

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



MẠNG MÁY TÍNH (CO3003)

Bài tập lớn

Thiết kế mạng máy tính cho building của ngân hàng

GVHD: Bùi Xuân Giang

SV thực hiện:	Phạm Công Hậu	1812143 (Nhóm trưởng)
	Lê Chung Hoàng	1812263
	Nguyễn Trọng Hoàng	1812280

Tp. Hồ Chí Minh, Tháng 12/2020



Mục lục

1	Danh sách thành viên	2
2	Nội dung đề bài	2
3	Phân tích nội dung và yêu cầu thiết kế của hệ thống	3
3.1	Software:	3
3.2	Quản lý mô hình:	3
3.3	Kết nối với bên ngoài:	4
4	Thiết kế hệ thống	4
4.1	Thiết kế cấu trúc hạ tầng mạng	4
4.1.1	Trụ sở chính:	4
4.1.2	Chi nhánh:	5
4.1.3	Phân hệ quản trị cho hệ thống:	5
4.1.4	Mô hình kết nối:	6
4.1.5	Mô hình địa chỉ IP trong mỗi VLAN:	6
4.2	Các thiết bị cần cho việc thiết kế hệ thống:	7
5	Tính toán hệ thống	8
6	Mô phỏng hệ thống	8
7	An toàn và bảo mật	8
7.1	Xác định các tài nguyên cần được bảo vệ:	8
7.2	Xác định các mối đe dọa tới hệ thống:	8
7.3	Các giải pháp bảo mật:	9
7.4	An toàn khi xảy ra sự cố:	9
8	Nâng cấp hệ thống	10



1 Danh sách thành viên

No.	Tên	MSSV	Công việc	Phần trăm hoàn thành
1	Nguyễn Trọng Hoàng	1812280	- Thiết kế hệ thống - Mô phỏng hệ thống	100%
2	Lê Chung Hoàng	1812263	- Thiết kế hệ thống - Mô phỏng hệ thống - Viết báo cáo	100%
3	Phạm Công Hậu	1812143	- Thiết kế hệ thống - Viết báo cáo	100%

2 Nội dung đề bài

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:

- Tòa 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 Phân tích nội dung và yêu cầu thiết kế của hệ thống

3.1 Software:

Ở đây có 2 loại là Licensed và Open Source Software:

- Licensed Software thường là các ứng dụng, phần mềm mà ta phải trả tiền để có thể sử dụng. Và ta ko thể tự thay đổi cấu trúc của phần mềm đó mà phải nhờ đến những nhân viên của công ty phần mềm sản xuất ra. Ưu điểm của phần mềm loại này là bạn có thể được bảo hành, nâng cấp, sửa chữa từ nhà sản xuất.
- Open Source Software (phần mềm mã nguồn mở) là khái niệm để chỉ tất cả phần mềm mà mã nguồn của nó được công bố rộng rãi và cho phép mọi người tiếp tục phát triển nó. Điều này không có nghĩa là chúng có thể được sao chép, sửa chữa thoải mái hay sử dụng vào mục đích nào cũng được.

Qua phân tích về 2 loại phần mềm trên ta thấy 1 công ty có thể chọn sử dụng loại 1 loại phần mềm nào hoặc có thể sử dụng cả hai trên:

- Hệ điều hành: Ta nên sử dụng hệ điều hành Windows của hãng Microsoft bởi vì đây là 1 hệ điều hành đơn giản, quen thuộc, dễ sử dụng đối với nhân viên. Điều này sẽ giúp nhân viên dễ dàng thao tác trên máy tính.
- Phần mềm văn phòng: Thường có 2 loại chính là Microsoft Office và Open Office. Mỗi loại đều có thể mạnh riêng. Microsoft Office thì quen thuộc đối với nhân viên và người sử dụng nhưng nó lại không miễn phí. Còn Open Office mặc dù là phần mềm miễn phí nhưng nó lại chưa được sử dụng nhiều ở Việt Nam. Từ đây ta thấy nên chọn Microsoft Office cho ngân hàng vì nó sẽ dễ dàng trong việc sử dụng đối với nhân viên, ngoài ra nó tích hợp nhiều công cụ và tính năng hơn Open Office.
- Các ứng dụng khác: Ta có thể dùng luôn các ứng dụng được tích hợp trên hệ điều hành Windows hoặc có thể dùng thêm 1 số ứng dụng phổ biến, có tính bảo mật cao khác (Ví dụ: trình duyệt web ta có thể dùng IE hoặc Firefox).
- File Server: Vì đặc thù của ngân hàng là nó chứa tài liệu theo từng phòng ban. Phòng ban này không có quyền truy xuất vào dữ liệu phòng ban kia khi chưa được phép, do đó ta dùng cơ chế quản lý theo User và theo Group. Vì vậy ta nên chọn hệ điều hành Windows Server 2003 cho File Servers.
- Các Server khác thì yêu cầu tính năng bảo mật cao do đó có thể dùng hệ điều hành Linux cho các Server này.
- Database Server: Nhằm đảm bảo tính bảo mật, độ tin cậy và quy mô của ngân hàng, chúng tôi quyết định sử dụng Oracle.

3.2 Quản lý mô hình:

Ta nên quản lý ngân hàng theo mô hình Client - Server. Các dữ liệu hệ thống đều được lưu trữ trên Server. Hoạt động tính toán đều phải dựa vào dữ liệu trên Server.

3.3 Kết nối với bên ngoài:

Có 2 kiểu là Leased Line và ADSL:

- Leased Line: Leased Line là dịch vụ cung cấp đường truyền cho các doanh nghiệp, tổ chức có nhu cầu sử dụng Internet tốc độ cao, ổn định một cách thường xuyên với dung lượng truyền tải lớn.
 - Ưu điểm : tối đa hóa tốc độ kết nối với tốc độ tải xuống và tải lên ngang bằng nhau tại mọi thời điểm. Chất lượng đường truyền có độ ổn định và đảm bảo kết nối 24/24.
 - Nhược điểm: giá thuê còn mắc.
- ADSL: cung cấp một phương thức truyền dữ liệu với băng thông rộng, tốc độ cao hơn nhiều so với phương thức truy cập qua đường dây điện thoại truyền thống theo phương thức quay số (Dial up).
- Ta sử dụng 1 đường Leased Line và 2 đường ADSL để kết nối với Internet. Với Leased Line ta có 1 đường dây ổn định, đảm bảo, chất lượng cho đường truyền ra mạng. Nhưng ta cần thêm 2 đường ADSL dự phòng trong trường hợp Leased Line quá tải hoặc có sự cố và cho những vùng không cần tải quá lớn. Vì ADSL tuy chất lượng không tốt bằng Leased Line nhưng nó rẻ hơn so với đường Leased Line rất nhiều.
- Ngoài ra ta sẽ thuê 2 đường Leased Line để nối từ trụ sở chính đến mỗi chi nhánh. Với đường Leased Line này thì dữ liệu từ chi nhánh đến trụ sở chính sẽ luôn được đảm bảo, làm giảm sự bất đồng bộ dữ liệu giữa 2 nơi.

Bên cạnh đó ta sử dụng Load balancing để cải thiện hiệu suất và độ tin cậy của các ứng dụng, cơ sở dữ liệu và các dịch vụ khác bằng cách phân phối khối lượng công việc trên nhiều máy chủ.

4 Thiết kế hệ thống

4.1 Thiết kế cấu trúc hạ tầng mạng

4.1.1 Trụ sở chính:

Tầng 1:

- Tầng 1 của trụ sở chính được bố trí là nơi giao dịch của khách hàng (gồm bộ phận giao dịch và bộ phận tiếp tân). Mỗi nhân viên được trang bị một PC (10 máy) có khả năng kết nối với Server.
- Hơn nữa, tầng 1 còn có 2 phòng: Phòng kỹ thuật mạng (20 máy) và phòng Cabling Central Local (nơi tập trung các thiết bị mạng, Server, dây nối,...).
- Ngân hàng cung cấp mạng không dây cho khách hàng truy cập bằng các thiết bị di động.
- Cuối cùng, Server sẽ có hệ thống bảo mật riêng, đường truyền tốc độ cao nhằm thực hiện các tác vụ đặc biệt.

Tầng 2, 3, 4, 5, 6:

- Các tầng này sẽ được sử dụng là nơi làm việc của các phòng ban gồm:
 - Tầng 2: Phòng Kế Toán Tài Chính và phòng Quan Hệ Khách Hàng. (20 máy)



- Tầng 3: Phòng Quản Lý Rủi Ro. (10 máy)
 - Phòng Công Quỹ và phòng Quản Lý Vốn Kinh Doanh. (15 máy)
 - Phòng Quản Lý Nhân Sự. (5 máy)
 - Phòng Thương Mại Điện Tử Marketing. (15 máy)
- Đối với các phòng này, mỗi nhân viên được trang bị một máy tính được kết nối mạng. Các máy được chia thành từng nhóm ứng với các phòng ban nhằm dễ quản lý. Bên cạnh đó, mỗi phòng ban được trang bị 2 máy in.

Tầng 7:

- Đây là tầng làm việc của ban giám đốc. Mỗi phòng sẽ được trang bị 5 máy tính (2 máy dành giám đốc và phó giám đốc, 3 máy dành cho thư ký). Máy tính của giám đốc và quản trị có chứa các tài liệu quan trọng nên yêu cầu độ bảo mật cao.

Phân bố Server cho trụ sở chính:

- Database Server: 1 máy.
- Backup Server: 1 máy.
- File Server: 1 máy.
- Mail Server: 1 máy.
- Web Server: 1 máy.

4.1.2 Chi nhánh:

Tầng 1: Tương tự tầng 1 của trụ sở chính.

Tầng 2: Tương tự tầng 7 của trụ sở chính.

Phân bố Server cho chi nhánh:

- Database Server: 1 máy.
- Backup Server: 1 máy.
- File Server: 1 máy.

Tất cả các Server đều được đặt tại phòng Cabling Central Local.

4.1.3 Phân hệ quản trị cho hệ thống:

Phân hệ kết nối Internet và truy cập từ xa: 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 mạng DMZ:

- Gồm hệ thống máy chủ Web, Email, 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, Home Banking, các thông tin quảng cáo, tra cứu các sản phẩm của ngân hàng, các hệ thống đào tạo, dạy học điện tử nội bộ.

- Máy chủ Email của các tài khoản nội bộ hay khách hàng, máy chủ Web được cài các bộ lọc theo các nội dung, các địa chỉ trang WEB, ngoài ra tại khu vực này còn có các máy chủ Virus để kiểm tra virus đối với các thông tin vào ra Internet.

Phân hệ mạng nội bộ:

- Bao gồm các Client đặt trên các tầng của tòa nhà, phục vụ cho các nhân viên làm việc, duyệt Web, gửi Email...
- Ngoài ra còn có thể phân theo cách sau:
 - Phân hệ máy chủ và ứng dụng: Các máy chủ ứng dụng chứa các CSDL dành cho các ứng dụng, hết sức quan trọng do vậy khu vực này cần được đảm bảo mức độ an ninh bảo mật cao.
 - Phân hệ quản trị mạng: Bao gồm các máy chủ quản trị an ninh, máy chủ xác thực, máy chủ quét các dịch vụ trên mạng (IDS).
 - Phân hệ kết nối ra bên ngoài (EXTRANET): Dành cho các kết nối từ các đơn vị bên ngoài hoặc bên ngoài truy cập vào mạng của Ngân hàng.
 - Phân hệ máy chủ CSDL: Các máy chủ ứng dụng chứa các CSDL chính, hết sức quan trọng do vậy khu vực này cần được đảm bảo mức độ an ninh bảo mật cao nhất.
 - Phân hệ kết nối WAN của ngân hàng: Phần kết nối vào cổng Gateway Firewall, nhằm bảo vệ các giao dịch từ bên ngoài vào.

4.1.4 Mô hình kết nối:

Hệ thống sử dụng 1 router chính sử dụng để kết nối tất cả các Workstations tại các phòng ban với hệ thống Server và kết nối ra ngoài Internet. Kết nối Internet từ bên ngoài đi vào hệ thống mạng công ty thông qua thiết bị trung gian Gateway và hệ thống tường lửa nhằm tăng cường độ bảo mật cho hệ thống mạng của ngân hàng. Kết nối này được truyền qua đường Leased Line do ISP cung cấp.

Kết nối từ chi nhánh đi vào hệ thống mạng công ty thông qua hệ thống tường lửa nhằm để phòng trường hợp giả mạo. Kết nối này được truyền qua đường Leased Line do ISP cung cấp.

Hệ thống DMZ được đưa vào sử dụng để tăng độ an toàn cho hệ thống mạng. Mọi kết nối hay dữ liệu từ bên ngoài sẽ được đưa vào hệ thống DMZ xử lý trước, nếu thông tin an toàn sẽ được chuyển tiếp đến các bộ phận trong công ty cũng như hệ thống Server của công ty.

Đường truyền ADSL sẽ được dùng cho kết nối Wifi trong ngân hàng và không được kết nối vào hệ thống mạng của công ty nhằm ngăn chặn các kết nối lạ thông qua mạng không dây. Wifi được đưa vào nhằm mục đích phục vụ cho nhu cầu truy cập Internet tại chỗ của khách hàng, hay nhu cầu giải trí, sử dụng các ứng dụng Internet khác của nhân viên công ty trong giờ nghỉ trưa, mà các ứng dụng đó không được cài đặt trong Application Server.

Các Workstations của mỗi tầng sẽ đưa vào cùng 1 VLAN theo từng phòng ban khác nhau. Tại chi nhánh số lượng Workstations nhỏ nên tất cả các Workstations cùng được nối vào 1 switch, và việc phân chia VLAN cũng được thiết lập tương tự như trụ sở chính. Ngoài ra hệ thống Server sẽ được chia thành 1 VLAN riêng.

4.1.5 Mô hình địa chỉ IP trong mỗi VLAN:

Tại trụ sở chính Tp.Hồ Chí Minh:



VLAN	Phòng ban	Địa chỉ IP	Chi tiết - Miền cung cấp IP
VLAN1	Phòng giao dịch và tiếp tân	192.168.9.0/24	192.168.9.1 -> 192.168.9.254
VLAN2	Phòng Kỹ thuật mạng	192.168.10.0/24	192.168.10.1 -> 192.168.10.254
VLAN3	Phòng kế toán và tài chính	192.168.11.0/24	192.168.11.1 -> 192.168.11.254
VLAN4	Phòng Quan Hệ Khách Hàng	192.168.12.0/24	192.168.12.1 -> 192.168.12.254
VLAN5	Phòng Quản Lý Rủi Ro	192.168.13.0/24	192.168.13.1 -> 192.168.13.254
VLAN6	Phòng Công Quỹ	192.168.14.0/24	192.168.14.1 -> 192.168.14.254
VLAN7	Phòng Quản Lý Vốn và Kinh Doanh	192.168.15.0/24	192.168.15.1 -> 192.168.15.254
VLAN8	Phòng Quản Lý Nhân Sự	192.168.16.0/24	192.168.16.1 -> 192.168.16.254
VLAN9	Phòng Thương Mại Điện Tử và Marketing	192.168.17.0/24	192.168.17.1 -> 192.168.17.254
VLAN10	Phòng Giám Đốc	192.168.18.0/24	192.168.18.1 -> 192.168.18.254

Tại chi nhánh Đà Nẵng:

VLAN	Phòng ban	Địa chỉ IP	Chi tiết - Miền cung cấp IP
VLAN1	Phòng giao dịch và tiếp tân	192.168.33.0/24	192.168.33.1 -> 192.168.33.254
VLAN2	Phòng Kỹ thuật mạng	192.168.34.0/24	192.168.34.1 -> 192.168.34.254
VLAN3	Phòng Giám Đốc	192.168.35.0/24	192.168.35.1 -> 192.168.35.254

Tại chi nhánh Nha Trang:

VLAN	Phòng ban	Địa chỉ IP	Chi tiết - Miền cung cấp IP
VLAN1	Phòng giao dịch và tiếp tân	192.168.33.0/24	192.168.33.1 -> 192.168.33.254
VLAN2	Phòng Kỹ thuật mạng	192.168.34.0/24	192.168.34.1 -> 192.168.34.254
VLAN3	Phòng Giám Đốc	192.168.35.0/24	192.168.35.1 -> 192.168.35.254

4.2 Các thiết bị cần cho việc thiết kế hệ thống:

Server:

- Web Server: Để những khách hàng bên ngoài truy cập vào để lấy thông tin về tài khoản của họ trong ngân hàng cũng như các dịch vụ khác.
- Mail Server: Để gửi và nhận Mail.
- File Server: Để chia sẻ các thông tin.
- Database Server: Để lưu trữ thông tin.
- Backup Server: Chứa thông tin Backup.
- Các server cần phải có cấu hình đủ mạnh để phục vụ cho nhiều truy xuất đồng thời và liên tục.

Workstations:

- Cả tòa nhà sẽ có 100 Workstation.
- Tất cả Workstation sẽ được kết nối vào hệ thống mạng máy tính thông qua các Switch và Core - Switch.

Switch: Theo thiết kế cấu trúc hạ tầng mạng thì chúng ta sẽ cho mỗi tầng 2 Switch 2950 và Switch 2960 (mỗi Switch có 24 ports).

Core - Switch: các Switch sẽ được kết nối lại với nhau và với mạng máy tính thông qua Core - Switch 3560.

Router: Sử dụng Router 2811 (có hỗ trợ Load Balancing).

Access - Point: Ngân hàng cung cấp dịch vụ truy cập mạng không dây để khách có thể truy cập khi đến giao dịch ở ngân hàng. Ta chọn Access - Point PT.

5 Tính toán hệ thống

Số workstation của ngân hàng: $100 + 50 * 2 = 200$.

Số server của ngân hàng: $5 + 3 * 2 = 11$.

Dung lượng sử dụng trong 1 ngày của ngân hàng:

- 1 Server: 500 MB.
- 1 Workstation: 100 MB.
- Laptop khách hàng: 50 MB.

Tổng dung lượng: $200 * 100 + 11 * 500 + 50 = 25550MB$.

Dung lượng sử dụng trong giờ cao điểm (3h): $25550 * 80\% = 20440MB$.

Throughput cần cung cấp cho ngân hàng trong 1 ngày làm việc (8h): $20440 * 8 / (3 * 60 * 60) = 15.14Mbps$.

Hệ thống mạng máy tính của ngân hàng cần mở rộng thêm 20%: $15.14 * 1.2 = 18.17Mbps$.

Ngân hàng nên sử dụng một đường truyền có độ ổn định cao và có băng thông 19 Mbps. Việc thiết kế như vậy đã đáp ứng nhu cầu làm việc tốt của nhân hàng kể cả trong giờ cao điểm.

6 Mô phỏng hệ thống

7 An toàn và bảo mật

7.1 Xác định các tài nguyên cần được bảo vệ:

Phần cứng: Các máy chủ mạng, các máy trạm, các thiết bị mạng như Router, Access Servers..

Phần mềm: Hệ điều hành của các máy chủ Unix, Windows NT..., các chương trình ứng dụng quản lý tài khoản, tín dụng, các chương trình kế toán, tự động hóa văn phòng, truyền dữ liệu, ATM..

Dữ liệu: Đây là phần quan trọng cần được bảo vệ nhất của ngân hàng. Dữ liệu này sẽ gồm các dữ liệu tài khoản liên quan đến khách hàng.

Tài liệu: Các công văn, báo cáo, tài liệu, sách vở, tài liệu hướng dẫn sử dụng...

7.2 Xác định các mối đe dọa tới hệ thống:

Mối đe dọa từ bên ngoài:

- Nguy cơ bị nghe trộm, thay đổi thông tin truyền đi trên mạng công cộng (PSTN). Đây là một nguy cơ tiềm ẩn và ảnh hưởng trực tiếp đến hoạt động kinh doanh của ngân hàng. Hacker có thể sử dụng các công cụ, thiết bị đặc biệt để móc nối vào hệ thống cáp truyền thông của ngân hàng để nghe trộm thông tin, nguy hiểm hơn hacker có thể sửa chữa, thay

đổi nội dung thông tin đó (Ví dụ: nội dung của điện chuyển tiền, thanh toán... gây ra những tổn thất nghiêm trọng).

Mối đe dọa từ bên trong:

- Người sử dụng bên trong mạng có nhiều cơ hội hơn để truy cập vào các tài nguyên hệ thống. Đối với ngân hàng có đặc thù lớn là do nhiều mạng LAN của trung tâm, chi nhánh kết nối vào, do đó nếu người sử dụng trong mạng có ý muốn truy cập vào những tài nguyên của hệ thống thì họ sẽ gây nên một mối đe dọa cho mạng. Người sử dụng bên trong có thể được gán những quyền không cần thiết, có thể bị mất mật khẩu... và đó sẽ là mối đe dọa lớn với hệ thống an toàn mạng.

7.3 Các giải pháp bảo mật:

Bảo mật mức mạng: Bảo mật đường truyền, bảo mật các thông tin lưu truyền trên mạng. Được thực hiện bằng hình thức mã hóa thông tin trên đường truyền, các công cụ xác định tính toàn vẹn và xác thực của thông tin. Bảo mật lớp truy cập: Bảo mật truy cập của người dùng quay số (Dial-up): Tạo các kênh VPN cho các kết nối Dial-up...

Firewall/IDS: Tại các khu vực cung cấp các máy chủ truy cập cần bố trí các tường lửa kèm các bộ dò tìm tấn công IDS đảm bảo ngăn chặn các truy cập trái phép hay các dạng tấn công ngay từ cổng vào mạng. Bảo mật thiết bị và máy chủ: Các thiết bị mạng như Router, Switch, Firewall là các điểm nút mạng hết sức quan trọng và cần được bảo vệ.

Bảo mật ở Hệ điều hành và ứng dụng: Thường xuyên sao lưu, cập nhật các bản vá lỗi của hệ điều hành, sử dụng các phần mềm bổ sung (Patch) vá lỗ hổng trên các hệ điều hành, đảm bảo hệ thống làm việc ổn định.

Bảo mật mức Cơ sở dữ liệu: Có thể nói CSDL là lõi của toàn bộ hệ thống bảo mật thông tin, toàn bộ thông tin quan trọng mang tính chất sống còn được tập trung trên các CSDL, trong thiết kế CSDL được đặt ở mức ưu tiên cao nhất.

7.4 An toàn khi xảy ra sự cố:

Với đường kết nối ra Internet: Ta thuê cả hai đường Leased Line 1.2Mbps và đường ADSL 8Mbps, đường kết nối chính là đường Leased Line và sử dụng cơ chế Load Balancing nhằm chia tải của đường Leased Line qua đường ADSL khi đường Leased Line bị quá tải hay gặp sự cố.

Với các thiết bị kết nối ra Internet: Phải có cơ chế dự phòng, lúc bình thường thì mọi kết nối diễn ra theo đường chính, khi một thiết bị trong đường kết nối chính gặp sự cố (chẳng hạn như Router) thì lập tức phải chuyển sang đường dự phòng, cơ chế này có thể thực hiện được bằng cách cài đặt thông số Priority cho thiết bị, thiết bị nào có Priority lớn hơn sẽ là thiết bị cho đường chính và khi thiết bị trong đường chính bị sự cố thì lập tức hệ thống sẽ sử dụng thiết bị của đường dự phòng đảm bảo cho kết nối được thông suốt.

Với miền DMZ: Cần có Backup Server cho các Server Web, Mail, Database... và phải sao lưu dữ liệu thường xuyên để khi xảy ra sự cố dữ liệu trên các Server thì ta sẽ không bị mất dữ liệu đảm bảo cho hệ thống mạng hoạt động bình thường.

Với phân hệ mạng nội bộ, việc sử dụng các Switch có cơ chế Spanning Tree giúp chúng ta tạo ra các đường kết nối dự phòng mà không bị lặp, nhằm đảm bảo khi Switchchings bị sự cố thì Switch dự phòng sẽ hoạt động và không làm cho hoạt động của ngân hàng bị gián đoạn.

Tổ chức một phòng kỹ thuật chuyên về hệ thống mạng để giải quyết các vấn đề khi hệ thống mạng xảy ra sự cố.

8 Nâng cấp hệ thống

Hệ thống mạng được xây dựng phải đảm bảo cho việc nâng cấp dễ dàng khi cần thiết, chẳng hạn như ngân hàng tăng thêm nhân sự, số lượng chi nhánh cũng như đối tác tăng lên, các server được truy cập nhiều hơn...

Do đó trong thiết kế ta cũng đã tính đến các vấn đề này. Hiện tại giả sử số nhân viên là khoảng 100 người giả sử được chia đều trên các tầng thì mỗi tầng có khoảng 14 người, ta bố trí mỗi tầng 1 switch 24 port tức là có thể đáp ứng cho mỗi tầng là 24 người, vì vậy khi có thêm nhân viên thì ta cũng không cần phải thiết kế lại hay mua thêm switch.

Đối với vấn đề băng thông ta cũng đã tính đến hệ số an toàn là 20% nhằm đảm bảo hệ thống hoạt động ổn định và khi có nhu cầu tăng băng thông thì chỉ cần đăng ký thay đổi gói cước với nhà cung cấp dịch vụ (ISP).

Việc sử dụng các thiết bị mạng của Cisco - công ty hàng đầu về thiết bị mạng giúp cho ta được hỗ trợ kỹ thuật tốt hơn, thiết bị ổn định hơn và nhất là trong các sản phẩm của Cisco thường được tích hợp sẵn các công nghệ mới, phù hợp với yêu cầu sử dụng...