

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC BÁCH KHOA

KHOA KHOA HỌC & KỸ THUẬT MÁY TÍNH



# **BÁO CÁO BÀI TẬP LỚN 2**

## **MÔN: MẠNG MÁY TÍNH 1**

GVHD: NGUYỄN HỒNG NAM

*Lớp: MT12KHTN*

*Nhóm: Aloha Solution*

*Thành viên:*

VÕ AN KHƯƠNG

51201761

HUỖNH TẤN PHÚC

51202787

NGUYỄN THANH TÙNG

51204401

## Mục lục

|             |  |           |
|-------------|--|-----------|
| <b>I.</b>   | <b>Tóm lược dự án .....</b>  | <b>3</b>  |
| 1.          | Mô tả dự án .....  | 3         |
| 2.          | Giả thiết dự án .....  | 4         |
| <b>II.</b>  | <b>Phân tích và đưa ra giải pháp .....</b>                         | <b>5</b>  |
| 1.          | Mạng trụ sở .....  | 5         |
| 2.          | Mạng nhà máy .....   | 6         |
| 3.          | Mạng WAN cho công ty .....   | 6         |
| 4.          | Throughput, bandwidth và các thông số an toàn .....                | 6         |
| <b>III.</b> | <b>Các công nghệ sử dụng.....</b>                                  | <b>8</b>  |
| 1.          | VLAN (Virtual Local Area Network) .....                            | 8         |
| 2.          | VTP (VLAN Trunking Protocol) .....                                 | 9         |
| 3.          | RIP (Routing Information Protocol) .....                           | 9         |
| 4.          | VPN (Virtual private network) .....                                | 9         |
| 5.          | DNS (Domain Name System) .....                                     | 10        |
| 6.          | NAT (Network Address Translation) .....                            | 10        |
| 7.          | Frame Relay .....  | 11        |
| 8.          | Tường lửa (Firewall) .....   | 11        |
| <b>IV.</b>  | <b>Thiết kế.....</b>   | <b>12</b> |
| 1.          | Sơ đồ tòa nhà.....   | 12        |
| 2.          | Sơ đồ kết nối dây .....  | 15        |
| 3.          | Sơ đồ mạng WAN giữa trụ sở và hai nhà máy.....                     | 18        |
| 4.          | Sơ đồ IP .....   | 18        |
| 5.          | Danh sách các thiết bị đề xuất và đặc điểm kỹ thuật điển hình..... | 19        |
| 6.          | Chọn lựa thiết bị và số lượng .....                                | 23        |
| <b>V.</b>   | <b>Kết luận .....</b>  | <b>25</b> |
| 1.          | Đánh giá hệ thống mạng.....  | 25        |
| 2.          | Những khó khăn trong thiết kế .....                                | 25        |
| 3.          | Định hướng phát triển.....   | 26        |
| 4.          | Những hạn chế của dự án .....                                      | 26        |

|    |                                      |    |
|----|--------------------------------------|----|
| 5. | Kiến thức, kinh nghiệm thu được..... | 26 |
| 6. | Góp ý.....                           | 26 |

## I. Tóm lược dự án

### 1. Mô tả dự án

Công ty có trụ sở đặt tại Quận 1 và hai nhà máy đặt tại Bình Định và Bình Dương.

Trụ sở công ty là tòa nhà cao 3 tầng:

- Có tổng cộng 100 máy tính, tất cả đều kết nối vào mạng. Trong đó: ban giám đốc và cấp quản lý có 15 máy, bộ phận văn phòng có 30 máy, bộ phận bán hàng có 30 máy, các bộ phận khác 25 máy. Các bộ phận cần được phân quyền phù hợp để đảm bảo tính riêng tư. Ban giám đốc và quản lý có quyền truy cập đến tất cả các máy.
- Các nhân viên và khách hàng đến giao dịch đa phần sử dụng smart-phone kết nối Internet thông qua Wifi
- Tại phòng kỹ thuật mạng (tầng 1) có 6 server: 4 server dùng để lưu trữ dữ liệu, 2 server dùng cho hệ thống web, mail và chạy các ứng dụng quản lý điều hành
- Hạ tầng mạng 100/1000 Mbps, Wired và Wireless
- Dùng kết hợp giữa Licensed và Open source Softwares
- Mỗi tầng có máy in dùng chung.
- Có 2 phòng họp trang bị hệ thống Teleconference.

Mỗi nhà máy có 2 tầng:

- Có 2 server (tầng 1) để lưu trữ dữ liệu và chạy các ứng dụng quản lý.
- Tại tầng 2 có 20 workstation, tất cả đều kết nối vào mạng. Bộ phận quản lý có 5 máy, phần còn lại là của các nhân viên. Yêu cầu phân quyền truy cập hợp lý.
- Có một phòng họp trang bị hệ thống Teleconference
- Có 2 máy in kết nối mạng.
- Các nhân viên văn phòng và khách hàng đến giao dịch đa phần sử dụng smart-phone kết nối Internet thông qua Wifi.

Kết nối giữa trụ sở và nhà máy được thực hiện thông qua đường kết nối WAN.

Lưu lượng và tải của hệ thống (tập trung khoảng 80% vào giờ cao điểm 8g-11g và 14g-16g) dùng chung cho trụ sở và nhà máy như sau:

- Servers dùng cho web access, database access,... lưu lượng upload và download vào khoảng 4GB/server/ngày.
- Mỗi workstation dùng cho duyệt web, tải tài liệu, giao dịch khách hàng,... lưu lượng upload và download vào khoảng 400MB/máy/ngày.

- Các thiết bị kết nối WiFi, lưu lượng sử dụng khoảng 50MB/thiết bị/ngày.

Hệ thống mạng máy tính của công ty được thiết kế cho mức độ phát triển 20% trong 5 năm (về số lượng người sử dụng, tải trọng mạng, mở rộng nhà xưởng,...). Yêu cầu bảo mật cao, an toàn khi xảy ra sự cố, dễ dàng nâng cấp hệ thống.

## **2. Giả thiết dự án**

Một số giả thiết được sử dụng cho dự án:

Công ty sử dụng dãy IP 172.16.0.0/23.

Khoảng cách giữa trụ sở (Q1) với nhà máy 1 (Bình Dương) là 50 km, giữa trụ sở với nhà máy 2 (Bình Định) là 600 km, khoảng cách giữa 2 nhà máy là 500 km.

Trụ sở được thiết kế như sau:

- Tầng 1: là nơi tập trung dây mạng, patch panel, 6 server và 1 máy in.
- Tầng 2: gồm 4 phòng:
  - Phòng 1: Có 30 máy cho bộ phận bán hàng.
  - Phòng 2: Có 25 máy cho bộ phận khác.
  - Phòng 3: Có 7 máy cho ban quản lý.
  - Phòng 4: Là phòng họp teleconference, có 1 TV kết nối internet.
- Tầng 3: gồm 4 phòng
  - Phòng 1: Có 30 máy cho bộ phận văn phòng.
  - Phòng 2: Có 7 máy cho ban quản lý.
  - Phòng 3: Có 1 máy cho giám đốc.
  - Phòng 4: Là phòng họp teleconference, có 1 TV kết nối internet.

Tại mỗi tầng có thể có 30 thiết bị kết nối wifi vào giờ cao điểm.

Nhà máy được thiết kế như sau:

- Tầng 1: là nơi tập trung dây mạng, patch panel, 2 server.
- Tầng 2: gồm 3 phòng:
  - Phòng 1: Có 15 workstation cho nhân viên, mỗi workstation có 1 máy. Trong phòng có 1 máy in.
  - Phòng 2: Có 5 workstation cho ban quản lý, mỗi workstation có 1 máy. Trong phòng có 1 máy in.
  - Phòng 3: Là phòng họp teleconference, có 1 TV kết nối internet.

Tại mỗi tầng có thể có 20 thiết bị kết nối wifi vào giờ cao điểm.

Mỗi TV trong phòng họp teleconference có tốc độ truyền tải là 1 Mbps.

## **II. Phân tích và đưa ra giải pháp**

### **1. Mạng trụ sở**

- Trong trụ sở có một phòng kỹ thuật đặt tại tầng 1, phòng này là nơi tập trung dây mạng, patch panel, 6 server và một router để kết nối với mạng WAN.
- Các server được cấu hình như sau: 4 server dùng để lưu dữ liệu, 1 server dùng cho hệ thống web/mail/dns và 1 server dùng để chạy các ứng dụng quản lý điều hành.
- Tại tầng 1, với ưu điểm dễ dàng kiểm soát và khắc phục sự cố, tận dụng được tối đa tốc độ truyền của đường truyền vật lý và dễ dàng mở rộng, chúng ta sẽ sử dụng mạng hình sao để kết nối các server với nhau: các server sẽ kết nối đến một switch phòng kỹ thuật và từ switch này nối đến switch của tầng 1.
- Trong mạng của trụ sở, vì có khá nhiều máy tính và các thiết bị mạng khác nên tại mỗi tầng của trụ sở đặt một switch chung cho mỗi tầng. Tùy theo số lượng máy của mỗi phòng mà cần sử dụng thêm switch hay không.
- Tầng 2 gồm 4 phòng. Bộ phận bán hàng và bộ phận khác dùng mô hình mạng lai vòng – sao. Do hai bộ phận này có nhiều máy nên với mô hình này khi một đường kết nối giữa hai switch bị lỗi thì mô hình vẫn hoạt động bình thường. Tính mở rộng của hệ thống cao và thừa kế được nhiều ưu điểm của mạng vòng và mạng sao. Bộ phận quản lý vì số lượng máy khá ít nên chỉ cần một switch cho phòng quản lý, switch này sẽ nối đến switch chung của tầng, các máy tính sẽ nối theo mô hình sao. Phòng họp teleconference có một TV kết nối internet, được nối trực tiếp đến switch chung của tầng.
- Tầng 3 gồm 3 phòng. Bộ phận văn phòng được thiết kế giống như mô hình của bộ phận bán hàng. Bộ phận quản lý được thiết kế giống như mô hình ở tầng 2. Phòng của giám đốc chỉ có 1 máy tính nên máy tính này sẽ kết nối trực tiếp với switch của tầng 3. Phòng họp teleconference có một TV kết nối internet, được nối trực tiếp đến switch chung của tầng.
- Các nhân viên và khách hàng đa phần đến giao dịch có sử dụng smart-phone để kết nối wifi nên chúng ta sẽ đặt giữa mỗi tầng 1 wireless access point để bảo đảm phủ sóng toàn tầng.
- Mỗi tầng đều có một máy in và máy in sẽ kết nối đến switch của tầng đó.
- Để đảm bảo tính riêng tư giữa các phòng ban, chúng tôi sẽ cấu hình mỗi phòng ban đó 1 VLAN riêng.
- Để đảm bảo ràng buộc về truy cập giữa giám đốc, ban quản lý và nhân viên, chúng tôi sẽ cài đặt phần mềm Windows Server 2015 trên server chạy các ứng dụng quản lý điều hành của trụ sở.

## 2. Mạng nhà máy

- Trong nhà máy có một phòng kỹ thuật đặt tại tầng 1, phòng này là nơi tập trung dây mạng, patch panel, 2 server và một router dùng để kết nối với mạng WAN.
- Các server được cấu hình như sau: 1 server để lưu dữ liệu và 1 server để chạy các ứng dụng quản lý điều hành.
- Trong mạng của nhà máy, vì có khá nhiều máy tính và các thiết bị mạng khác nên tại mỗi tầng của trụ sở đặt một switch cung cho mỗi tầng. Tùy theo số lượng máy của mỗi phòng mà cần sử dụng thêm switch hay không.
- Tại tầng 1, với ưu điểm dễ dàng kiểm soát và khắc phục sự cố, tận dụng được tối đa tốc độ truyền của đường truyền vật lý và dễ dàng mở rộng, chúng ta sẽ sử dụng mạng hình sao để kết nối các server với nhau: các server sẽ kết nối đến một switch phòng kỹ thuật và từ switch này nối đến switch của tầng 1.
- Tầng 2 gồm 3 phòng. Phòng nhân viên dùng mô hình mạng lai vòng – sao. Do phòng này có nhiều máy nên với mô hình này khi một đường kết nối giữa hai switch bị lỗi thì mô hình vẫn hoạt động bình thường. Tính mở rộng của hệ thống cao và thừa kế được nhiều ưu điểm của mạng vòng và mạng sao. Phòng quản lý vì số lượng máy khá ít nên chỉ cần một switch cho phòng quản lý, switch này sẽ nối đến switch chung của tầng, các máy tính sẽ nối theo mô hình sao. Phòng họp teleconference có một TV kết nối internet, được nối trực tiếp đến switch chung của tầng. Phòng nhân viên và phòng quản lý đều có một máy in kết nối trực tiếp đến switch của từng phòng.
- Các nhân viên và khách hàng đa phần đến giao dịch có sử dụng smart-phone để kết nối wifi nên chúng ta sẽ đặt giữa mỗi tầng 1 wireless access point để bảo đảm phủ sóng toàn tầng.
- Để đảm bảo tính riêng tư giữa các phòng ban, chúng tôi sẽ cấu hình mỗi phòng ban đó 1 VLAN riêng.
- Để đảm bảo ràng buộc về truy cập giữa ban quản lý và nhân viên, chúng tôi sẽ cài đặt phần mềm Windows Server 2015 trên server chạy các ứng dụng quản lý điều hành của nhà máy.

## 3. Mạng WAN cho công ty

Do khoảng cách giữa trụ sở và các nhà máy quá xa nhau, nên chúng ta sử dụng dịch vụ VPN (Virtual Private Network) được cung cấp bởi Viettel để giảm thiểu chi phí đi dây, tính ổn định và bảo mật cao.

Đồng thời chúng ta cũng thuê một kênh truy cập Internet bởi Viettel.

## 4. Throughput, bandwidth và các thông số an toàn

### • Mạng trụ sở:

Throughput của PC: Bao gồm có 100 PC, mỗi PC tập trung cao nhất khoảng 80% vào 5 giờ cao điểm, trong đó download và upload khoảng 400MB/máy/ngày.

$$\frac{100 \times 400 \times 80\%}{5 \times 3600} = 1.778MB/s = 14.913Mbps$$

Throughput của server: Bao gồm 6 server, mỗi server tập trung cao nhất khoảng 80% vào 5 giờ cao điểm, trong đó download và upload khoảng 4GB/server/ngày.

$$\frac{6 \times (4 \times 1024) \times 80\%}{5 \times 3600} = 1.092MB/s = 9.163Mbps$$

Throughput của 2 phòng họp: Mỗi phòng họp có 1 TV với tốc độ truyền tải là 1Mbps.

$$2 \times (1 Mbps) = 2 Mbps$$

Throughput của 3 máy in: Mỗi máy in có tốc độ truyền tải là 600 Kbps.

$$3 \times (600 \times 10^{-3}) = 1.8 Mbps$$

Throughput của các thiết bị kết nối wifi: Giả sử mỗi tầng có 30 thiết bị kết nối wifi, mỗi thiết bị tập trung 80% vào 5 giờ cao điểm, tốc độ download và upload 50MB/thiết bị/ngày.

$$\frac{3 \times 30 \times 50 \times 80\%}{5 \times 3600} = 0.2 MB/s = 1.678 Mbps$$

Tổng throughput của trụ sở với khả năng mở rộng là 20%:

$$(14.913 + 9.163 + 2 + 1.8 + 1.678) \times 120\% = 35.465 Mbps$$

Vậy bandwidth của trụ sở là 36 Mbps.

- **Mạng nhà máy:**

Throughput của PC: 20 PC, mỗi máy có độ tập trung cao nhất khoảng 80% trong 5 giờ, bao gồm download và upload khoảng 400MB/máy/ngày.

$$\frac{20 \times 400 \times 80\%}{5 \times 3600} = 0.356MB/s = 2.913Mbps$$

Throughput của Server: 2 server, mỗi server có độ tập trung cao nhất khoảng 80% trong 5 giờ, bao gồm download và upload khoảng 4GB/server/ngày.

$$\frac{2 \times 4 \times 1024 \times 80\%}{5 \times 3600} = 0.364MB/s = 2.983Mbps$$

Throughput của 1 phòng họp: 1 Teleconference, có 1 tivi có tốc độ truyền là 1Mbps.

$$1Mbps$$

Throughput của 2 máy in: mỗi máy in có tốc độ truyền là 600Kbps

$$600 \times 2 \times 10^{-3} = 1.2Mbps$$



Throughput của thiết bị kết nối mạng: giả sử nhà máy có 20 thiết bị/ tầng, mỗi tầng tập trung cao nhất 80% trong 5 giờ cao điểm, với tốc độ download và upload khoảng 50MB/thiết bị/ngày.

$$\frac{50 \times 2 \times 20 \times 80\%}{5 \times 3600} = 0.089 \text{ MB/s} = 0.728 \text{ Mbps}$$

Tổng throughput của nhà máy với khả năng mở rộng 20% :

$$(2.913 + 2.983 + 1 + 1.2 + 0.728) \times 120\% = 10.589 \text{ Mbps}$$

Vậy bandwidth của mạng nhà máy là 11Mbps

- **Mạng WAN của công ty:**

Tổng throughput trong đường dây mạng WAN bao gồm throughput của trụ sở và cả 2 công ty.

$$35.465 + 10.589 \times 2 = 56.643 \text{ Mbps}$$

Vậy bandwidth của mạng WAN cho công ty là 57 Mbps.

### III. Các công nghệ sử dụng

#### 1. VLAN (Virtual Local Area Network)

VLAN là một kỹ thuật cho phép tạo lập các mạng LAN độc lập một cách logic trên cùng một kiến trúc hạ tầng vật lý. Trong tình huống bài tập lớn này nhóm chúng tôi đã thiết kế cho mỗi phòng ban một VLAN riêng để đảm bảo tính riêng tư. Việc tạo lập nhiều mạng LAN ảo trong cùng một mạng cục bộ giúp giảm thiểu vùng quảng bá (broadcast domain) cũng như tạo thuận lợi cho việc quản lý một mạng cục bộ rộng lớn.

- Phân loại:
  - VLAN dựa trên cổng (port based VLAN). Loại này phổ biến nhất và được sử dụng trong bài tập lớn này. Mỗi máy tính kết nối tới một cổng trên switch đều thuộc một VLAN nào đó.
  - VLAN dựa trên địa chỉ vật lý MAC.
  - VLAN dựa trên giao thức.
- Ưu nhược điểm:
  - Tiết kiệm băng thông của mạng: Do VLAN có thể chia nhỏ LAN thành các vùng( vùng quảng bá – broadcast domain). Khi một gói tin quảng bá, nó sẽ lan truyền trong một mạng VLAN duy nhất, không truyền sang các VLAN khác nên tiết kiệm được băng thông đường truyền.

- Tăng khả năng bảo mật: Các VLAN khác nhau không truy cập vào nhau được (ngoại trừ có việc khai báo định tuyến).
- Dễ dàng thêm hay bớt các máy tính vào VLAN nên mạng có tính linh động cao.

## 2. VTP (VLAN Trunking Protocol)

VTP là công nghệ giúp cho đường truyền có thể truyền nhiều gói tin của các VLAN khác nhau.

- Ưu và nhược điểm:
  - Giúp tiết kiệm chi phí đường truyền.
  - Hoạt động hiệu quả.

## 3. RIP (Routing Information Protocol)

RIP là giao thức định tuyến bên trong miền sử dụng thuật toán định tuyến distance-vector (gửi 1 bản sao của bản định tuyến từ router này đến router kia theo chu kì 30s). Các router trong bài tập lớn đều sử dụng RIP để định tuyến.

- Ưu và nhược điểm:
  - Cấu hình cho router đơn giản hơn so với định tuyến bằng static.
  - Được hỗ trợ bởi nhiều loại thiết bị.
  - Tốc độ hội tụ khá chậm.

## 4. VPN (Virtual private network)

Công nghệ VPN cung cấp một phương thức giao tiếp an toàn giữa các mạng riêng dựa trên hạ tầng công cộng (Internet). Trong bài tập lớn này đường dây cáp quang nối vào router tổng đại học quốc gia được sử dụng làm hạ tầng thiết lập VPN. VPN thường dùng để kết nối các văn phòng chi nhánh (branch-office), các người dùng từ xa về văn phòng chính (remote access). Giải pháp VPN của Cisco dựa trên một vài sản phẩm khác nhau gồm Pix Firewall, Cisco routers, VPN 3000/5000 Concentrator. Các protocol được sử dụng trong VPN bao gồm DES(Data Encryption Standard), Triple Des (3DES), IP Security (IP Sec) và Internet key Exchange(IKE).

- Phân loại:
  - Site to Site: Bằng việc sử dụng một thiết bị chuyên dụng và cơ chế bảo mật diện rộng, mỗi công ty có thể tạo kết nối với rất nhiều các site qua mạng công cộng như Internet. Mô hình này được áp dụng trong bài tập lớn này.
  - Remote access: đây là dạng kết nối user-to-lan áp dụng cho các công ty mà các nhân viên có nhu cầu kết nối tới mạng riêng (private network) từ các địa điểm từ xa và bằng các thiết bị khác nhau.

- Bảo mật trong VPN:
- IPSec: Giao thức bảo mật này cung cấp những tính năng an ninh cao cấp như các thuật toán mã hóa tốt hơn, quá trình thẩm định quyền đăng nhập toàn diện hơn.
- IPSec có 2 cơ chế mã hóa là Tunnel và Transport. Chỉ những hệ điều hành nào hỗ trợ IPSec mới có thể tận dụng được giao thức này. Trong packet tracer, chỉ có một số loại router được hỗ trợ VPN, loại router 1841 được sử dụng trong bài tập lớn này.
- Mật mã truy cập: Khi một máy tính mã hóa dữ liệu và gửi nó tới một máy tính khác thì chỉ có máy đó mới có thể giải mã được. Gồm 2 loại là mật mã riêng (Symmetric-Key Encryption) và mật mã chung (Public-Key Encryption).
- Ngoài ra còn các công nghệ mã hóa khác như DES, Triple DES, IKE.
- Ưu nhược điểm:
- VPN có đầy đủ tính năng và công nghệ bảo mật tốt hơn nhiều cho mạng của doanh nghiệp.
- Đây là biện pháp kinh tế vì người sử dụng không phải đầu tư các thiết bị ban đầu cho WAN hay trả phí sử dụng cao như Leased Line.
- Dễ dàng trong việc quản trị, khả năng mở rộng mạng dễ dàng.
- Tuy nhiên, công nghệ này còn khá mới chưa phổ biến tại Việt Nam.

## 5. DNS (Domain Name System)

Là một hệ thống thiết lập tương ứng giữa địa chỉ IP và tên miền. Hệ thống này phục vụ như một “Danh bạ điện thoại” để tìm trên Internet bằng cách dịch tên máy chủ thành địa chỉ IP. Trong bài tập lớn này có một DNS server đặt tại tầng 1 trụ sở.

## 6. NAT (Network Address Translation)

Là quá trình thay đổi thông tin địa chỉ IP trong gói tin đang được truyền qua một thiết bị định tuyến.

Loại NAT đơn giản nhất cung cấp việc biên dịch một - một cho một địa chỉ IP. Chuẩn RFC 2663 gọi loại NAT này là NAT cơ bản. Nó đôi khi cũng được gọi là NAT một-một. Trong kiểu phiên dịch này chỉ có địa chỉ IP, IP header, phần kiểm lỗi cần phải thay đổi (đối với TCP/UDP thì như vậy là đủ, nhưng một số giao thức tầng cao hơn có thể yêu cầu biên dịch nhiều hơn). NAT cơ bản có thể sử dụng để kết nối hai mạng máy tính có địa chỉ không tương thích.

Thông thường trong một mạng máy tính, các máy trong mạng được gán địa chỉ IP riêng, mạng chỉ có một hoặc một vài địa chỉ công cộng được gán cho thiết bị trực tiếp kết nối với mạng toàn cầu. Để các máy trong mạng có thể kết nối với bên ngoài, người ta sử dụng loại NAT một-nhiều. Trong kiểu NAT này, thông tin ở bậc cao trong các gói gửi đi hơn như cổng TCP/UDP được thay đổi và lưu trữ một bảng biên dịch, các gói tin trả về sẽ được tham chiếu với bảng này để thay đổi số cổng trước khi gửi tới máy cần nhận. Trong chuẩn RFC

2663, người ta còn gọi loại NAT này là NAPT (network address and port translation: biên dịch địa chỉ mạng và cổng). Các tên gọi khác là PAT (port address translation: biên dịch địa chỉ cổng), giả dạng IP, quá tải NAT. Do đây là loại thường gặp nhất của NAT nên khi gọi NAT, ta ngầm hiểu đó là NAT một-nhiều.

Trong những năm giữa thập niên 90, NAT trở thành một công cụ phổ biến để giải quyết vấn đề cạn kiệt địa chỉ IPv4. Nó trở thành một chức năng thiết yếu trong thiết bị định tuyến cho các kết nối tại nhà và công ty nhỏ. Hầu hết các hệ thống sử dụng thiết lập NAT để cho phép nhiều máy chủ trong mạng cục bộ có thể kết nối mạng toàn cầu thông qua chỉ một địa chỉ IP công cộng.

Biên dịch địa chỉ mạng bị hạn chế bởi chất lượng của kết nối mạng và yêu cầu nghiêm ngặt trong việc cài đặt.

## **7. Frame Relay**

Frame relay là dịch vụ nối mạng dữ liệu theo phương thức chuyển mạch gói, hoạt động ở mức liên kết (link level) và rất thích hợp với truyền số liệu với dung lượng lớn.

- Ưu nhược điểm:
- Frame relay bỏ qua các tiện ích sửa lỗi trong cấu trúc khung, điều khiển luồng thông tin (flow control). Khung có lỗi sẽ bị hủy bỏ chứ không sửa chữa, nhờ vậy thời gian xử lý tại bộ chuyển mạch giảm, Frame relay đạt mức thông lượng cao.
- Frame relay tiết kiệm đáng kể so với đường thuê riêng (private line) nhờ tính năng dồn kênh cho phép thiết lập nhiều kết nối trên cùng một đường dây vật lý. Nhờ vậy tiết kiệm được chi phí băng thông, đường dây cũng như thiết bị truyền dẫn.
- Frame relay có thể dùng cho kết nối liên mạng các LAN. Trong bài tập lớn này là mạng LAN. Frame relay có thể tạo mạch ảo liên kết các LAN, nâng cao hiệu quả kinh tế. Có thể dùng nó thay thế cho VPN. Mặc dù frame-relay chỉ để sử dụng cho việc trao đổi dữ liệu giữa các vùng xác định nhằm tăng tính bảo mật. Nhưng do packet Tracer không thể giả lập Internet nên nhóm tạm dùng kỹ thuật này để mô phỏng Internet (Internet cloud).

## **8. Tường lửa (Firewall)**

Là rào chắn mà một số cá nhân, tổ chức, doanh nghiệp, cơ quan nhà nước lập ra nhằm ngăn chặn người dùng mạng Internet truy cập các thông tin không mong muốn hoặc/và ngăn chặn người dùng từ bên ngoài truy nhập các thông tin bảo mật nằm trong mạng nội bộ.

Tường lửa là một thiết bị phần cứng và/hoặc một phần mềm hoạt động trong một môi trường máy tính nối mạng để ngăn chặn một số liên lạc bị cấm bởi chính sách an ninh của cá

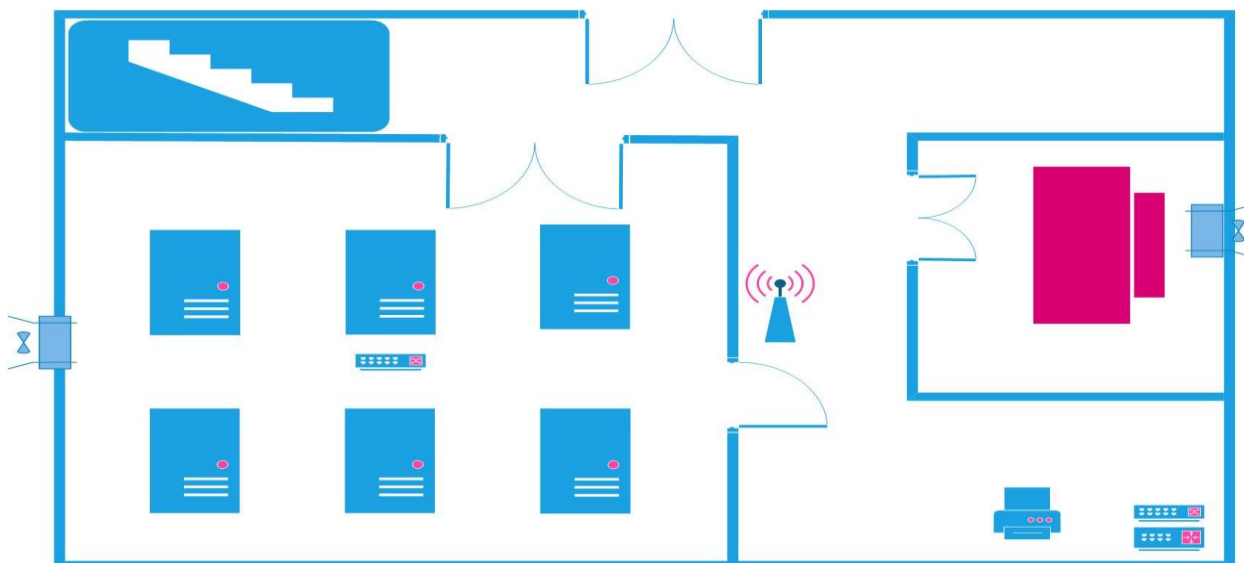
nhân hay tổ chức, việc này tương tự với hoạt động của các bức tường ngăn lửa trong các tòa nhà.

Công ty chúng ta đặt thiết bị tường lửa sau router để tăng tính bảo mật.

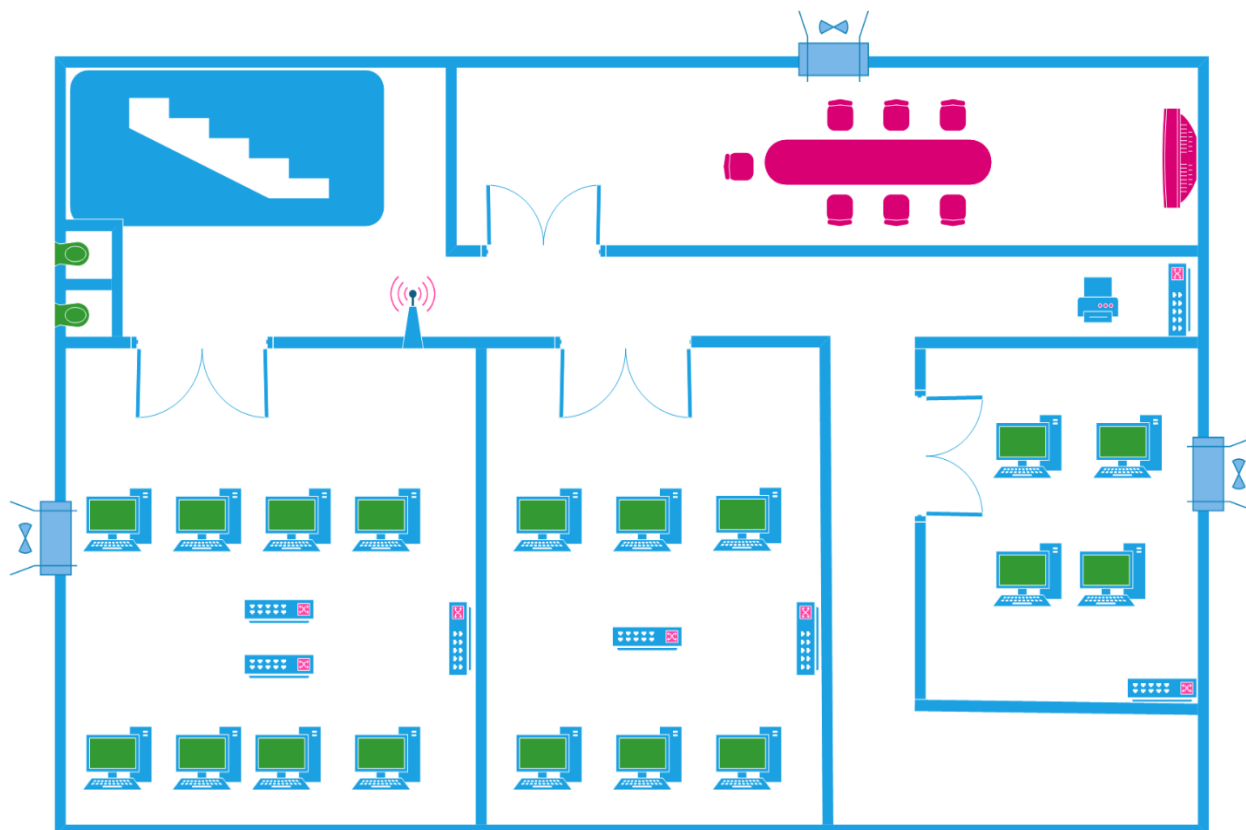
#### IV. Thiết kế

##### 1. Sơ đồ tòa nhà

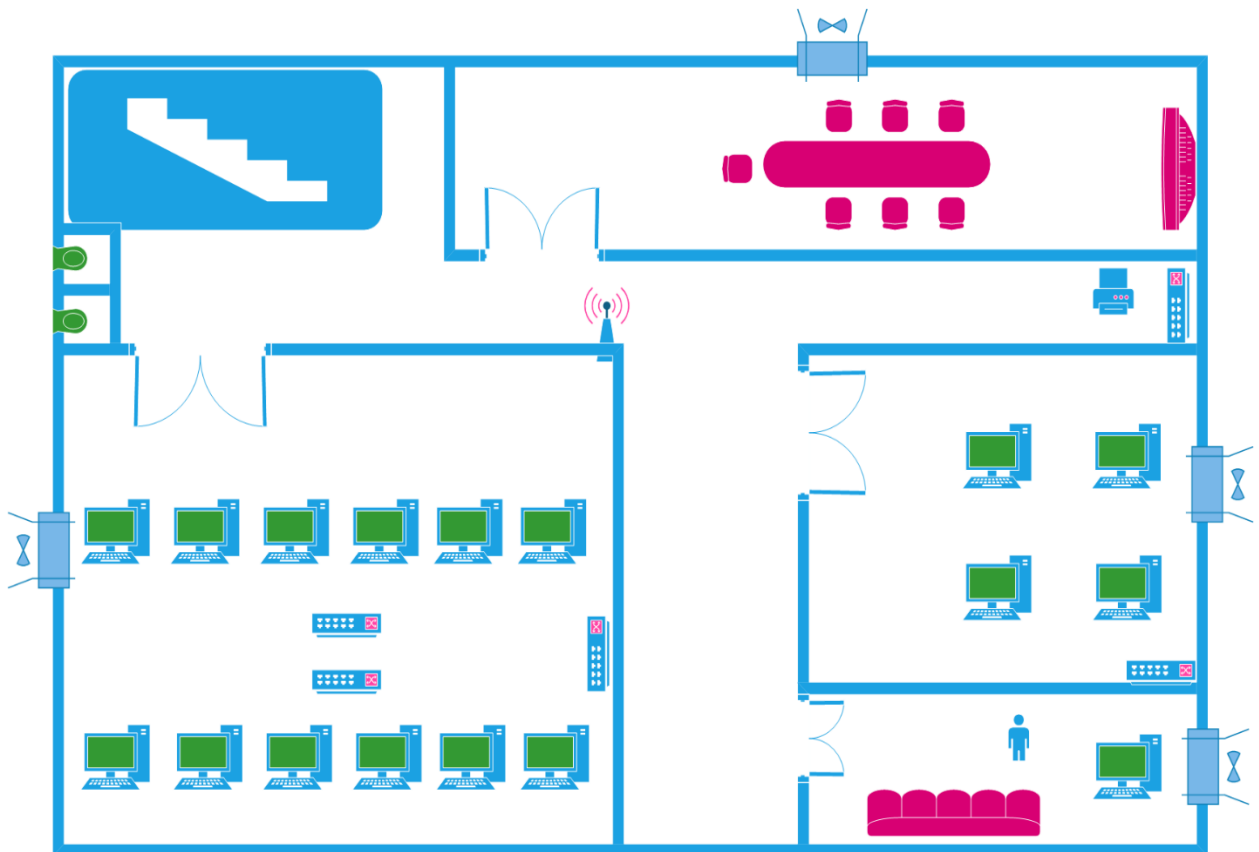
- Trụ sở:



Hình 1: Trụ sở tầng 1

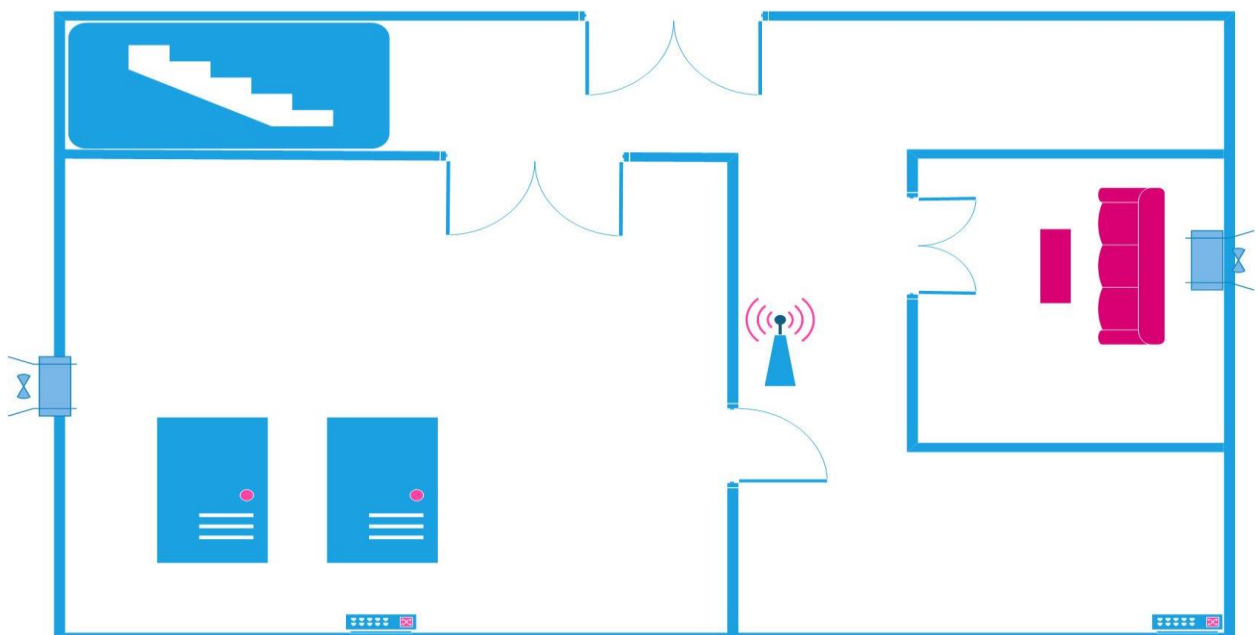


Hình 2: Trụ sở tầng 2

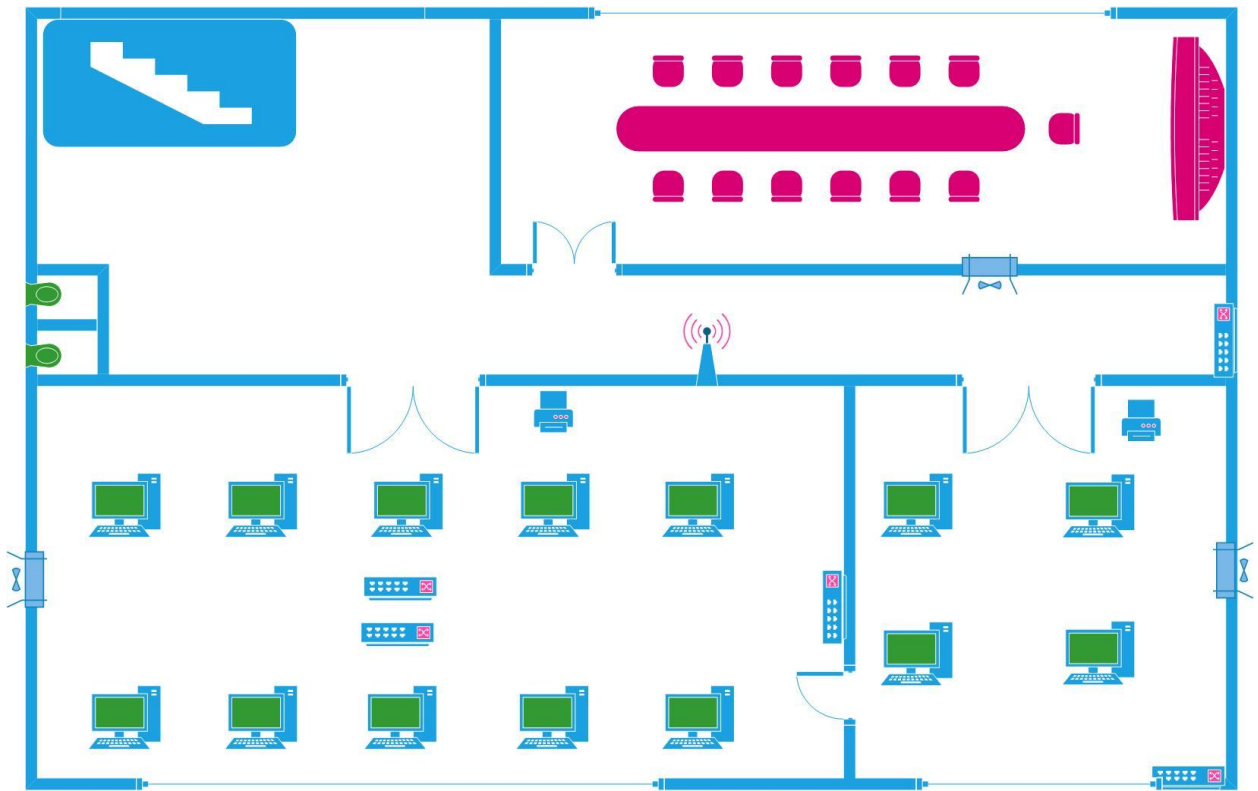


Hình 3: Trụ sở tầng 3

- Nhà máy:**



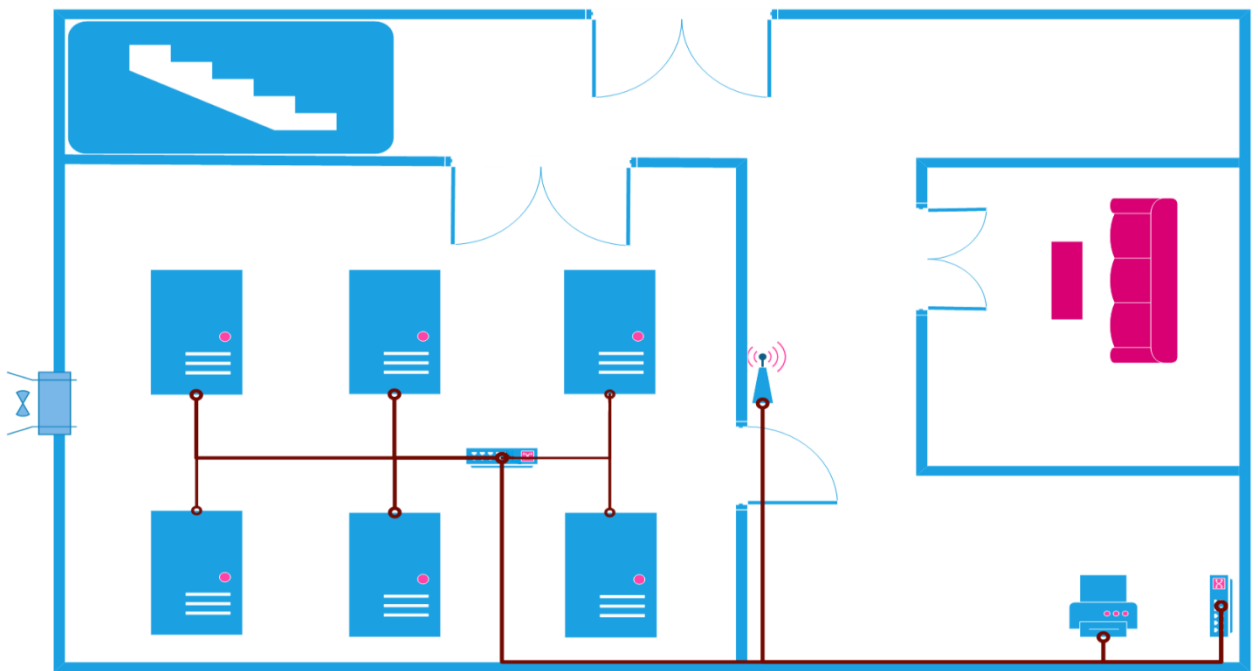
Hình 4: Nhà máy tầng 1



Hình 5: Nhà máy tầng 2

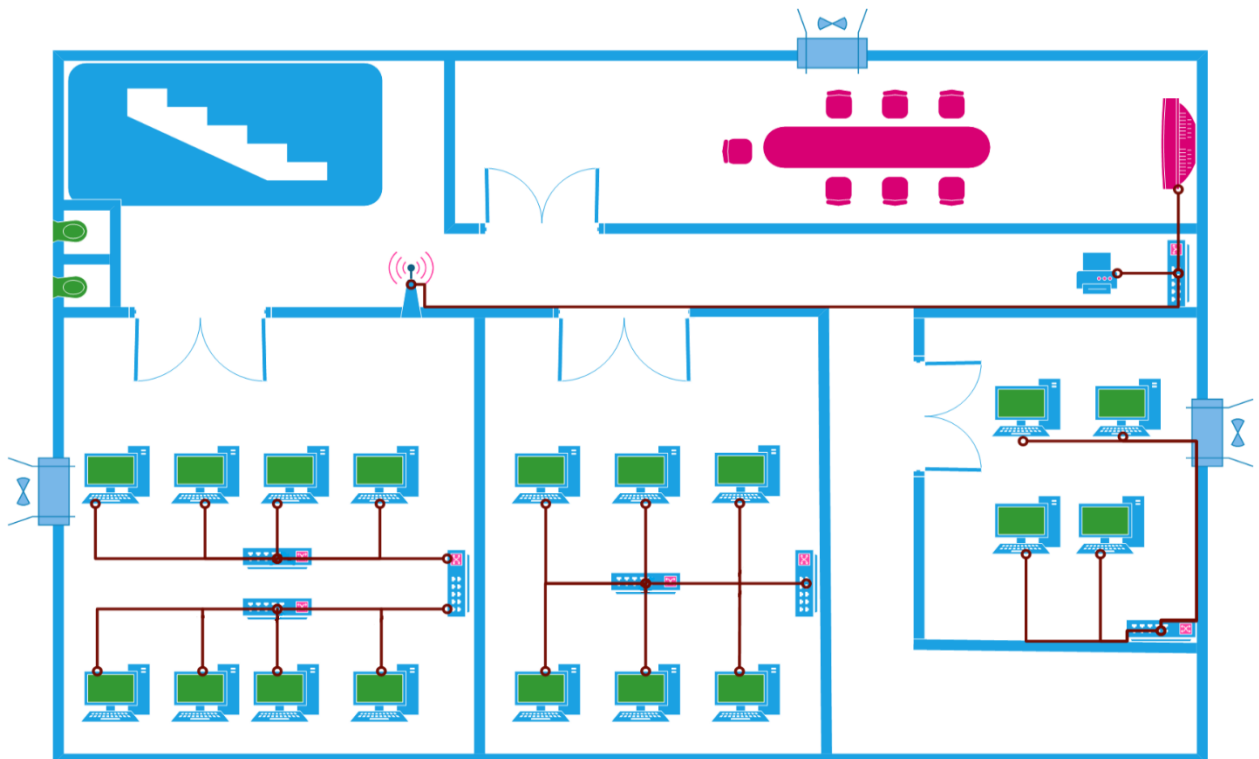
## 2. Sơ đồ kết nối dây

- Trụ sở:

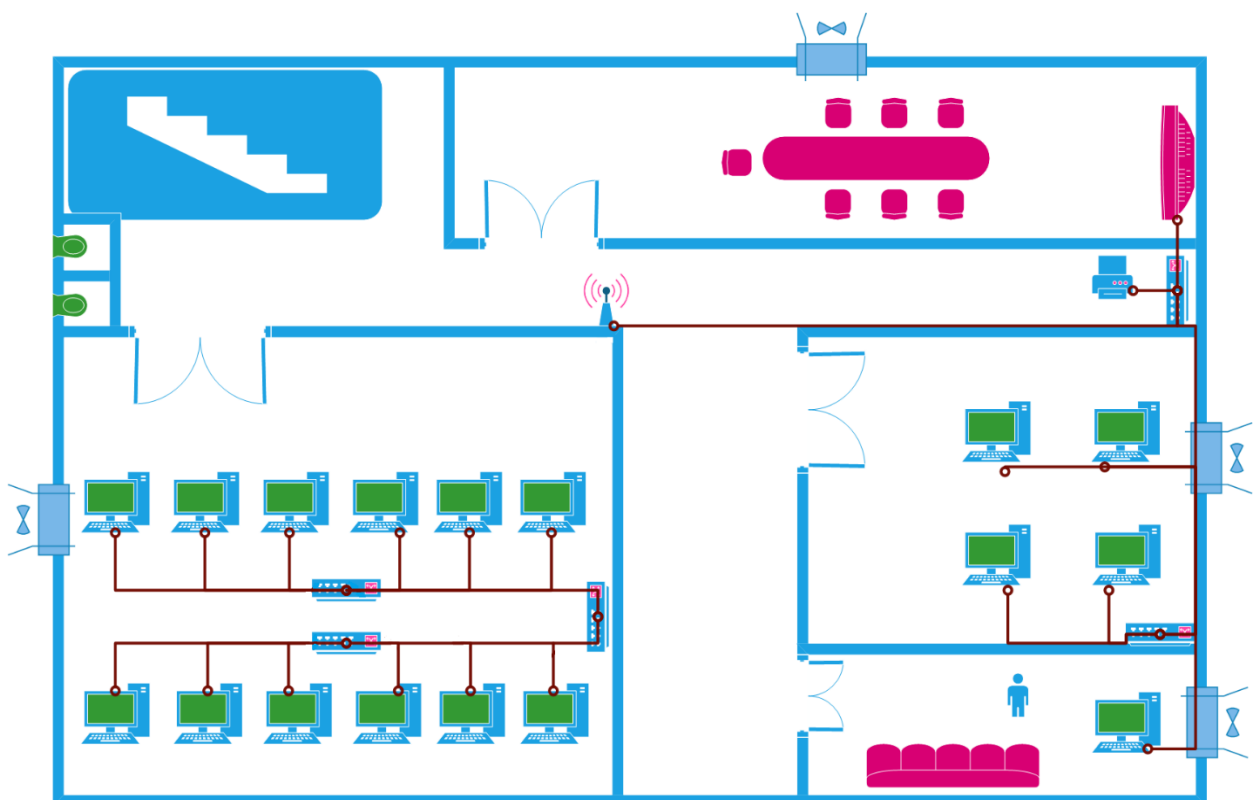


Hình 6: Trụ sở tầng 1 – Sơ đồ nối dây



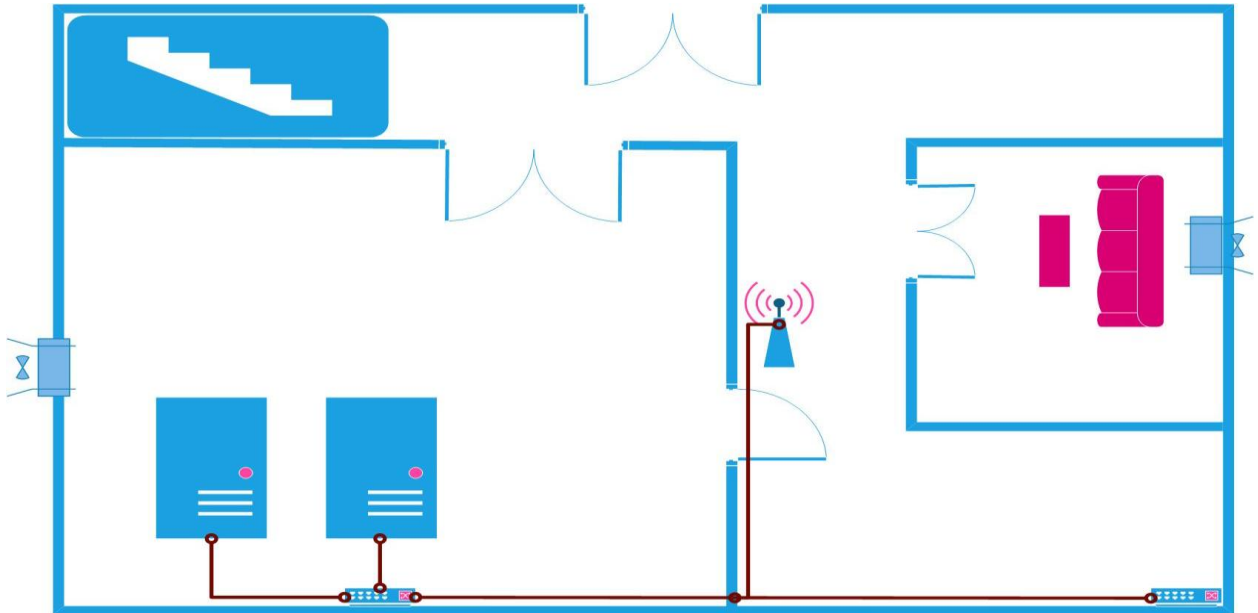


Hình 7: Trụ sở tầng 2 - Sơ đồ nối dây

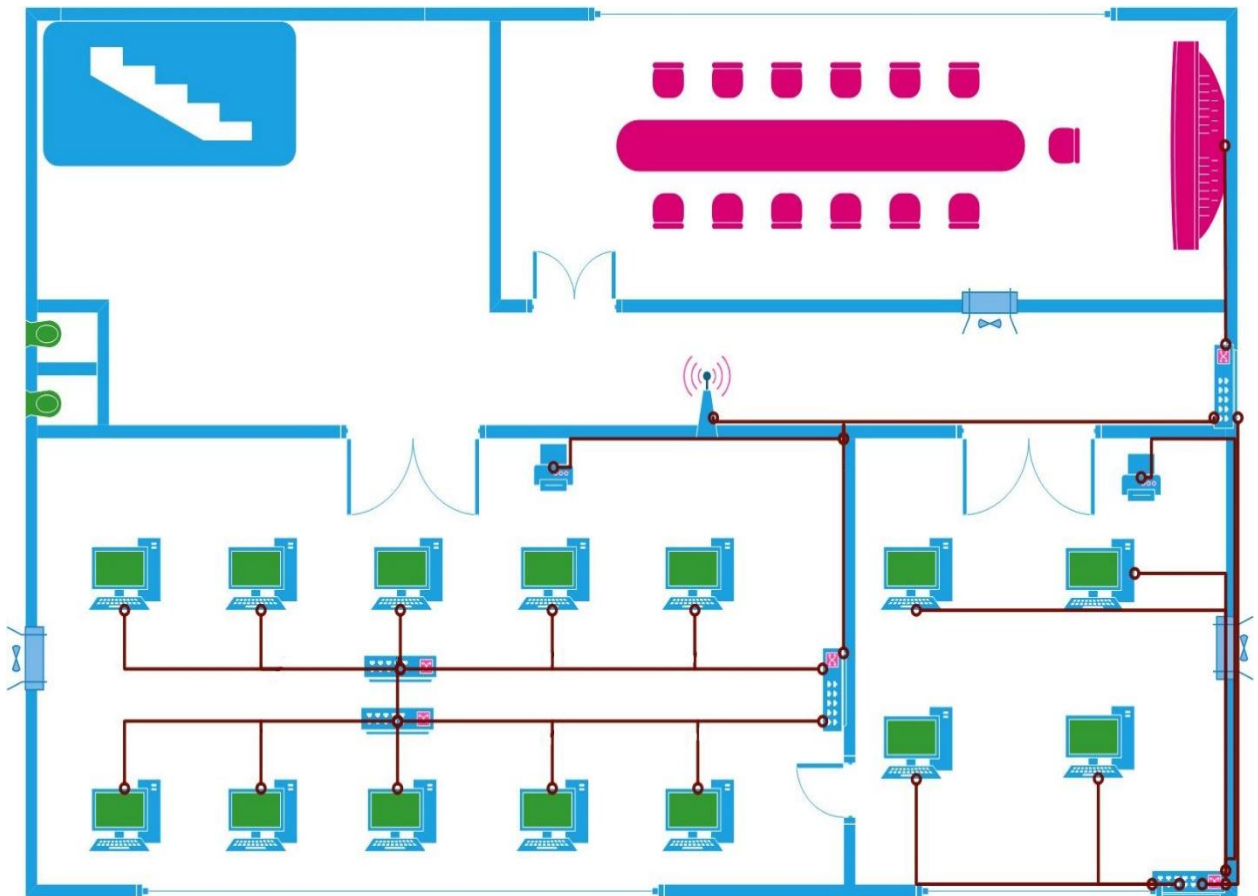


Hình 8: Tầng 3 - Sơ đồ nối dây

- **Nhà máy:**

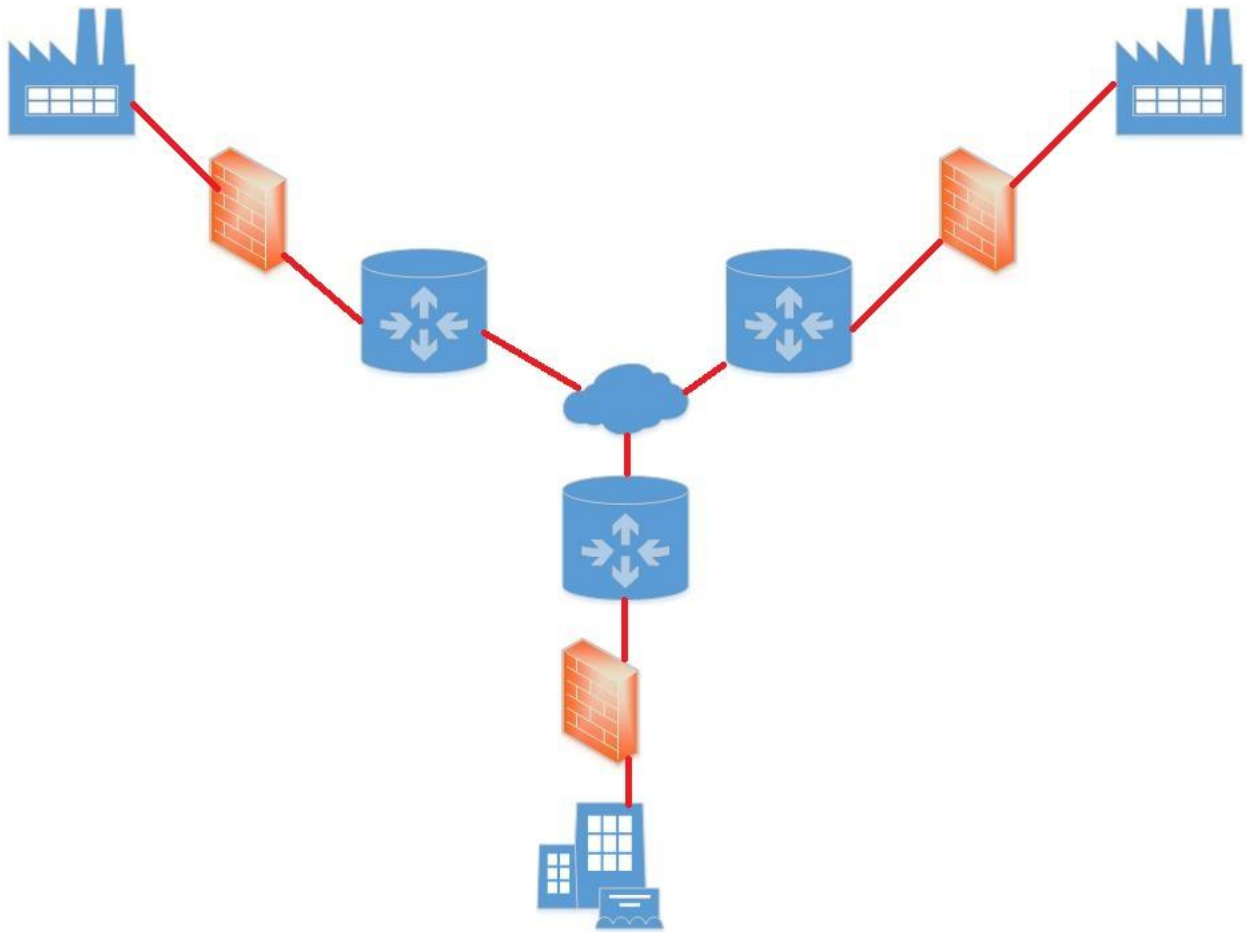


Hình 9: Nhà máy tầng 1 - Sơ đồ nối dây



Hình 10: Nhà máy tầng 2 - Sơ đồ nối dây

### 3. Sơ đồ mạng WAN giữa trụ sở và hai nhà máy



Hình 13: Sơ đồ mạng WAN

### 4. Sơ đồ IP

| Chi nhánh          | Máy                   | Dãy IP  |
|--------------------|-----------------------|---|
| Trụ sở Quận 1      | IP:                   | 172.16.0.0/24   |
|                    | Server lưu trữ 1      | 172.16.0.2/24   |
|                    | Server lưu trữ 2      | 172.16.0.3/24   |
|                    | Server lưu trữ 3      | 172.16.0.4/24   |
|                    | Server lưu trữ 4      | 172.16.0.5/24   |
|                    | Server quản lý        | 172.16.0.6/24   |
|                    | Server Web- Mail- DNS | 172.16.0.7/24   |
|                    | Các thiết bị khác     | Start from:<br>172.16.0.8/24<br>Default Gateway:<br>172.16.0.1/24 |
| Nhà máy Bình Dương | IP:                   | 172.16.1.0/25   |

|                          |                   |   |
|--------------------------|-------------------|---|
|                          | Server lưu trữ    | 172.16.1.2/25   |
|                          | Server quản lý    | 172.16.1.3/25   |
|                          | Các thiết bị khác | Start from:<br>172.16.1.4/25<br>Default Gateway:<br>172.16.1.1/25     |
|                          |                   |   |
| <b>Nhà máy Bình Định</b> | IP                | 172.16.1.128/25   |
|                          | Server lưu trữ    | 172.16.1.130/25   |
|                          | Server quản lý    | 172.16.1.131/25   |
|                          | Các thiết bị khác | Start from:<br>172.16.1.132/25<br>Default Gateway:<br>172.16.1.129/25 |

## 5. Danh sách các thiết bị đề xuất và đặc điểm kỹ thuật điển hình

Các thiết bị được đề xuất dựa trên việc đáp ứng nhu cầu hiện tại và sự mở rộng, phát triển trong tương lai:

- **20-Port Gigabit Managed Switch CISCO SG300-20**



- 18 10/100/1000Mbps ports; 2 Combo mini-GBIC ports.
- Gigabit Switching with Fiber Expansion and Browser Configurability.
- Performance: Switching capacity 40.0 Gbps, nonblocking, Forwarding rate 29.76 mpps wire-speed performance.
- QoS: Priority levels 4 hardware queues, Scheduling Priority queuing and weighted round-robin (WRR), Queue assignment based on DSCP and class of service (802.1p/CoS).
- IPv4 / IPv6 Support.
- MAC Table: Up to 8000 MAC addresses.

- **8-Port Gigabit Ethernet Switch Cisco SG200-08**



- 8-Port Gigabit Ethernet 10/100/1000Mbps with MDI and MDI crossover (MDI-X); auto negotiated port.
- Performance: Switching capacity 13.6 Gbps, Forwarding capacity (base on 64-byte packets) 11.9 mpps
- QoS feature.
- IPv4 / IPv6 Support.
- MAC Table: Up to 8000 MAC addresses.

- **Cisco ASR 1001 Router**



- ESP bandwidth 2.5 Gbps (default) to 5 Gbps of forwarding performance (optional software option).
- ESP memory: 1-GB DRAM default; 1-GB DRAM maximum.
- Route-processor memory comes with 4-GB DRAM (default); 8-GB DRAM maximum.
- 4-Gigabit Ethernet Small Form-Factor Pluggable (SFP) ports.
- External USB flash memory 1-GB USB flash memory support.

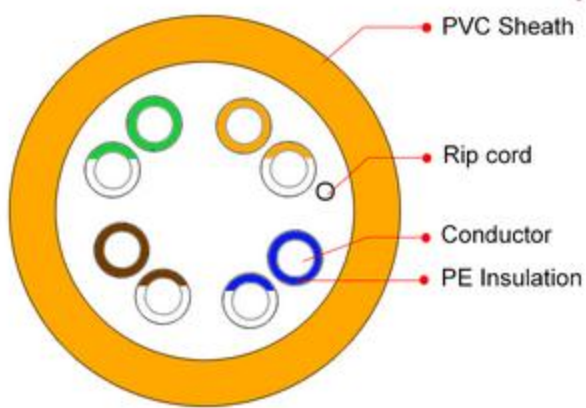
- **Cisco-Linksys WAP610N Wireless-N Access Point with Dual-Band**



- Data Link Protocol: IEEE 802.11n (draft), IEEE 802.11b, IEEE 802.11a, IEEE 802.11g.
- Wireless Security WEP, Wi-Fi Protected Access™ 2 (WPA2), Wireless MAC Filtering.
- Interfaces: 1 x Network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45.
- Bandwidth: 2.4GHz – 5 GHz.
- **Cisco Firewall ASA 5525**

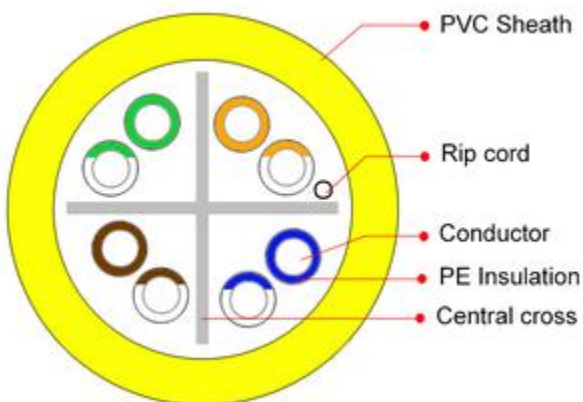


- Stateful Inspection Throughput (Maximum): 2 Gbps.
- IPS Throughput: 600 Mbps (Extra hardware not required).
- Next-Generation Throughput(Multiprotocol): 650 Mbps.
- 3DES/AES VPN Throughput: 300 Mbps
- IPsec VPN Peers: 750.
- Concurrent Connections: 500,000.
- Virtual Interfaces (VLANs): 200.
- Integrated I/O: 8 GE copper.
- **Cáp mạng Cat 5E, U/UTP**



|                               |   |
|-------------------------------|---|
| Tốc độ                        | 10/100Mbps, hỗ trợ truyền tốc độ 10/100/1000Mbps                  |
| Tần số                        | Up to 100MHz  |
| Hoạt động                     | Ít nhiễu chéo (cross talk) so với Cat5 nhưng không tốt bằng Cat 6 |
| Khoảng cách làm việc tốt nhất | 100m, có thể chạy xa 150m với cáp UTP Cat 5e                      |
| AWG                           | 24 AWG  |
| Lỗi chữ thập                  | Không có  |

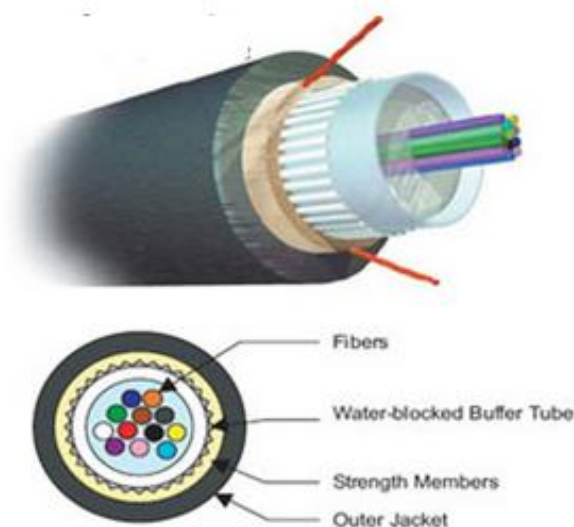
- Cáp mạng AMP STP CAT6**



|        |  |
|--------|--|
| Tốc độ | 10/100/1000 Mbps và 10 Gigabit Ethernet (Khoảng cách ngắn) |
| Tần số | Up to 250MHz   |

|                               |  |
|-------------------------------|--|
| Hoạt động                     | Chống nhiễu chéo tốt, tỉ lệ tín hiệu nhiễu (SNR - Signal to Noise Ratio) cao, tỉ số cao sẽ ít bị nhiễu ảnh còn ngược lại thì sẽ nhiễu nhiễu ảnh. |
| Khoảng cách làm việc tốt nhất | 70-90m, có thể chạy xa 150m với cáp UTP Cat 6  |
| AWG                           | 23 AWG   |
| Lõi chữ thập                  | có   |

- **Cáp quang AMP, Multimode 50/125 um**



- Vỏ cáp được làm bằng nhựa HDPE có độ bền và chịu được mưa nắng lâu ngày.
- Cáp được bọc một lớp thép mỏng giúp tăng cường độ bảo vệ của cáp.
- Có lõi thép gia cường nhằm hạn chế độ võng của cáp.
- Khoảng cách làm việc đến vài km.
- Loại sợi quang: Multimode 50/125  $\mu\text{m}$  hoặc 62.5/125  $\mu\text{m}$ .
- Dung lượng: 4 Sợi.
- Tốc độ truyền tối đa: 1 Gigabit/s.
- Đường kính cáp: 8 mm.

## 6. Chọn lựa thiết bị và số lượng

- Để nối giữa các thiết bị trong phòng với switch ta dùng cáp Cat 5E, U/UTP.



- Để nối giữa các switch với nhau và giữa các switch với router, ở cự li ngắn dưới 100m, ta dùng cáp AMP STP CAT6.
- Để kết nối giữa nối giữa các switch với nhau, giữa các switch với router và giữa các router với nhau, ở cự li trên 100m và phải đi dây ngoài trời, chịu ảnh hưởng của thời tiết, ta dùng cáp quang AMP, Multimode 50/125 um để đảm bảo tín hiệu không bị sai lệch, ít mất mát hơn.
- Hơn nữa, đối với hai thiết bị đồng đẳng ta bấm cáp chéo và ngược lại thì ta bấm cáp thẳng.

**Đối với riêng Trụ sở:**

- 1 switch 20 port để tổng kết nối các switch trong trụ sở, 1 router để ra mạng ngoài và 1 firewall để tăng tính bảo mật.

**Tầng 1:**

- Phòng kỹ thuật mạng có 6 server nên ta sẽ chọn switch 20 port. Số port dư ra để dự trữ cho phép mở rộng hệ thống sau này.
- Ngoài ra còn có 1 wireless access point.
- Đồng thời ta sử dụng 1 switch 20 port để tổng kết nối các switch, thiết bị tầng 1.

**Tầng 2:**

- Bộ phận bán hàng có 30 máy nên ta sử dụng 2 switch 20 port để kết nối các máy và 1 switch 8 port để tổng kết nối các switch trong phòng của bộ phận này. Số port dư ra cho phép mở rộng sau này.
- Chọn lựa switch cho bộ phận khác có 25 máy tương tự như bộ phận bán hàng.
- Phòng cho ban quản lý có 7 máy, ta sử dụng 1 switch 20 port cho phòng này.
- Ngoài ra còn có 1 Wireless Access Point.
- Đồng thời ta sử dụng switch 20 port để tổng kết nối các switch, thiết bị tầng 2.

**Tầng 3:**

- Bộ phận bán hàng có 30 máy nên ta sử dụng 2 switch 20 port để kết nối các máy và 1 switch 8 port để tổng kết nối các switch trong phòng của bộ phận này. Số port dư ra cho phép mở rộng sau này.
- Phòng cho ban quản lý có 7 máy, ta sử dụng 1 switch 20 port cho phòng này.
- Ngoài ra còn có 1 wireless access point.
- Đồng thời ta sử dụng 1 switch 20 port để tổng kết nối các switch, thiết bị tầng 3.

**Đối với riêng Nhà máy:**

- 1 switch 20 port để tổng kết nối các switch trong nhà máy , 1 router để ra mạng ngoài và 1 firewall để tăng tính bảo mật.

**Tầng 1:**

- Phòng kỹ thuật mạng có 2 server ta sử dụng 1 switch 8 port. Số port dư ra để dự trữ cho phép mở rộng hệ thống sau này.
- Ngoài ra còn có 1 wireless access point.
- Đồng thời ta sử dụng 1 switch 20 port để tổng kết nối các switch, thiết bị tầng 1.

**Tầng 2:**

- Phòng cho nhân viên có 15 máy nên ta sử dụng 2 switch 20 port để kết nối các máy và 1 switch 8 port để tổng kết nối các switch trong phòng của bộ phận này. Số port dư ra cho phép mở rộng sau này.
- Phòng cho ban quản lý có 5 máy, ta sử dụng 1 switch 20 port cho phòng này.
- Ngoài ra còn có 1 wireless access point.
- Đồng thời ta sử dụng 1 switch 20 port để tổng kết nối các switch, thiết bị tầng 2.

Bảng danh sách số lượng các thiết bị đề xuất

| Thiết bị                                      | Số lượng |
|---|----------|
| Switch Cisco SG300-20                         | 26       |
| Switch Cisco SG200-08                         | 7        |
| Cisco ASR 1001 Router                         | 3        |
| Cisco-Linksys WAP610N Wireless-N Access Point | 7        |
| Cisco Firewall ASA 5525                       | 3        |
| Cat 5E, U/UTP Cable                           | 2500 m   |
| AMP STP CAT6 Cable                            | 2000 m   |

Nhưng vì ta sử dụng dịch vụ VPN do Viettel cung cấp nên ta cũng thuê đường truyền WAN cáp quang của họ.

## V. Kết luận

### 1. Đánh giá hệ thống mạng

- Hệ thống mạng của chúng tôi về căn bản đã đáp ứng đủ các yêu cầu của đề, cũng như với khả năng mở rộng 20% trong 5 năm. Ngoài ra còn có tính năng thêm như xác định Physical của mô hình bằng Packet Tracer.

### 2. Những khó khăn trong thiết kế

- Không có kinh nghiệm thiết kế hệ thống mạng trong thực tế.

- Thời gian ngắn, tài liệu tham khảo ít.
- Đề bài chưa được rõ ràng về các chi tiết của công ty.

### **3. Định hướng phát triển**

- Hệ thống có khả năng mở rộng và đáp ứng được các công nghệ mới sẽ được phổ biến trong tương lai.

### **4. Những hạn chế của dự án**

- Do dùng 1 kênh truyền chung cho dịch vụ cho VPN và Internet nên hệ thống có thể bị chậm hoặc nghẽn mạng trong giờ cao điểm.

### **5. Kiến thức, kinh nghiệm thu được**

- Qua bài tập này chúng tôi đã học được nhiều kinh nghiệm trong thiết kế 1 hệ thống mạng cho 1 doanh nghiệp vừa và nhỏ.
- Việc lên kế hoạch cho dự án dựa vào nhiều yếu tố như địa lý, cách bố trí, cấu trúc tòa nhà và giá thành phù hợp.
- Trau dồi thêm kiến thức khi tìm hiểu các công nghệ thích hợp cho hệ thống.
- Hiểu thêm nhiều kiến thức về mạng từ cơ bản đến nâng cao.
- Rèn luyện thêm kỹ năng làm việc nhóm.

### **6. Góp ý**

- Cần có 1 chuyến tham quan thực tế để cho sinh viên tham khảo 1 quy trình thiết kế mạng trong thực tế của doanh nghiệp.
- Đề bài cần chi tiết hơn.

-----HẾT-----