

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



MẠNG MÁY TÍNH (CO3003)

Bài tập lớn 2

COMPUTER NETWORK DESIGN FOR BUILDING OF THE BANK

GV ra đề và HD: Bùi Xuân Giang

Nhóm SV thực hiện :

Phan Anh Tú - 1915822 (Nhóm trưởng)

Huỳnh Tuấn Đạt - 1913026

Trần Quốc Việt - 1915919

Nguyễn Văn Quốc - 1914864

Nguyễn Việt Đức - 1913167

Thành phố Hồ Chí Minh, 11/2021

Mục lục

1	Cấu trúc mạng cho các tòa nhà	2
1.1	Yêu cầu kiến trúc hệ thống	2
1.2	Phân tích yêu cầu hệ thống thiết kế mạng	2
1.3	Lựa chọn thiết kế cấu trúc mạng thích hợp	3
1.3.1	Về cấu trúc bảo mật	3
1.3.2	Về các phần mềm được sử dụng	4
1.3.3	Về mô hình sử dụng cho web server	4
1.4	Tổng quan về hệ thống cấu trúc mạng	4
2	Danh sách các trang thiết bị có trong hệ thống	5
2.1	Danh sách các thiết bị	5
2.1.1	Danh sách các server	5
2.1.2	Danh sách các thiết bị	5
2.2	Sơ đồ mạng WAN	6
3	Tính toán thông năng, băng thông, và các thông số an toàn của Mạng máy tính	7
3.1	Tại trụ sở chính	7
3.1.1	Đối với mạng dây	7
3.1.2	Đối với mạng không dây	7
3.2	Tại chi nhánh	8
3.2.1	Đối với mạng dây	8
3.2.2	Đối với mạng không dây	8
4	Thiết kế mạng máy tính sử dụng Packet Tracer hoặc GNS3	9
4.1	Giới thiệu công cụ được sử dụng	9
4.2	Sơ đồ luận lý	9
4.2.1	Sơ đồ luận lý tại trụ sở chính	9
4.2.2	Sơ đồ luận lý tại 2 chi nhánh	10
5	Kiểm thử hệ thống	11
6	Đánh giá lại hệ thống đã thiết kế	15
6.1	Yêu cầu đối với hệ thống	15
6.2	Xác định các tài nguyên được bảo vệ	16
6.3	Các mối đe dọa đối với hệ thống	16
6.4	An toàn khi xảy ra sự cố	16
6.5	An toàn khi xảy ra sự cố	17
6.6	Nâng cấp hệ thống	17
6.7	Những hạn chế của dự án	18
6.8	Định hướng phát triển trong tương lai	18

1 Cấu trúc mạng cho các tòa nhà

1.1 Yêu cầu kiến trúc hệ thống

Ngân hàng BBB (B Bank Building) chuẩn bị xây dựng, gồm 1 trụ sở chính và 2 chi nhánh. Các thông số yêu cầu quan trọng của việc sử dụng CNTT và lắp đặt mạng ở trụ sở chính là:

- Tòa nhà cao khoảng 7 tầng, tầng 1 được trang bị 1 phòng kỹ thuật Mạng và Cabling Central Local (Phòng tập trung dây mạng và patch panels).
- BBB dạng Small Enterprise: 100 workstations, 5 Servers, 10 Network devices.
- Dùng công nghệ mới (new technology) về hạ tầng mạng, 100/1000 Mbps và wireless.
- Tổ chức hệ thống mạng theo cấu trúc VLAN.
- Dùng kết hợp giữa Licensed và Open source softwares.
- Kết nối với bên ngoài bằng 2 Leased line và 1 ADSL, dùng 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.

Các thông số yêu cầu quan trọng của việc sử dụng CNTT và lắp đặt mạng ở 2 chi nhánh (Nha Trang và Đà Nẵng) là:

- Tòa nhà cao khoảng 2 tầng, tầng 1 được trang bị 1 phòng kỹ thuật Mạng và Cabling Central Local.
- BBB dạng chi nhánh: 50 workstations, 3 Servers, 5 Network Equipments.

1.2 Phân tích yêu cầu hệ thống thiết kế mạng

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 chính và Chi nhánh như sau:

- Servers dùng cho máy chủ updates, truy cập web, truy cập database,... 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.
- Wifi để kết nối laptop dùng cho khách hàng sử dụng khoảng 50 MB/ngày.

Hệ thống Mạng máy tính của Ngân hàng BBB được ước tính tăng trưởng 20% sau 5 năm (về số lượng người sử dụng, tải trọng mạng, số lượng chi nhánh,...). Việc thực hiện kết nối giữa trụ sở chính và 2 chi nhánh với nhau thông qua đường links WAN. Có 2 loại đó là:

- **Leased line** (kênh truyền riêng) 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 tải lớn. Đường truyền này có thể đáp ứng từ 128Kbps đến hàng chục Gbps.
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. Có độ an toàn bảo mật cao, độ trễ thấp, tích hợp đa dịch vụ, cung cấp kết nối giữa các mạng WAN – LAN.
Nhược điểm: giá thành còn khá cao.

- **ADSL** là một dạng của DSL.[1] ADSL cung cấp một phương thức truyền dữ liệu với băng thông rộng, tốc độ cao hơn nhiều so với giao thức truy cập qua đường dây điện thoại truyền thống theo phương thức truy cập quay số (Dial up). Khi truyền băng thông trên đường dây điện thoại được tách ra làm 2 phần, một phần nhỏ dùng cho các tín hiệu như Phone, Fax. Phần lớn còn lại dùng cho truyền tải tín hiệu ADSL.

Ưu điểm: Giá thành rẻ, phù hợp để sử dụng ở những công ty có quy mô nhỏ.

Nhược điểm: ADSL là đường kết nối dung chung, nên tình bao mật không cao. Mặt khác ADSL càng nhiều người dùng thì tốc độ càng chậm. Do đó, ta sẽ sử dụng 2 leased – line để nối từ trụ sở chính đến mỗi chi nhánh. Với 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. Và 1 đường ADSL để kết nối 2 chi nhánh với nhau.

Do đó, ta sẽ sử dụng 2 leased – line để nối từ trụ sở chính đến mỗi chi nhánh. Với 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. Và 1 đường ADSL để kết nối 2 chi nhánh với nhau.

1.3 Lựa chọn thiết kế cấu trúc mạng thích hợp

1.3.1 Về cấu trúc bảo mật

Việc tổ chức cấu trúc mạng của hệ thống ngân hàng cần phải tuyệt đối bảo mật. Vì thế tổ chức cấu trúc mạng theo mô hình mạng bảo mật có thể hạn chế được các tấn công từ bên trong và bên ngoài một cách hiệu quả. Cấu trúc bảo mật mạng dự kiến xây dựng sẽ bao gồm các phần chính 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 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, E-mail, 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 mail...

Ngoài ra cách phân chia vùng như trên, ta có thể kết hợp thêm những 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:** 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:** Phân kết nối vào cổng Gateway Firewall, nhằm bảo vệ các giao dịch từ bên ngoài vào.

1.3.2 Về các phần mềm được sử dụng

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 không 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.

Về 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 bên trong.

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.

Đối với 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.

1.3.3 Về mô hình sử dụng cho web server

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 đó.

1.4 Tổng quan về hệ thống cấu trúc mạng

- 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 Danh sách các trang thiết bị có trong hệ thống

2.1 Danh sách các thiết bị

2.1.1 Danh sách các server

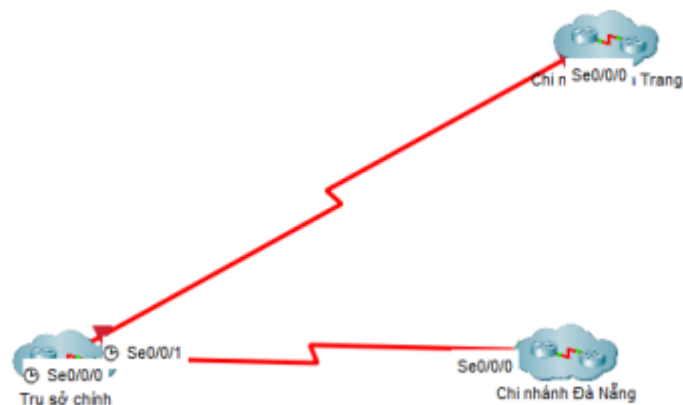
STT	Tên server	Chức năng
1	Web Server	Để những khách hàng bên ngoài truy cập vào để lấy thông tin về tài khoản của họ trong ngân hàng cũng như các dịch vụ khác.
2	Mail Server	Để gửi và nhận mail.
3	DNS Server	Dịch tên miền ra địa chỉ IP.
4	Database Server	Lưu trữ thông tin.

2.1.2 Danh sách các thiết bị

STT	Tên Thiết bị	Một số thông số kỹ thuật
1	Router CISCO 2911	RAM: 512MB/2GB, Bộ nhớ Flash: 256MB/8GB, Trọng lượng: 16.15kg, Kích thước: 43.8cm*30.5cm*8.9cm.
2	Switch POE 24 cổng HIKVISION DS3E0326P- E/M(B)	Switch mạng 24 cổng PoE 100M, 1 cổng uplink 1000M, 1 cổng SFP độc lập 10/100/1000M, Layer 2.

3	Cisco Wifi AIR-AP2802ES-K9	Số cổng kết nối: 24, công nghệ kết nối: 10/100/1000Base-T, công nghệ ethernet: Gigabit Ethernet.
4	Dây cáp mạng	

2.2 Sơ đồ mạng WAN



Hình 1: Sơ đồ mạng WAN.

3 Tính toán thông năng, băng thông, và các thông số an toàn của Mạng máy tính

- Throughput (Thông lượng): là lượng thông tin hữu ích được truyền đi trên mạng trong một đơn vị thời gian và chính thông lượng mới là chỉ số để đánh giá mạng nhanh hay chậm.
- Bandwidth (Băng thông): là thuật ngữ dùng để chỉ tốc độ truyền tải dữ liệu của đường truyền. Băng thông được đo bằng đơn vị bit/giây. Hiện nay, các mạng máy tính có tốc độ băng thông lên hàng triệu bit mỗi giây (Mbps) hay có khi lên tới hàng tỷ bit một giây (Gbps). Còn với website, bandwidth được dùng để chỉ số lượng dữ liệu tối đa mà người truy cập được phép trao đổi (upload và download) giữa website và máy tính 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 đó trong một đơn vị thời gian. Việc xác định throughput và bandwidth trong một mạng là rất quan trọng bởi vì 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 email, 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 Đối với mạng dây

- Servers: có 5 servers và tổng dung lượng upload và download 500 MB/ngày. Giờ cao điểm trao đổi 80% dữ liệu trong ngày:
 $\text{Bandwidth} = (5 \times 500 \times 0.8) / (3 \times 3600) = 0.185 \text{ MB/s}$
 $\text{Throughput} = (5 \times 500) / (8 \times 3600) = 0.087 \text{ MB/s}$ (thời gian làm việc 8h/ngày)
- Workstations: có 100 workstations và tổng dung lượng upload và download 100 MB/ngày. Giờ cao điểm mỗi laptop trao đổi 80% dữ liệu trong ngày.
 $\text{Bandwidth} = (100 \times 100 \times 0.8) / (3 \times 3600) = 0.741 \text{ MB/s}$ (giờ cao điểm 3h)
 $\text{Throughput} = (100 \times 100) / (8 \times 3600) = 0.347 \text{ MB/s}$ (thời gian làm việc 8h/ngày)
- Tổng:
 $\text{Bandwidth} = 0.185 + 0.741 = 0.926 \text{ MB/s} = 7.408 \text{ Mb/s}$

3.1.2 Đối với mạng không dây

Máy laptop kết nối WIFI dùng cho khách hàng truy xuất khoảng 50 MB/ngày.
Giờ cao điểm trao đổi 80% dữ liệu trong ngày
Số lượt khách hàng vào lúc cao điểm rơi vào khoảng 80 lượt.

Kết quả tính toán:

- $\text{Bandwidth} = (80 \times 50 \times 0.8) / (3 \times 3600) = 0.296 \text{ MB/s} = 2.37 \text{ Mb/s}$ (giờ cao điểm 3h).
- $\text{Throughput} = (170 \times 100) / (8 \times 3600) = 0.278 \text{ MB/s} = 2.222 \text{ Mb/s}$ (Giờ làm việc 8h/ngày).

3.2 Tại chi nhánh

3.2.1 Đối với mạng dây

- Servers: có 3 servers và tổng dung lượng upload và download 500 MB/ngày. Giờ cao điểm trao đổi 80% dữ liệu trong ngày:
 $\text{Bandwidth} = (3 \times 500 \times 0.8) / (3 \times 3600) = 0.111 \text{ MB/s}$ (giờ cao điểm 3h).
 $\text{Throughput} = (3 \times 500) / (8 \times 3600) = 0.052 \text{ MB/s}$ (thời gian làm việc 8h/ngày).
- Workstations: có 50 workstations và tổng dung lượng upload và download 100 MB/ngày. Giờ cao điểm trao đổi 80% dữ liệu trong ngày:
 $\text{Bandwidth} = (50 \times 100 \times 0.8) / (3 \times 3600) = 0.370 \text{ MB/s}$ (giờ cao điểm 3h).
 $\text{Throughput} = (50 \times 100) / (3 \times 3600) = 0.174 \text{ MB/s}$ (thời gian làm việc 8h/ngày)
- Tổng:
 $\text{Bandwidth} = 0.111 + 0.370 = 0.481 \text{ MB/s} = 3.848 \text{ Mb/s}$.
 $\text{Throughput} = 0.052 + 0.174 = 0.226 \text{ MB/s} = 1.808 \text{ Mb/s}$

3.2.2 Đối với mạng không dây

Máy laptop kết nối WIFI dùng cho khách hàng truy xuất khoảng 50 MB/ngày.
Giờ cao điểm mỗi laptop trao đổi 80% dữ liệu trong ngày.
Số lượt khách hàng trong 1 ngày rơi vào khoảng 100 lượt.
Số lượt khách hàng vào lúc cao điểm rơi vào khoảng 60 lượt.

Kết quả tính toán:

- $\text{Bandwidth} = (60 \times 50 \times 0.8) / (3 \times 3600) = 0.222 \text{ MB/s} = 1.778 \text{ Mb/s}$
- $\text{Throughput} = (100 \times 50) / (8 \times 3600) = 0.174 \text{ MB/s} = 1.389 \text{ Mb/s}$

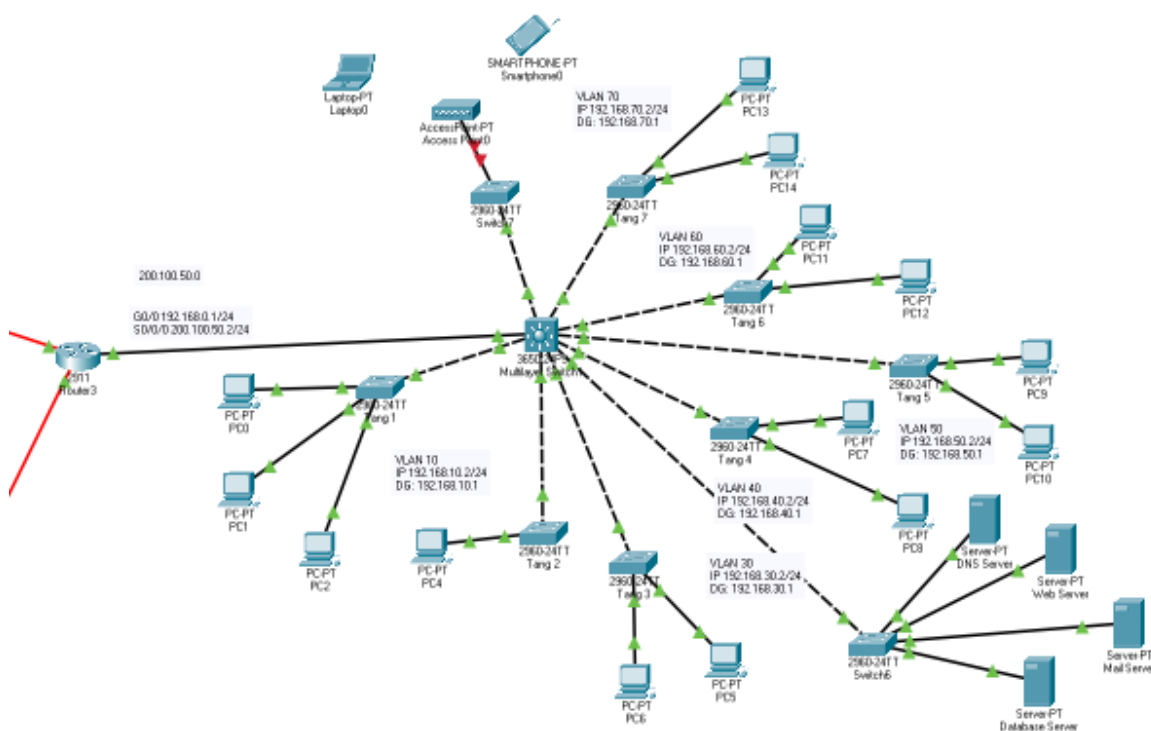
4 Thiết kế mạng máy tính sử dụng Packet Tracer hoặc GNS3

4.1 Giới thiệu công cụ được sử dụng

Sơ đồ mạng được thiết kế trên phần mềm Cisco Packet Tracer 7.3.1

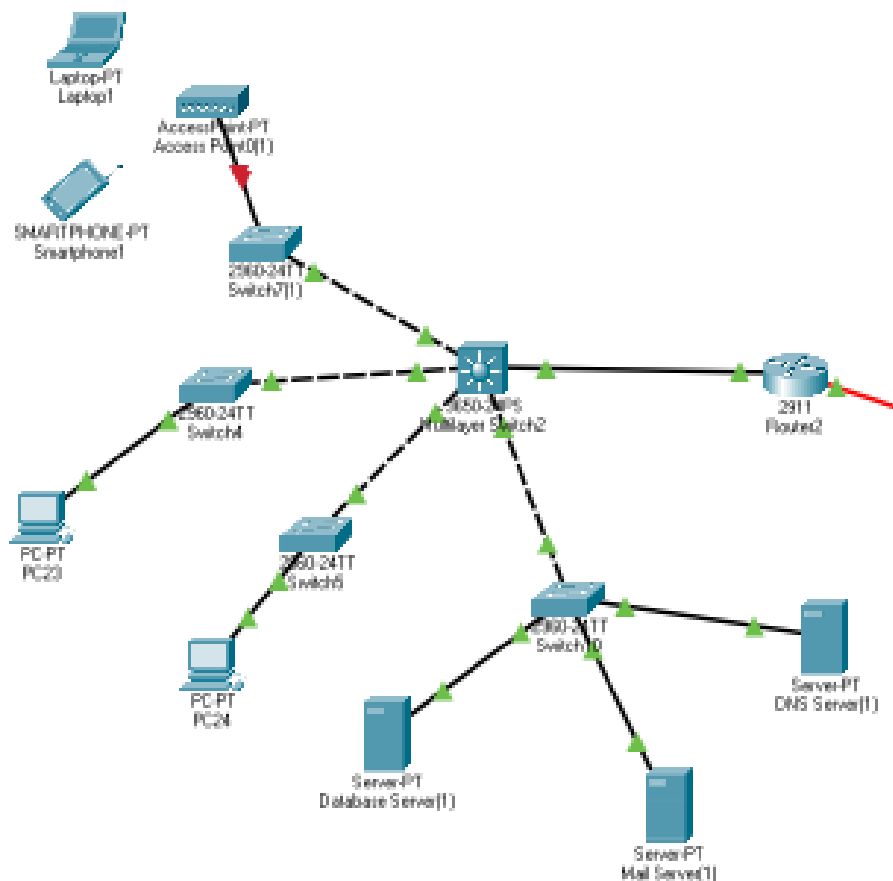
4.2 Sơ đồ luận lý

4.2.1 Sơ đồ luận lý tại trụ sở chính



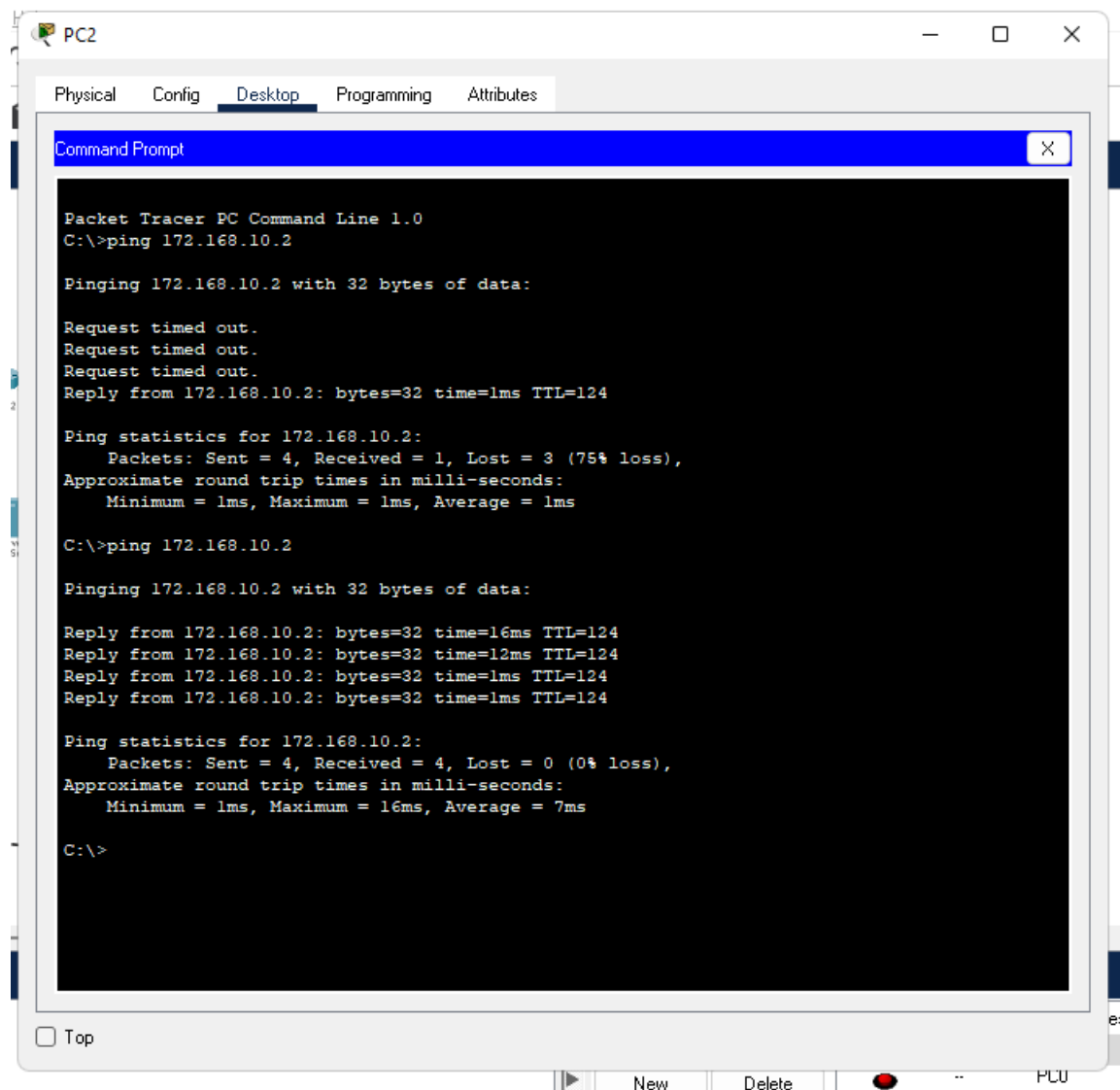
Hình 2: Sơ đồ luận lý tại trụ sở chính.

4.2.2 Sơ đồ luận lý tại 2 chi nhánh

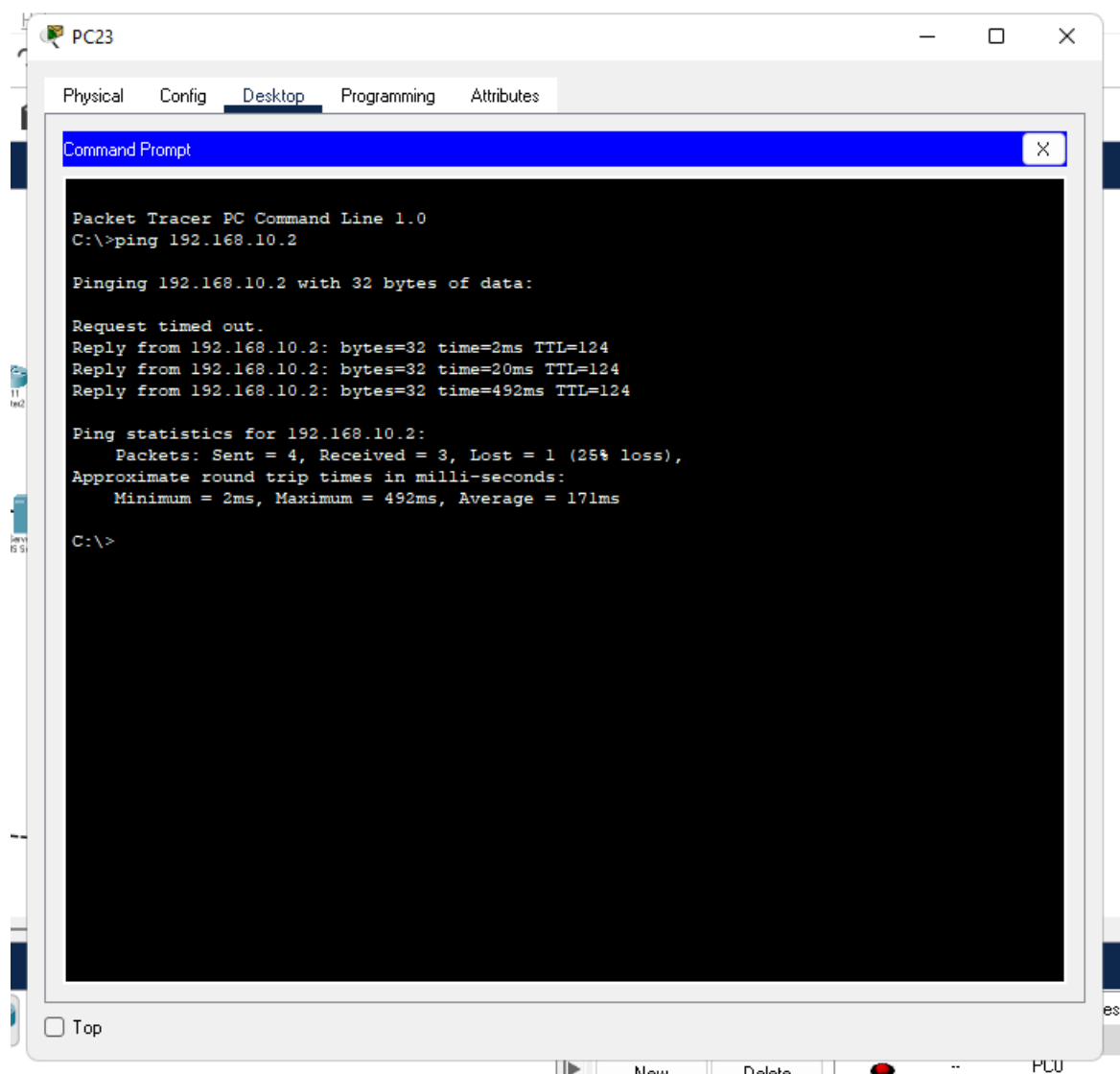


Hình 3: Sơ đồ luận lý tại 2 chi nhánh.

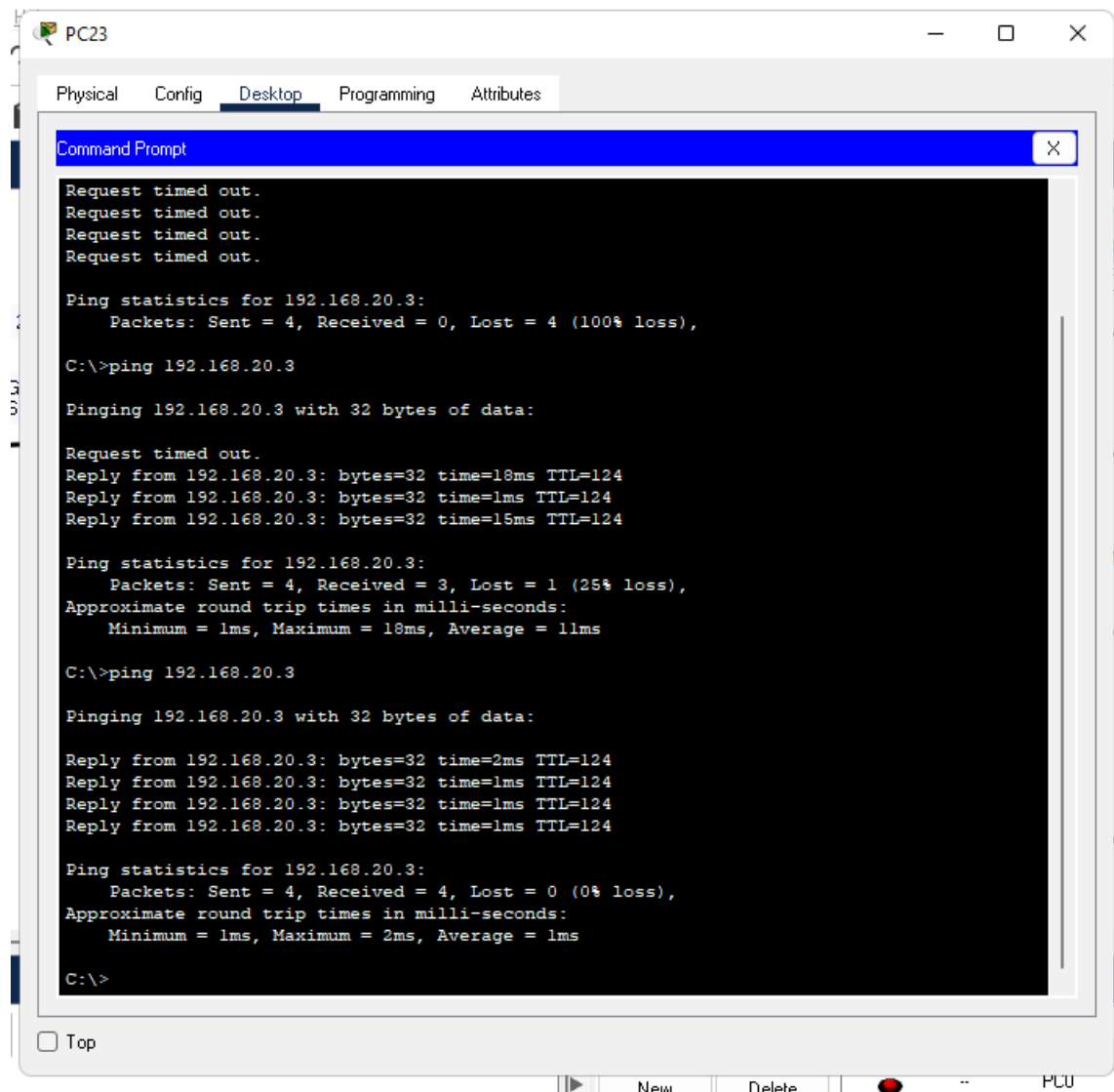
5 Kiểm thử hệ thống



Hình 4: Ping từ máy của trụ sở chính sang máy của chi nhánh.



Hình 5: Ping từ máy của chi nhánh sang máy của trụ sở chính tầng 1.



The screenshot shows a window titled "PC23" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a Command Prompt window. The Command Prompt shows the results of a ping command to 192.168.20.3. The first attempt shows a 100% loss of packets. The second attempt shows a 25% loss of packets. The third attempt shows a 0% loss of packets.

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.3: bytes=32 time=18ms TTL=124
Reply from 192.168.20.3: bytes=32 time=1ms TTL=124
Reply from 192.168.20.3: bytes=32 time=15ms TTL=124

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 18ms, Average = 11ms

C:\>ping 192.168.20.3

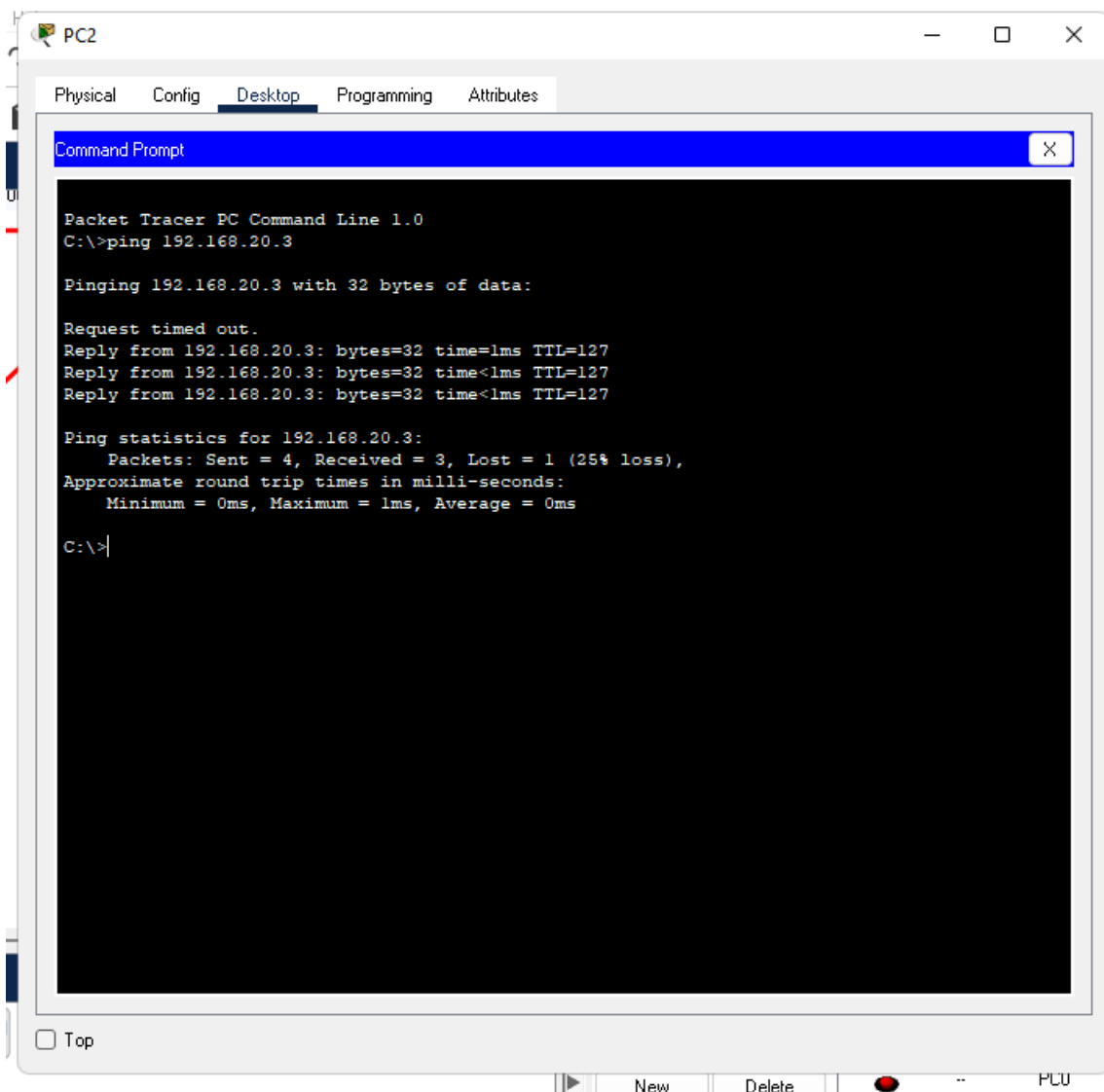
Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time=2ms TTL=124
Reply from 192.168.20.3: bytes=32 time=1ms TTL=124
Reply from 192.168.20.3: bytes=32 time=1ms TTL=124
Reply from 192.168.20.3: bytes=32 time=1ms TTL=124

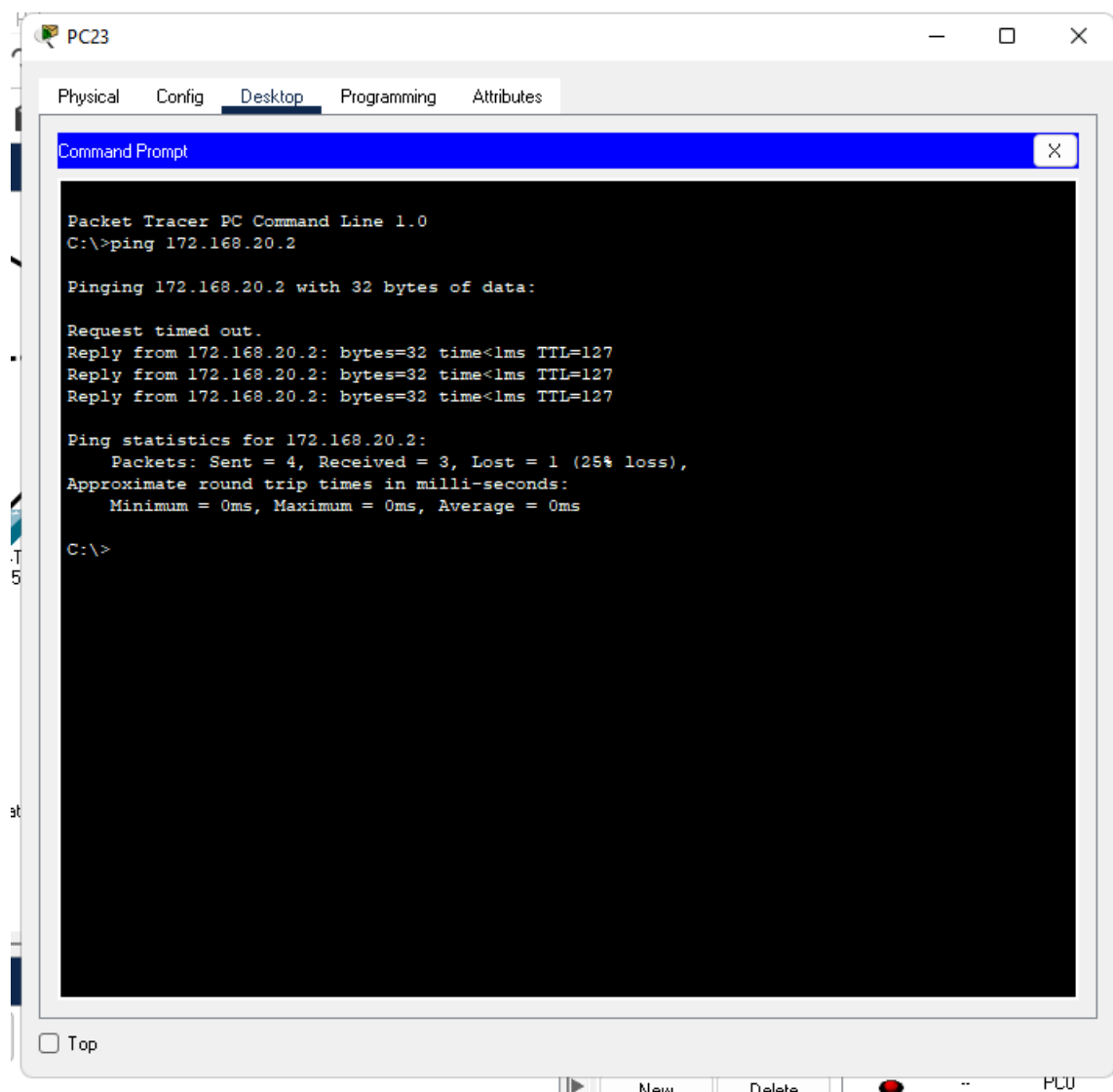
Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Hình 6: Ping từ máy của chi nhánh sang máy của trụ sở chính tầng 2.



Hình 7: Ping từ máy của trụ sở chính tầng 1 sang máy của trụ sở chính tầng 2.



Hình 8: Ping từ máy của chi nhánh tầng 1 sang máy của chi nhánh tầng 2.

6 Đánh giá lại hệ thống đã thiết kế

6.1 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.
- Được kiểm tra và nâng cấp định kì.

6.2 Xác định các tài nguyên 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:** gồm dữ liệu của ngân hàng và dữ liệu của khách hàng. 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...

6.3 Các mối đe dọa đối với hệ thống

Gồm 2 mối đe dọa chính :

- **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.

6.4 An toàn khi xảy ra sự cố

- **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 truy lớp:** 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 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 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.

6.5 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 switchchính 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.

6.6 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 210 người giả sử được chia đều trên các tầng thì mỗi tầng có 30 người, ta bố trí mỗi tầng 2 switch 24 port tức là có thể đáp ứng cho mỗi tầng là 48 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 kí 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.

6.7 Những hạn chế của dự án

- Do phải đặt nhiều giả thiết nên giải pháp chưa sát với thực tế.
- Chưa có nhiều kiến thức về hệ thống server, cấu hình các thiết bị như router, firewall,...
- Chưa có kinh nghiệm nhiều trong việc thiết kế một hệ thống mạng.
- Chưa có sơ đồ xây dựng của các toà nhà nên còn khó khăn trong việc thiết kế vật lý cho các tầng
- Vấn đề bảo mật còn khá nan giải

6.8 Định hướng phát triển trong tương lai

Trong tương lai, khi công ty phát triển và có thêm nhiều chi nhánh, thì ta vẫn có thể áp dụng mô hình mạng máy tính này cho các chi nhánh đó