

VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY  
UNIVERSITY OF TECHNOLOGY  
FACULTY OF COMPUTER SCIENCE AND ENGINEERING



Mạng Máy Tính (CO3003)

---

Assignment

# THIẾT KẾ MẠNG MÁY TÍNH CHO NGÂN HÀNG HK2

---

Giáo viên hướng dẫn: Bùi Xuân Giang  
Sinh viên: Nguyễn Hoàng Quang Khánh - 2013458  
Nguyễn Tuấn Kiệt - 2013577  
Đặng Phú Quốc - 2014294  
Vũ Trần Hoàng - 2013245

HO CHI MINH CITY, JUNE 2022



## Contents

<b>1</b>	<b>Member list &amp; Workload</b>	<b>3</b>
<b>2</b>	<b>Mô tả thiết kế</b>	<b>3</b>
<b>3</b>	<b>Các thông số về hệ thống</b>	<b>3</b>
<b>4</b>	<b>Yêu cầu</b>	<b>4</b>
<b>5</b>	<b>Phân tích yêu cầu</b>	<b>4</b>
5.1	Trụ sở chính . . . . .	4
5.2	Các chi nhánh . . . . .	5
5.3	Hệ thống mạng . . . . .	5
5.4	Kết nối Internet và ADSL . . . . .	5
<b>6</b>	<b>Thiết bị</b>	<b>6</b>
6.1	Các thiết bị đề xuất . . . . .	6
6.2	Tổng hợp số lượng . . . . .	10
<b>7</b>	<b>Tính toán tải mạng</b>	<b>10</b>
7.1	Trụ sở chính . . . . .	10
7.2	Các chi nhánh . . . . .	12
<b>8</b>	<b>Sơ đồ IP của Ngân Hàng</b>	<b>13</b>
8.1	Tại trụ sở chính . . . . .	13
8.2	Tại chi nhánh . . . . .	13
8.3	khác . . . . .	14
<b>9</b>	<b>Sơ đồ kết nối WAN</b>	<b>14</b>
<b>10</b>	<b>Thiết kế sơ đồ mạng dùng Packet Tracer</b>	<b>15</b>
10.1	Sơ đồ tổng thể . . . . .	15
10.2	Thiết kế mạng tại trụ sở . . . . .	16
10.3	Thiết kế mạng tại 2 chi nhánh . . . . .	17
<b>11</b>	<b>Kiểm tra</b>	<b>18</b>
11.1	Thực hiện kiểm tra các kết nối . . . . .	18
11.2	Thực hiện kiểm tra kết nối với phương thức bảo mật . . . . .	18
<b>12</b>	<b>Bảo mật và an toàn khi xảy ra sự cố</b>	<b>19</b>
12.1	Yêu cầu đối với hệ thống . . . . .	19
12.2	Xác định các tài nguyên cần được bảo vệ . . . . .	20
12.3	Xác định các tài nguyên cần được bảo vệ . . . . .	20
12.3.1	Mối đe dọa từ bên trong . . . . .	20
12.3.2	Mối đe dọa từ bên ngoài . . . . .	20
12.4	Các giải pháp bảo mật . . . . .	20



<b>13 Đánh giá hệ thống</b>	<b>21</b>
13.1 Ưu điểm . . . . .	21
13.2 Hạn chế . . . . .	21
13.3 Định hướng phát triển tương lai . . . . .	21



## 1 Member list & Workload

No.	Fullname	Student ID	Problems	Work %
1	Nguyễn Hoàng Quang Khánh	2013458	- Viết báo cáo và tính toán tốc độ mạng. - Thiết kế tổng quan	20%
2	Nguyễn Tuấn Kiệt	2013577	- Thực hiện mạng LAN ở 2 chi nhánh.	20%
3	Đặng Phú Quốc	2014294	- Thực hiện mạng LAN ở trụ sở chính	20%
4	Vũ Trần Hoàng	2013245	- Thực hiện kết nối WAN giữa các chi nhánh - Kết nối internet, tường lửa và DMZ	40%

## 2 Mô tả thiết kế

Mô tả thiết kế mạng máy tính của công ty IT HK2 như sau:

- Toà building tại trụ sở cao 7 tầng. Tầng 1 trang bị một phòng kỹ thuật Mạng và Cabling Central Local (phòng tập trung dây mạng và patch panels).
- Trụ sở chính bao gồm: 100 workstations, 5 servers và 12 thiết bị mạng
- Sử dụng công nghệ mới về hạ tầng mạng bao gồm 100/1000 Mbps công nghệ mạng có dây và mạng không dây.
- Tổ chức hệ thống theo cấu trúc VLAN.
- Kết nối với bên ngoài bằng 2 Leased line (dành cho kết nối WAN) và 1 ADSL (dành cho truy cập internet), dùng cơ chế load-balancing
- Sử dụng kết hợp phần mềm nguồn mở và được cấp phép, ứng dụng văn phòng, ứng dụng máy khách-máy chủ, đa phương tiện và cơ sở dữ liệu.
- Bảo mật cao, an toàn khi xảy ra sự cố, dễ dàng nâng cấp hệ thống.

Ngân hàng cần kết nối với 2 chi nhánh tại 2 thành phố lớn là Nha Trang và Đà Nẵng. Mỗi chi nhánh cũng được thiết kế tương tự như trụ sở chính nhưng với quy mô nhỏ hơn:

- Mỗi chi nhánh gồm 2 tầng, tầng 1 được trang bị 1 phòng kỹ thuật và Cabling Central Local (phòng tập trung dây mạng và patch panels)
- Chi nhánh BBB: 50 workstations, 3 servers, 5 thiết bị mạng trở lên

Thực hiện kết nối giữa trụ sở chính và chi nhánh thông qua các kết nối WAN, chúng ta có thể chọn một trong các công nghệ được sử dụng cho kết nối này tùy theo tính kinh tế của giải pháp.

- Phân tích ưu nhược điểm của giải pháp đã chọn

## 3 Các thông số về hệ thống

Các thông số về lưu lượng và tải của hệ thống (tập trung khoảng 80% vào các giờ cao điểm 9h-11h và 15-16h) dùng cho Trụ sở chính và các chi nhánh như sau:

- Servers dùng cho updates, web access, database access,... Tổng dung lượng upload và download vào khoảng 500MB/ngày.
- Mỗi workstation dùng cho duyệt web, tải tài liệu, giao dịch khách hàng,... Tổng dung lượng upload và download vào khoảng 100MB/ngày.
- Máy laptop kết nối WiFi dùng cho khách hàng truy xuất có dung lượng upload, download vào khoảng 50MB/ngày.
- Cấu hình VPN site-to-site và cho một nhân viên làm việc từ xa kết nối với mạng LAN

Hệ thống mạng máy tính của công ty được dự toán cho mức độ phát triển 20% trong 5 năm (về số lượng, tải mạng và mở rộng nhiều chi nhánh)

## 4 Yêu cầu

Các yêu cầu liên quan đến mô tả và thông số của hệ thống mạng như sau:

1. Tìm hiểu cấu trúc mạng thích hợp cho các toà nhà
2. Lập danh sách các thiết bị tối thiểu, sơ đồ IP và sơ đồ đi dây (cabling)
3. Tính toán throughput, bandwidth và các thông số an toàn cho hệ thống mạng
4. Thiết kế sơ đồ mạng dùng phần mềm mô phỏng
5. Kiểm tra lại hệ thống thông qua các công cụ phổ biến như ping, traceroute,... trên hệ thống được mô phỏng
6. Đánh giá lại hệ thống mạng được thiết kế thông qua các đặc tính:
  - Độ tin cậy, dễ dàng nâng cấp, phần mềm hỗ trợ đa dạng, tính an toàn, bảo mật của dữ liệu,...
  - Những hạn chế còn vướng mắc trong dự án
  - Định hướng phát triển trong tương lai
7. Tải tệp mô phỏng (sử dụng Packet Tracer hoặc GNS3) và báo cáo dự án lên BkeL trước thời hạn

## 5 Phân tích yêu cầu

Từ yêu cầu thiết kế, nhóm chúng em đề xuất việc thiết lập mô hình mạng của Ngân hàng HK2 bằng trình giả lập mạng Packet Tracer như sau:

### 5.1 Trụ sở chính

Tầng 1 của trụ sở được trang bị phòng kỹ thuật và Cabling Central Local, nơi tập trung các router và các switch của trụ sở.

Tầng 1 của trụ sở chính được bố trí làm nơi giao dịch với khách hàng (gồm bộ giao dịch và bộ phận tiếp tân). Bên cạnh đó, trụ sở còn bố trí thêm một lượng máy tính nhằm phục vụ khách hàng có nhu cầu tra cứu thông tin tài khoản,...

Thêm vào đó, tầng 1 còn có 2 phòng: phòng IT dành cho bộ phận IT của ngân hàng và phòng

tập trung dây mạng và patch panel (nơi tập trung các thiết bị mạng, server, dây nối,...) Do đó tầng 1 được lắp đặt 5 Servers, các thiết bị mạng. Bên cạnh đó các hoạt động giao dịch diễn ra tại tầng 1 nên cần lắp đặt 1 mạng Wireless để cung cấp mạng cho khách. Mỗi laptop sẽ truy xuất khoảng 50Mb/ngày

Tầng 2-7 mỗi tầng được lắp đặt 15 máy, tầng 1 sẽ có 10 máy. Đồng thời mỗi tầng sẽ sử dụng Switch 24 ports để kết nối với các máy và 1 switch layer 3 để kết nối từng tầng. Nếu có nhu cầu mở rộng máy 20% trong khoảng 5 năm, ta vẫn có thể đáp ứng vì số lượng port còn khá nhiều. Nếu cần thêm có thể nối thêm switch.

## 5.2 Các chi nhánh

Tại các chi nhánh Đà Nẵng và Nha Trang, thiết kế hệ thống mạng đều đặt phòng kỹ thuật tại tầng 1, các tầng còn lại đặt các hệ thống mạng cho máy trạm và máy của nhân viên.

Tầng 1 là nơi lắp đặt 3 Servers, các thiết bị mạng. Cần lắp model wifi để khách hàng có thể truy cập mạng. Đồng thời tầng 1 được trang bị 25 máy và sử dụng Switch để kết nối với các máy.

Tầng 2 được trang bị 25 máy tương tự như tầng 1 sử dụng Switch để kết nối với các máy.

Sử dụng Multilayer Switch để làm Switch tổng tương tự như trung tâm.

## 5.3 Hệ thống mạng

Ta phân chia hệ thống mạng theo 4 cấp

- Cấp 1: Router trung tâm, Router chi nhánh và mạng Internet
- Cấp 2: Switch tổng của tòa nhà
- Cấp 3: Switch tổng của từng tầng và các Switch con của Switch tổng trên các tầng của tòa nhà
- Cấp 4: Mạng VLAN của từng phòng ban.

Hệ thống mạng 4 cấp này được thiết kế cho cả trụ sở chính và hai chi nhánh.

## 5.4 Kết nối Internet và ADSL

Trụ sở của mỗi chi nhánh đều có một đường truyền ADSL đến ISP router để kết nối Internet, Mỗi router có một địa chỉ IP riêng cấp bởi DHCP.

- Vì công ty kinh doanh trong lĩnh vực ngân hàng nên nhu cầu sử dụng đường truyền mạng tốc độ cao rất cấp thiết. Ta sử dụng 2 Leased Line để kết nối trung tâm với các chi nhánh, đảm bảo việc liên lạc, truyền dữ liệu giữa các chi nhánh và trung tâm ổn định, tốc độ cao.
- Dùng đường truyền ADSL để kết nối với Internet.

## 6 Thiết bị

### 6.1 Các thiết bị đề xuất

- 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.
- File server: Để chia sẻ các thông tin
- DNS server: Dịch tên miền ra địa chỉ IP
- Database server: Để lưu trữ thông tin
- Mail server: để gửi và nhận email

a) Router

Sử dụng Router CISCO ISR4331/K9



Hình 1: Router

Những thông số đặc trưng của Router CISCO ISR4331/K9:

- Bộ định tuyến Router Cisco cung cấp bộ nhớ là 4G và bộ nhớ Flash có thể tối đa lên 16G. Mặt sau là các cổng RJ45 và SFP cùng với các khe cắm SM-X. Các khe cắm này hỗ trợ một mô đun rộng gấp đôi hoặc 2 tín hiệu rộng.
- Tổng thông lượng: 100 Mbps đến 300 Mb / giây
- Tổng số cổng WAN hoặc LAN 10/100/1000 trên bo mạch: 3

b) Core Switch

Sử dụng Switch Cisco WS-C3560-24TS-S



Hình 2: switch tổng

Những thông số đặc trưng của Cisco WS-C3560-24TS-S:

- Dòng Switch Cisco Catalyst 3650 được trang bị công nghệ Cisco StackWise-160 có thể xếp chồng 9 switch và hỗ trợ băng thông xếp chồng lên đến 160Gbps. Tích hợp 24 cổng Ethernet và 4 cổng 1G SFP uplink
- Băng thông chuyển tiếp: 65.47 Mbps
- Khả năng chuyển mạch: 88 Gbps

c) Switch phụ

Sử dụng Switch CISCO Catalyst 2960 WS-C2960-24TT-L



Hình 3: switch phụ

Những thông số đặc trưng của Switch CISCO Catalyst 2960 WS-C2960-24TT-L:

- Thuộc dòng switch Cisco Catalyst 2960 có hỗ trợ truy cập voice, video, data và khả năng bảo mật cao. Nó cũng cung cấp khả năng quản lý có thể mở rộng khi nhu cầu kinh doanh thay đổi
- Số cổng: 24 cổng Ethernet 10/100 và 2 cổng Ethernet Uplink 10/100/1000



- VLAN tối đa: 255

d) Accesspoint

Sử dụng Wireless-G Access Point LINKSYS WAP54G



Hình 4: accesspoint

Những thông số đặc trưng của Wireless-G Access Point LINKSYS WAP54G:

- Tốc độ tối đa đạt 54Mbps theo chuẩn G không dây (802.11g) và 11Mbps theo chuẩn B không dây (802.11b)
- Phím nhấn giúp bạn cấu hình mạng không dây đơn giản và nhanh chóng
- An ninh mạng không dây: mã hoá 128-bit WPA, lọc địa chỉ MAC, miễn phí dùng thử các dịch vụ an ninh mạng cao cấp Linksys Wireless Guard WPA-RADIUS

e) Bảo mật

Sử dụng Security Cisco ASA 5506-X with FirePOWER Services

Những thông số đặc trưng của Cisco ASA 5506-X with FirePOWER Services:

- Khả năng hiển thị và kiểm soát ứng dụng chính xác
- Cisco ASA hàng đầu trong ngành: ngăn chặn các mối đe dọa rủi ro cao và nhận thức đầy đủ về người dùng, cơ sở hạ tầng, ứng dụng và các dữ liệu giúp phát hiện sớm các mối đe dọa từ nhiều hướng, phòng vệ một cách tự động
- Lọc URL dựa theo danh mục và danh tiếng
- Bảo vệ nâng cao trước phần mềm độc hại



Hình 5: Security

f) Modun DSL

Sử dụng Cisco 881 Integrated Services Router with Integrated 802.11n Access Point



Hình 6: Modem DSL

Những thông số đặc trưng của dụng Cisco 881 Integrated Services Router with Integrated

802.11n Access Point:

- Hiệu quả cao khi chạy các dịch vụ đồng thời, bảo mật được nâng cấp
- Nhiều loại kết nối WAN như FastEthernet, VDSL2/ADSL2/2+, G.SHDSL, 3G,...
- Các liên kết WAN dự phòng
- Switch bốn cổng 10-/100-Mbps
- Access point 802.11g/n tùy chọn

## 6.2 Tổng hợp số lượng

- Trụ sở chính
  - 1 Router CISCO ISR4331/K9 để kết nối mạng với công ty và 2 chi nhánh, đồng thời để kết nối mạng internet
  - 1 Switch CISCO WS-C3650-24TS-S để kết nối tới Switch quản lý mỗi tầng
  - Từ tầng 1 tới tầng 7 mỗi tầng sử dụng 1 Switch CISCO Catalyst 2960 WS-C2960-24TT-L để kết nối mạng VLAN của riêng từng tầng, đồng thời trang bị Wireless-G Access Point LINKSYS WAP54G để nhân viên có thể kết nối wifi.
  - Trang bị 1 ASA 5506-X firewall để ngăn chặn việc truy cập từ bên ngoài vào mạng LAN của trụ sở, đồng thời cấu hình vùng DMZ với 1 Switch CISCO Catalyst 2960 WS-C2960-24TT-L nối thẳng tới firewall
- Các chi nhánh
  - 1 Router CISCO ISR4331/K9 để kết nối mạng chi nhánh với công ty và chi nhánh khác, đồng thời để kết nối mạng internet
  - 1 Switch CISCO WS-C3650-24TS-S để kết nối tới Switch quản lý mỗi tầng
  - Mỗi tầng sử dụng 1 Switch CISCO Catalyst 2960 WS-C2960-24TT-L để kết nối mạng VLAN của riêng từng tầng
  - Tại tầng 2 cung cấp thêm dịch vụ wireless cho khách nên cần 1 thiết bị Wireless-G Access Point LINKSYS WAP54G được nối vào Switch CISCO Catalyst 2960 WS-C2960-24TT-L

## 7 Tính toán tải mạng

### 7.1 Trụ sở chính

- Kết nối có dây

Ở trụ sở chính gồm 5 servers, 80% tổng lượng tải tập trung vào 3 tiếng của các giờ cao điểm (9h-11h: 2 tiếng và 15h-16h: 1 tiếng), tổng thời gian làm việc với thời lượng 8 tiếng/ngày với tổng dung lượng 500MB/ngày đối với 1 server:

$$Bandwidth = \frac{Số\ server \times Lượng\ tài\ giờ\ cao\ điểm}{Tổng\ thời\ gian\ cao\ điểm} = \frac{5 \times (500 \times 0.8 \times 8)}{3 \times 3600} = 1.481 \text{Mbps}$$

$$Throughput = \frac{Số\ server \times Tổng\ lượng\ tài}{Tổng\ thời\ gian} = \frac{5 \times (500 \times 8)}{8 \times 3600} = 0.694 \text{Mbps}$$

Đối với 100 workstations, 80% tổng lượng tải tập trung vào 3 tiếng giờ cao điểm (9h-11h: 2 tiếng và 15h-16h: 1 tiếng), tổng thời gian làm việc với thời lượng 8 tiếng/ngày với tổng dung lượng 100MB/ngày đối với 1 máy:

$$Bandwidth = \frac{Số\ máy \times Lượng\ tài\ giờ\ cao\ điểm}{Tổng\ thời\ gian\ cao\ điểm} = \frac{100 \times (100 \times 0.8 \times 8)}{3 \times 3600} = 5.926 \text{Mbps}$$

$$Throughput = \frac{Số\ máy \times Tổng\ lượng\ tài}{Tổng\ thời\ gian} = \frac{100 \times (100 \times 8)}{8 \times 3600} = 2.78 \text{Mbps}$$

Tổng bandwidth và throughput cho kết nối có dây của hệ thống là:

$$\begin{aligned} \sum Bandwidth &= 1.481 + 5.926 = 7.407 \text{Mbps} \\ \sum Throughput &= 0.694 + 2.78 = 3.474 \text{Mbps} \end{aligned}$$

- Kết nối không dây

Đối với các thiết bị kết nối không dây của các khách hàng, 80% tổng lượng tải tập trung vào 3 tiếng giờ cao điểm (9h-11h: 2 tiếng và 15h-16h: 1 tiếng), tổng thời gian làm việc với thời lượng 8 tiếng/ngày với tổng dung lượng trung bình 50MB/ngày đối với tất cả thiết bị của khách hàng:

$$Bandwidth = \frac{Lượng\ tài\ giờ\ cao\ điểm}{Tổng\ thời\ gian\ cao\ điểm} = \frac{50 \times 0.8 \times 8}{3 \times 3600} = 0.0296 \text{Mbps}$$

$$Throughput = \frac{Tổng\ lượng\ tài}{Tổng\ thời\ gian} = \frac{50 \times 8}{8 \times 3600} = 0.0139 \text{Mbps}$$

## 7.2 Các chi nhánh

- Kết nối có dây

Ở trụ sở chính gồm 3 servers, 80% tổng lượng tải tập trung vào 3 tiếng của các giờ cao điểm (9h-11h: 2 tiếng và 15h-16h: 1 tiếng), tổng thời gian làm việc với thời lượng 8 tiếng/ngày với tổng dung lượng 500MB/ngày đối với 1 server:

Đối với 50 workstations, 80% tổng lượng tải tập trung vào 3 tiếng giờ cao điểm (9h-11h:

$$Bandwidth = \frac{Số\ server \times Lượng\ tải\ giờ\ cao\ điểm}{Tổng\ thời\ gian\ cao\ điểm} = \frac{3 \times (500 \times 0.8 \times 8)}{3 \times 3600} = 0.889 Mbps$$

$$Throughput = \frac{Số\ server \times Tổng\ lượng\ tải}{Tổng\ thời\ gian} = \frac{3 \times (500 \times 8)}{8 \times 3600} = 0.417 Mbps$$

2 tiếng và 15h-16h: 1 tiếng), tổng thời gian làm việc với thời lượng 8 tiếng/ngày với tổng dung lượng 100MB/ngày đối với 1 máy:

$$Bandwidth = \frac{Số\ máy \times Lượng\ tải\ giờ\ cao\ điểm}{Tổng\ thời\ gian\ cao\ điểm} = \frac{50 \times (100 \times 0.8 \times 8)}{3 \times 3600} = 2.963 Mbps$$

$$Throughput = \frac{Số\ máy \times Tổng\ lượng\ tải}{Tổng\ thời\ gian} = \frac{50 \times (100 \times 8)}{8 \times 3600} = 1.39 Mbps$$

Tổng bandwidth và throughput cho kết nối có dây của hệ thống là:

$$\begin{aligned} \sum Bandwidth &= 0.889 + 2.963 = 3.852 Mbps \\ \sum Throughput &= 0.417 + 1.39 = 1.807 Mbps \end{aligned}$$

- Kết nối không dây

Đối với các thiết bị kết nối không dây của các khách hàng, 80% tổng lượng tải tập trung vào 3 tiếng giờ cao điểm (9h-11h: 2 tiếng và 15h-16h: 1 tiếng), tổng thời gian làm việc với thời lượng 8 tiếng/ngày với tổng dung lượng trung bình 50MB/ngày đối với tất cả thiết bị của khách hàng::

$$Bandwidth = \frac{Lượng\ tài\ giờ\ cao\ điểm}{Tổng\ thời\ gian\ cao\ điểm} = \frac{50 \times 0.8 \times 8}{3 \times 3600} = 0.0296 \text{Mbps}$$

$$Throughput = \frac{Tổng\ lượng\ tài}{Tổng\ thời\ gian} = \frac{50 \times 8}{8 \times 3600} = 0.0139 \text{Mbps}$$

## 8 Sơ đồ IP của Ngân Hàng

### 8.1 Tại trụ sở chính

Địa chỉ từ Switch tổng được chia thành các VLAN:

- Tầng 1 - Phòng IT và Phòng Cabling Central Local (VLAN 10)
  - Địa chỉ IP và Subnet Mask của mạng con là: 192.168.1.1/24
- Tầng 2 (VLAN 20)
  - Địa chỉ IP và Subnet Mask của mạng con là: 192.168.2.1/24
- Tầng 3 (VLAN 30)
  - Địa chỉ IP và Subnet Mask của mạng con là: 192.168.3.1/24
- Tầng 4 (VLAN 40)
  - Địa chỉ IP và Subnet Mask của mạng con là: 192.168.4.1/24
- Tầng 5 (VLAN 50)
  - Địa chỉ IP và Subnet Mask của mạng con là: 192.168.5.1/24
- Tầng 6 (VLAN 60)
  - Địa chỉ IP và Subnet Mask của mạng con là: 192.168.6.1/24
- Tầng 7 (VLAN 70)
  - Địa chỉ IP và Subnet Mask của mạng con là: 192.168.7.1/24

### 8.2 Tại chi nhánh

Tại chi nhánh Đà Nẵng

Địa chỉ từ Switch tổng được chia thành các VLAN:

- Phòng IT và Phòng Cabling Central Local (VLAN 90)
  - Địa chỉ IP và Subnet Mask của mạng con tại chi nhánh Đà Nẵng là : 192.168.9.1/24
- Tầng 2 (VLAN 80)
  - Địa chỉ IP và Subnet Mask của mạng con tại chi nhánh Đà Nẵng là : 192.168.8.1/24

Tại chi nhánh Nha Trang

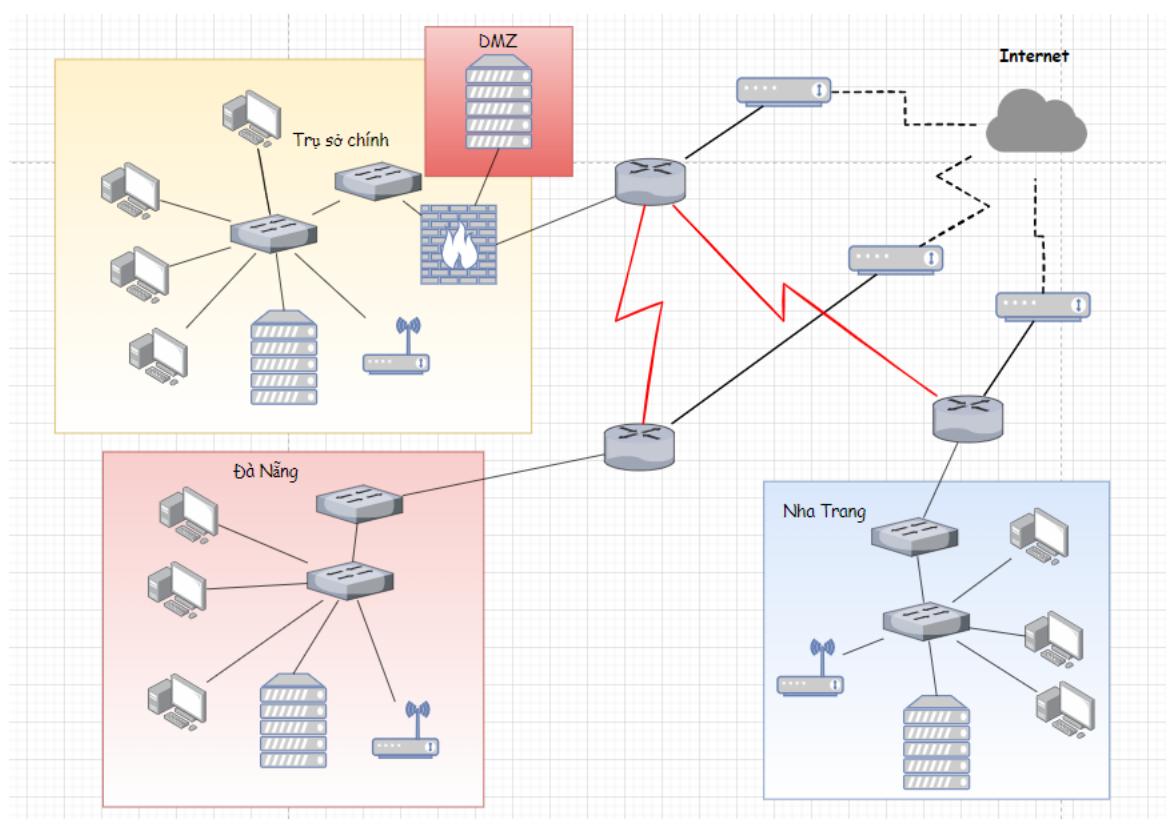
Địa chỉ từ Switch tổng được chia thành các VLAN:

- Phòng IT và Phòng Cabling Central Local (VLAN 110)
  - Địa chỉ IP và Subnet Mask của mạng con tại chi nhánh Nha Trang là : 192.168.11.1/24
- Phòng giao dịch (VLAN 100)
  - Địa chỉ IP và Subnet Mask của mạng con tại chi nhánh Nha Trang là : 192.168.10.1/24

### 8.3 khác

- Địa chỉ IP từ router chi nhánh Đà Nẵng và trụ sở chính: 14.0.0.1/8
- Địa chỉ IP từ router chi nhánh Nha Trang và trụ sở chính: 15.0.0.1/8
- Địa chỉ IP từ switch layer 3 đến tường lửa trụ sở chính: 192.168.100.0/24
- Địa chỉ IP từ tường lửa tới router của trụ sở chính: 192.168.101.0/24
- Địa chỉ IP vùng DMZ của trụ sở chính: 192.168.12.0/24
- Địa chỉ IP từ switch layer 3 đến router chi nhánh Đà Nẵng: 192.168.150/24
- Địa chỉ IP từ switch layer 3 đến router chi nhánh Nha Trang: 192.168.200/24
- Địa chỉ IP của router mỗi chi nhánh kết nối tới router của ISP: 20.110.24.1/24
- Địa chỉ IP của server public trên mạng internet 8.8.8.0/24

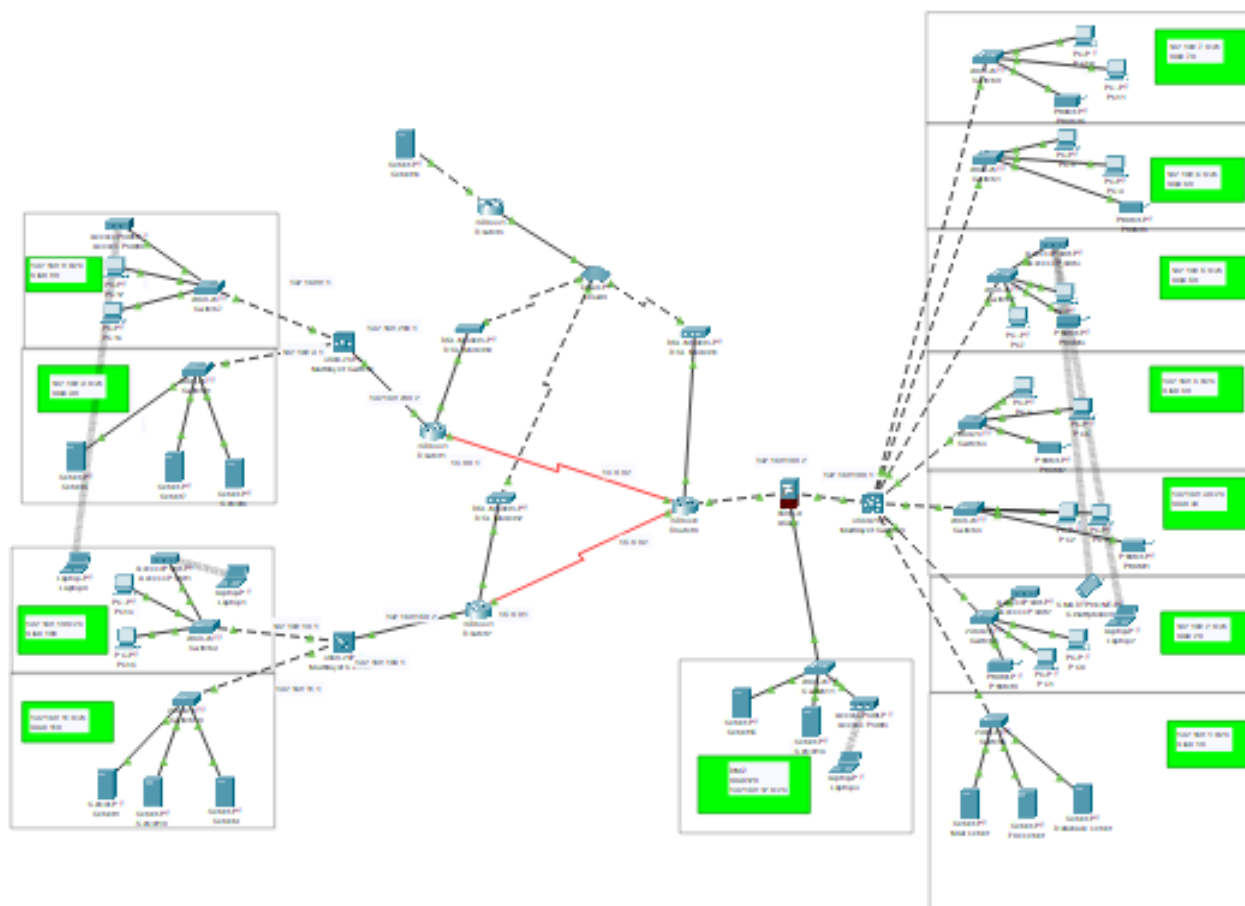
## 9 Sơ đồ kết nối WAN



Hình 7: Sơ đồ kết nối WAN

## 10 Thiết kế sơ đồ mạng dùng Packet Tracer

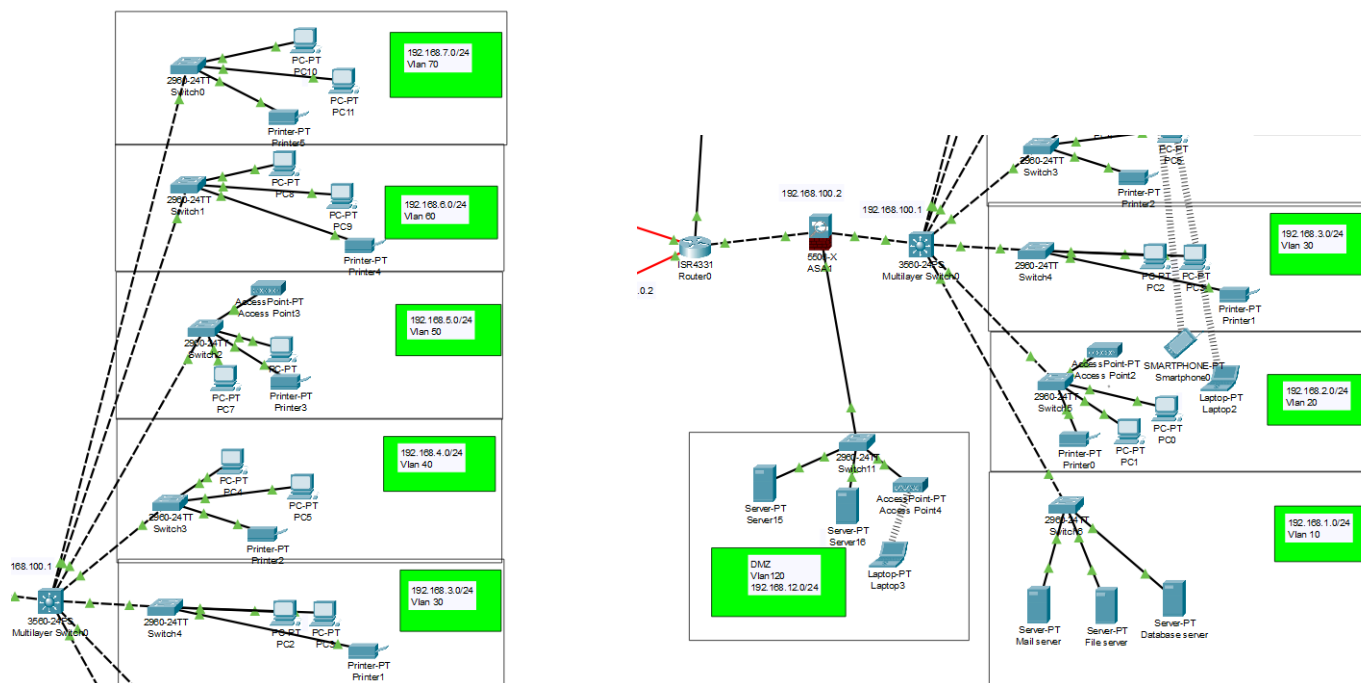
### 10.1 Sơ đồ tổng thể



Hình 8: Sơ đồ toàn bộ hệ thống mạng

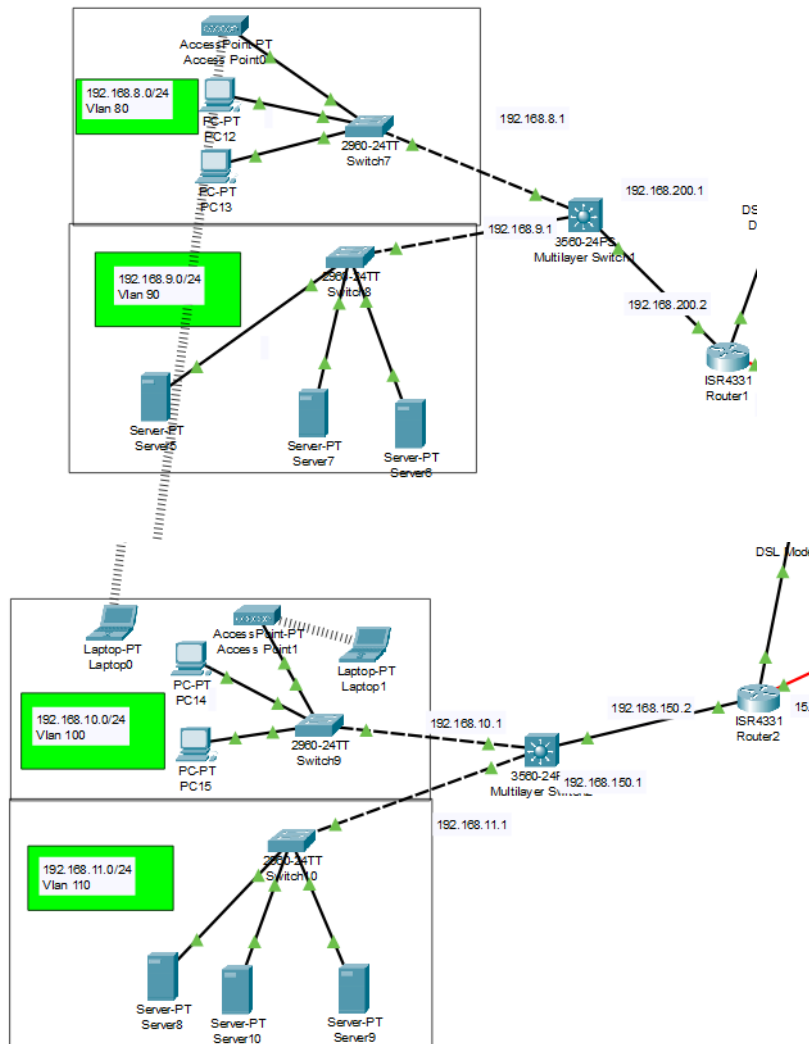


## 10.2 Thiết kế mạng tại trụ sở



Hình 9: Thiết kế mạng tại trụ sở















### 10.3 Thiết kế mạng tại 2 chi nhánh



Hình 10: Thiết kế mạng hai chi nhánh

## 11 Kiểm tra

### 11.1 Thực hiện kiểm tra các kết nối

PDU List Window								
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC1	PC12	ICMP		0.000	N	0
	Successful	PC1	PC14	ICMP		0.000	N	1
	Failed	PC12	PC1	ICMP		0.000	N	2
	Successful	PC12	PC14	ICMP		0.000	N	3
	Successful	PC1	Server14	ICMP		0.000	N	4
	Successful	Laptop3	Server14	ICMP		0.000	N	5
	Successful	PC13	Server14	ICMP		0.000	N	6

Hình 11: Kiểm tra các kết nối thông qua việc ping các thành phần

Thứ tự	Kết nối	Chi tiết	Kết quả
1	Kết nối từ trụ sở đến chi nhánh	Kiểm tra kết nối từ tầng 1 trụ sở chính đến tầng 2 của chi nhánh Đà Nẵng	Successful
2	Kết nối từ trụ sở đến chi nhánh	Kiểm tra kết nối từ tầng 1 trụ sở chính đến tầng 2 của chi nhánh Nha Trang	Successful
3	Kết nối từ chi nhánh đến trụ sở	Kiểm tra kết nối từ tầng 2 của chi nhánh Đà Nẵng đến tầng 1 của trụ sở chính	Failed
4	Kết nối giữa các chi nhánh với nhau	Kiểm tra kết nối từ tầng 2 chi nhánh Đà Nẵng đến tầng 2 chi nhánh Nha Trang	Successful
5	Kết nối Internet thông qua ISP từ trụ sở	Kiểm tra kết nối từ tầng 1 trụ sở chính đến 1 server nằm bên ngoài mạng WAN	Successful
6	Kết nối Internet thông qua ISP từ vùng DMZ của trụ sở	Kiểm tra kết nối từ thiết bị wireless của khách hàng trong vùng DMZ đến 1 server nằm bên ngoài mạng WAN	Successful
7	Kết nối Internet thông qua ISP từ chi nhánh	Kiểm tra kết nối từ tầng 2 của chi nhánh Đà Nẵng đến 1 server nằm bên ngoài mạng WAN	Successful









### 11.2 Thực hiện kiểm tra kết nối với phương thức bảo mật

Nhờ cấu hình tường lửa với từng security-level như sau:

- Mạng LAN trụ sở chính: 100

- Vùng dmz: 50
- Vùng phía ngoài router của trụ sở: 0

Với cơ chế từ vùng có security-level cao có thể truy cập tới vùng thấp hơn. Từ trụ sở chính có thể truy cập tới dmz, internet và 2 chi nhánh. Từ dmz có thể truy cập tới internet và 2 chi nhánh. Ngược lại dmz và bên ngoài không thể truy cập trụ sở chính. Đồng thời ta cấu hình access-list để từ bên ngoài có thể truy cập tới server public của dmz (192.168.12.2)

PDU List Window								
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Failed	PC12	PC1	ICMP		0.000	N	0
	Failed	Server16	Mail server	ICMP		0.000	N	1
	Failed	Server14	Database server	ICMP		0.000	N	2
	Successful	PC12	Server15	ICMP		0.000	N	3

Hình 12: Thực hiện kiểm tra kết nối với phương thức bảo mật

Thứ tự	Kết nối	Chi tiết	Kết quả
1	Kết nối từ chi nhánh đến trụ sở chính	Kiểm tra kết nối từ tầng 1 trụ sở chính đến tầng 2 của chi nhánh Đà Nẵng	Failed
2	Kết nối từ vùng DMZ đến server của trụ sở	Kết nối từ thiết bị wireless của khách hàng trong vùng DMZ đến server bảo mật của trụ sở	Failed
3	Kết nối từ bên ngoài đến mạng LAN của trụ sở	Kiểm tra kết nối từ 1 thiết bị nằm ngoài mạng LAN của trụ sở đến 1 máy tính thuộc mạng LAN của trụ sở	Failed
4	Kết nối đến public server của trụ sở	Kết nối thiết bị nằm ngoài mạng LAN của trụ sở đến server được public trong vùng DMZ của trụ sở	Successful

## 12 Bảo mật và an toàn khi xảy ra sự cố

### 12.1 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:

- Kiểm soát việc truy cập của người sử dụng

- Đảm bảo an toàn cho dữ liệu truyền, nhận qua các dịch vụ đường truyền internet
- Hệ thống phải đạt chuẩn và phù hợp với kinh tế của ngân hàng
- Đáp ứng được nhu cầu mở rộng của ngân hàng trong tương lai

## 12.2 Xác định các tài nguyên cần được bảo vệ

- Phần cứng: Các máy chủ mạng, các máy trạm, các thiết bị mạng như Router, Switch, Server,...
- Phần mềm: Hệ điều hành của các máy chủ Linux, Windows NT, . . . , chương trình quản lý thông tin khách hàng (tài khoản, thẻ tín dụng, ...), các chương trình diệt virus, chương trình kế toán, tự động hóa văn phòng, truyền dữ liệu, ATM, ...
- Dữ liệu: rất quan trọng đối với hệ thống ngân hàng. Dữ liệu này bao gồm các dữ liệu liên quan đến thông tin cá nhân khách hàng, các giao dịch, danh sách nhân viên, dữ liệu doanh thu,...
- Tài liệu: Các công văn, báo cáo, tài liệu, sách vở, tài liệu hướng dẫn sử dụng, ...

## 12.3 Xác định các tài nguyên cần được bảo vệ

### 12.3.1 Mối đe dọa từ bên trong

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 giao dịch chuyển tiền, thanh toán, ... gây ra những tổn thất nghiêm trọng.

### 12.3.2 Mối đe dọa từ bên ngoài

Người sử dụng bên trong mạng có thể truy cập vào các tài nguyên của hệ thống. Đối với ngân hàng có đặc thù lớn do nhiều mạng LAN của trụ sở và các chi nhánh kết nối vào, vì vậy người sử dụng cố ý muốn truy cập muốn truy cập vào dữ liệu bên trong hệ thống có thể gây tổn hại đến hệ thống như: ăn cắp dữ liệu nhằm mục đích xấu, làm hệ thống nhiễm virus,...

## 12.4 Các giải pháp bảo mật

- Bảo mật 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.
- Hệ thống tường lửa (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: 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

## 13 Đánh giá hệ thống

### 13.1 Ưu điểm

- Hệ thống mạng đáp ứng tương đối phù hợp với yêu cầu đưa ra, dễ dàng nâng cấp phù hợp sự phát triển sau này.
- Hệ thống mạng Wifi cho khách được tách biệt với hệ thống mạng LAN nội bộ của nhân viên, đảm bảo an toàn thông tin.
- Mạng chia thành các Vlan nên dễ dàng trong việc nâng cấp, sửa chữa
- Khi một mạng con có vấn đề sẽ không ảnh hưởng đến toàn bộ mạng LAN
- Thiết kế dùng có thể dùng 2 lớp switch cho phép mở rộng thêm số lượng tầng trong tòa nhà và số lượng máy trong mỗi tầng.
- Thực hiện được bảo mật bằng cách sử dụng cơ chế khoanh vùng VLAN truy cập
- Đem lại những lợi ích của kiến trúc 3 ngôi: gọn gàng, hiệu quả cao, dễ nâng cấp, quản lý và sửa lỗi.

### 13.2 Hạn chế

- Chi phí dự trù thực hiện giải pháp khá cao
- Chưa có kinh nghiệm trong việc thiết kế một hệ thống mạng tối ưu cho ngân hàng.
- Mức truy cập giữa người dùng internet và những chi nhánh là như nhau khiến chi nhánh chưa thể truy cập được dmz của trụ sở chính

### 13.3 Định hướng phát triển tương lai

- Duy trì kết nối ổn định, thực hiện bảo trì hệ thống định kỳ.
- Thêm vào switch multiplayer ở các chi nhánh để tăng khả năng mở rộng hệ thống mạng.
- Tiếp tục xây dựng mô hình của các thiết bị chưa được mô phỏng như Firewall
- Kết nối thêm nhiều server với các chức năng khác.
- Hoàn thiện thiết kế để giảm thiểu chi phí đầu tư ban đầu, lựa chọn thêm các thiết bị phù hợp với yêu cầu sử dụng.
- Tìm biện pháp khắc phục các nhược điểm đã trình bày ở phần trên.