết nối với Switch tổng.
 - Switch **layer 3 3560** : 24 cổng FastEthernet 10/100 ports, nhóm sử dụng chúng để kết nối với các Switch tại các node và 2 cổng Gigabit Ethernet để kết nối với tường lửa. Ngoài chức năng chuyển mạch Switch layer 3 còn có thể định tuyến nên khi kết nối các mạng con có nhiều Vlan khác nhau sử dụng Switch layer 3 mà một lựa chọn phù hợp, ngoài ra với yêu cầu chúng ta cũng có thể lựa chọn Router thay thế.
3. **Router**
 - **Wireless Router** : Một thiết bị thực hiện các chức năng của bộ định tuyến và cũng bao gồm các chức năng của Access Point. Nó được sử dụng để cung cấp quyền truy cập vào Internet hoặc mạng máy tính riêng.
 - **Router PT**: Thiết bị mạng có chức năng chuyển tiếp gói dữ liệu giữa các mạng máy tính. Ở hệ thống này chúng ta cần kết nối mạng cục bộ ngân hàng với mạng Internet, mạng WAN nên việc sử dụng Router là một yêu cầu bắt buộc. Chúng ta cần lựa chọn các Router có các cổng Gigabit Ethernet để kết nối với Modem, tường lửa và các cổng serial để kết nối với mạng WAN. Khi sử dụng Router, chúng ta cần cấu hình các giải thuật định tuyến và có cân bằng tải để tối ưu đường truyền, cải thiện tốc độ truyền mạng.

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

- Throughput - Thông lượng : thông lượng mạng đề cập đến lượng dữ liệu có thể được truyền từ nguồn đến đích trong một khung thời gian nhất định. Công suất thông lượng được đo bằng bit trên giây, nhưng nó cũng có thể được đo bằng dữ liệu trên giây
- Bandwidth - Băng thông : Định nghĩa băng thông mạng có thể gây nhầm lẫn, nhưng về cơ bản, băng thông mạng được định nghĩa là dung lượng thông lượng truyền tối đa của mạng. Đó là thước đo lượng dữ liệu có thể được gửi và nhận tại một thời điểm. Băng thông được đo bằng bit, megabit hoặc gigabit trên giây. Khi mọi người sử dụng các chương trình hoặc phần mềm, họ muốn các yêu cầu của họ được lắng nghe và đáp ứng kịp thời. Các gói bị mất khi truyền dẫn đến hiệu suất mạng kém hoặc chậm và thông lượng thấp cho thấy các vấn đề như mất gói. Sử dụng thông lượng để đo tốc độ mạng rất tốt cho việc khắc phục sự cố vì nó có thể tìm ra nguyên nhân chính xác của mạng chậm và cảnh báo cho quản trị viên về các vấn đề cụ thể liên quan đến mất gói.
- Việc tính toán thông lượng và băng thông của mạng là cần thiết, bởi nó sẽ cho chúng ta biết thiết kế mạng đã đáp ứng được những yêu cầu dịch vụ mà hệ thống mạng cung cấp hay chưa và có thể điều chỉnh sao cho phù hợp. Các yêu cầu dịch vụ mà hệ thống cần đáp ứng như là:
 - Truy cập Internet lướt web, chạy các ứng dụng khác trên máy tính, điện thoại thông minh.
 - Nhận và hồi đáp yêu cầu Web Server từ bên ngoài, hoặc nội bộ trong ngân hàng.
 - Nhận yêu cầu dữ liệu từ các trụ sở khác của ngân hàng.
 - Gửi mail, các dịch vụ gửi tin nhắn khác.

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 15g-16h. (3 giờ).

- Lượng upload và download 500MB/ngày cho mỗi Server. Ở trụ sở chính chúng ta có 5 Server, tổng dung lượng upload và download : $5 \times 500 = 2500$ (MB).
- Với mỗi Workstation có tổng dung lượng upload và download khoảng 100MB/ngày. Chúng ta có 100 Workstations: tổng dung lượng cần đáp ứng cho các Workstations: $100 \times 100 = 10.000$ (MB/ngày) Với mạng không dây: mỗi laptop kết nối khoảng 50MB/ngày. Với trụ sở: trụ sở có khoảng 200 thiết bị mạng truy cập mỗi ngày. Tổng dung lượng cho mạng Wireless: $50 \times 200 = 10.000$ (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: $((2500 + 10.000 + 10.000) \times 0.8) / (3 \times 3600) = 1.667$ (MB/s) = 13.333 (Mb/s).
- Thourghput: $(2500 + 10.000 + 10.000) / (24 \times 3600) = 0.260$ MB/s = 2.083 (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 15g-16h. (3 giờ).

- Lượng upload và download 500MB/ngày cho mỗi Server. Ở trụ sở chính chúng ta có 3 Server, tổng dung lượng upload và download : $3 \times 500 = 1500$ (MB).
- Với mỗi Workstations có tổng dung lượng upload và download khoảng 100MB/ngày. Chúng ta có 50 Workstations: tổng dung lượng cần đáp ứng cho các Workstations: $50 \times 100 = 5.000$ (MB/ngày). Với mạng không dây: mỗi laptop kết nối khoảng 50MB/ngày. Với trụ sở trụ sở có khoảng 150 thiết bị mạng truy cập mỗi ngày. Tổng dung lượng cho mạng Wireless: $50 \times 150 = 7.500$ (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: $((1.500 + 5.000 + 7.500) \times 0.8) / (3 \times 3600) = 1.037$ (MB/s) = 8.296 (Mb/s).
- Thourghput: $(1.500 + 5.000 + 7.500) / (24 \times 3600) = 0.162$ (MB/s) = 1.296 (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 Dễ dàng nâng cấp.

Trong thời kì công nghệ không ngừng phát triển, hệ thống mạng được thiết kế cần đảm bảo có thể nâng cấp khi cần thiết. Chẳng hạn như tăng nhân sự, tăng chi nhánh hay tăng số lượng Server khi lượng khách hàng và nhu cầu của họ tăng lên. Hiện tại với nhu cầu 100 workstations tại trụ sở chính, nhóm đang sử dụng 6 switch với 24 port cho mỗi switch có thể đáp ứng cho 138 host, nên với nhu cầu tăng nhân viên hệ thống hiện tại vẫn đáp ứng được. Nếu trong trường hợp các Switch hiện tại không thể đáp ứng được nữa, chúng ta chỉ cần thêm Switch để kết nối các workstations mới và nối nó vào Switch layer 3 trung tâm. Với nhu cầu tăng Server, nếu Server cần tăng để phục vụ nhu cầu mới của hệ thống thì chúng ta chỉ cần kết nối các Server mới và Switch trung tâm tại mạng server và thiết lập địa chỉ private và ánh xạ địa chỉ public tĩnh cho nó. 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, thì 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 cân bằng tải để phân chia tải xuống các Server, đảm bảo các Server làm việc đồng đều.

6.3 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 kỹ 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.

6.4 Tính an toàn vào bảo mật của hệ thống.

1. Yêu cầu mà hệ thống 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 những 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.
2. Các tài nguyên cần bảo vệ trong hệ thống: Phần 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 phần 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.
3. Những mối đe dọa mà hệ thống có thể gặp phải: Hacker sử dụng các công cụ, phần mềm mã độc tấn công hệ thống lấy cắp thông tin khách hàng, kiểm soát các máy tính trong ngân hàng. Ngoài những nguy cơ tiềm 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.
4. 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 những mối nguy cơ bên ngoài và bên trong của hệ thống. Ngoài ra với 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 với 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,...Bảo mật các thiết bị mạng trong hệ thống.
5. 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.

6.5 Những hạn chế còn vướng mắc trong dự án.

Những vấn đề về bảo mật luôn là những những nguy cơ tiềm ẩn đối với các hệ thống ngân hàng, chúng có thể mang lại những hậu quả vô cùng lớn khi hệ thống bị tấn công, mặc dù các hệ thống ngân hàng đã có các biện pháp bảo mật nhưng các vụ tấn công vẫn xảy ra mỗi năm, nên vấn đề xây dựng hệ thống bảo mật sao cho tối ưu nhất an toàn nhất vẫn là một vướng mắc của dự án. Có rất nhiều các thiết bị mạng trên thị trường với nhiều kỹ thuật và công nghệ mới, khi thiết kế một hệ thống mạng máy tính việc lựa chọn các thiết bị mạng sao cho phù hợp cũng là một công việc khó khăn bởi không chỉ yêu cầu về đáp ứng lưu lượng dữ liệu mà còn những yêu cầu về giá cả, công nghệ bảo mật, hiệu năng cũng cần được xem xét kĩ càng.

6.6 Định hướng tương lai.

Cải thiện khả năng bảo mật của hệ thống mà một công việc cần nhiều thời gian, công sức, cần cải thiện liên tục nên đây là một công việc mà chúng ta cần chú trọng trong tương lai. Thay mới các thiết bị mạng, kịp thời cập nhật các phần mềm công nghệ mới. Nâng cấp và bảo trì hệ thống cũng là những nhiệm vụ không chỉ của hiện tại mà cần chú trọng hơn ở tương lai.

7 Mô phỏng trên phần mềm

Sử dụng phần mềm mô phỏng Packet Tracer (Cisco)

Các bước thực hiện:

1. Lựa chọn các thiết bị mạng cần sử dụng.
2. Thiết kế sơ đồ mạng LAN của trụ sở và chi nhánh.
3. Liên kết các trụ sở và chi nhánh trong qua mạng WAN với Leased line.
4. Kết nối mạng LAN tại trụ sở và chi nhánh ra Internet qua Modem theo đường truyền mà nhà cung cấp dịch vụ Internet Cấu hình các thiết bị mạng, cấu hình địa chỉ IP private static cho các Workstations, accept chúng vào các VLAN tương ứng.
5. Thiết lập DHCP server tại Wireless Router để cung cấp IP private động cho các thiết bị truy cập mạng không dây.
6. Cấu hình tường lửa xác định các gói tin được phép đi qua.
7. Sử dụng cơ chế NAT tại Router để ánh xạ các địa chỉ IP private sang địa chỉ IP public để các host có thể liên kết đến Internet.
8. Định tuyến tại các Router.
9. Kiểm tra bằng các lệnh ping,...