REPORT PROJECT

**Design Network**

KẾ HOẠCH THIẾT KẾ MẠNG CÔNG TY OUTSOURCE

O-UIT

**CLASS: NT113.O11.MMCL**

**MEMBER (Group 13):**

|  |  |  |
| --- | --- | --- |
|  | **Full Name** | **Student ID** |
| 1 | Nguyễn Đoàn Khắc Huy | 21522151 |
| 2 | Trương Thị Minh Quỳnh | 21522540 |
| 3 | Lê Ngọc Hân | 21520813 |

**Another assessment:**

|  |  |  |
| --- | --- | --- |
|  | Name of work | Volume of work |
| Division of work | * Nguyễn Đoàn Khắc Huy | 100% |
| * Trương Thị Minh Quỳnh | 100% |
| * Lê Ngọc Hân | 100% |
| Opinion *(if any)*  + Difficulty  +Suggestions, recommendations | None | |

The lower part of this report is the detailed report of the execution team.

Contents

[**A.** Giới thiệu tổng quan 5](#_Toc153313615)

[I. Mục đích 5](#_Toc153313616)

[II. Tổng quan 5](#_Toc153313617)

[III. Yêu cầu 6](#_Toc153313618)

[**B.** PHÂN TÍCH YÊU CẦU 7](#_Toc153313619)

[I. Trụ sở chính(Thủ Đức) 7](#_Toc153313620)

[II. Trụ sở chi nhánh (Quận 3) 7](#_Toc153313621)

[**C.** THIẾT KẾ HỆ THỐNG MẠNG 7](#_Toc153313622)

[I. Thiết kế mô hình mạng logic 7](#_Toc153313623)

[1. Các thiết bị dùng trong hệ thống 8](#_Toc153313624)

[**a.** **Router** 8](#_Toc153313625)

[**b.** **Switch** 8](#_Toc153313626)

[**c.** **Switch layer 3** 9](#_Toc153313627)

[**d.** **Wireless controler** 9](#_Toc153313628)

[**e.** **Access Point** 10](#_Toc153313629)

[**2.** **Các dịch vụ cần thuê** 10](#_Toc153313630)

[**a.** **Dịch vụ Internet** 10](#_Toc153313631)

[II. Đặt địa chỉ IP cho hệ thống mạng và thiết bị 11](#_Toc153313632)

[1. Tại trụ sở chính 11](#_Toc153313633)

[2. Tại chi nhánh 13](#_Toc153313634)

[III. Thiết kế sơ đồ vật lý của toàn bộ hệ thống mạng 14](#_Toc153313635)

[1. Sơ đồ vật lý cho toàn hệ thống 14](#_Toc153313636)

[2. Tại trụ sở chính 14](#_Toc153313637)

[**a.** **Lớp core layer và distribution layer** 14](#_Toc153313638)

[**b.** **Khối server và các Access point** 16](#_Toc153313639)

[**c.** **Sơ đồ hệ thống tầng trệt** 18](#_Toc153313640)

[**d.** **Sơ đồ hệ thống tầng 1** 19](#_Toc153313641)

[**e.** **Sơ đồ hệ thống tầng 2** 19](#_Toc153313642)

[**f.** **Sơ đồ hệ thống tầng 3** 20](#_Toc153313643)

[**g.** **Sơ đồ hệ thống tầng 4** 21](#_Toc153313644)

[**h.** **Sơ đồ hệ thống tầng 5** 21](#_Toc153313645)

[**3.** **Tại chi nhánh đặt tại Quận 3** 22](#_Toc153313646)

[**a.** **Tầng 1 có phòng developer và hệ thống Wireless controler** 23](#_Toc153313647)

[**b.** **Tầng 2 gồm phòng Tester và hệ thống wifi public** 23](#_Toc153313648)

[**D.** CÁC DỊCH VỤ CỦA HỆ THỐNG VÀ CHI PHÍ HOẠT ĐỘNG 24](#_Toc153313649)

[I. Các dịch vụ cung cấp 24](#_Toc153313650)

[a. OSPF 24](#_Toc153313651)

[**b.** **NAT** 25](#_Toc153313652)

[**c.** **VLAN** 25](#_Toc153313653)

[**d.** **Trunking** 26](#_Toc153313654)

[**e.** **HSRP** 26](#_Toc153313655)

[**f.** **VPN** 27](#_Toc153313656)

[**g.** **RSTP** 27](#_Toc153313657)

[II. Chi phí cho toàn hệ thống 28](#_Toc153313658)

[a. Chi phí cho dịch vụ 28](#_Toc153313659)

[**b.** **Chi phí cho thiết bị** 28](#_Toc153313660)

[**E.** KẾT LUẬN 31](#_Toc153313661)

[**F.** THAM KHẢO 31](#_Toc153313662)

# Giới thiệu tổng quan

## Mục đích

* Nhằm hoàn thiện hệ thống mạng của công ty Outsource O-UIT trong thời gian sắp tới.
* Phục vụ cho các nhân viên tại chi nhánh Thủ Đức của các phòng CEO, HR, Project manager, Technical Manager, Business Analyst, IT manager và các nhóm developer và tester cho các project thuộc thị trường nước ngoài
* Phục vụ cho các nhân viên tại chi nhánh Quận 3 là văn phòng làm việc của các nhóm developer và tester cho các project thuộc thị trường trong nước

## Tổng quan

* Công ty Outsource O-UIT có 1 trụ sở chính tại Thủ Đức và một chi nhánh tại Quận 3.
* Trụ sở chính là một tòa nhà 5 tầng gồm Data Center và các văn phòng làm việc dành cho CEO, HR, Project manager, Technical Manager, Business Analyst, IT manager và các nhóm developer và tester cho các project thuộc thị trường nước ngoài.

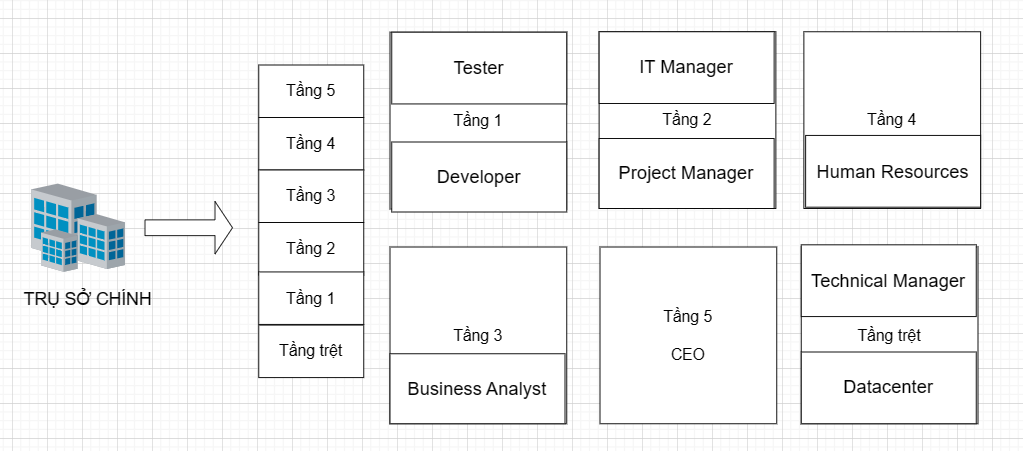


Figure .: Mô hình tòa nhà trụ sở chính

* Chi nhánh tại Quận 3 là văn phòng làm việc của các nhóm developer và tester cho các project thuộc thị trường trong nước.

A grid with a grid and a square with black text

Description automatically generated with medium confidence

Figure .: Mô hình trụ sở chi nhánh

|  |  |  |
| --- | --- | --- |
| SỐ LƯỢNG NHÂN VIÊN MỖI PHÒNG BAN | | |
| Chi nhánh | Phòng ban | Số lượng |
| TRỤ SỞ CHÍNH | Developer | 20 |
| Tester | 20 |
| IT manager | 10 |
| Project Manager | 10 |
| HR | 10 |
| Business Analyst | 10 |
| CEO | 5 |
| Technical Manager | 10 |
| CHI NHÁNH | Developer | 20 |
| Tester | 20 |

Table ‑. Số lượng nhân viên mỗi phòng ban

## Yêu cầu

* Tại trụ sở chính:
  + Developer và Tester chỉ được sử dụng máy bàn tại công ty, không được sử dụng laptop riêng để truy cập vào mạng của công ty.
  + CEO, HR, Project manager, Technical Manager, Business Analyst, IT manager được sử dụng Laptop, truy cập vào hệ thống wifi nội bộ sử dụng tài khoản xác thực.
  + Một hệ thống wifi public với đường kết nối Internet riêng.
  + Hệ thống phần cứng để triển khai hệ thống server ảo phục vụ cho việc deploy các ứng dụng trong giai đoạn test.
  + Sử dụng các dịch vụ Cloud deploy các ứng dụng trong giai đoạn staging đểkhách hàng sử dụng thử trước khi đưa ra thực tế.
* Tại chi nhánh:
  + Developer và Tester chỉ được sử dụng máy bàn tại công ty, không được sử dụng laptop riêng để truy cập vào mạng của công ty.
  + Sử dụng kết nối VPN site-to-site để deploy ứng dụng lên hệ thống tại Data Center.
  + Một hệ thống wifi với đường kết nối Internet riêng.

# PHÂN TÍCH YÊU CẦU

## Trụ sở chính(Thủ Đức)

* Quy định sử dụng thiết bị:
  + Developer và Tester chỉ được phép sử dụng máy bàn của công ty.
  + CEO, HR, Project Manager, Technical Manager, Business Analyst, IT Manager được phép sử dụng quyền truy cập vào hệ thống wifi nội bộ bằng tài khoản xác thực.
* Hệ Thống Wifi:
  + Wifi nội bộ cho nhân viên sử dụng tài khoản xác thực.
  + Wifi public với đường truyền Internet riêng.
* Hệ Thống Phần Cứng và Server Ảo:
  + Triển khai hệ thống server ảo để phục vụ việc deploy các ứng dụng trong giai đoạn test.
* Sử Dụng Dịch Vụ Cloud:
  + Deploy các ứng dụng trong giai đoạn staging trên Cloud để khách hàng có thể sử dụng thử trước khi chính thức triển khai.

## Trụ sở chi nhánh (Quận 3)

* Quy Định Sử Dụng Thiết Bị:
  + Tương tự như tại trụ sở chính, Developer và Tester chỉ được sử dụng máy bàn của công ty và không được sử dụng laptop cá nhân để truy cập mạng công ty.
* Kết Nối VPN Site-to-Site:
  + Sử dụng kết nối VPN site-to-site để deploy ứng dụng lên hệ thống tại Data Center.

# THIẾT KẾ HỆ THỐNG MẠNG

## Thiết kế mô hình mạng logic

* Nguyên tắc đặt tên: Tên thiết bị + Phòng ban (+ Số tầng)
  + Đối với các thiết bị sẽ lấy chữ cái đầu tiên của thiết bị.(ví dụ: Router = R, Access Point = AP)
  + Đối với phòng ban sẽ lấy chữ cái đầu tiên trong tên của phòng ban theo tiếng anh.(ví dụ: Project Manager = PM)
  + Đối với phòng ban tên 1 chữ hoặc 2 phòng ban trùng tên sẽ lấy từ 2 đến 3 chữ cái đầu.(ví dụ: Developer = Dev)
  + Đối với tầng sẽ thể hiện bằng 1->9 số 0 là tầng trệt

### Các thiết bị dùng trong hệ thống

1. **Router**

Router là một thiết bị mạng được sử dụng để kết nối hai hoặc nhiều mạng khác nhau và chuyển tiếp dữ liệu giữa chúng dựa trên địa chỉ IP. Router là một thành phần quan trọng trong hạ tầng mạng, cho phép giao tiếp giữa các mạng khác nhau và đảm bảo định tuyến của dữ liệu từ nguồn đến đích.

Một số đặc điểm quan trọng của router bao gồm:

* Chuyển tiếp địa chỉ IP: Router sử dụng thông tin địa chỉ IP để xác định cách chuyển tiếp dữ liệu giữa các mạng. Nó lưu giữ bảng định tuyến để quyết định đường đi tốt nhất cho gói tin.
* Phân loại và chia mạng: Router có khả năng phân loại dữ liệu theo các địa chỉ IP và chia mạng thành các mạng con (subnetting). Điều này giúp tối ưu hóa quản lý và sử dụng tài nguyên mạng.
* Quản lý giao tiếp giữa các mạng khác nhau: Router cho phép các mạng LAN khác nhau liên lạc với nhau thông qua việc chuyển tiếp dữ liệu giữa chúng.
* Tính năng bảo mật: Router có thể thực hiện các chức năng bảo mật như tường lửa (firewall) để kiểm soát lưu lượng mạng và bảo vệ mạng khỏi các mối đe dọa.
* Kết nối với Internet: Router thường được sử dụng để kết nối các mạng doanh nghiệp với Internet, cho phép các thiết bị trong mạng truy cập và tương tác với các nguồn thông tin và dịch vụ trực tuyến.

1. **Switch**

Switch là một thiết bị mạng được sử dụng để kết nối và chuyển tiếp dữ liệu giữa các thiết bị trong một mạng cục bộ (LAN - Local Area Network). Switch hoạt động ở tầng 2 (tầng liên kết dữ liệu) của mô hình OSI và thường được sử dụng để nâng cao hiệu suất mạng và tăng khả năng kết nối.

Một số đặc điểm quan trọng của switch bao gồm:

* Chuyển mạch: Switch có khả năng chuyển tiếp dữ liệu giữa các thiết bị trong mạng LAN dựa trên địa chỉ MAC (Media Access Control). Nó hoạt động bằng cách xem địa chỉ MAC của gói tin và quyết định cổng nào nên chuyển gói tin tới.
* Tăng băng thông: So với hub (trạm phát tín hiệu) truyền thống, switch có khả năng cung cấp băng thông lớn hơn cho mỗi cổng và giảm va chạm dữ liệu, cải thiện hiệu suất mạng.
* Loại bỏ va chạm: Switch có khả năng tạo các đường kết nối độc lập (dedicated connection) giữa các thiết bị, giúp loại bỏ va chạm trên mạng và tăng hiệu suất truyền dữ liệu.
* Học địa chỉ MAC: Switch tự động học địa chỉ MAC của các thiết bị kết nối với nó và lưu trữ thông tin này trong bảng chuyển mạch (MAC address table).
* Đa cổng: Switch thường có nhiều cổng Ethernet để kết nối với nhiều thiết bị trong mạng.
* Quản lý VLAN: Một số switch cung cấp khả năng quản lý VLAN (Virtual Local Area Network), cho phép phân chia mạng thành các phân đoạn ảo để tăng cường hiệu suất và bảo mật.

1. **Switch layer 3**

Switch Layer 3, còn được gọi là Layer 3 Switch hoặc Multilayer Switch, là một thiết bị mạng kết hợp giữa tính năng của một switch ở tầng 2 (liên kết dữ liệu) và một router ở tầng 3 (mạng). Nó có khả năng chuyển tiếp dữ liệu dựa trên địa chỉ MAC ở tầng 2 và địa chỉ IP ở tầng 3, cung cấp khả năng định tuyến giữa các mạng con.

Một số đặc điểm quan trọng của Switch Layer 3 bao gồm:

* Chuyển đổi ở cả hai tầng: Switch Layer 3 có khả năng chuyển tiếp dữ liệu ở cả tầng liên kết dữ liệu (Layer 2) và tầng mạng (Layer 3). Điều này giúp nó thực hiện cả chức năng chuyển đổi và định tuyến.
* Định tuyến tốc độ cao: Switch Layer 3 thường có hiệu suất cao và khả năng định tuyến với tốc độ cao, giúp nhanh chóng chuyển tiếp gói tin giữa các mạng.
* Quản lý đa lớp: Cung cấp các tính năng quản lý ở cả tầng 2 và tầng 3, bao gồm quản lý VLAN, chia mạng thành các mạng con (subnetting), và các tính năng bảo mật như ACL (Access Control List).
* Chế độ chuyển đổi hoặc chuyển đổi định tuyến: Switch Layer 3 có thể được cấu hình để hoạt động như một switch thông thường ở tầng 2 hoặc như một thiết bị định tuyến ở tầng 3.
* Hỗ trợ các giao thức định tuyến: Có thể hỗ trợ các giao thức định tuyến như RIP, OSPF, EIGRP, và BGP, tùy thuộc vào model và hãng sản xuất của thiết bị.

1. **Wireless controler**

Wireless Controller là một thiết bị quản lý mạng không dây (wireless network) được sử dụng để quản lý và kiểm soát các Access Point (AP) trong một mạng không dây. Chức năng chính của Wireless Controller là cung cấp quản lý tập trung, cấu hình, giám sát và bảo mật cho hạ tầng mạng Wi-Fi.

Một số đặc điểm quan trọng của Wireless Controller bao gồm:

* Quản lý AP: Wireless Controller giúp quản lý và cấu hình các Access Point trong mạng. Việc này giúp đơn giản hóa quá trình triển khai, cấu hình và bảo trì hạ tầng Wi-Fi.
* Tự động cấu hình: Wireless Controller cung cấp khả năng tự động cấu hình các thiết bị không dây, giúp giảm công đoạn cấu hình thủ công và tối ưu hóa hiệu suất mạng.
* Chuyển đổi tập trung: Wireless Controller có thể quản lý chuyển đổi không dây (Wireless LAN Controller) để thực hiện các chức năng chuyển đổi trong mạng không dây.
* Quản lý tập trung: Các Wireless Controller thường có khả năng quản lý hàng trăm hoặc thậm chí hàng nghìn Access Point từ một địa điểm duy nhất, giúp giảm bớt công sức quản lý và đảm bảo đồng nhất cấu hình trên toàn mạng.
* Tính năng bảo mật: Wireless Controller cung cấp các tính năng bảo mật như mã hóa dữ liệu, xác thực người dùng, và theo dõi các sự cố bảo mật trong mạng không dây.

1. **Access Point**

Access Point (AP) là một thiết bị mạng không dây (wireless) được sử dụng để kết nối các thiết bị không dây như laptop, điện thoại di động hoặc máy tính bảng vào mạng có dây. Access Point hoạt động ở tầng vật lý (tầng 1) và tầng liên kết dữ liệu (tầng 2) trong mô hình OSI.

Một số đặc điểm quan trọng của Access Point bao gồm:

* Phát sóng Wi-Fi: Access Point tạo ra một điểm truy cập không dây, cho phép các thiết bị không dây kết nối vào mạng.
* Chuyển tiếp dữ liệu: Access Point chuyển tiếp dữ liệu giữa thiết bị không dây và mạng có dây, giúp thiết bị không dây có thể truy cập tài nguyên mạng.
* Quản lý kết nối: Access Point có khả năng quản lý số lượng thiết bị không dây kết nối đến nó và điều tiết lưu lượng mạng.
* Bảo mật: Access Point thường hỗ trợ các tính năng bảo mật như mã hóa dữ liệu (WPA2, WPA3), giả mạo địa chỉ MAC, và các chức năng xác thực để đảm bảo an toàn cho mạng không dây.
* Cấu hình linh hoạt: Access Point có thể được cấu hình để hoạt động trong nhiều chế độ khác nhau như chế độ điểm truy cập duy nhất, chế độ mạng mở rộng (extender), hoặc chế độ cầu (bridge mode).

1. **Các dịch vụ cần thuê**
2. **Dịch vụ Internet**

Để lựa chọn được nhà cung cấp dịch vụ Internet phù hợp với nhu cầu và yêu cầu của doanh nghiệp, nhóm chúng em đã đề ra một số yếu tố quan trọng cần xem xét:

**Băng Thông và Tốc Độ:**

* Yêu cầu một băng thông đủ lớn để đáp ứng nhu cầu sử dụng hiện tại và có khả năng mở rộng tương lai.
* Tốc độ Internet phải đảm bảo ổn định và nhanh chóng.

**Dịch Vụ Đảm Bảo và Dự Phòng:**

* Đòi hỏi các dịch vụ đảm bảo chất lượng (SLA) cao, bao gồm thời gian hoạt động và khả năng khôi phục sau sự cố.
* Yêu cầu các giải pháp dự phòng để giảm thiểu thời gian chết của dịch vụ khi có sự cố.

**Bảo Mật và Quản Lý Rủi Ro:**

* Đảm bảo các biện pháp bảo mật mạng cao, bao gồm mã hóa và giám sát liên tục.
* Yêu cầu các công cụ quản lý rủi ro để theo dõi và giảm thiểu nguy cơ an ninh mạng.

**Hỗ Trợ Kỹ Thuật:**

* Yêu cầu dịch vụ hỗ trợ kỹ thuật 24/7 và thời gian phản hồi nhanh chóng.
* Mong muốn một đội ngũ hỗ trợ chuyên nghiệp và có kinh nghiệm.

**Chi Phí và Hiệu Suất:**

* Đánh giá chi phí dịch vụ và so sánh với hiệu suất cung cấp.
* Tìm kiếm sự cân bằng giữa chất lượng và chi phí.

Qua các tiêu chí trên thì nhóm chúng em lựa chọn Tập đoàn VNPT và Tập đoàn Viettel làm nhà cung cấp dịch vụ Internet cho doanh nghiệp.

## Đặt địa chỉ IP cho hệ thống mạng và thiết bị

### Tại trụ sở chính

Với cơ sở phòng ban tại trụ sở chính thì dự kiến sẽ có 10 Vlan được chia và dùng DHCP để cấp phát IP tự động cho các thiết bị. Các Vlan được chia như sau:

* Vlan 1 dành cho Data Center và các ip quản lý ở tầng trệt của tòa nhà sử dụng lớp mạng 172.20.0.0/24
* Vlan 2 dành cho Wifi public có lớp mạng 172.20.10.0/24
* Vlan 3 dành cho Developer ở tầng một của tòa nhà có lớp mạng 172.20.20.0/24
* Vlan 4 dành cho Project Manager ở tầng hai của tòa nhà có lớp mạng 172.20.30.0/24
* Vlan 5 dành cho Tester ở tầng một của tòa nhà có lớp mạng 172.20.40.0/24
* Vlan 6 dành cho Business Analyst ở tầng ba của tòa nhà có lớp mạng 172.20.50.0/24
* Vlan 7 dành cho HR ở tầng bốn của tòa nhà có lớp mạng 172.20.60.0/24
* Vlan 8 dành cho IT Manager ở tầng một hai của tòa nhà có lớp mạng 172.20.70.0/24
* Vlan 9 dành cho Technical Manager ở tầng trệt của tòa nhà có lớp mạng 172.20.80.0/24
* Vlan 10 dành cho CEO ở tầng 5 của tòa nhà có địa chỉ IP 172.20.90.0/24
* Chi tiết về địa chỉ IP và subnet mask của từng phòng ban tại trụ sở chính được thể hiện qua bảng sau:

|  |  |  |  |
| --- | --- | --- | --- |
| **Subnet Name** | **Address** | **Mask** | **Dec Mask** |
| **Data Center** | 172.20.0.0 | /24 | 255.255.255.0 |
| **Wifi public** | 172.20.10.0 | /24 | 255.255.255.0 |
| **Developer** | 172.20.20.0 | /24 | 255.255.255.0 |
| **Project Manager** | 172.20.30.0 | /24 | 255.255.255.0 |
| **Tester** | 172.20.40.0 | /24 | 255.255.255.0 |
| **Business Analyst** | 172.20.50.0 | /24 | 255.255.255.0 |
| **HR** | 172.20.60.0 | /24 | 255.255.255.0 |
| **IT manager** | 172.20.70.0 | /24 | 255.255.255.0 |
| **Technical Manager** | 172.20.80.0 | /24 | 255.255.255.0 |
| **CEO** | 172.20.90.0 | /29 | 255.255.255.0 |

Table ‑. IP table của trụ sở chính

### Tại chi nhánh

Tương tự như tại trụ sở chính thì ở chi nhánh ta chia hệ thống mạng ra 4 Vlan và dùng DHCP để cấp phát địa chỉ tự động cho các thiết bị tham gia vào mạng tại đây. Các Vlan được chia như sau:

* Vlan 1 dành cho Wireless Manager có địa chỉ IP nằm trong dãy địa chỉ 172.20.100.0/24.
* Vlan 2 dành cho Developer tại tầng một của tòa nhà có địa chỉ IP nằm trong dãy địa chỉ 172.20.110.0/24.
* Vlan 3 dành cho Tester ở tầng hai của tòa nhà có địa chỉ IP nằm trong dãy địa chỉ 172.20.120.0/24.
* Vlan 4 dành cho Wifi Public có địa chỉ IP nằm trong dãy địa chỉ 172.20.130.0/24.

Chi tiết về địa chỉ IP và subnet mast của từng phòng ban được thể hiện qua bảng sau:

|  |  |  |  |
| --- | --- | --- | --- |
| **Subnet Name** | **Address** | **Mask** | **Dec Mask** |
| **Wireless Manager** | 172.20.100.0 | /24 | 255.255.255.0 |
| **Wifi public** | 172.20.130.0 | /24 | 255.255.255.0 |
| **Developer** | 172.20.110.0 | /24 | 255.255.255.0 |
| **Project Manager** | 172.20.120.0 | /24 | 255.255.255.0 |

Table ‑. IP table của chi nhánh

## Thiết kế sơ đồ vật lý của toàn bộ hệ thống mạng

### Sơ đồ vật lý cho toàn hệ thống

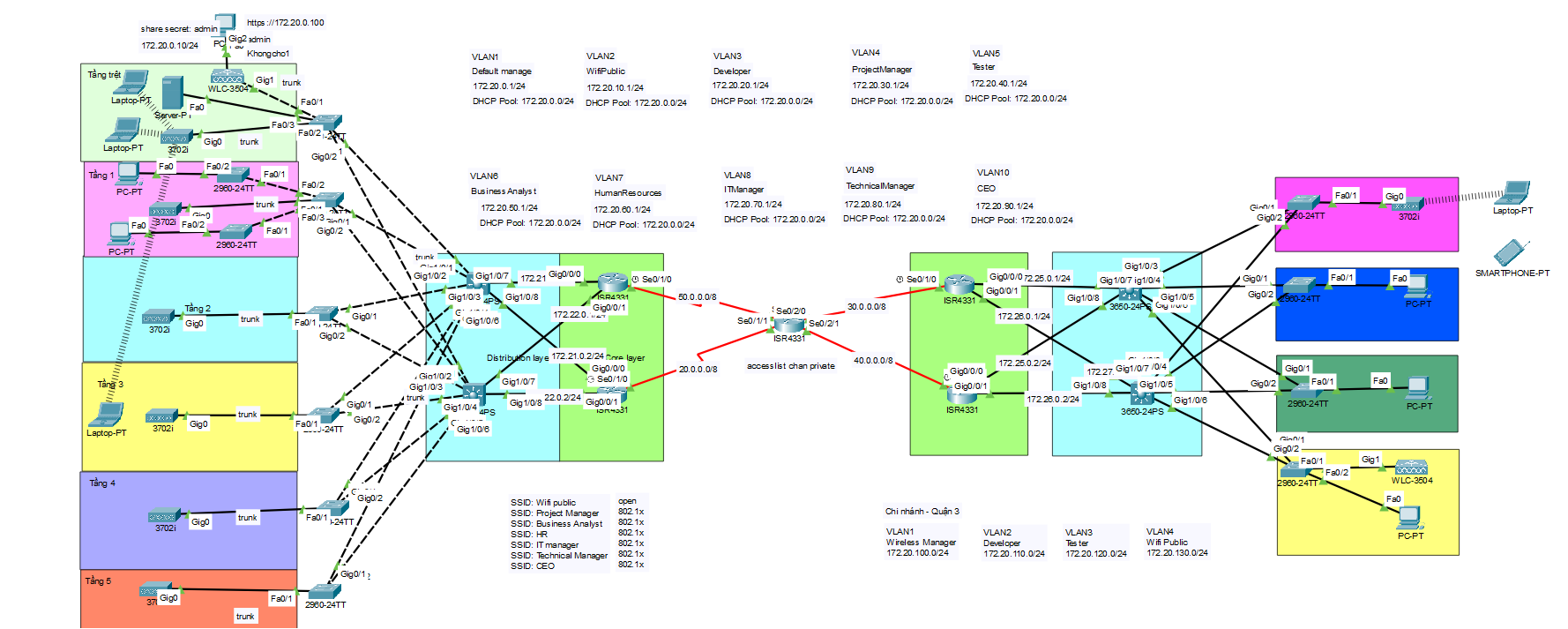


Figure .. Sơ đồ vật lí cho toàn hệ thống

Trong sơ đồ trên, ta sử dụng một router ISR để kết nối VPN giữa 2 chi nhánh

### Tại trụ sở chính

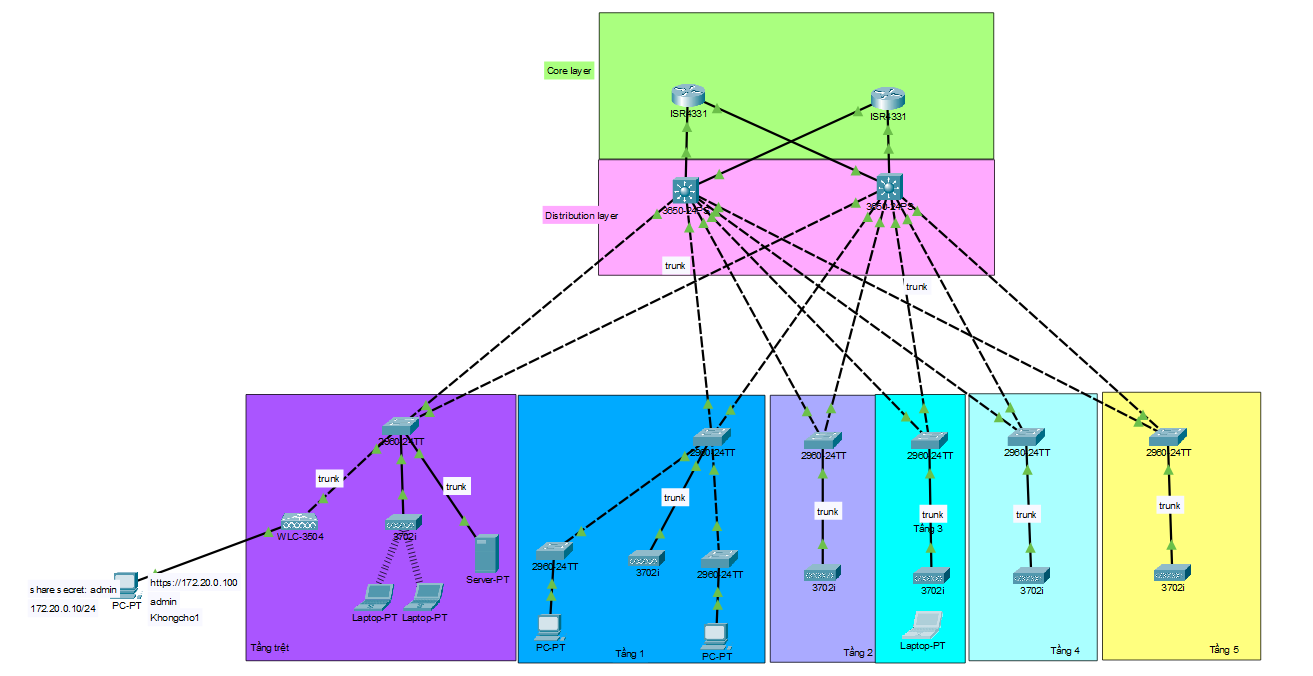


Figure .. sơ đồ vật lí tại trụ sở chính

1. **Lớp core layer và distribution layer**

Đầu tiên trong hệ thống mạng tại trụ sở chính là 2 lớp core layer và distribution layer chịu trách nhiệm vận chuyển khối lượng lớn dữ liệu và đảm bảo độ tin cậy nhanh chóng.

**Lớp Distribution layer:**

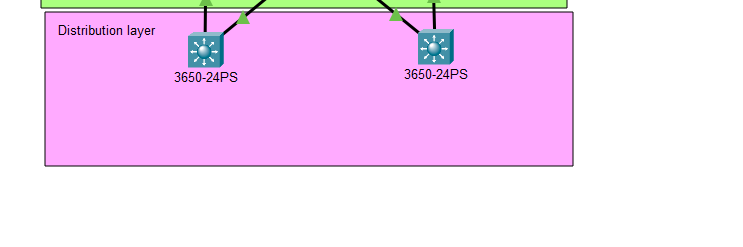


Figure .. Distribution layer tại trụ sở chính

* Bao gồm 2 switch layer 3: một switch chính và một switch phụ để đảm bảo khi xảy ra sự cố tại một trong hai switch thì hệ thống mạng vẫn hoạt động bình thường. Bằng cách cấu hình giao thức HRSP, chúng ta có thể xác định độ ưu tiên của từng switch và tùy chỉnh switch nào có độ ưu tiên cao hơn thì switch đó là switch chính. Ví dụ cụ thể:
  + Tại sw\_core1:

int vlan 1

standby 1 ip 172.20.0.3

standby 1 priority 105 // Đặt độ ưu tiên của router hiện tại là 105

standby 1 preempt // Kích hoạt tính năng preempt,

exit

* Tại sw\_core2:

int vlan 1

standby 1 ip 172.20.0.3

standby 1 preempt

exit

Trong ví dụ trên vì sw\_core1 có độ ưu tiên cao hơn nên là switch chính của hệ thống

* Cài đặt các ACL trên lớp này để phù hợp với yêu cầu của khách hàng:
  + các Vlan được truy cập server

Vlan1 management

Vlan3 developer

Vlan4 projectmanager

Vlan5 tester

Vlan8 itmanager

Vlan9 TechnicalManager

Vlan10 CEO

* + các Vlan được sử dụng các dịch vụ DNS, DHCP: tất cả Vlan
  + các Vlan được sử dụng các dịch vụ mail FTP, HTTP: trừ Vlan 2
  + các Vlan không được giao tiếp với Vlan1: tất cả các Vlan từ Vlan2 đến Vlan 9
  + chặn guest đến mạng internel

Ví dụ tại sw\_core1:

ip access-list extended ACL1

permit udp 172.20.0.0 0.0.255.255 172.20.0.10 0.0.0.0 eq 67

permit udp 172.20.0.0 0.0.255.255 172.20.0.10 0.0.0.0 eq 68

permit tcp 172.20.0.0 0.0.255.255 172.20.0.10 0.0.0.0 eq 53

permit udp 172.20.0.0 0.0.255.255 172.20.0.10 0.0.0.0 eq 53

deny ip 172.20.10.0 0.0.0.255 172.0.0.0 0.255.255.255

permit ip 172.20.20.0 0.0.0.255 172.20.0.10 0.0.0.0

permit ip 172.20.30.0 0.0.0.255 172.20.0.10 0.0.0.0

permit ip 172.20.40.0 0.0.0.255 172.20.0.10 0.0.0.0

permit ip 172.20.70.0 0.0.0.255 172.20.0.10 0.0.0.0

permit ip 172.20.80.0 0.0.0.255 172.20.0.10 0.0.0.0

permit ip 172.20.90.0 0.0.0.255 172.20.0.10 0.0.0.0

permit ip 172.20.120.0 0.0.0.255 172.20.0.10 0.0.0.0

permit ip 172.20.110.0 0.0.0.255 172.20.0.10 0.0.0.0

permit tcp 172.20.0.0 0.0.255.255 172.20.0.10 0.0.0.0 eq 20

permit tcp 172.20.0.0 0.0.255.255 172.20.0.10 0.0.0.0 eq 21

permit tcp 172.20.0.0 0.0.255.255 172.20.0.10 0.0.0.0 eq 25

permit tcp 172.20.0.0 0.0.255.255 172.20.0.10 0.0.0.0 eq 80

permit tcp 172.20.0.0 0.0.255.255 172.20.0.10 0.0.0.0 eq 110

deny ip any 172.20.0.0 0.0.0.255

permit ip any any

exit

int vlan 1

ip access-group ACL1 in

exit

int vlan 2

ip access-group ACL1 in

exit

int vlan 3

ip access-group ACL1 in

exit

int vlan 4

ip access-group ACL1 in

exit

int vlan 5

ip access-group ACL1 in

exit

int vlan 6

ip access-group ACL1 in

exit

int vlan 7

ip access-group ACL1 in

exit

int vlan 8

ip access-group ACL1 in

exit

int vlan 9

ip access-group ACL1 in

exit

int vlan 10

ip access-group ACL1 in

exit

end

wr

* Thiết lập RSTP để chống xảy ra Loop khi sử dụng nhiều thiết bị switch trong mạng bằng cách thiết lập một cổng root để làm cổng gốc.

Ví dụ:

|  |  |  |
| --- | --- | --- |
| Tại core 1 | Tại core 2 | Tại các switch  (cụ thể sw1) |
| spanning-tree mode rapid  spanning-tree vlan 1 root primary  spanning-tree vlan 2 root primary  spanning-tree vlan 3 root primary  spanning-tree vlan 4 root primary  spanning-tree vlan 5 root primary  spanning-tree vlan 6 root primary  spanning-tree vlan 7 root primary  spanning-tree vlan 8 root primary  spanning-tree vlan 9 root primary  spanning-tree vlan 10 root primary  end  write | spanning-tree mode rapid  spanning-tree vlan 6 root secondary  spanning-tree vlan 7 root secondary  spanning-tree vlan 8 root secondary  spanning-tree vlan 9 root secondary  spanning-tree vlan 10 root secondary  spanning-tree vlan 1 root secondary  spanning-tree vlan 2 root secondary  spanning-tree vlan 3 root secondary  spanning-tree vlan 4 root secondary  spanning-tree vlan 5 root secondary  end  write | spanning-tree mode rapid  int range f0/1-2  spanning-tree portfast trunk  spanning-tree bpduguard enable  exit  int f0/3  spanning-tree portfast  spanning-tree bpduguard enable  end  write |

* Thiết lập các Vlan tương ứng với các phòng ban và thiết lập các cổng trunk.

**Lớp core layer:**

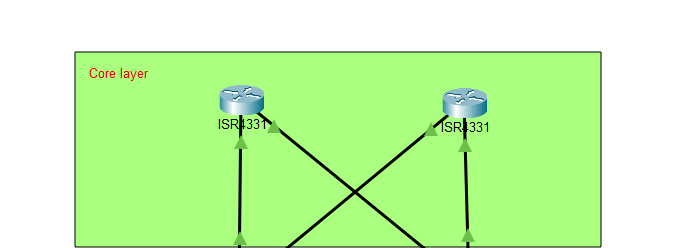


Figure .. Core layer tại trụ sở chính

* Tương tự như Distribution layer thì core layer cũng bao gồm 2 router: một router chính và một router phụ để đảm bảo khi xảy ra sự cố tại một trong hai router thì hệ thống mạng vẫn hoạt động bình thường. Bằng cách cấu hình giao thức HRSP, chúng ta có thể xác định độ ưu tiên của từng router và tùy chỉnh router nào có độ ưu tiên cao hơn thì router đó là router chính.
* Cấu hình giao thức OSPF cho các Vlan trong mạng.
* Cấu hình NAT để:
  + Xác định xem là IP nội bộ hay công cộng để được NAT đúng.
  + Tạo một ACL để cho phép tất cả các gói tin đi qua.
  + Thiết lập NAT overload (PAT - Port Address Translation) cho phép nhiều địa chỉ IP nội bộ được dịch sang một địa chỉ IP công cộng duy nhất với sự chia sẻ cổng (overload).

Ví dụ: tại core 1 và core 2

int range g0/0/0-1

ip nat inside

exit

int s0/1/0

ip nat outside

exit

access-list 1 permit any

ip nat inside source list 1 int s0/1/0 overload

* Thiết lập VPN cho hệ thống mạng

1. **Khối server và các Access point**

Gồm có 1 Wireless Controler để kiểm soát wifi và server để chạy các dịch vụ khác.

**=A screenshot of a computer

Description automatically generated**

Figure .: cấu hình Radius authentication server để sử dụng 802.1x

=A screenshot of a computer

Description automatically generated

Figure .: liên kết với wlc và tạo tài khoản

**A screenshot of a computer

Description automatically generated**

Figure .: danh sách các accesspoint trong mô hình mạng

**A screenshot of a computer

Description automatically generated**

Figure .: Danh sách ssid có trong mạng

1. **Sơ đồ hệ thống tầng trệt**

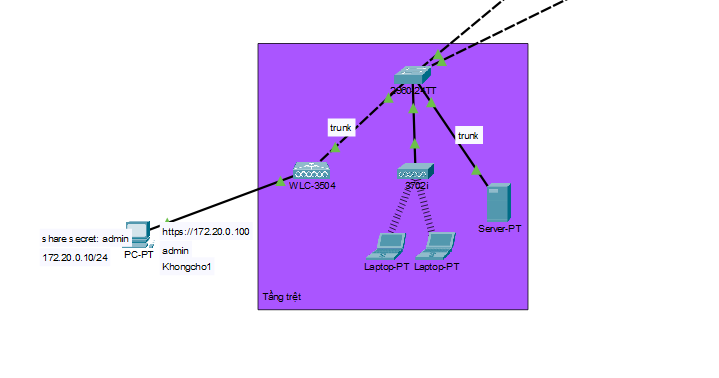


Figure .. Sơ đồ tầng trệt tại trụ sở chính

* Tại tầng trệt ta có hệ thống bao gồm khối server chứa Wireless controler và Vlan9 thuộc phòng Technical Manager có Access point để tạo điểm truy cập.

1. **Sơ đồ hệ thống tầng 1**

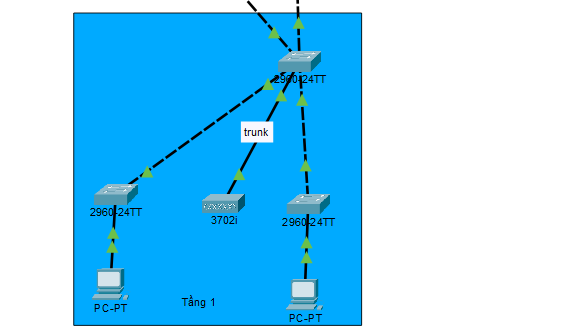


Figure .. Sơ đồ tầng 1 tại trụ sở chính

Tại tầng 1 của trụ sở chính gồm các switch quản lí các Vlan3 và Vlan5 lần lượt của các phòng Developer và Tester. Tại tầng này sử dụng một Access Point để tạo điểm truy cập wifi public.

1. **Sơ đồ hệ thống tầng 2**

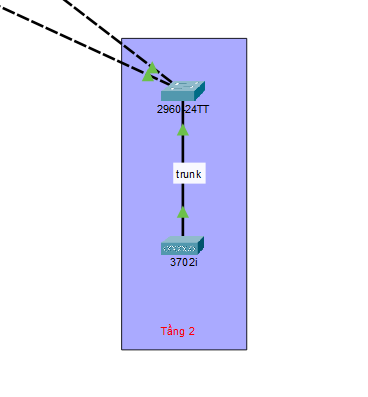


Figure .. Sơ đồ tầng 2 tại trụ sở chính

Tại tầng 2 của trụ sở chính gồm 1 switch quản lí các Vlan8 và Vlan5 lần lượt của các phòng IT manager và Project manager. Tại tầng này sử dụng một Access Point để tạo điểm truy cập wifi public.

1. **Sơ đồ hệ thống tầng 3**

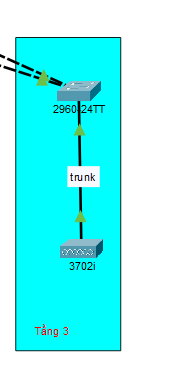


Figure .. Sơ đồ tầng 3 tại trụ sở chính

Tại tầng 3 của trụ sở chính gồm 1 switch quản lí các Vlan6 của phòng Business Analyst. Tại tầng này sử dụng một Access Point để tạo điểm truy cập wifi public.

1. **Sơ đồ hệ thống tầng 4**

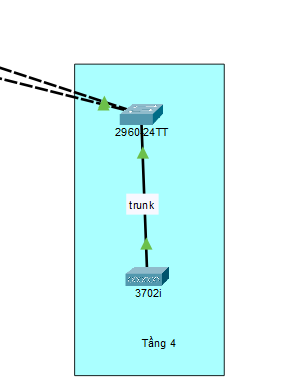


Figure .. Sơ đồ tầng 4 tại trụ sở chính

Tại tầng 4 của trụ sở chính gồm 1 switch quản lí các Vlan7 của phòng HR. Tại tầng này sử dụng một Access Point để tạo điểm truy cập wifi public.

1. **Sơ đồ hệ thống tầng 5**

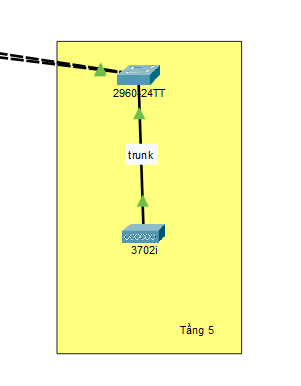


Figure .. Sơ đồ tầng 5 tại trụ sở chính

Tại tầng 5 của trụ sở chính gồm 1 switch quản lí các Vlan10 của phòng CEO. Tại tầng này sử dụng một Access Point để tạo điểm truy cập wifi public.

1. **Tại chi nhánh đặt tại Quận 3**

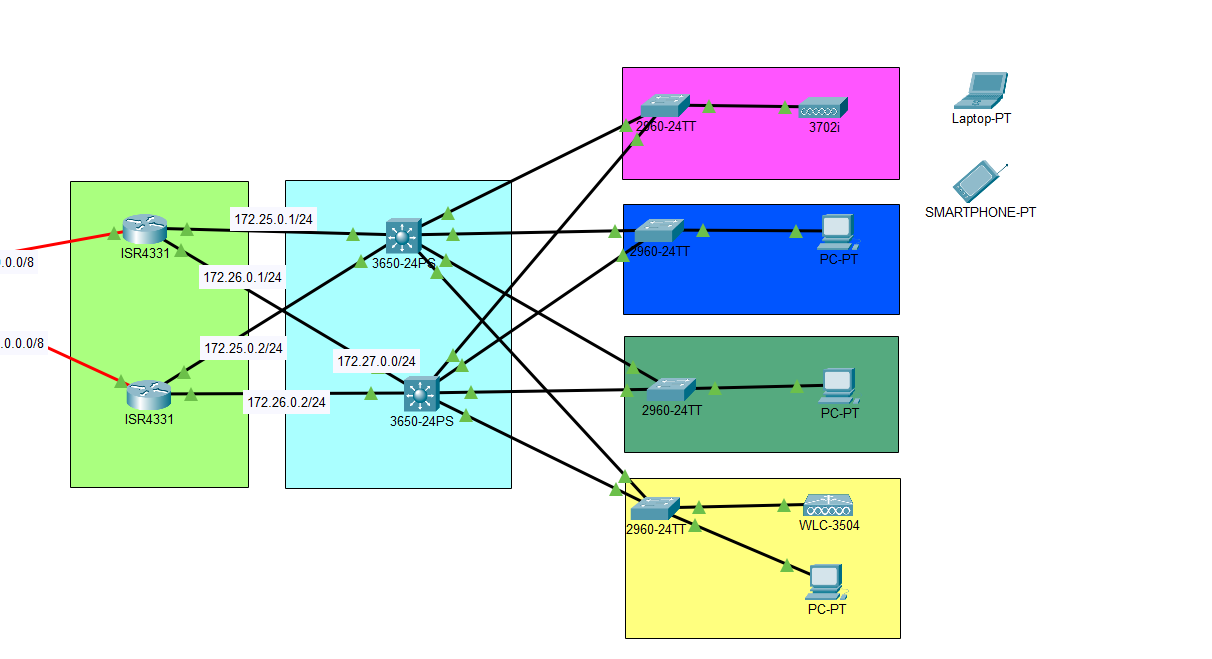


Figure .. Sơ đồ hệ thống tại chi nhánh

Cũng tương tự như tại trụ sở chính, ở đây cũng được trang bị hệ thông các core layer và distribuion layer để chịu trách nhiệm vận chuyển khối lượng lớn dữ liệu và đảm bảo độ tin cậy nhanh chóng.

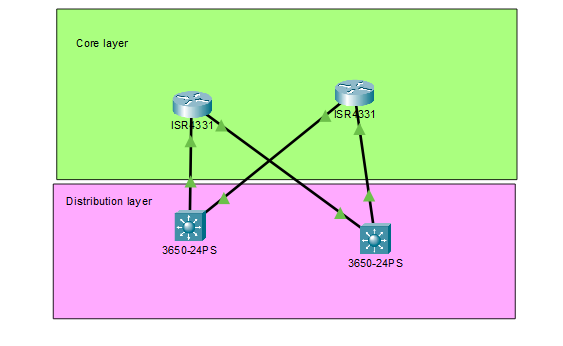


Figure ..Distribution layer và core layer tại chi nhánh

Và cũng được thiết kế cấu hình các giao thức như HRSP, OSPF, RSTP, NAT, ACL để hệ thống có thể hoạt động.

Kế tiếp là các tầng và phòng ban

1. **Tầng 1 có phòng developer và hệ thống Wireless controler**

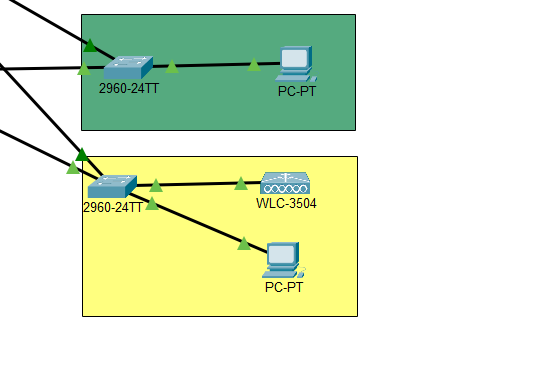


Figure .. Sơ đồ tầng 1 tại chi nhánh

Tầng này bao gồm 1 switch kết nối với các PC nằm trong Vlan2 của phòng developer và hệ thống gồm 1 switch kết nối với Wireless controler và PC để điều khiển wifi thuộc Vlan1 tên Wireless Manager.

1. **Tầng 2 gồm phòng Tester và hệ thống wifi public**

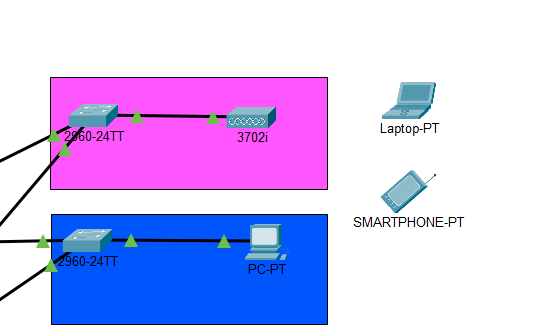


Figure .. Sơ đồ tầng 2 tại chi nhánh

Tầng này bao gồm 1 switch kết nối với các PC nằm trong Vlan3 của phòng tester và hệ thống gồm 1 switch kết nối với Access point.

# CÁC DỊCH VỤ CỦA HỆ THỐNG VÀ CHI PHÍ HOẠT ĐỘNG

## Các dịch vụ cung cấp

### OSPF

OSPF là viết tắt của cụm từ Open Shortest Path First. Đây là một giao thức định tuyến nội, tức là được sử dụng trong phạm vi một khu vực hay một hệ thống mạng. OSPF hoạt động dựa trên thuật toán Link state routing, mỗi bộ định tuyến sữ chứa thông tin của tất cả tên miền. OSPF dựa trên các thông tin này để xác định quảng đường ngắn nhất.

Sử dụng cấu hình định tuyến OSPF mang lại nhiều lợi ích trong môi trường mạng, đặc biệt là trong các mạng lớn và phức tạp. Dưới đây là một số lý do mà OSPF thường được ưa chuộng:

**Hiệu suất cao và linh hoạt:**

* OSPF sử dụng thuật toán SPF (Shortest Path First) để xác định đường đi tối ưu, giúp tối ưu hóa hiệu suất mạng bằng cách chọn đường đi ngắn nhất.
* Khả năng tự động thích nghi với thay đổi trong cấu trúc mạng, giúp nhanh chóng đáp ứng với sự thay đổi trong môi trường.

**Hỗ trợ mạng lớn:**

* OSPF làm việc hiệu quả trên các mạng lớn với số lượng lớn các router và mạng con.
* Hỗ trợ phân chia mạng thành các khu vực (area), giúp giảm bớt gánh nặng thông tin định tuyến và làm tăng hiệu suất.

**Độ tin cậy cao:**

* OSPF sử dụng nhiều tính năng đảm bảo độ tin cậy như Hello Protocol để kiểm tra tình trạng kết nối và cập nhật thông tin định tuyến.
* Khi có sự thay đổi trong mạng, OSPF có khả năng hồi phục nhanh chóng và cập nhật thông tin định tuyến mà không làm gián đoạn dịch vụ.

**Tính đa kết nối:**

* OSPF hỗ trợ nhiều đường đi đến một đích, giúp cải thiện bảo đảm khả năng sẵn sàng và đáng tin cậy của mạng.
* Điều này làm giảm rủi ro khi một đường đi bị chặn hoặc một router gặp sự cố.

**Quản lý thông tin định tuyến:**

* OSPF cung cấp nhiều cơ chế quản lý thông tin định tuyến, giúp người quản trị mạng dễ dàng theo dõi và kiểm soát định tuyến trong hệ thống.

1. **NAT**

NAT hay còn gọi là Network Address Translation là một kỹ thuật cho phép một hoặc nhiều địa chỉ IP cục bộ chuyển đổi sang một hoặc nhiều địa chỉ IP công cộng. Vị trí để thực hiện kỹ thuật NAT là router biên, nơi kết nối 2 loại mạng này.

**Nhiệm vụ của NAT:**

* Như một router có thể chuyển tiếp các gói tin giữa những lớp mạng khác nhau. Có thể thay đổi địa chỉ bên trong một gói tin khi gói tin đi qua router hay các thiết bị khác
* Một Firewall cơ bản, duy trì một bange thông tin về mỗi gói tin được được gửi qua. NAT có thể lọc các gói tin được gửi đến hay gửi từ một địa chỉ IP và cho phép hay ngăn chặn truy cập đến một port cụ thể.

1. **VLAN**

Là viết tắt của Virtual Local Area Network hay còn gọi là mạng LAN ảo. Mạng LAN ảo (VLAN) là một nhóm các máy tính được kết nối với cùng một mạng nhưng không ở gần nhau. Sử dụng VLAN cho phép sử dụng tài nguyên mạng hiệu quả hơn và có thể hữu ích khi có quá nhiều thiết bị cho một mạng. Sau đây là một vài lí do nên sử dụng VLAN:

**Tiết kiệm băng thông**

* Vì VLAN có thể chia một mạng thành nhiều đoạn khác nhau. Khi gửi gói tin sẽ chỉ gửi trong một VLAN duy nhất, không gửi trong các VLAN khác, tiết kiệm băng thông, làm giảm lưu lượng, không làm giảm tốc độ đường truyền.

**Cải thiện bảo mật**

* Các VLAN khác nhau không thể giao tiếp với nhau (trừ khi có khai báo định tuyến). Nếu một trong các VLAN bị lỗi, VLAN khác sẽ không bị ảnh hưởng.

**Dễ dàng thêm và loại bỏ máy tính khỏi VLAN**

* Bộ chuyển đổi nhiều cổng cho phép bạn định cấu hình các VLAN khác nhau cho mỗi cổng, giúp việc kết nối nhiều máy tính hơn với VLAN trở nên đơn giản.

**Mạng có tính di động cao**

* VLAN cho phép các thiết bị được di chuyển dễ dàng. VLAN có thể được thiết lập động hoặc tĩnh. Người quản trị mạng phải cấu hình từng cổng của mỗi bộ chuyển mạch trong cấu hình tĩnh. Sau đó, gán nó cho một VLAN cụ thể. Mỗi cổng chuyển mạch trong cấu hình động có thể cấu hình VLAN của riêng nó dựa trên địa chỉ MAC của thiết bị mà nó được kết nối.

1. **Trunking**

Trunking là thành phần kiến trúc quan trọng của VLAN. Trong VLANS, một mạng vật lý được ảo hóa để tạo ra một số mạng logic là các miền quảng bá độc lập. Liên kết truyền thông vật lý chính là đường trục (trunk); các switch được kết nối với đường trục cung cấp các nhánh để hỗ trợ nhiều thiết bị khách.

Chức năng chính của trunking:

Sử dụng port trunking sẽ mở rộng quyền truy cập Vlan trên toàn bộ mạng. Khái niệm này còn được gọi là tổng hợp liên kết. Nhiều liên kết Ethernet được nhóm lại với nhau để hoạt động như một liên kết logic duy nhất. Phương pháp tổng hợp các liên kết được xác định theo tiêu chuẩn IEEE 802.1aq và theo tiêu chuẩn 802.1AX cho mạng LAN và mạng khu vực đô thị, cũng như bằng các phương pháp độc quyền khác nhau của nhà cung cấp. Chức năng trung kế phải được kích hoạt thông qua các lệnh song song ở cả hai đầu gửi và nhận.

1. **HSRP**

HSRP là một giao thức mạng được sử dụng để tạo khả năng dự phòng và độ tin cậy trong việc sử dụng các bộ định tuyến trong mạng máy tính. Giao thức này cho phép nhiều bộ định tuyến trong mạng con hoạt động cùng nhau và tạo thành một nhóm. Giao thức này sẽ hoạt động theo phương thức Active – Standby. Nếu bộ định tuyến chính bị lỗi, bộ định tuyến dự phòng sẽ tự động đảm nhận vai trò của bộ định tuyến chính mà không cần can thiệp thủ công. Cụm từ viết tắt của HSRP là Hot Standby Router Protocol

**Các chức năng chính của HSRP:**

* HSRP được sử dụng để tăng tính khả dụng của mạng bằng cách cung cấp giải pháp chuyển đổi dự phòng tự động và nhanh chóng. Nếu bộ định tuyến chính bị lỗi, bộ định tuyến dự phòng có thể ngay lập tức tiếp quản và duy trì kết nối mạng.
* HSRP cho phép chia sẻ tải lưu lượng giữa bộ định tuyến chính và bộ định tuyến dự phòng. Nó giúp tối ưu hóa việc sử dụng tài nguyên mạng và cải thiện hiệu suất mạng.
* HSRP cho phép các thiết bị trong mạng giao tiếp với các mạng bên ngoài bằng cùng một gateway mặc định, ngay cả khi bộ định tuyến chính thay đổi.

1. **VPN**

VPN là một mạng riêng ảo – viết tắt của từ Virtual Private Network. VPN có khả năng tạo ra kết nối mạng riêng tư khi kết nối với bất kỳ hệ thống mạng Internet công cộng nào. Nghe có vẻ khó hiểu với người dùng bình thường, nhưng nói một cách đơn giản là tạo một lối đi riêng cho người dùng truy cập Internet an toàn hơn thay vì phải đối mặt với hàng ngàn nguy cơ khi kết nối với Wi-Fi công cộng bên ngoài.

**Các chức năng chính của VPN:**

* Bảo mật Dữ Liệu: Cung cấp một lớp bảo mật bằng cách mã hóa dữ liệu trên đường truyền, giúp ngăn chặn người ngoại vi theo dõi hoặc đánh cắp thông tin nhạy cảm.
* Kết nối an Toàn từ xa: Cho phép người dùng kết nối và truy cập mạng nội bộ của tổ chức một cách an toàn từ xa, giúp bảo vệ dữ liệu và thông tin.
* Ẩn Địa Chỉ IP Thực: Ẩn địa chỉ IP thực của người dùng và thay thế bằng địa chỉ IP của máy chủ VPN, giúp bảo vệ quyền riêng tư và làm tăng khả năng ẩn danh.
* Vượt Tường Lửa (Bypass Firewalls): Giúp người dùng vượt qua các rào cản mạng, như tường lửa, để truy cập vào các nguồn thông tin hoặc dịch vụ bị chặn trong một số quốc gia hoặc mạng.
* Kết nối an Toàn giữa Chi Nhánh và Trụ Sở: Cho phép tạo ra một kết nối an toàn giữa các chi nhánh và trụ sở của một tổ chức, giúp nhân viên ở các địa điểm khác nhau có thể truy cập vào tài nguyên nội bộ một cách an toàn.
* Giả mạo Địa Lý (Geo-spoofing): VPN có thể giúp người dùng giả mạo vị trí địa lý của họ bằng cách kết nối thông qua máy chủ ở một quốc gia khác, đặc biệt hữu ích cho việc truy cập nội dung có giới hạn địa lý.
* Quản lý Băng Thông và Tăng Tốc Kết Nối: Một số dịch vụ VPN cung cấp tính năng quản lý băng thông, giúp tối ưu hóa hiệu suất kết nối và giảm độ trễ.
* Bảo mật Wi-Fi Công Cộng: Bảo vệ thông tin khi kết nối tới các mạng Wi-Fi công cộng không an toàn bằng cách tạo một kết nối an toàn và mã hóa dữ liệu.

1. **RSTP**

RSTP là viết tắt của "Rapid Spanning Tree Protocol" (Giao thức Chồng cây cầu nhanh), là một giao thức mạng được sử dụng để tạo ra một cấu trúc mạng dựa trên chồng cây cầu (spanning tree) nhằm tránh loop (vòng lặp) trong các mạng Ethernet. Giao thức này là một phiên bản cải tiến của giao thức Spanning Tree Protocol (STP).

RSTP giúp giảm thời gian khôi phục mạng sau khi có sự thay đổi trong cấu trúc mạng, chẳng hạn như khi một đường dẫn mạng bị ngắt hoặc khi một đường dẫn mới được thêm vào. So với STP, RSTP có thời gian khôi phục nhanh hơn do nó giảm bớt thời gian chờ và quảng bá khi có sự thay đổi.

RSTP hoạt động bằng cách chọn một cổng chính (root port) trên mỗi switch và chặn các cổng không cần thiết để tạo thành một cấu trúc mạng không có loop. Nó giúp cải thiện hiệu suất mạng bằng cách cung cấp đường dẫn dự phòng và giảm thời gian hồi phục sau khi có sự thay đổi trong mạng.

## Chi phí cho toàn hệ thống

### Chi phí cho dịch vụ

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Đơn giá** |
| 1 | VPN  Site to site |  |
| 2 | Mail |  |
| 3 | DNS |  |
| 4 | HTTP |  |
| 5 | Dịch vụ mạng FTTH VIP600 viettel | 6.600.000VNĐ |
| 7 | Dịch vụ mạng Fiber Xtra5 | 5.000.000VNĐ |

1. **Chi phí cho thiết bị**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Tên thiết bị** | **Đặc tính kĩ thuật** | **Đơn giá**  **(VND)** | **Số lượng** | **Thành tiền**  **(VND)** |
| 1 | Switch | - Thiết bị có thiết kế nhỏ gọn tinh tế với 24 cổng Ethernet tốc độ 10/100 và kèm theo đó là 2 cổng Uplink với 2 tính năng riêng biệt. Trong đó một cổng Uplink 10/100/1000 là cổng Ethernet và cổng còn lại là cổng Gigabit Ethernet 1 cổng SFP.  - Được sử dụng chính để kết nối các thiết bị trong hệ thống mạng LAN với nhau.Nó thực hiện các tính năng quản lý thông dụng như SPAN, CiscoWiew, giaothuwcs CDP, giao thức Trunking ảo (VTP)... | 7,050,000 | 12 | 84,600,000 |
| 2 | Switch layer 3  Cisco WS-C3560-24TS-S | Tự động nhận ra mỗi thiết bị, định tuyến IP, hỗ trợ DHCP, tự động đàm phán, hỗ trợ ARP, trunking, hỗ trợ VLAN, auto-uplink (tự động MDI / MDI-X), IGMP snooping, quản lý, hỗ trợ IPv6 | 24,200,000 | 4 | 96,800,000 |
| 3 | ISR Router  Router Cisco ISR4331-V/K9 | Thiết bị cung cấp định tuyến, lưu trữ, bảo mật và chuyển đổi – tất cả trong một nền tảng duy nhất, đáng tin cậy.  Xây dựng chi nhánh kỹ thuật số an toàn, nhanh chóng và có thể mở rộng.  Đồng thời đáp ứng nhu cầu hiệu năng mạng bùng nổ được thúc đẩy bởi các ứng dụng đám mây và chuyển đổi kỹ thuật số. | 77,190,000 | 4 | 308,760,000 |
| 4 | Access Point  CISCO Catalyst 9105AX C9105AXI-EWC-S | Là điểm truy cập trong nhà, có ăng-ten bên trong; Wi-Fi 6; 2×2 MIMO với hai luồng không gian và miền quy định S. | 11.800.000 | 7 | 82,600,000 |
| 5 | Wireless LAN controller | Cisco AIR-CT3504-K9  Cung cấp khả năng điều khiển, quản lý và xử lý sự cố tập trung cho các doanh nghiệp và văn phòng chi nhánh.  Cung cấp tính linh hoạt để hỗ trợ nhiều chế độ triển khai trong cùng một bộ điều khiển — một chế độ tập trung cho môi trường  Các chi nhánh được quản lý tinh gọn qua mạng WAN và chế độ lưới (cầu nối) để triển khai trong đó không có hệ thống cáp Ethernet đầy đủ. | 56,150,000 | 2 | 112,300,000 |
|  | Tổng cộng | | | | 685,060,000 |

# THAM KHẢO

<https://www.youtube.com/watch?v=xqFuDviJINE>

https://vietteltelecom.vn/internet-doanh-nghiep