

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 – CO3094
BÀI TẬP LỚN 2
THIẾT KẾ VÀ MÔ PHỎNG HỆ THỐNG MẠNG MÁY TÍNH CHO MỘT
CÔNG TY

Giảng viên hướng dẫn: Bùi Xuân Giang

STT	Sinh viên thực hiện	Mã số sinh viên
1	Nguyễn Công Huy	2113499
2	Bùi Lê Văn	2115257
3	Đậu Đức Quân	2114531
4	Nguyễn Lê Phúc	2112048

Thành phố Hồ Chí Minh – năm 2023

MỤC LỤC

1. TÌM HIỂU CẤU TRÚC MẠNG PHÙ HỢP CHO CÔNG TY	1
1.1. Yêu cầu kiến trúc của hệ thống mạng	1
1.2. Khảo sát khu vực có tải lớn trong công ty	2
1.3. Thiết kế cấu trúc mạng phù hợp	2
2. DANH SÁCH CÁC THIẾT BỊ ĐƯỢC SỬ DỤNG TRONG QUÁ TRÌNH MÔ PHỎNG MẠNG MÁY TÍNH	3
2.1. Router	3
2.2. Switch	3
2.3. Access point	3
3. TÍNH TOÁN CÁC THÔNG SỐ CHO HỆ THỐNG MẠNG	3
3.1. Tại trụ sở chính	3
3.2. Tại các chi nhánh	4
4. THIẾT KẾ BẢN MÔ PHỎNG HỆ THỐNG MẠNG VỚI CISCO PACKET TRACER	4
4.1. Các bước thực hiện	4
4.2. Kết quả thiết kế hệ thống mạng	5
5. KẾT QUẢ KIỂM THỬ KẾT NỐI HỆ THỐNG	7
5.1. Kết nối giữa các PC trong cùng một VLAN	7
5.3. Kết nối PC giữa trụ sở chính và các chi nhánh	9
5.4. Kết nối với server trong DMZ	9
5.5. Không có kết nối từ các thiết bị của khách hàng đến PC trong mạng LAN	10
5.6. Kết nối Internet với Web Server	11
6. ĐÁNH GIÁ LẠI HỆ THỐNG	11
6.1. Độ tin cậy của hệ thống	11
6.2. Dễ dàng nâng cấp hệ thống	11
6.3. Phần mềm hỗ trợ cho hệ thống	11
6.4. Tính an toàn và bảo mật của hệ thống	11
6.5. Những hạn chế còn vướng mắc	12
6.6. Định hướng trong tương lai	13

1. TÌM HIỂU CẤU TRÚC MẠNG PHÙ HỢP CHO CÔNG TY

1.1. Yêu cầu kiến trúc của hệ thống mạng

1.1.1. Hệ thống mạng tại trụ sở chính

Các thông số quan trọng trong việc thiết lập mạng máy tính trong công ty như sau:

- Tòa nhà gồm 7 tầng, tầng 1 được trang bị được trang bị 1 phòng kỹ thuật mạng và 1 Cabling Central Local (phòng chứa các dây mạng và patch panels).
- Công ty có quy mô dạng Medium – scale: 120 workstations, 5 servers, 12 network devices (hoặc nhiều hơn dành cho các thiết bị bảo mật mạng cụ thể).
- Sử dụng new technology cho hạ tầng mạng, bao gồm kết nối có dây, không dây và cáp quang.
- Tổ chức hệ thống mạng theo cấu trúc VLAN và sử dụng Ethernet loại GigaEthernet 1GbE/10GbE.
- Kết nối với bên ngoài bằng 2 Leased line và 2 DSL, cùng cơ chế Load – balancing.
- Dùng kết hợp giữa Licensed và Open source Softwares, ứng dụng office, ứng dụng client – server, multimedia, database.
- Yêu cầu tính bảo mật cao, an toàn khi xảy ra sự cố, dễ dàng nâng cấp hệ thống.
- Kết nối với 2 chi nhánh khác ở Hà Nội và Đà Nẵng.

1.1.2. Hệ thống mạng tại chi nhánh Hà Nội và Đà Nẵng

Mỗi chi nhánh cũng được thiết kế tương tự như ở Trụ sở chính nhưng có quy mô nhỏ hơn.

- Tòa nhà bao gồm 2 tầng, tầng 1 được trang bị 1 phòng kỹ thuật mạng và 1 Cabling Central Local.
- Các chi nhánh có quy mô dạng small - scale: 30 workstation, 3 server, 5 hoặc nhiều hơn network devices.

1.1.3. Thông lượng và tải của hệ thống

Các thông số về thông lượng và tải của hệ thống (tập trung khoảng 80% vào giờ cao điểm 9 – 11 giờ và 15 – 16 giờ) có thể dùng chung cho trụ sở chính và các chi nhánh như sau:

- Server dùng cho updates, web access, database access,... Tổng dung lượng download khoảng 1000 MB/ngày và upload khoảng 2000 MB/ngày.
- Mỗi workstation dùng cho duyệt web, tải tài liệu,... Dung lượng upload khoảng 100 MB/ngày và dung lượng download khoảng 500 MB/ngày.
- Thiết bị kết nối WIFI dùng cho truy xuất của khách hàng khoảng 500 MB/ngày.

1.1.4. Quy mô phát triển của hệ thống

Hệ thống mạng máy tính của công ty được ước tính tỉ lệ cho mức độ phát triển khoảng 20% trong 5 năm (về số lượng người dùng, tải trọng mạng, mở rộng thêm các chi nhánh,...).

1.2. Khảo sát khu vực có tải lớn trong công ty

- Network Load Balancing:

+ Network Load Balancing là một trong những tính năng rất quan trọng với những nhà phát triển và lập trình mạng. Là việc phân bố đồng đều lưu lượng truy cập giữa hai hay nhiều các server có cùng chức năng trong cùng một hệ thống.

+ Bằng việc sử dụng Network Load Balancing, hệ thống sẽ giảm thiểu tối đa tình trạng một server bị quá tải và ngưng hoạt động. Hoặc khi có một server gặp sự cố, cân bằng tải sẽ chỉ đạo phân phối công việc của server đó cho các server còn lại, đẩy thời gian uptime của hệ thống lên cao nhất và cải thiện năng suất hoạt động tổng thể. Điều này đảm bảo tính khả dụng và độ tin cậy của hệ thống, có thể dễ dàng thêm vào hoặc loại bớt các server theo yêu cầu nâng cấp trong tương lai một cách linh hoạt.

- Về kỹ thuật, hệ thống server cho phép người dùng Internet có thể tìm kiếm thông tin, trao đổi thông tin với các bộ phận được cấp phép trong công ty. Do vậy, cần phải đảm bảo về tốc độ truy cập và tính ổn định.

- Nhận thấy, các tầng cơ sở tại trung tâm có sự truy cập liên tục từ các thiết bị bên dưới (máy tính, máy in,...) nên phải đảm bảo tới cân bằng tải tại đây, để giữ cho sự truy cập thông tin tại đây được ổn định và trơn tru.

1.3. Thiết kế cấu trúc mạng phù hợp

- Thiết kế hệ thống mạng theo mô hình client – server.

- Hệ thống được bố trí hỗn hợp chia theo các chi nhánh, gồm các switch 100/1000 Mbps.

- Hệ thống server được đặt tại các phòng kỹ thuật bao gồm:

+ Web server là server mà tại đó cài đặt phần mềm phục vụ cho việc giao tiếp trong công ty, gửi thông báo,...

+ FTP (File Transfer Protocol) server được dùng để trao đổi tập tin qua mạng lưới truyền thông, sử dụng giao thức TCP/IP (ví dụ như Internet – mạng ngoại bộ hoặc Intranet – mạng nội bộ).

+ DNS (Domain Name System) server là máy chủ phân giải tên miền, được sử dụng để ánh xạ tên miền thành địa chỉ IP.

- Trong hệ thống mạng sử dụng multi layer switch để kết nối với hệ thống server và workstation thông qua các switch layer và router. Có 7 switch layer ở trụ sở chính và 2 switch layer ở từng chi nhánh kết nối vào multi layer switch. Đường kết nối từ switch layer và access point đến switch layer 3 bằng cáp quang để đảm bảo chất lượng và tốc độ đường truyền.

- Kết nối từ thiết bị bên ngoài đi vào hệ thống công ty qua leased line và đường dây DSL.

2. DANH SÁCH CÁC THIẾT BỊ ĐƯỢC SỬ DỤNG TRONG QUÁ TRÌNH MÔ PHỎNG MẠNG MÁY TÍNH

2.1. Router

- Router là thiết bị định tuyến, xác định một số thông tin như là thông tin của người gửi, kiểu dữ liệu, kích thước dữ liệu nhưng quan trọng nhất là địa chỉ IP đích để nó thực hiện nhiệm vụ là xác định đường đi tốt nhất cho thông tin gửi đi. Ta chọn Router CISCO 1941/K9 vì router này cung cấp dịch vụ bảo mật dữ liệu cao, tính di động cao và các dịch vụ ứng dụng.

2.2. Switch

- Switch layer 2: hoạt động trên tầng 2 của mô hình OSI tức là tầng data link được dùng để gửi các frame đến cổng đích sử dụng địa chỉ MAC thông qua bảng lưu trữ địa chỉ MAC của thiết bị được liên kết với cổng đó. Ta chọn CISCO WS-C2960+24TT-L.

- Switch layer 3: Với 24 port nó kết nối các switch lại với nhau, làm cho chúng có thể hoạt động song song cùng lúc với nhau nhằm mục đích đạt được tốc độ cao khi xử lý dữ liệu. Switch layer 3 hoạt động trên tầng network của mô hình OSI, được gắn thêm bảng định tuyến IP, đóng vai trò giống như một router nhưng không có cổng WAN có chức năng định tuyến các gói tin bằng cách sử dụng địa chỉ IP, được sử dụng rộng rãi để chia VLAN. Ta chọn Cisco WS-C3650-24PS-S.

2.3. Access point

- Access point được sử dụng cho trụ sở chính, phục vụ cho nhu cầu truy xuất thông tin của nhân viên. Ưu điểm của nó là đảm bảo tính tiện lợi khi truy cập mạng mà không thông qua hệ thống dây mạng. Ta chọn Cisco-Linksys WRT300N Wireless-N Broadband Router.

3. TÍNH TOÁN CÁC THÔNG SỐ CHO HỆ THỐNG MẠNG

3.1. Tại trụ sở chính

Các thông số về lưu lượng và tải của hệ thống tập trung khoảng 80% vào giờ cao điểm 9 – 11 giờ và 15 – 16 giờ (3 giờ).

- Dung lượng upload là 2000 MB/ngày và dung lượng download là 1000 MB/ngày cho mỗi Server. Ở trụ sở chính chúng ta có 5 Server, tổng dung lượng upload và download:
 $5 \times (2000 + 1000) = 15000 \text{ (MB)}.$

- Với mỗi Workstations có dung lượng upload là 100 MB/ngày và dung lượng download là 500 MB/ngày. Chúng ta có 120 Workstations, tổng dung lượng cần đáp ứng cho các Workstations: $120 \times (500 + 100) = 72000 \text{ (MB/ngày)}.$

- Với mạng không dây: mỗi thiết bị của khách hàng truy cập tải về khoảng 500 MB/ngày. Giả sử trụ sở có khoảng 200 thiết bị mạng truy cập mỗi ngày. Tổng dung lượng cho mạng Wireless: $500 \times 200 = 100000 \text{ (MB/ngày)}.$

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.

- Bandwidth: $((15000 + 72000 + 100000) * 0.8) / (3 * 3600) = 13.8519 \text{ (MB/s)} = 110.8148 \text{ (Mbps)}$

- Throughput: $(15000 + 72000 + 100000) / (24 * 3600) = 2.1644 \text{ (MB/s)} = 17.3148 \text{ (Mbps)}$

3.2. Tại các chi nhánh

Các thông số về lưu lượng và tải của hệ thống tập trung khoảng 80% vào giờ cao điểm 9 – 11 giờ và 15 – 16 giờ (3 giờ).

- Dung lượng upload là 2000 MB/ngày và dung lượng download là 1000 MB/ngày cho mỗi Server. Ở mỗi chi nhánh chúng ta có 3 Server, tổng dung lượng upload và download: $3 * (2000 + 1000) = 9000 \text{ (MB)}$.

- Với mỗi Workstations có dung lượng upload là 100 MB/ngày và dung lượng download là 500 MB/ngày. Chúng ta có 30 Workstations, tổng dung lượng cần đáp ứng cho các Workstations: $30 * (500 + 100) = 18000 \text{ (MB/ngày)}$.

- Với mạng không dây: mỗi thiết bị của khách hàng truy cập tải về khoảng 500 MB/ngày. Giả sử trụ sở có khoảng 100 thiết bị mạng truy cập mỗi ngày. Tổng dung lượng cho mạng Wireless: $500 * 100 = 50000 \text{ (MB/ngày)}$.

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.

- Bandwidth: $((9000 + 18000 + 50000) * 0.8) / (3 * 3600) = 5.7037 \text{ (MB/s)} = 45.6296 \text{ (Mbps)}$

- Throughput: $(9000 + 18000 + 50000) / (24 * 3600) = 0.8912 \text{ (MB/s)} = 7.1296 \text{ (Mbps)}$

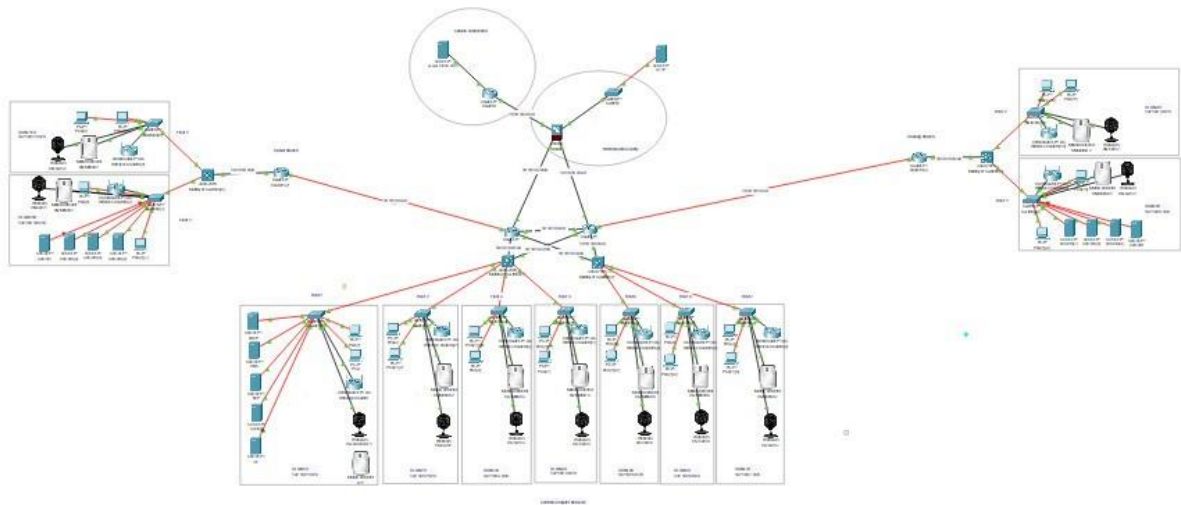
4. THIẾT KẾ BẢN MÔ PHỎNG HỆ THỐNG MẠNG VỚI CISCO PACKET TRACER

4.1. Các bước thực hiện

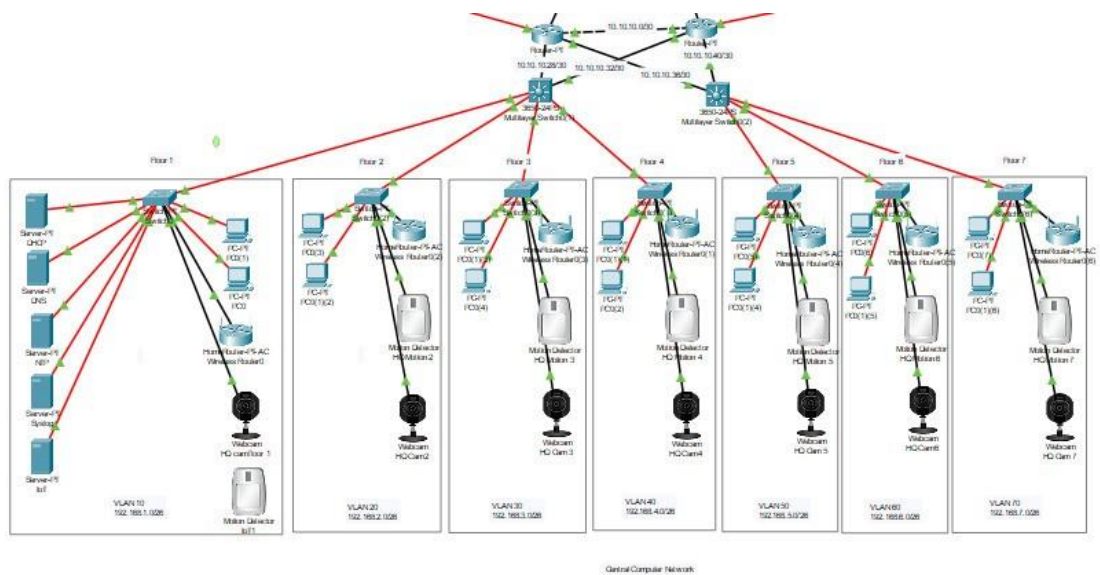
- Giả lập mô hình kết nối trụ sở và các chi nhánh.
- Tiến hành chia VLAN trong trụ sở và các chi nhánh.
- Tiến hành cấu hình DHCP tại core router để cấp phát IP cho các máy ở trụ sở và chi nhánh.
- Giả lập mạng internet để mô phỏng kết nối giữa trụ sở và chi nhánh.
- Tiến hành Routing mô hình giả lập.
- Tiến hành kiểm tra bằng cách ping, traceroute và chế độ simulation có sẵn.

4.2. Kết quả thiết kế hệ thống mạng

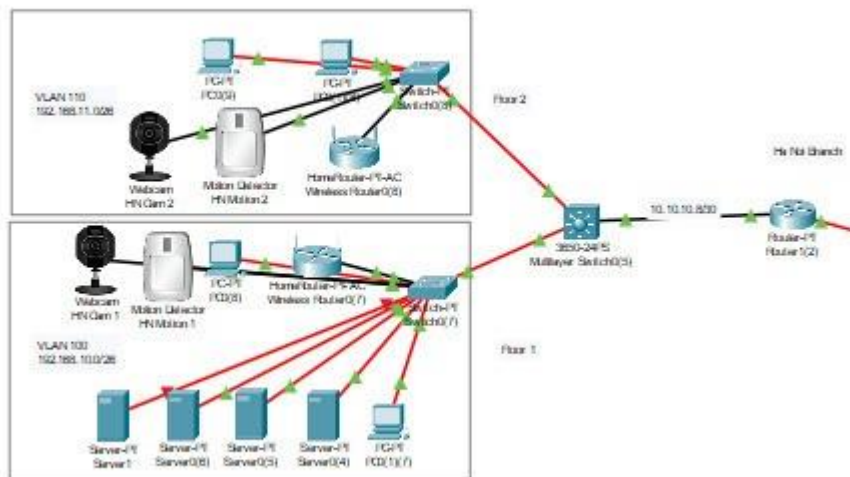
4.2.1. Toàn bộ hệ thống



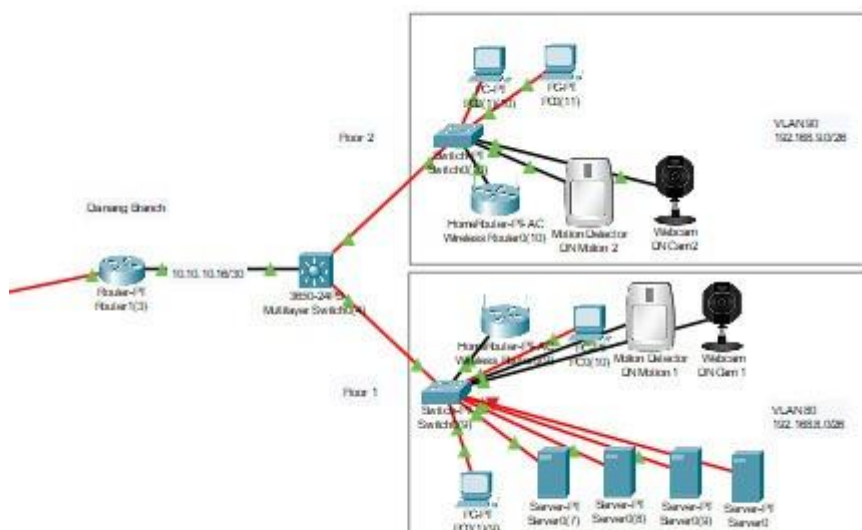
4.2.2. Trụ sở chính



4.2.3. Chi nhánh Hà Nội

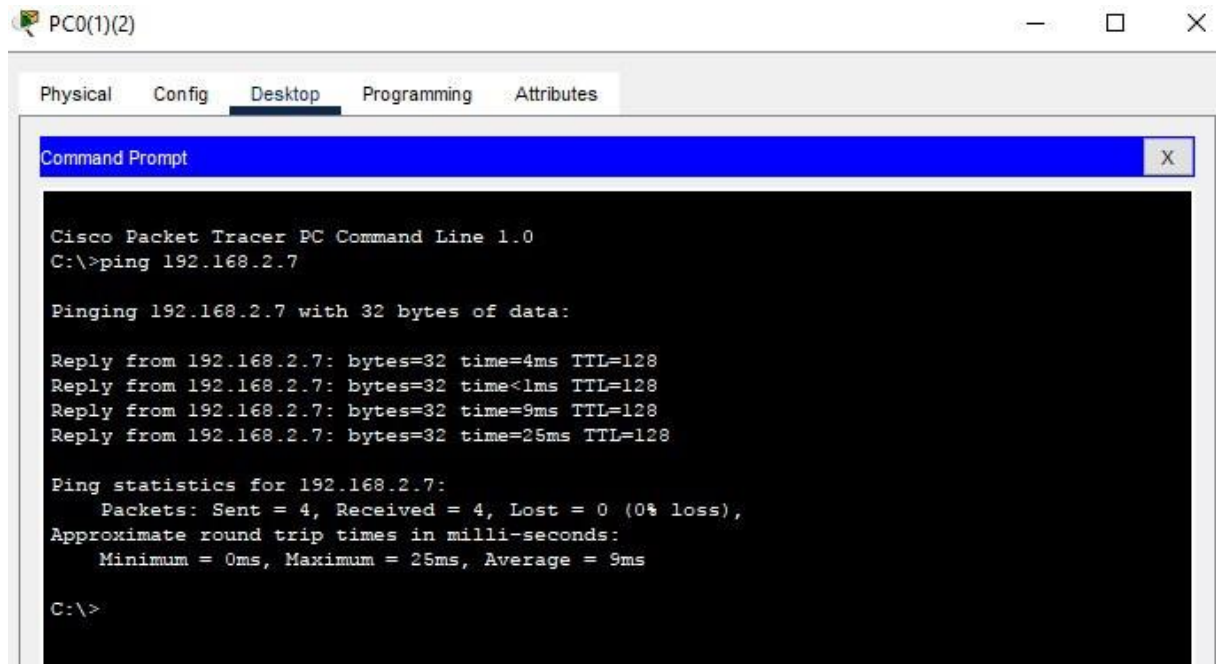


4.2.4. Chi nhánh Đà Nẵng

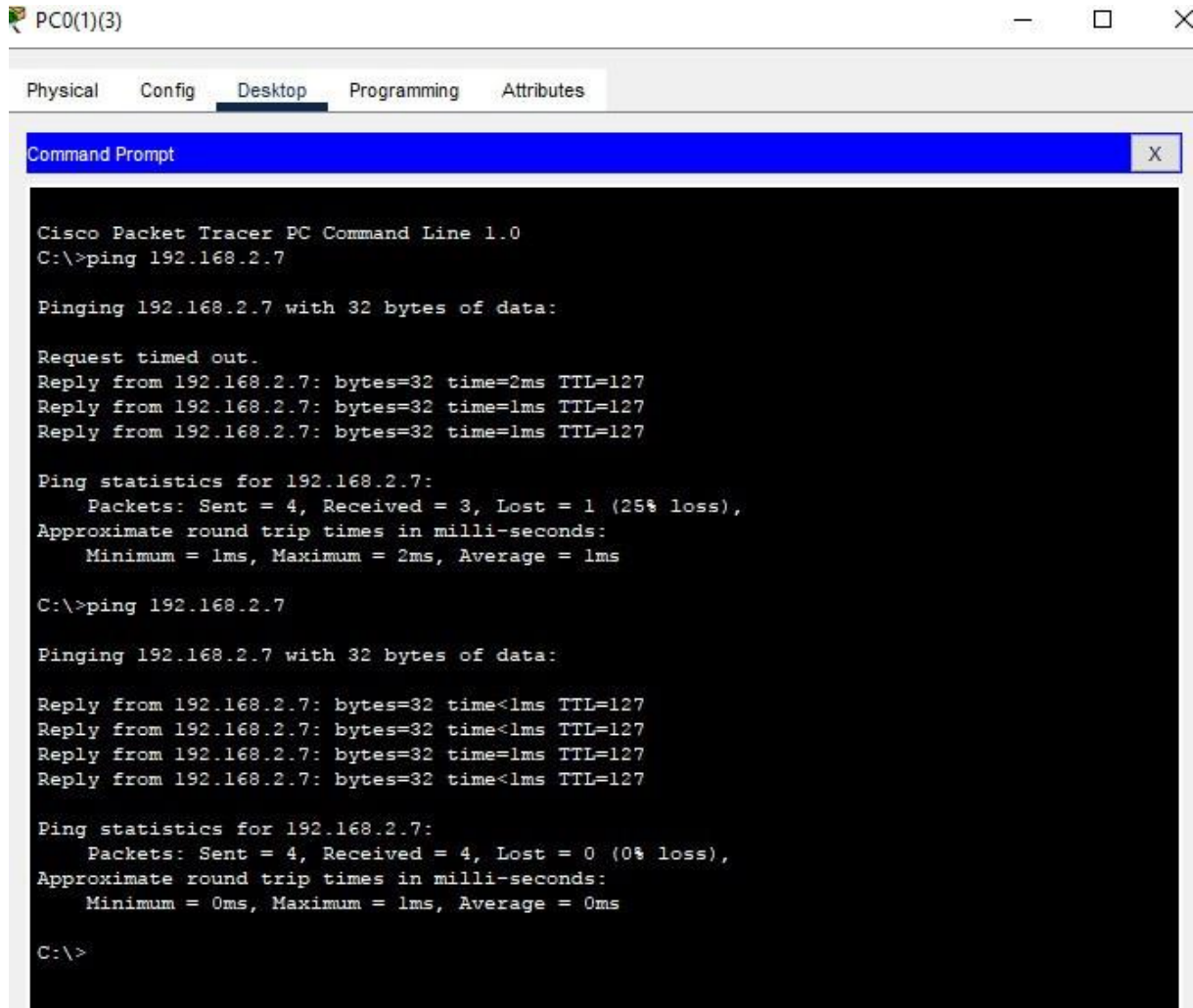


5. KẾT QUẢ KIỂM THỬ KẾT NỐI HỆ THỐNG

5.1. Kết nối giữa các PC trong cùng một VLAN



5.2. Kết nối PC giữa các VLAN



PC0(1)(3)

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.7

Pinging 192.168.2.7 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.7: bytes=32 time=2ms TTL=127
Reply from 192.168.2.7: bytes=32 time=1ms TTL=127
Reply from 192.168.2.7: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.7:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 192.168.2.7

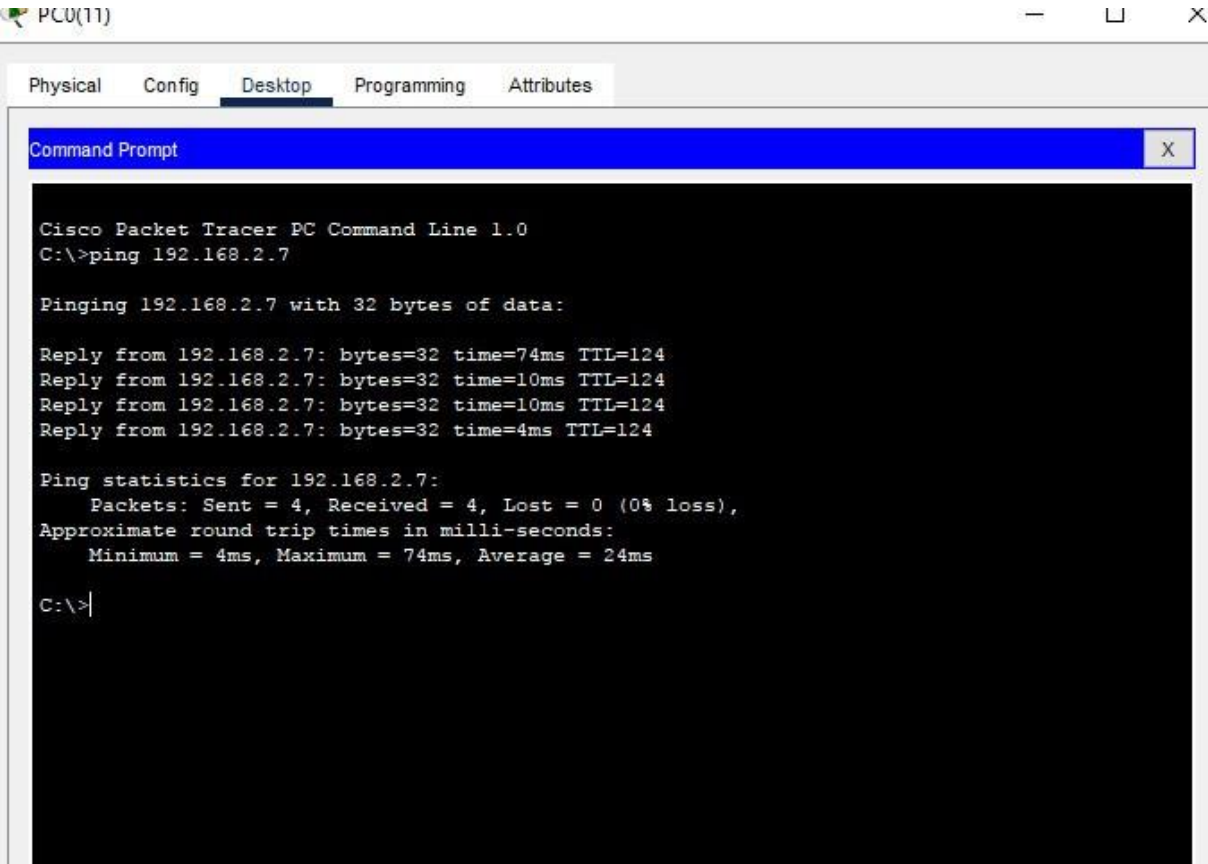
Pinging 192.168.2.7 with 32 bytes of data:

Reply from 192.168.2.7: bytes=32 time<1ms TTL=127
Reply from 192.168.2.7: bytes=32 time<1ms TTL=127
Reply from 192.168.2.7: bytes=32 time=1ms TTL=127
Reply from 192.168.2.7: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

5.3. Kết nối PC giữa trụ sở chính và các chi nhánh



The screenshot shows a Cisco Packet Tracer PC Command Line window for PC0(11). The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a Command Prompt window. The Command Prompt shows the execution of the command 'ping 192.168.2.7'. The output indicates a successful ping with 32 bytes of data, showing four replies from 192.168.2.7 with varying times (74ms, 10ms, 10ms, 4ms) and a TTL of 124. The ping statistics show 4 packets sent, 4 received, and 0 lost (0% loss), with an average round trip time of 24ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.7

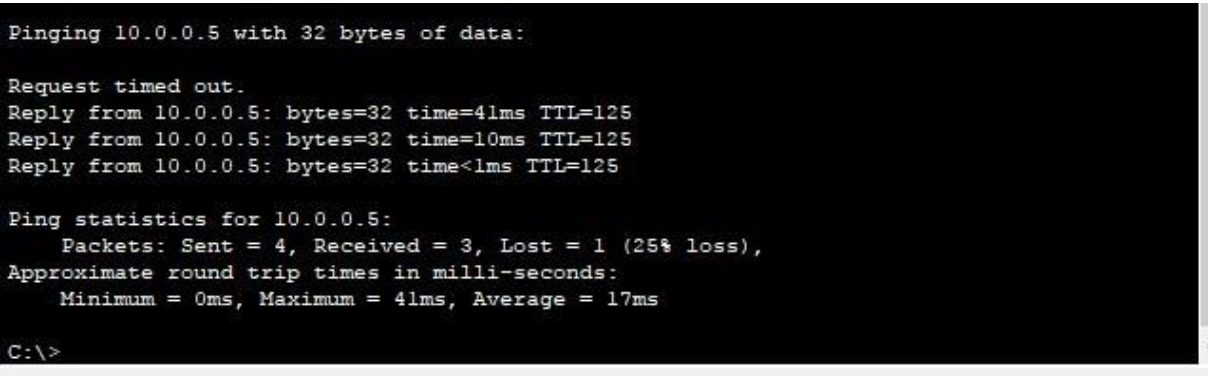
Pinging 192.168.2.7 with 32 bytes of data:

Reply from 192.168.2.7: bytes=32 time=74ms TTL=124
Reply from 192.168.2.7: bytes=32 time=10ms TTL=124
Reply from 192.168.2.7: bytes=32 time=10ms TTL=124
Reply from 192.168.2.7: bytes=32 time=4ms TTL=124

Ping statistics for 192.168.2.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 74ms, Average = 24ms

C:\>|
```

5.4. Kết nối với server trong DMZ



The screenshot shows a Cisco Packet Tracer PC Command Line window for PC0(11). The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a Command Prompt window. The Command Prompt shows the execution of the command 'ping 10.0.0.5'. The output indicates a failed ping with 32 bytes of data, showing three replies from 10.0.0.5 with times (41ms, 10ms, <1ms) and a TTL of 125. The ping statistics show 4 packets sent, 3 received, and 1 lost (25% loss), with an average round trip time of 17ms.

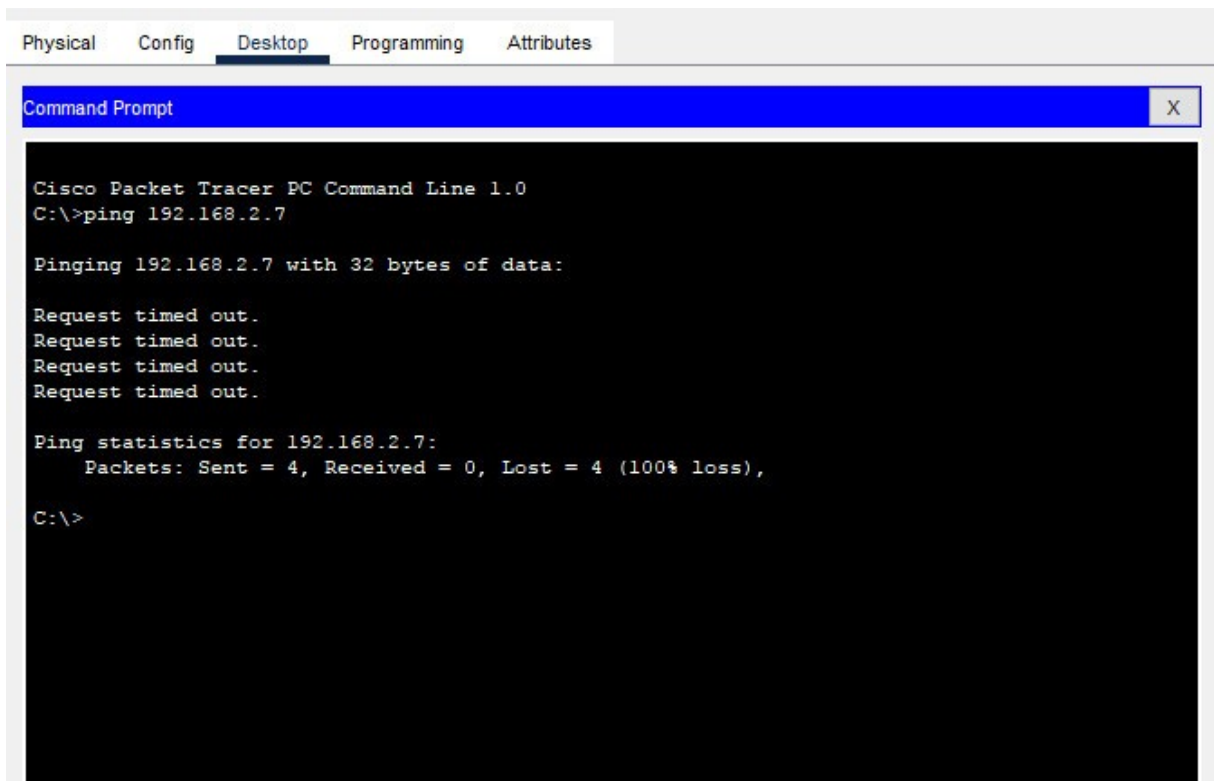
```
Pinging 10.0.0.5 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.5: bytes=32 time=41ms TTL=125
Reply from 10.0.0.5: bytes=32 time=10ms TTL=125
Reply from 10.0.0.5: bytes=32 time<1ms TTL=125

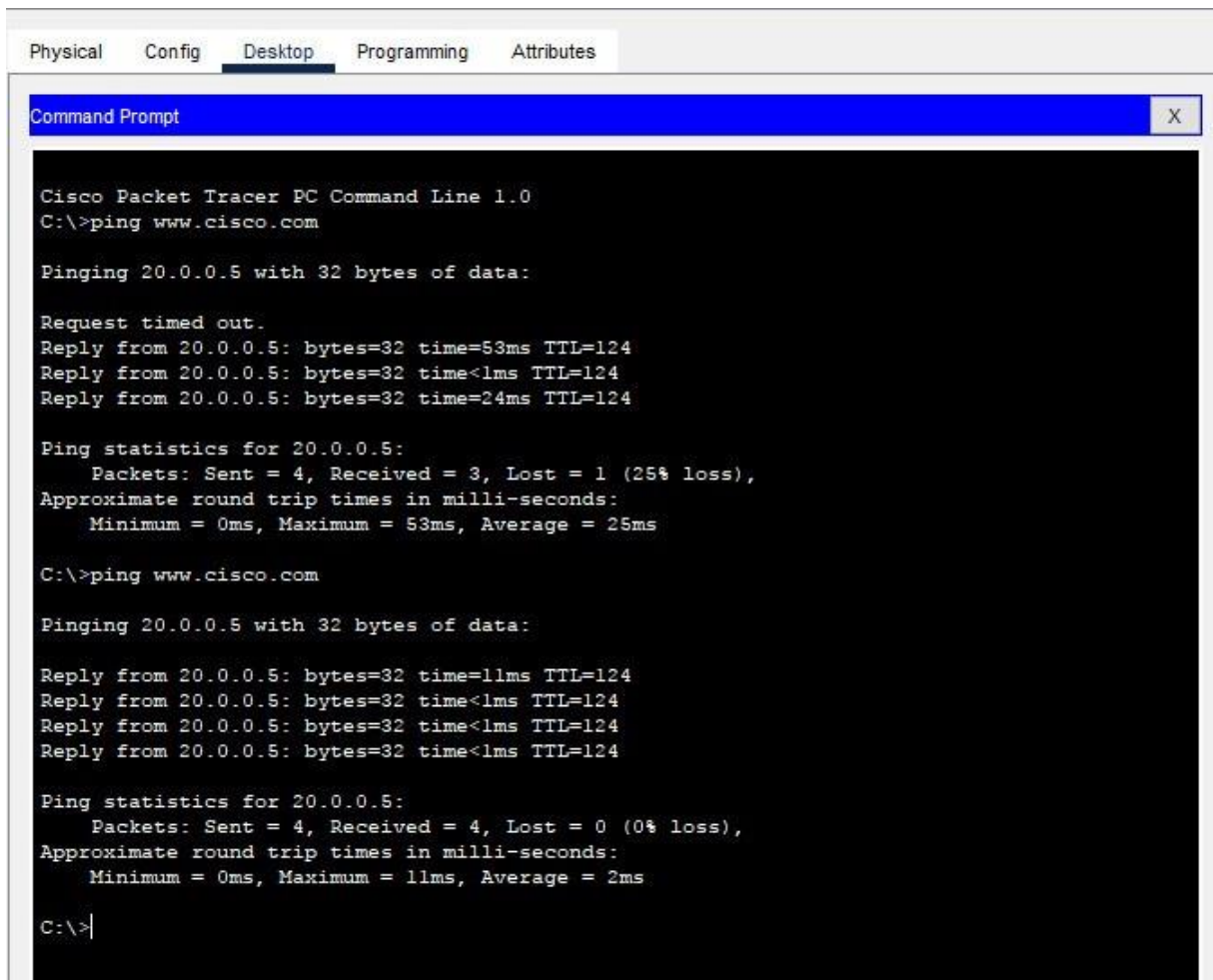
Ping statistics for 10.0.0.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 41ms, Average = 17ms

C:\>
```

5.5. Không có kết nối từ các thiết bị của khách hàng đến PC trong mạng LAN



5.6. Kết nối Internet với Web Server



```
Physical  Config  Desktop  Programming  Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping www.cisco.com

Pinging 20.0.0.5 with 32 bytes of data:

Request timed out.
Reply from 20.0.0.5: bytes=32 time=53ms TTL=124
Reply from 20.0.0.5: bytes=32 time<1ms TTL=124
Reply from 20.0.0.5: bytes=32 time=24ms TTL=124

Ping statistics for 20.0.0.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 53ms, Average = 25ms

C:\>ping www.cisco.com

Pinging 20.0.0.5 with 32 bytes of data:

Reply from 20.0.0.5: bytes=32 time=11ms TTL=124
Reply from 20.0.0.5: bytes=32 time<1ms TTL=124
Reply from 20.0.0.5: bytes=32 time<1ms TTL=124
Reply from 20.0.0.5: bytes=32 time<1ms TTL=124

Ping statistics for 20.0.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 2ms

C:\>
```

6. ĐÁNH GIÁ LẠI HỆ THỐNG

6.1. Độ tin cậy của hệ thống

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 hệ thống

Trong thời kỳ 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.

6.3. Phần mềm hỗ trợ cho hệ thống

Sử dụng các thiết bị mạng của công ty Cisco, 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 và bảo mật của hệ thống

6.4.1. Yêu cầu hệ thống

- Hệ thống ngân hàng phải đáp ứng nhu cầu xử lý thông tin dữ liệu nghiệp vụ quan trọng.

- Yêu cầu bảo mật bao gồm việc ngăn chặn truy cập từ đối tượng bên ngoài, kiểm soát truy cập người sử dụng, và đảm bảo an toàn cho dữ liệu.

6.4.2. Tài nguyên cần bảo vệ

- Phân hệ Server, chứa dữ liệu quan trọng về khách hàng và các giao dịch, là một tài nguyên chính cần bảo vệ để tránh ảnh hưởng nghiêm trọng đến khách hàng và hoạt động của ngân hàng.

6.4.3. Môi đe dọa

- Hacker có thể sử dụng công cụ và mã độc để đánh cắp thông tin khách hàng và kiểm soát máy tính trong ngân hàng.

- Người sử dụng trong mạng LAN cũng đại diện cho môi đe dọa khi có ý định tấn công hệ thống, tạo ra nguy cơ khó kiểm soát.

6.4.4. Biện pháp khắc phục

- Sử dụng tường lửa để kiểm soát gói tin và ngăn chặn cả nguy cơ từ bên trong và bên ngoài hệ thống.

- Bảo trì và cập nhật định kỳ hệ điều hành và ứng dụng để phát hiện và khắc phục lỗ hổng bảo mật.

- Sao lưu, bảo trì, và nâng cấp thường xuyên để đảm bảo an toàn và hiệu suất hệ thống.

- Bảo mật các thiết bị mạng trong hệ thống.

6.4.5. Yêu cầu khi gặp sự cố

- Ngắt kết nối Internet để ngăn chặn kết nối trái phép.

- Sử dụng backup Server để sao lưu dữ liệu và có phòng ban quản lý sự cố.

- Xây dựng biện pháp dự phòng và chuẩn bị đối mặt với rủi ro khi chúng xảy ra.

6.5. Những hạn chế còn vướng mắc

Những thách thức liên quan đến bảo mật luôn đặt ra những rủi ro tiềm ẩn đối với hệ thống ngân hàng. Mặc dù các biện pháp bảo mật đã được triển khai, tuy nhiên, những vụ tấn công vẫn không ngừng diễn ra hàng năm. Vì vậy, việc xây dựng hệ thống bảo mật với mức độ an toàn và tối ưu nhất vẫn là một thách thức lớn cho các dự án.

Trong lĩnh vực thiết kế hệ thống mạng máy tính, việc chọn lựa các thiết bị mạng phù hợp cũng là một công việc phức tạp. Trên thị trường, có nhiều loại thiết bị mạng với đa dạng về kỹ thuật và công nghệ mới. Quá trình này không chỉ đòi hỏi sự đáp ứng đối với lưu lượng dữ liệu mà còn phải xem xét kỹ lưỡng về giá cả, công nghệ bảo mật, và hiệu suất.

Mặc dù các hệ thống ngân hàng đã đặt ra những biện pháp an toàn cao cấp, nhưng việc duy trì và nâng cao hệ thống bảo mật là một quá trình không ngừng. Sự thay đổi liên tục trong môi trường an ninh mạng đòi hỏi sự linh hoạt và sẵn sàng để đối mặt với những thách thức mới.

6.6. Định hướng trong tương lai

Cải thiện khả năng bảo mật của hệ thống đòi hỏi sự đầu tư liên tục. Thay mới thiết bị mạng, cập nhật phần mềm, nâng cấp hệ thống, và chuẩn bị cho tương lai là những bước quan trọng. Đồng thời, đào tạo nhân viên, kiểm tra định kỳ, và đánh giá rủi ro giúp duy trì và nâng cao mức độ an toàn, đồng thời đảm bảo sự linh hoạt và ứng phó với thách thức an ninh ngày càng phức tạp.