Trường Đại Học Bách Khoa Thành Phố Hồ Chí Minh
Khoa Khoa Học & Kỹ Thuật Máy Tính
Bộ Môn: Hệ Thống & Mạng Máy Tính
Mạng Máy Tính 2

EBOOKBKMT.COM

HỖ TRỢ TÀI LIỆU HỌC TẬP

Báo Cáo Bài Tập Lớn

Thiết Kế Mạng Máy Tính Cho Building Ngân Hàng

GVHD: **Nguyễn Anh Thư**

SVTH:

1. Lê Chí Hiếu	**50600682**
2. Phạm Văn Điền	**50802744**
3. Hồ Đặng Duy Hải	**50700658**

TP. Hồ Chí Minh 12/2011

Mục lục:

1. Yêu cầu kiến trúc hệ thống:

Mạng máy tính dùng trong trụ sở của một ngân hàng BBB(B Bank Building) chuẩn bị xây mới tại TP.HCM. Các thông số quan trọng của việc sử dụng CNTT trong ngân hàng này là:

- Tòa building tại trụ sở cao khoảng 2 tầng, tầng 1 được trang bị 1 phòng kỹ thuật mạng và Cabling Central Local (Phòng tập trung dây mạng và patch panel).
- Ngân hàng dạng Small Enterpirise, bao gồm: 100 workstations, 3 servers, 20 network equipment.
- Dùng công nghệ mới về hạ tầng mạng, 100/1000MBps, sử dụng công nghệ mạng dây và mạng không dây.
- Dùng kết hợp giữa Licensed và Open source Softwares.
- Kết nối với bên ngoài bằng Leased line và ADSL.
- 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 như Nha Trang và Đà Nẵng. Mỗi chi nhánh cũng được thiết kế tương tự như trụ sở nhưng quy mô nhỏ hơn:

- Tòa nhà cao khoảng 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.

2. Thiết kế hệ thống

2.1. Cấu trúc hạ tầng mạng trụ sở ngân hàng:

Tìm hiểu cấu trúc mạng liên quan đến tòa nhà:
Cấu trúc bảo mật mạng dự kiến xây dựng sẽ dựa trên cấu trúc mạng bao gồm các phần sau:

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 mạngInternet, cho phép mở rộng và nâng cấp tốc độ cổng kết nối Internet tuỳ theo nhu cầu phát triển. Người dùng truy nhập vào mạng được xác thực tuỳ theo quyền truy nhập để vào mạng nội bộhoặc Internet và CSDL dùng để xác thực được quản lý tập trung trên máy chủ ACS đặt ở vùngquản trị hệ thống.

Phân hệ mạng DMZ
Gồm hệ thống máy chủ Web, E-mail, dành cho khách hàng, nội bộ truy nhập, trên máychủ 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, các hệ thống đào tạo, dạyhọc 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 kiển 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 mail...

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 dovậy khu vực này cần được đảm bảo mức độ an ninh bảo mật cao.

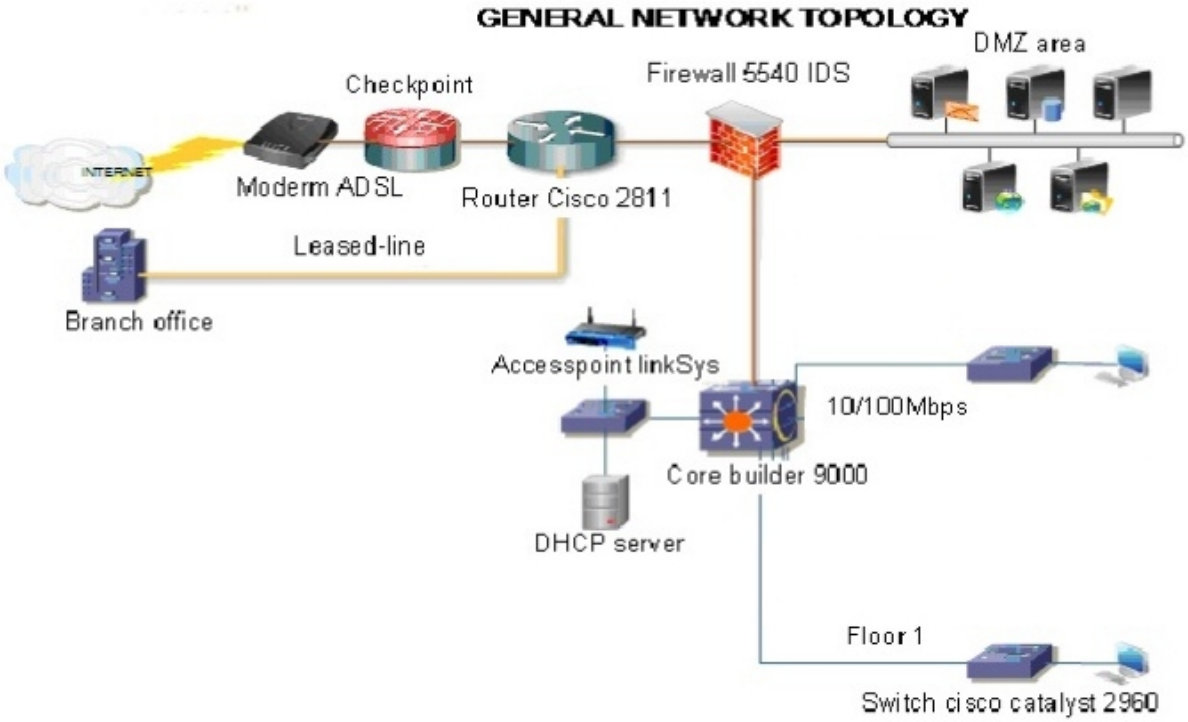
Phân hệ quản trị mạng
Bao gồm các máy chủ quản trị an ninh, máy chủ xác thực , máy chủ quét các dịch vụ trênmạng (IDS)

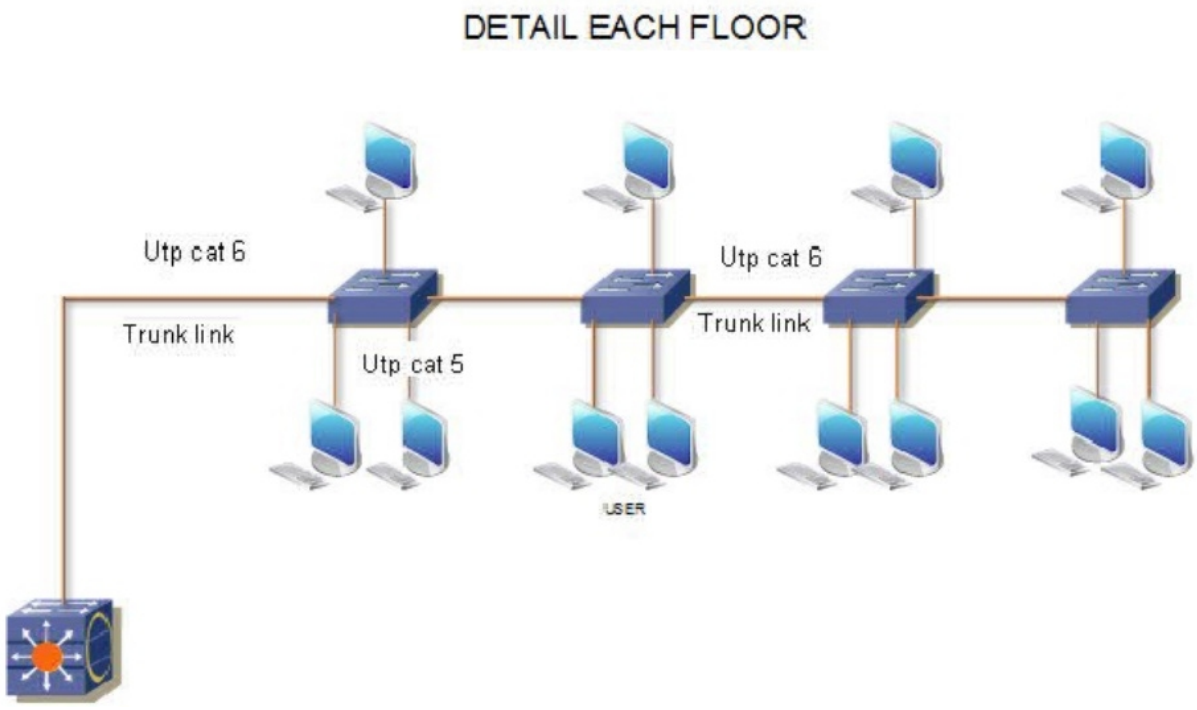
Phân hệ kết nối ra bên ngoài (EXTRANET)
Dành cho các kết nối từ các đơn vị bên ngoài hoặc bên ngoài truy cập vào mạng của Ngânhàng

Phân hệ máy chủ CSDL
Các máy chủ ứng dụng chứa các CSDL chính, hết sức quan trọng do vậy khu vực này cầnđược đảm bảo mức độ an ninh bảo mật cao nhất.

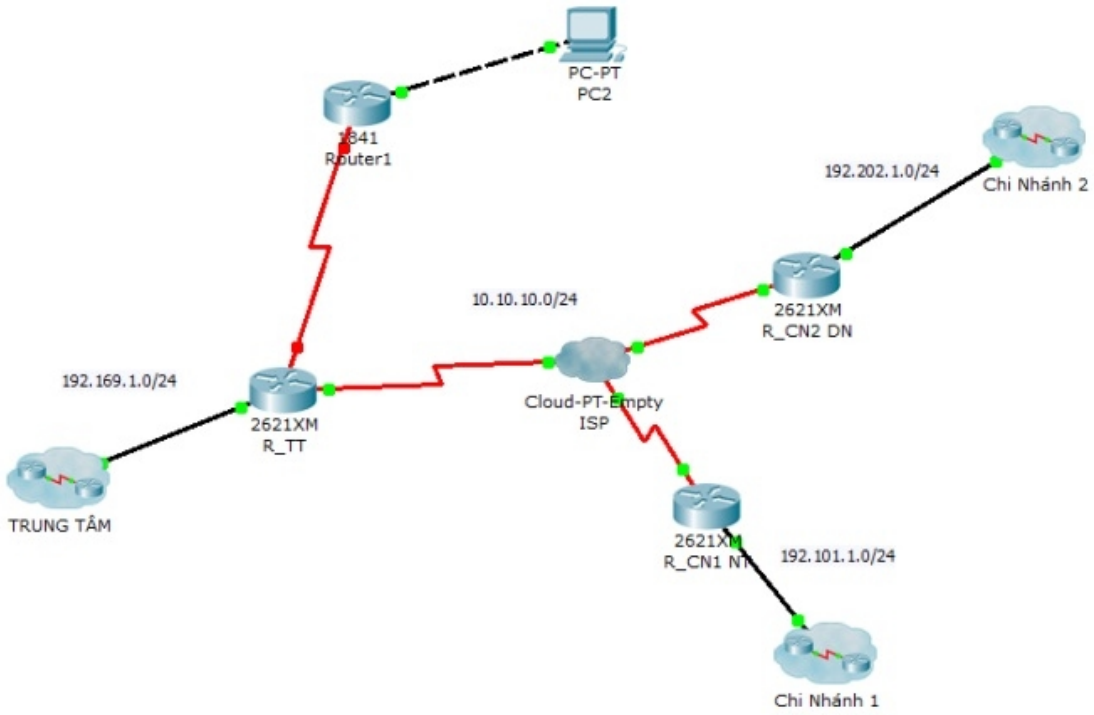
Phân hệ kết nối WAN của ngân hàng
Phần kết nối vào cổng Gateway Firewall, nhằm bảo vệ các giao dịch từ bên ngoài vào.

Sơ đồ thiết kế được mô tả theo sơ đồ dưới đây:


GENERAL NETWORK TOPOLOGY
DMZ area
Checkpoint
Firewall 5540 IDS
INTERNET
Moderm ADSL
Router Cisco 2811
Leased-line
Branch office
Accesspoint linkSys
10/100Mbps
Core builder 9000
DHCP server
Floor 1
Switch cisco catalyst 2960


DETAIL EACH FLOOR
Utp cat 6
Trunk link
Utp cat 5
Utp cat 6
Trunk link
USER

Kết nối giữa Trụ sở và chi nhánh:



2.2. Mô hình:

- Hệ thống sử dụng 1 router chính dùng 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 đề 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.

2.2.1 Sơ đồ chia địa chỉ IP trong mỗi VLAN

Sơ đồ VLAN tại trụ sở được chia bởi bảng IP sau:

VLAN	Phòng Ban	Địa chỉ IP danh định	Chi tiết - Miền cung cấp IP
VLAN1	Phòng Server	192.168.9.0/24	192.168.9.1 ->192.168.9.254
VLAN2	Giám Đốc	192.168.10.0/24	192.168.10.1->192.168.10.254
VLAN3	Phòng Hành Chính	192.168.13.0/24	192.168.13.1->192.168.13.254
VLAN4	Phòng Marketing	192.168.15.0/24	192.168.15.1->192.168.15.254
VLAN5	Phòng Quản Lý Nhân Sự	192.168.14.0/24	192.168.14.1->192.168.14.254
VLAN6	Tài Chính & Kế Toán	192.168.17.0/24	192.168.17.1->192.168.17.254
VLAN7	Quản Lý Rủi Ro	192.168.18.0/24	192.168.18.1->192.168.18.254
VLAN8	Quản Lý Vốn & Kinh Doanh	192.168.19.0/24	192.168.19.1->192.168.19.254
VLAN9	Quan Hệ Khách Hàng	192.168.21.0/24	192.168.21.1->192.168.21.254
VLAN10	Phòng Tác Nghiệp	192.168.20.0/24	192.168.20.1->192.168.20.254

Sơ đồ VLAN tại chi nhánh 1 được chia bởi bảng IP sau:

VLAN	Phòng Ban	Địa chỉ IP danh định	Chi tiết - Miền cung cấp IP
VLAN1	Phòng Server	192.100.2.0/24	192.100.2.1 ->192.100.2.254
VLAN2	Giám Đốc	192.100.6.0/24	192.100.6.1->192.100.6.254
VLAN3	Phòng Hành Chính	192.100.8.0/24	192.100.8.1->192.100.8.254
VLAN4	Phòng Quản Lý Nhân Sự	192.100.4.0/24	192.100.4.1->192.100.4.254
VLAN5	Tài Chính & Kế Toán	192.100.9.0/24	192.100.9.1->192.100.9.254
VLAN6	Quan Hệ Khách Hàng	192.100.11.0/24	192.100.11.1->192.100.11.254

Sơ đồ VLAN tại chi nhánh 2 được chia bởi bảng IP sau:

VLAN	Phòng Ban	Địa chỉ IP danh định	Chi tiết - Miền cung cấp IP
VLAN1	Phòng Server	192.200.2.0/24	192.200.2.1->192.200.2.254
VLAN2	Giám Đốc	192.200.6.0/24	192.200.6.1->192.200.6.254
VLAN3	Phòng Hành Chính	192.200.8.0/24	192.200.8.1->192.200.8.254
VLAN4	Phòng Quản Lý Nhân Sự	192.200.4.0/24	192.200.4.1->192.200.4.254
VLAN5	Tài Chính & Kế Toán	192.200.9.0/24	192.200.9.1->192.200.9.254
VLAN6	Quan Hệ Khách Hàng	192.200.11.0/24	192.200.11.1->192.200.11.254

2.3. Danh sách các thiết bị cần thiết.

2.3.1. Các server:

Trong một ngân hàng thiết yếu phải có các server sau:

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.

DNS server: Dịch tên miền ra địa chỉ IP.

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.

2.3.2. Hệ thống máy tính trên các tầng:

Số lượng máy của tòa nhà là khoảng 100 máy giả sử được phân bốđều trên 2 tầng, như vậy ta ước lượng mỗi tầng có khoảng 50 máy, do đó ta sử dụng mỗi tầng 4 switch Cisco Catalyst 2960(mỗi switchcó 24 port), và được kết nối đến core-switch Builder 9000, và hệ thống máy tính cho ngân hàng được đặt trên một interface khác củafirewall.

2.3.3. Core-switch:

Là một switch layer 2 nhưng có tốc độ cao dùng để kết nối cácswitch trên các tầng lại với nhau. Ta chọn Core Builder 9000.

2.3.4. Firewall:

Để đảm bảo tính bảo mật thông tin thì việc xây dựng một firewall là vấn đề thiết yếu, nhất là đối với ngân hàng. Ta chọn firewall 5540 IDS..

2.3.5. Router:

Một thiết bị không thể thiếu đối với bất kỳ một hệ thống mạng nào muốn kết nối ra ngoài, ta chọn router cisco 3662 và router 2650XM.

2.3.6.Checkpoint :

Ngăn chặn một số dịch vụ và hạn chế sự tấn công từ bên ngoài vàoDMZ , khi bên ngoài kết nối với các Vlan, ở đây ta sử dụng PIX51

2.3.7. Access-point:

Ngân hàng cung cấp dịch vụ truy cập mạng không dâyđể khách có thể truy cập khi đến giao dịch ở ngân hàng.

3. Tính toán throughput,bandwidth và các thông số an toàn

Throughput: Là lượng thông tin truyền qua một mạng trong một đơn vị thời gian.
Bandwidth: Là lượng thông tin có thể truyền qua một mạng trong một đơn vị thời gian.

Có thể hiểu một cách hình tượng thì bandwidth giống như là một đường ống có thể cho một lượng thông tin tối đa có thể chạy qua trên một đơn vị thời gian, còn throughput là lượng thông tin thực tế chạy qua đường ống đótrong một đơn vị thời gian.Việc xác định throughput và bandwidth trong một mạng là rất quan trọng bởivì nó giúp cho người quản trị mạng xác định được cần thuê đường truyền như thế nào để cho mạng vừa chạy ổn định lại vừa tiết kiệm được chi phí cho việc thuê đường truyền. Các dịch vụ sử dụng như:

- Gửi và nhận mail.
- Duyệt web.
- Cung cấp dịch vụ web server để bên ngoài truy cập.
- Cập nhật cơ sở dữ liệu với các trụ sở khác.

3.1. Tại trụ sở chính:
3.1.1. Mạng có dây:
3 Server: Tổng dung lượng upload và download 500MB/ngày.
Giờ cao điểm:
Sáng: 9h – 11h (thời lượng 2 tiếng)
Chiều: 15h – 16h (thời lượng 1 tiếng)
Giờ cao điểm trao đổi 80% dữ liệu trong ngày:
-> Bandwith = 3 x 500 x 0.8/(3 x 3600) = 0.111 MB/s
-> Thourghput = 3 x 500 / (8x 3600) = 0.052 MB/s

100 Workstations: Tổng dung lượng upload và down load 100MB/ngày.
Giờ cao điểm:
Sáng: 9h – 11h (thời lượng 2 tiếng)
Chiều: 15h – 16h (thời lượng 1 tiếng)
Giờ cao điểm trao đổi 80% dữ liệu trong ngày:
-> Bandwith = 100 x 100 x 0.8/(3 x 3600) = 0.74 MB/s
-> Thourghput = 100 x 100 / (8x 3600) = 0.35 MB/s

Tổng Thourghput = 0.052 + 0.35 = 0.4MB/s =3.2Mb/s.
Tổng Bandwith = 0.111 + 0.74 = 0.851 MB/s = 6.8Mb/s

3.1.2. Hệ thống mạng không dây:
Lượng dữ liệu trao đổi mỗi laptop trong 1 ngày vào khoảng 50MB
Giờ cao điểm:
Sáng: 9h – 11h (thời lượng 2 tiếng)
Chiều: 15h – 16h (thời lượng 1 tiếng)
Giờ cao điểm mỗi laptop trao đổi 80% dữ liệu trong ngày.
Số lượt khách hàng trong 1 ngày vào khoảng 200 lượt.
Số lượt khách hàng vào lúc cao điểm vào khoảng 80 lượt.
-> Throughput = 200 x 50 /(8 x 3600) = 0.35MB/s = 2.8Mb/s.
->Bandwidth = 80 x 50 x 0.8/(3 x 3600) = 0.3MB/s = 2.4Mb/s

3.2. Tại Chi nhánh:

3.2.1. Mạng có dây:

3 Server: Tổng dung lượng upload và download 500MB/ngày.
Giờ cao điểm:
Sáng: 9h – 11h (thời lượng 2 tiếng)
Chiều: 15h – 16h (thời lượng 1 tiếng)
Giờ cao điểm trao đổi 80% dữ liệu trong ngày:
-> Bandwith = 3 x 500 x 0.8/(3 x 3600) = 0.111 MB/s
-> Thourghput = 3 x 500 / (8x 3600) = 0.052 MB/s

50 Workstations: Tổng dung lượng upload và down load 100MB/ngày.
Giờ cao điểm:
Sáng: 9h – 11h (thời lượng 2 tiếng)
Chiều: 15h – 16h (thời lượng 1 tiếng)
Giờ cao điểm trao đổi 80% dữ liệu trong ngày:
-> Bandwith = 50 x 100 x 0.8/(3 x 3600) = 0.37 MB/s
-> Thourghput = 50 x 100 / (8x 3600) = 0.175 MB/s

Tổng Thourghput = 0.052 + 0.175 = 0.227MB/s = 1.816Mb/s
Tổng Bandwith = 0.111 + 0.37 = 0.481MB/s = 3.848 Mb/s

3.2.2. Hệ thống mạng không dây:

Lượng dữ liệu trao đổi mỗi laptop trong 1 ngày vào khoảng 50MB
Giờ cao điểm:
Sáng: 9h – 11h (thời lượng 2 tiếng)
Chiều: 15h – 16h (thời lượng 1 tiếng)
Giờ cao điểm mỗi laptop trao đổi 80% dữ liệu trong ngày.
Số lượt khách hàng trong 1 ngày vào khoảng 100 lượt.
Số lượt khách hàng vào lúc cao điểm vào khoảng 50 lượt.
Throughput = 100 x 50 /(8 x 3600)= 0.087MB/s = 0.7Mb/s.
Bandwidth = 50 x 50 x 0.8/(3 x 3600) = 0.185MB/s = 1.48Mb/s.

Việc tính throughput và bandwidth như vậy ta đã tính toán mức đáp ứng ở giờ cao điểm thì mạng vẫn hoạt động tốt.

4. Dùng kết hợp giữa Priopriety và Open source Softwares

Opensource software hiểu theo nghĩa rộng là một khái niệm chung được sử dụng cho tất cả các phần mềm mà mã nguồn của nó được công bố rộng rãi công khai và cho phép mọi người tiếp tục phát triển phần mềm đó. Mã nguồn mở được công bố dưới rất nhiều điều kiện khác nhau, một số trongđó cho phép phát triển, sử dụng và bán tùy ý miễn là giữ nguyên các dòng về nguồngốc sản phẩm, một số bắt buộc tất cả các sản phẩm làm ra từ đó cũng phải là open-source, một số khác đòi hỏi phải công bố trọn vẹn mã nguồn, một số khác khôngcho phép sử dụng vào mục đích thương mại, một số khác lại không có ràng buộc gì đáng kể v.v.

Một số Open source software phổ biến nhất hiện nay:

- Hệ điều hành Linux: Hệ điều hành mã nguồn mở bao gồm nhiều phiên bản như: Ubuntu, Fedora, Redhat...

- Phần mềm văn phòng OpenOffice: Bộ phần mềm văn phòng có các tính năng tương tự như Microsoft Office nhưng xây dựng từ mã nguồn mở, có thể hoạt động trên nhiều hệ điều hành khác nhau, các phiên bản của hệ điều hành Linux hay tích hợp sẵn OpenOffice cho người sử dụng.

- Trình duyệt Mozilla Firefox: Trình duyệt Firefox là một sản phẩm miễn phí và mã nguồn mở của hãng Mozilla. Firefox có khả năng chạy trên nhiều hệ điều hành, có kích thước nhỏ gọn, tốc độ cao và rất dễ sử dụng, nó đang là đối thủ cạnh tranh trực tiếp với Internet Explorer của Microsoft và ngày càng được nhiều người sử dụng.

- Unikey: Phần mềm gõ tiếng Việt thông dụng nhất ở Việt Nam hiện nay, có thể chạy trên nhiều hệ điều hành, trong Windows nó là Unikey, trong Linux nó là X-Unikey.

Việc sử dụng phần mềm trong hệ thống ngân hàng tùy thuộc vào chức năngđặc thù của mỗi máy tính, vấn đề đặt ra ở đây là việc ưu tiên sử dụng Open sourceSoftwares và sự quen thuộc, dễ sử dụng của phần mềm đối với người sử dụng.

Hệ điều hành:
- Đối với các máy client ta sử dụng hệ điều hành windows XP vì nó đãquá quen thuộc và rất dễ sử dụng đối với người dùng.
- Đối với File server vì đặc thù của nó có chứa tài liệu của từng phòng ban, phòng ban này không được truy xuất vào cơ sở dữ liệu của phòng bankhác khi chưa được phép, do đó ta phải sử dụng cơ chế quản lý user và 12 group, trong việc quản lý user và group thì windows server có tính năng bảomật tốt hơn so với linux, nên ta sử dụng windows server 2k3 cho File server.
- Với các server khác được quản lý bởi các chuyên viên quản trị, vàcần tính năng bảo mật cao do đó có thể sử dụng hệ điều hành linux cho cácserver này.

Bộ phần mềm văn phòng:
Có thể lựa chọn Microsoft Office hoặc OpenOffice. Nhưng xét về sự phổ biến và dễ sử dụng thì nên chọn bộ phần mềm Microsoft Office.

Phần mềm gửi và nhận mail:
Trong hệ điều hành của Mifcrosoft đã tích hợp sẵn phần mềm Outlook cho người dùng gửi và nhận thư. Tuy nhiên có nhiều phần mềm có chức năng tương tự như Mozilla Thunderbird cũng là một lựa chọn tốt, mà quan trọng hơn nó là phần mềm Open source.

Trình duyệt web:
Internet Explorer (IE) được tích hợp sẵn trong Windows, nhưng Mizilla Firefox lại là trình duyệt web có nhiều tính năng ưu việt hơn, Firefox cũng là một phần mềm Open Source.

Web server:
Sử dụng bộ phần mềm tích hợp như WAMP server hỗ trợ cả Apache, Mysql, Php đây là bộ phần mềm mã nguồn mở tương đối tốt cho web server.

5. Bảo mật và an toàn khi xảy ra sự cố, nâng cấp hệ thống.

5.1. Yêu cầu đối với hệ thống:

Hoạt động của ngân hàng luôn có khối lượng thông tin xử lý trong hoạt động nghiệp vụ rất lớn. Tuy nhiên không phải ai cũng có quyền truy cập những kho thông tin này. Do đó ngân hàng có nhu cầu xây dựng một hệ thống bảo mật cho mạng tin học phục vụ điều hành, kinh doanh. Hệ thống bảo mật này phải đảm bảo:

- An toàn cho toàn bộ thông tin trên mạng, chống lại mọi sự truy cập bất hợp pháp vào mạng.

- Kiểm soát được việc truy cập của người sử dụng.

- Bảo đảm an toàn dữ liệu truyền, nhận qua các dịch vụ đường truyền ra internet.

- Chi phí phù hợp với dự trù kinh phí của ngân hàng.

- Đáp ứng được khả năng mở rộng của mạng ngân hàng trong tương lai.

5.2. 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...

5.3. Xác định các mối đe dọa tới hệ thống:

5.3.1. 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 đẻ 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.

5.3.2. 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 sẻ 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.

5.4. 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) bịt 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.

5.5. An toàn khi xảy ra sự cố:

- Với đường kết nối ra internet: Ta thuê cả hai đường leased-line 1.2Mps 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 set 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 backup 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 loop, nhằm đảm bảo khi switchchinhs 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.

5.6. Nâng cấp hệ thống:

Hệ thống mạng được xây dựng phải đảm bảo cho việc nâng cấpdễ dàng khi cần thiết, chẳng hạn như ngân hàng tăng thêm nhân sự, số lương chi nhánh cũng như đối tác tăng lên, các server được truy cậpnhiều 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 50 người, ta bố trí mỗi tầng 4 switch 24 port tứclà có thể đáp ứng cho mỗi tầng là 96 người, vì vậy khi có thêm nhânviên 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% nhằmđảm bảo hệ thống hoạt động ổn định và khi có nhu cầu tăng băng thông thì chỉ cần đăng kí thay đổi gói cước với nhà cung cấp dịchvụ(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 ổnđịnh 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…

6. Mô phỏng bằng phần mềm.

6.1. Phần mềm sử dụng:

- Sử dụng phần mềm mô phỏng Packet Tracer.

- File mô phỏng assigment.pkt được đính kèm.

6.2. Các bước thực hiện:

- Giả lập mô hình kết nối trị sở và các chi nhánh.

- Giả lập mô hình các phòng ban.

- Tiến hành chia Vlan trong trụ sở và các chi nhánh.

- Tiến hành cấu hình DHCP tại core router để cấp phát IP cho các máy ở trụ sở và chi nhánh

- Giả lập mạng internet để mô phỏng kết nối giữa trụ sở và chi nhánh.

- Tiến hành Routing mô hình giả lập.

- Tiến hành cấu hình NAT để kết nối internet.

- Tiến hành kiểm tra bằng cách ping, tracerouter và chế độ simulation có sẵn.