**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO BÀI TẬP**

Môn học: Thiết Kế Mạng

Giáo viên hướng dẫn: ThS. Bùi Thanh Bình

Mã lớp: NT113.P11

Thành viên trong nhóm:

22521490 – Nguyễn Đức Toàn

22521469 – Nguyễn Cao Tiến

22521344 – Đặng Chí Thành

22521212 – Nguyễn Đặng Khánh Quốc

NĂM HỌC : 2024 – 2025

Mục lục

[1. Giới thiệu tổng quan 4](#_Toc184759968)

[2. Các thông tin cơ bản về đề tài 4](#_Toc184759969)

[2.1 Yêu cầu của khác hàng 4](#_Toc184759970)

[2.2 Giải quyết các yêu cầu 4](#_Toc184759971)

[3. Thiết kế hệ thống mạng 6](#_Toc184759978)

[3.1 Thiết kế mô hình mạng logic 6](#_Toc184759979)

[3.2 Thiết kế sơ đồ vật lý của toàn bộ hệ thống mạng 7](#_Toc184759980)

[3.2.1 Sơ đồ vật lý 7](#_Toc184759981)

[3.2.2 Các thiết bị dùng trong hệ thống mạng 8](#_Toc184759982)

[3.2.3 Các dịch vụ cần thuê 8](#_Toc184759983)

[3.3 Địa chỉ IP của hệ thống mạng và thiết bị 9](#_Toc184759987)

[4. Các dịch vụ cung cấp và chi phí hoạt động 15](#_Toc184759988)

[4.1 Các dịch vụ cung cấp 15](#_Toc184759989)

[4.2 Chi phí cho toàn hệ thống 18](#_Toc184760000)

[4.2.1 Chi phí cho thiết bị 18](#_Toc184760001)

[4.2.2 Chi phí cho dịch vụ: 18](#_Toc184760002)

[5. Kết luận 19](#_Toc184760003)

[6. Các nguồn tài liệu tham khảo 19](#_Toc184760004)

# Giới thiệu tổng quan

Báo cáo này nhằm mục đích trình bày kế hoạch thiết kế hệ thống mạng cho Công ty Outsource O-UIT, với yêu cầu xây dựng một hạ tầng mạng hiệu quả và bảo mật cho trụ sở chính tại Thủ Đức và chi nhánh tại Quận 3. Thiết kế mạng là một yếu tố quan trọng trong việc đảm bảo sự hoạt động hiệu quả của một tổ chức. Một hệ thống mạng tốt không chỉ giúp tăng cường giao tiếp giữa các phòng ban mà còn bảo vệ thông tin nhạy cảm và tối ưu hóa hiệu suất làm việc. Đồ án sẽ phân tích nhu cầu của công ty, xác định các thiết bị và công nghệ cần thiết, đồng thời đề xuất giải pháp mạng tối ưu.

# Các thông tin cơ bản về đề tài

## Yêu cầu của khác hàng

Công ty Outsource O-UIT yêu cầu thiết kế một hệ thống mạng với các yếu tố sau:

**Mạng có 2 địa điểm**: Trụ sở chính và chi nhánh. Việc kết nối giữa hai địa điểm này là rất quan trọng để đảm bảo sự liên lạc và chia sẻ thông tin hiệu quả.

**Hệ thống mạng hỗ trợ các phòng ban khác nhau**: Mỗi phòng ban cần một VLAN riêng để dễ dàng quản lý và phân tách lưu lượng mạng. Điều này không chỉ giúp quản lý mạng dễ dàng hơn mà còn tăng cường bảo mật, vì mỗi phòng ban sẽ hoạt động trong một không gian mạng riêng biệt.

**Kết nối qua VPN site-to-site**: Để đảm bảo bảo mật cho dữ liệu khi truyền qua Internet, công ty yêu cầu thiết lập một kết nối VPN giữa trụ sở chính và chi nhánh. Điều này sẽ bảo vệ thông tin nhạy cảm khỏi các mối đe dọa bên ngoài.

**Tính sẵn sàng cao**: Công ty mong muốn sử dụng các giải pháp dự phòng như HSRP (Hot Standby Router Protocol) để đảm bảo rằng không có điểm thất bại đơn lẻ trong mạng. Điều này rất quan trọng trong môi trường làm việc hiện đại, nơi mà thời gian chết có thể gây ra thiệt hại lớn.

**Khả năng mở rộng**: Hệ thống mạng phải có thể dễ dàng mở rộng trong tương lai khi có nhu cầu tăng trưởng. Việc thiết kế một hệ thống có khả năng mở rộng sẽ giúp công ty tiết kiệm chi phí và thời gian trong việc nâng cấp hệ thống.

**Bảo mật**: Mạng phải bảo vệ thông tin nhạy cảm và chỉ cho phép truy cập hợp lệ vào các tài nguyên mạng. Việc triển khai các chính sách bảo mật như Access Control Lists (ACL) sẽ là cần thiết để hạn chế truy cập giữa các VLAN không cần thiết.

## Giải quyết các yêu cầu

### Phân chia mạng thành các VLAN

* Tại Trụ sở Chính:

VLAN 30: Developer: Nhóm phát triển phần mềm, chịu trách nhiệm thiết kế và lập trình ứng dụng.

VLAN 40: Tester: Nhóm kiểm thử, đảm bảo chất lượng sản phẩm trước khi ra mắt.

VLAN 50: IT Manager: Quản lý công nghệ thông tin, giám sát hoạt động của hệ thống mạng.

VLAN 60: Technical Manager: Quản lý kỹ thuật, hỗ trợ các vấn đề liên quan đến công nghệ.

VLAN 70: Project Manager: Quản lý dự án, điều phối các hoạt động liên quan đến dự án.

VLAN 80: HR: Bộ phận nhân sự, quản lý thông tin nhân viên và các vấn đề liên quan đến nhân sự.

VLAN 90: Business Analyst: Phân tích kinh doanh, hỗ trợ các quyết định chiến lược.

VLAN 100: CEO: Giám đốc điều hành, quản lý toàn bộ hoạt động của công ty.

VLAN 110: Data Center: Trung tâm dữ liệu, nơi lưu trữ và quản lý thông tin quan trọng của công ty.

* Tại Chi nhánh:

VLAN 10: Developer: Nhóm phát triển phần mềm tại chi nhánh.

VLAN 20: Tester: Nhóm kiểm thử tại chi nhánh.

Việc phân chia này không chỉ giúp quản lý lưu lượng mạng hiệu quả hơn mà còn tăng cường bảo mật, ngăn chặn việc truy cập trái phép giữa các phòng ban khác nhau.

### Định tuyến giữa các VLAN (Inter-VLAN Routing)

Mỗi VLAN cần có một gateway để định tuyến lưu lượng mạng giữa các VLAN. Việc cấu hình Inter-VLAN Routing có thể được thực hiện trên Switch Layer 3 hoặc Router. Điều này cho phép các VLAN giao tiếp với nhau một cách hiệu quả, đồng thời đảm bảo rằng lưu lượng mạng được quản lý tốt.

**Cấu hình Gateway**: Mỗi VLAN sẽ có một địa chỉ IP riêng làm gateway, giúp định tuyến lưu lượng giữa các VLAN khác nhau.

**Thiết lập Routing Protocol**: Sử dụng giao thức định tuyến OSPF để đảm bảo rằng các thông tin định tuyến được cập nhật kịp thời.

### Kết nối VPN giữa Trụ sở Chính và Chi nhánh

Do Trụ sở Chính và Chi nhánh nằm ở hai vị trí địa lý khác nhau, việc thiết lập một VPN site-to-site sử dụng giao thức GRE làm nền tảng là rất quan trọng để tạo một đường hầm kết nối an toàn và hiệu quả qua Internet.

Cấu hình GRE VPN giữa hai router tại mỗi địa điểm, đảm bảo truyền tải dữ liệu qua đường hầm GRE một cách đáng tin cậy. Có thể tích hợp với giao thức mã hóa như IPsec để bảo vệ dữ liệu khỏi các rủi ro an ninh mạng.

Kiểm tra kết nối: Thực hiện các bài kiểm tra như ping, traceroute, và kiểm tra thông lượng để đảm bảo rằng kết nối GRE VPN hoạt động ổn định, đạt hiệu suất mong muốn và bảo mật tối đa.

### Tính sẵn sàng cao với HSRP

Để đảm bảo tính khả dụng cao cho mạng, HSRP (Hot Standby Router Protocol) sẽ được sử dụng để tạo ra một gateway ảo cho các VLAN.

Cấu hình HSRP: Thiết lập HSRP trên các router để tạo ra một IP ảo mà tất cả các VLAN sẽ sử dụng. Nếu router chính gặp sự cố, router dự phòng sẽ tự động thay thế mà không làm gián đoạn dịch vụ.

Giám sát trạng thái: Theo dõi trạng thái của các router để phát hiện sớm các vấn đề và khắc phục kịp thời.

### Phân bổ địa chỉ IP cho các thiết bị

Việc phân bổ địa chỉ IP cho các thiết bị trong các VLAN là rất quan trọng để đảm bảo rằng mọi thiết bị đều có thể kết nối và giao tiếp với nhau.

Sử dụng địa chỉ IP riêng: Mỗi VLAN sẽ được cấp phát một dải địa chỉ IP riêng, giúp quản lý và phân loại thiết bị dễ dàng hơn.

Cấu hình DHCP: Thiết lập DHCP server để tự động cấp phát địa chỉ IP cho các thiết bị người dùng trong các VLAN, đảm bảo rằng không có sự xung đột địa chỉ IP.

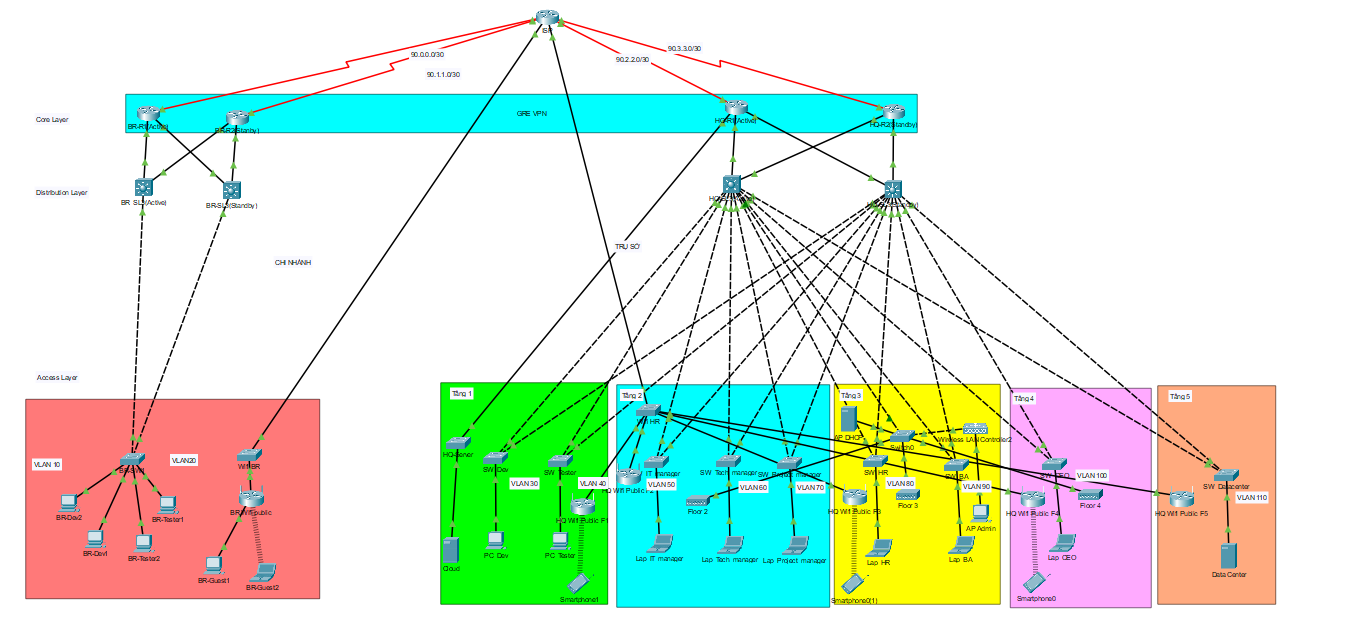
### Quản lý mạng

Để duy trì an ninh và hiệu suất của mạng, việc quản lý và giám sát là rất cần thiết.

Triển khai ACL (Access Control Lists): Sử dụng ACL để hạn chế truy cập giữa các VLAN không cần thiết, bảo vệ thông tin nhạy cảm và ngăn chặn các mối đe dọa từ bên ngoài.

# Thiết kế hệ thống mạng

## Thiết kế mô hình mạng logic



Mô hình mạng Top-Down gồm ba tầng: Core Layer, Distribution Layer, và Access Layer được lựa chọn trong thiết kế mạng nhờ tính cấu trúc chặt chẽ, khả năng mở rộng linh hoạt và hiệu quả trong quản lý.

* Khả năng mở rộng: Mô hình 3 lớp giúp mở rộng mạng một cách dễ dàng và có thể đáp ứng được nhu cầu gia tăng của người dùng hoặc dịch vụ.
* Hiệu suất tối ưu: Chia mạng thành các lớp giúp tối ưu hóa hiệu suất, giảm độ trễ và tải lên từng lớp.
* Quản lý và bảo mật dễ dàng: Việc phân tách các chức năng giúp dễ dàng áp dụng các chính sách bảo mật và quản lý mạng một cách tập trung và hiệu quả.
* Tính khả dụng cao: Sự phân tách giữa các lớp giúp tăng tính dự phòng và giảm thiểu sự cố hệ thống, cải thiện tính ổn định của mạng.
* Tối ưu hóa chi phí: Việc chia nhỏ các chức năng và phân phối lưu lượng giúp tối ưu hóa tài nguyên, giảm thiểu chi phí triển khai và duy trì mạng.

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

## Sơ đồ vật lý

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Loại thiết bị | Mẫu sản phẩm | Số lượng thiết bị | Đơn giá, ước tính | Số lượng và loại cổng giao tiếp | Mô tả, chức năng | Thành tiền |
| Router | [Router Integrated ISR 4331 Cisco ISR4331/K9](https://www.sieuthivienthong.com/router-integrated-isr-4331-cisco-isr4331k9-31359.html) | 4 | 40.000.000 đ | - 3 cổng Gigabit Ethernet (10/100/1000 Mbps). - 2 cổng RJ45 và 2 cổng SFP (cho kết nối cáp quang).  - 2 Cổng NIM cho phép mở rộng cổng | - Hỗ trợ thay thế module nóng mà không cần tắt router, tăng tính linh hoạt và giảm thời gian gián đoạn.  - Hỗ trợ cấp nguồn qua Ethernet với công suất tối đa 250W, thích hợp cho các thiết bị như Access Point hoặc camera IP.  - Hỗ trợ 1 khe cắm module dịch vụ nâng cao để mở rộng tính năng (ví dụ: tường lửa, VoIP, VPN). | 160.000.000 đ |
| Switch Layer 2 | [Switch CISCO Catalyst 2960 WS-C2960X-24TS-L](https://www.sieuthivienthong.com/switch-cisco-catalyst-2960-ws-c2960x-24ts-l-12401.html) | 15 | 39.000.000 đ | 24 cổng Ethernet Gigabit 10/100/1000 và 4 cổng uplink 1G SFP. | - Bộ vi xử lý lõi kép với 512MB bộ nhớ DRAM và 128MB bộ nhớ flash.  - Hỗ trợ xếp chồng lên đến 8 switch, cung cấp băng thông ngăn xếp 80G.  - Hỗ trợ nguồn dự phòng bên ngoài (RPS) giúp đảm bảo nguồn điện dự phòng.  - Giải pháp tiết kiệm năng lượng giúp giảm mức tiêu thụ điện.  - Bộ tính năng phần mềm LAN Base Cisco IOS | 585.000.000 đ |
| Switch Layer 3 | [Data Switch Cisco C9200-24P-E](https://www.sieuthivienthong.com/24-port-poe-data-switch-cisco-c9200-24p-e-42295.html) | 4 | 80.000.000 đ | 24 cổng PoE+ (cấp nguồn qua Ethernet) | - Tích hợp phần mềm Network Essentials.  - Thiết bị nổi bật với bộ nguồn và quạt FRU, mô-đun uplink, hỗ trợ cấp nguồn vĩnh viễn qua PoE, và có thời gian trung bình giữa các lần hỏng hóc (MTBF) cao.  - C9200-24P-E được trang bị mạch tích hợp ASAD 2.0 và CPU ARM, chạy trên hệ điều hành Cisco IOS® XE, mang lại khả năng lập trình, bảo mật nâng cao với MACsec, và hỗ trợ băng thông cao hơn so với dòng Catalyst 2960-X. | 320.000.000 đ |
| Acess Point | [Wi-Fi 6 Access Point CISCO CBW150AX-S](https://www.sieuthivienthong.com/150ax-wi-fi-6-access-point-cisco-cbw150ax-s-86206.html) | 6 | 4.000.000 đ | Cổng kết nối LAN GB hỗ trợ PoE | - Hỗ trợ Wi-Fi 6 (802.11ax) với băng tần kép 2.4GHz và 5GHz, cho tốc độ tối đa lên đến 1.488Gb/s.  - Thiết bị trang bị 1GB DRAM, 512MB flash và bộ xử lý quad-core 1GHz. Hỗ trợ bảo mật WPA2/WPA3, 802.1X  - Hỗ trợ tối đa 400 clients kết nối đồng thời. Nó có tính năng MU-MIMO, OFDMA, và BSS coloring, cùng với khả năng hỗ trợ 50 Access Points trong hệ thống | 24.000.000 đ |
| **Tổng cộng** | | | | | **1.089.000.000 đ** | |

### 3.2.2 Các thiết bị dùng trong hệ thống mạng

Router là thiết bị mạng đảm nhiệm vai trò định tuyến dữ liệu giữa các mạng khác nhau, ví dụ như giữa mạng LAN và WAN, hoặc giữa các mạng con trong một mạng nội bộ.

Switch Layer 3 kết hợp chức năng của switch và router, giúp chuyển tiếp dữ liệu giữa các VLAN khác nhau và cung cấp khả năng định tuyến nội bộ trong mạng.

Switch Layer 2 hoạt động trong phạm vi cùng một mạng con (LAN), chịu trách nhiệm chuyển tiếp các gói tin dựa trên địa chỉ MAC của các thiết bị.

Server là thiết bị cung cấp các dịch vụ như lưu trữ, chia sẻ tài nguyên và ứng dụng cho các máy khách trong mạng, có thể là máy chủ web, email, hoặc cơ sở dữ liệu.

Access Point (AP) là thiết bị mạng cho phép kết nối không dây giữa các thiết bị di động và mạng nội bộ, giúp mở rộng phạm vi và khả năng tiếp cận của mạng LAN không dây (Wi-Fi).

## Các dịch vụ cần thuê

Để đảm bảo rằng hệ thống mạng của Công ty Outsource O-UIT hoạt động hiệu quả và đáp ứng được các yêu cầu kinh doanh, công ty cần thuê một số dịch vụ thiết yếu. Các dịch vụ này không chỉ giúp tối ưu hóa hiệu suất mạng mà còn đảm bảo an toàn và bảo mật cho thông tin. Dưới đây là các dịch vụ cụ thể mà công ty cần xem xét:

## Dịch vụ Internet

Công ty cần thuê một dịch vụ Internet với băng thông rộng và tốc độ cao để đảm bảo rằng tất cả các hoạt động trực tuyến diễn ra mượt mà và không bị gián đoạn. Dịch vụ Internet này sẽ phục vụ cho nhiều mục đích khác nhau, bao gồm:

Truy cập thông tin: Nhân viên cần truy cập vào các nguồn tài nguyên trực tuyến, bao gồm các ứng dụng đám mây, hệ thống quản lý dự án và các công cụ giao tiếp.

Giao tiếp nội bộ và ngoại bộ: Việc sử dụng email, video call và các ứng dụng nhắn tin yêu cầu một kết nối Internet ổn định và nhanh chóng.

Chạy các ứng dụng và dịch vụ trực tuyến: Nhiều ứng dụng mà công ty sử dụng có thể yêu cầu kết nối Internet liên tục để hoạt động hiệu quả.

Việc lựa chọn nhà cung cấp dịch vụ Internet cần được thực hiện cẩn thận, với các tiêu chí như tốc độ, độ tin cậy và khả năng hỗ trợ kỹ thuật.

## Dịch vụ VPN

Để bảo vệ thông tin nhạy cảm khi truyền tải giữa trụ sở chính và chi nhánh, công ty cần thiết lập một dịch vụ VPN (Virtual Private Network). Dịch vụ VPN sẽ cung cấp một kết nối an toàn và mã hóa dữ liệu, giúp ngăn chặn các mối đe dọa từ bên ngoài. Lợi ích của dịch vụ VPN bao gồm:

**Bảo mật thông tin**: Dữ liệu được mã hóa khi truyền qua Internet, giúp bảo vệ thông tin quan trọng khỏi các cuộc tấn công và rò rỉ dữ liệu.

**Kết nối an toàn giữa các địa điểm**: VPN cho phép nhân viên làm việc từ xa hoặc kết nối từ chi nhánh đến trụ sở chính một cách an toàn, đảm bảo rằng thông tin luôn được bảo vệ.

**Truy cập vào các tài nguyên nội bộ**: Nhân viên có thể truy cập vào các ứng dụng và tài nguyên nội bộ của công ty từ xa, tạo điều kiện thuận lợi cho việc làm việc linh hoạt.

## Dịch vụ bảo trì và hỗ trợ kỹ thuật

Để đảm bảo rằng hệ thống mạng luôn hoạt động hiệu quả và liên tục, công ty cần thuê dịch vụ bảo trì và hỗ trợ kỹ thuật. Dịch vụ này sẽ bao gồm:

**Bảo trì định kỳ**: Thực hiện các công việc bảo trì định kỳ như cập nhật phần mềm, kiểm tra thiết bị và tối ưu hóa cấu hình để đảm bảo rằng hệ thống luôn hoạt động ở hiệu suất tối ưu.

**Hỗ trợ kỹ thuật**: Cung cấp hỗ trợ kỹ thuật khi có sự cố xảy ra, giúp nhân viên nhanh chóng khắc phục vấn đề và giảm thiểu thời gian chết của hệ thống.

Dịch vụ bảo trì và hỗ trợ kỹ thuật không chỉ giúp duy trì hoạt động của hệ thống mà còn cung cấp sự yên tâm cho công ty rằng mọi vấn đề sẽ được giải quyết một cách nhanh chóng và hiệu quả.

## 3.3 Địa chỉ IP của hệ thống mạng và thiết bị

Đặt địa chỉ IP cho hệ thống mạng và thiết bị

Chi nhánh, có tổng cộng 9 subnet và VLAN:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Địa chỉ mạng | Dãy địa chỉ dùng được | Subnet mask | Địa chỉ broadcast | Ghi chú |
| 90.0.0.0 | 90.0.0.1 – 90.0.0.2 | 255.255.255.252 | 90.0.0.3 | ISP – BR1 (Active) |
| 90.1.1.0 | 90.1.1.1 – 90.1.1.2 | 255.255.255.252 | 90.1.1.3 | ISP – BR2 (Standby) |
| 10.100.200.0 | 10.100.200.1 – 10.100.200.254 | 255.255.255.0 | 10.100.200.255 | ISP – Wifi BR |
| 192.168.1.0 | 192.168.1.1 - 192.168.1.2 | 255.255.255.252 | 192.168.1.3 | BR1 – BR\_SL3(Active) |
| 192.168.1.4 | 192.168.1.5 -192.168.1.6 | 255.255.255.252 | 19.168.1.7 | BR1 – BR\_SL3(Standby) |
| 192.168.1.8 | 192.168.1.9 - 192.168.1.10 | 255.255.255.252 | 192.168.1.11 | BR2 – BR\_SL3(Active) |
| 192.168.1.12 | 192.168.1.13- 192.168.1.14 | 255.255.255.252 | 192.168.1.15 | BR2 – BR\_SL3(Standby) |
| 192.168.10.0 | 192.168.10.1 - 192.168.10.62 | 255.255.255.192 | 192.168.100.63 | VLAN 10 - Developer |
| 192.168.20.0 | 192.168.20.1 - 192.168.20.62 | 255.255.255.192 | 192.168.200.63 | VLAN 20 – Tester |

Trụ sở có tổng cộng 17 subnet và VLAN:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Địa chỉ mạng | Dãy địa chỉ dùng được | Subnet mask | Địa chỉ broadcast | Ghi chú |
| 90.2.2.0 | 90.2.2.1 – 90.2.2.2 | 255.255.255.252 | 90.2.2.3 | ISP-HQ1 |
| 90.3.3.0 | 90.3.3.1 – 90.3.3.2 | 255.255.255.252 | 90.3.3.3 | ISP-HQ2 |
| 10.100.100.0 | 10.100.100.1 – 10.100.100.254 | 255.255.255.0 | 10.100.100.255 | ISP-HQ\_WiFi |
| 192.168.2.0 | 192.168.2.1-  192.168.2.2 | 255.255.255.252 | 192.168.2.3 | HQ1-HQ-SL3(Active) |
| 192.168.2.4 | 192.168.2.5  192.168.2.6 | 255.255.255.252 | 192.168.2.7 | HQ1-HQ-SL3(Stanby) |
| 192.168.2.8 | 192.168.2.9-  192.168.2.10 | 255.255.255.252 | 192.168.2.11 | HQ2 - HQ-SL3(Active) |
| 192.168.2.12 | 192.168.2.13-  192.168.2.14 | 255.255.255.252 | 192.168.2.5 | HQ2 - HQ-SL3(Standby) |
| 192.168.3.0 | 192.168.3.1-  192.168.3.254 | 255.255.255.25 | 192.168.3.255 | HQ1 – HQ-Server |
| 192.168.30.0/26 | 192.168.30.1 - 192.168.30.62 | 255.255.255.192 | 192.168.30.63 | VLAN30 -Developer |
| 192.168.40.0/26 | 192.168.40.1 - 192.168.40.62 | 255.255.255.192 | 192.168.40.63 | VLAN40-Tester |
| 192.168.50.0/26 | 192.168.50.1 - 192.168.50.62 | 255.255.255.192 | 192.168.50.63 | VLAN50-IT Manager |
| 192.168.60.0/26 | 192.168.60.1 - 192.168.60.62 | 255.255.255.192 | 192.168.60.63 | VLAN60-Technical Manager |
| 192.168.70.0/26 | 192.168.70.1 - 192.168.70.62 | 255.255.255.192 | 192.168.70.63 | VLAN70-Project Manager |
| 192.168.80.0/26 | 192.168.80.1 - 192.168.80.62 | 255.255.255.192 | 192.168.80.63 | VLAN80-HR |
| 192.168.90.0/26 | 192.168.90.1 - 192.168.90.62 | 255.255.255.192 | 192.168.90.63 | VLAN90-Business Analyst |
| 192.168.100.0/26 | 192.168.100.1 - 192.168.100.62 | 255.255.255.192 | 192.168.100.63 | VLAN100-CEO |
| 192.168.110.0/26 | 192.168.110.1 - 192.168.110.62 | 255.255.255.192 | 192.168.110.63 | VLAN110-Data Center |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Thiết bị | Interface | Ip address | Subnet mask | Default Gateway |
| ISP | Serial 0/1/0 | 90.1.1.1 | 255.255.255.252 |  |
| Serial 0/1/1 | 90.0.0.1 | 255.255.255.252 |  |
| Serial 0/2/0 | 90.2.2.1 | 255.255.255.252 |  |
| Serial 0/2/1 | 90.3.3.1 | 255.255.255.252 |  |
| GigabitEthernet 0/0/0 | 10.100.100.1 | 255.255.255.0 |  |
| GigabitEthernet 0/0/1 | 10.100.200.1 | 255.255.255.0 |  |
| BR\_Active | Serial 0/1/0 | 90.0.0.2 | 255.255.255.252 | 90.0.0.1 |
| GigabitEthernet 0/0/0 | 192.168.1.1 | 255.255.255.252 |  |
| GigabitEthernet 0/0/1 | 192.168.1.5 | 255.255.255.252 |  |
| Tunnel1 | 172.16.100.1 | 255.255.255.252 |  |
| Tunnel2 | 172.16.101.1 | 255.255.255.252 |  |
| BR\_Standby | Serial 0/1/0 | 90.1.1.2 | 255.255.255.252 | 90.1.1.1 |
| GigabitEthernet 0/0/0 | 192.168.1.13 | 255.255.255.252 |  |
| GigabitEthernet 0/0/1 | 192.168.1.9 | 255.255.255.252 |  |
| Tunnel3 | 172.16.102.1 | 255.255.255.252 |  |
| Tunnel4 | 172.16.103.1 | 255.255.255.252 |  |
| BR-SL3(Active) | GigabitEthernet1/0/1 | 192.168.1.2 | 255.255.255.252 |  |
| GigabitEthernet1/0/2 | 192.168.1.10 | 255.255.255.252 |  |
| VLAN10 | 192.168.10.1 | 255.255.255.192 |  |
| VLAN20 | 192.168.20.1 | 255.255.255.192 |  |
| BR\_SL3(Standby) | GigabitEthernet1/0/1 | 192.168.1.4 | 255.255.255.252 |  |
| GigabitEthernet1/0/2 | 192.168.1.6 | 255.255.255.252 |  |
| VLAN10 | 192.168.10.1 | 255.255.255.192 |  |
| VLAN20 | 192.168.20.1 | 255.255.255.192 |  |
| HQ\_Active | Serial 0/1/0 | 90.2.2.2 | 255.255.255.252 | 90.2.2.1 |
| GigabitEthernet 0/0/0 | 192.168.2.1 | 255.255.255.252 |  |
| GigabitEthernet 0/0/1 | 192.168.2.5 | 255.255.255.252 |  |
| GigabitEthernet 0/0/2 | 192.168.3.1 | 255.255.255.0 |  |
| Tunnel1 | 172.16.100.2 | 255.255.255.252 |  |
| Tunnel3 | 172.16.102.2 | 255.255.255.252 |  |
| HQ\_Standby | Serial 0/1/0 | 90.3.3.2 | 255.255.255.252 | 90.3.3.1 |
| GigabitEthernet 0/0/0 | 192.168.2.13 | 255.255.255.252 |  |
| GigabitEthernet 0/0/1 | 192.168.2.9 | 255.255.255.252 |  |
| GigabitEthernet 0/0/2 | 192.168.3.17 | 255.255.255.248 |  |
| Tunnel2 | 172.16.101.2 | 255.255.255.252 |  |
| Tunnel4 | 172.16.103.2 | 255.255.255.252 |  |
| BR-SL3(Active) | GigabitEthernet0/1 | 192.168.2.2 | 255.255.255.252 |  |
| GigabitEthernet0/2 | 192.168.2.10 | 255.255.255.252 |  |
| VLAN30 | 192.168.30.2 | 255.255.255.192 |  |
| VLAN40 | 192.168.40.2 | 255.255.255.192 |  |
| VLAN50 | 192.168.50.2 | 255.255.255.192 |  |
| VLAN60 | 192.168.60.2 | 255.255.255.192 |  |
| VLAN70 | 192.168.70.2 | 255.255.255.192 |  |
| VLAN80 | 192.168.80.2 | 255.255.255.192 |  |
| VLAN90 | 192.168.90.2 | 255.255.255.192 |  |
| VLAN100 | 192.168.100.2 | 255.255.255.192 |  |
| VLAN110 | 192.168.110.2 | 255.255.255.192 |  |
| BR-SL3(Standby) | GigabitEthernet0/1 | 192.168.2.6 | 255.255.255.252 |  |
| GigabitEthernet0/2 | 192.168.2.14 | 255.255.255.252 |  |
| VLAN30 | 192.168.30.3 | 255.255.255.192 |  |
| VLAN40 | 192.168.40.3 | 255.255.255.192 |  |
| VLAN50 | 192.168.50.3 | 255.255.255.192 |  |
| VLAN60 | 192.168.60.3 | 255.255.255.192 |  |
| VLAN70 | 192.168.70.3 | 255.255.255.192 |  |
| VLAN80 | 192.168.80.3 | 255.255.255.192 |  |
| VLAN90 | 192.168.90.3 | 255.255.255.192 |  |
| VLAN100 | 192.168.100.3 | 255.255.255.192 |  |
| VLAN110 | 192.168.110.3 | 255.255.255.192 |  |
| BR Wifi | LAN | 10.100.200.2 | 255.255.255.0 | 10.100.200.1 |
| Wifi Tang1 | LAN | 10.100.100.5 | 255.255.255.0 | 10.100.100.1 |
| Wifi Tang2 | LAN | 10.100.100.2 | 255.255.255.0 | 10.100.100.1 |
| Wifi Tang3 | LAN | 10.100.100.3 | 255.255.255.0 | 10.100.100.1 |
| Wifi Tang4 | LAN | 10.100.100.4 | 255.255.255.0 | 10.100.100.1 |
| Wifi Tang5 | LAN | 10.100.100.6 | 255.255.255.0 | 10.100.100.1 |
| BR-Dev1 | FastEthernet 0 | DHCP |  | 192.168.10.63 |
| BR-Dev2 | FastEthernet 0 | DHCP |  | 192.168.10.63 |
| BR-Tester1 | FastEthernet 0 | DHCP |  | 192.168.20.63 |
| BR-Tester2 | FastEthernet0 | DHCP |  | 192.168.20.63 |
| BR-Laptop | Wireless 0 | DHCP |  | 172.16.0.1 |
| BR-PC | FastEthernet 0 | DHCP |  | 172.16.0.1 |
| PC-Dev | FastEthernet 0 | DHCP |  | 192.168.30.1 |
| PC-Tester | FastEthernet 0 | DHCP |  | 192.168.40.1 |
| Lap-IT-manger | FastEthernet 0 | DHCP |  | 192.168.50.1 |
| Lap-Tech-manager | FastEthernet 0 | DHCP |  | 192.168.60.1 |
| Lap-Project-manager | FastEthernet 0 | DHCP |  | 192.168.70.1 |
| Lap-HR | FastEthernet 0 | DHCP |  | 192.168.80.1 |
| Lap-BA | FastEthernet 0 | DHCP |  | 192.168.90.1 |
| Lap-CEO | FastEthernet 0 | DHCP |  | 192.168.100.1 |
| Datacenter | FastEthernet 0 | DHCP |  | 192.168.110.1 |

Bảng VPN Tunnel:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Địa chỉ mạng | Dãy địa chỉ dùng được | Địa chỉ broadcast | Tổng số host dùng được | Subnet mask | Ghi chú |
| 172.16.100.0 | 172.16.100.1 - 172.16.100.2 | 172.16.100.3 | 2 | 255.255.255.252 | BR1– HQ1 |
| 172.16.101.0 | 172.16.101.1 - 172.16.101.2 | 172.16.101.3 | 2 | 255.255.255.252 | BR1 – HQ2 |
| 172.16.102.0 | 172.16.102.1 - 172.16.102.2 | 172.16.102.3 | 2 | 255.255.255.252 | BR2 – HQ1 |
| 172.16.103.0 | 172.16.103.1 –  172.16.103.2 | 172.16.103.3 | 2 | 255.255.255.252 | BR2 – HQ2 |

Bảng HSRP:

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | Ip address | Subnet mask |
| VL10 | Virtual | 192.168.10.63 | 255.255.255.192 |
| VL20 | Virtual | 192.168.20.63 | 255.255.255.192 |
| VL30 | Virtual | 192.168.30.1 | 255.255.255.192 |
| VL40 | Virtual | 192.168.40.1 | 255.255.255.192 |
| VL50 | Virtual | 192.168.50.1 | 255.255.255.192 |
| VL60 | Virtual | 192.168.60.1 | 255.255.255.192 |
| VL70 | Virtual | 192.168.70.1 | 255.255.255.192 |
| VL80 | Virtual | 192.168.80.1 | 255.255.255.192 |
| VL90 | Virtual | 192.168.90.1 | 255.255.255.192 |
| VL100 | Virtual | 192.168.100.1 | 255.255.255.192 |
| VL110 | Virtual | 192.168.110.1 | 255.255.255.192 |

# Các dịch vụ cung cấp và chi phí hoạt động

## Các dịch vụ cung cấp

### Cấu hình HSRP cho SWLayer 3

Mô tả: HSRP (Hot Standby Router Protocol) đã được thiết lập thành công tại hai chi nhánh, với một router hoạt động ở chế độ "Active" và router còn lại ở chế độ "Standby". Khi router chính gặp sự cố, router dự phòng sẽ tự động đảm nhận vai trò của nó.

Lợi ích:

* Tính sẵn sàng cao: Giúp duy trì kết nối liên tục cho người dùng, giảm thiểu thời gian ngừng hoạt động.
* Quản lý đơn giản: Người dùng chỉ cần biết địa chỉ IP ảo của HSRP, không cần nhớ địa chỉ IP của từng router.
* Tăng cường bảo mật: Kiểm soát lưu lượng và giảm nguy cơ tấn công từ chối dịch vụ (DoS).

### Thiết lập VPN Tunnel

Mô tả: VPN tunnel đã được cấu hình bằng GRE (Generic Routing Encapsulation) để tạo kết nối giữa các chi nhánh và trụ sở chính, cho phép truyền dữ liệu giữa các mạng với giao thức đóng gói linh hoạt. GRE có thể kết hợp với giao thức mã hóa như IPsec để đảm bảo tính bảo mật và an toàn thông tin.

Lợi ích:

* **Kết nối linh hoạt**: Hỗ trợ nhiều giao thức truyền tải, cho phép các mạng sử dụng các hệ thống khác nhau kết nối dễ dàng.
* **Giảm chi phí**: Cung cấp giải pháp kết nối hiệu quả qua Internet mà không cần đầu tư nhiều vào hạ tầng riêng.

### Phân chia VLAN

Mô tả: Các VLAN (Virtual Local Area Network) đã được thiết lập cho từng phòng ban, cho phép tách biệt lưu lượng mạng theo chức năng và nhu cầu sử dụng. Mỗi VLAN được cấu hình với các chính sách bảo mật riêng biệt, đảm bảo rằng thông tin nhạy cảm không bị truy cập bởi các phòng ban không liên quan.

Lợi ích:

* Tăng cường bảo mật: Giảm thiểu nguy cơ rò rỉ thông tin giữa các phòng ban, giúp bảo vệ dữ liệu nhạy cảm.
* Quản lý lưu lượng hiệu quả: Giúp tối ưu hóa băng thông và giảm tắc nghẽn mạng bằng cách phân chia lưu lượng theo từng nhóm người dùng.
* Dễ dàng mở rộng: Khi có nhu cầu mở rộng, việc thêm VLAN mới sẽ dễ dàng hơn mà không làm ảnh hưởng đến cấu trúc mạng hiện tại.

### Cấu hình Wireless Router

Mô tả: Wireless router đã được triển khai tại các khu vực làm việc chung và phòng họp, cung cấp kết nối không dây cho nhân viên.

Lợi ích:

* Tiện lợi cho người dùng: Nhân viên có thể kết nối với mạng một cách dễ dàng và linh hoạt, tăng cường năng suất làm việc.
* Khả năng mở rộng: Dễ dàng mở rộng mạng không dây khi cần thiết, đáp ứng nhu cầu sử dụng ngày càng tăng.

### Cấu hình DHCP

Mô Tả: Cấu hình DHCP (Dynamic Host Configuration Protocol) cho phép tự động cấp phát địa chỉ IP và thông tin mạng cho các thiết bị trong mạng. Điều này giúp giảm thiểu công sức quản lý địa chỉ IP thủ công và đảm bảo không có xung đột địa chỉ.

Lợi ích:

* Tiết kiệm thời gian: Giảm thiểu thời gian cấu hình địa chỉ IP cho từng thiết bị.
* Giảm xung đột địa chỉ IP: Tự động cấp phát địa chỉ IP duy nhất cho mỗi thiết bị.
* Dễ dàng quản lý: Cung cấp giao diện quản lý trung tâm cho việc theo dõi và điều chỉnh cấu hình.

### Cấu hình OSPF

Mô Tả: OSPF (Open Shortest Path First) đã được cấu hình để quản lý định tuyến giữa các router trong mạng, giúp tối ưu hóa đường đi của dữ liệu. OSPF sử dụng thuật toán Dijkstra để tìm đường đi ngắn nhất và tự động cập nhật thông tin định tuyến khi có sự thay đổi trong mạng.

Lợi ích:

* Hiệu quả và nhanh chóng: OSPF cung cấp khả năng định tuyến nhanh và chính xác hơn, phù hợp với các mạng lớn và phức tạp.
* Tối ưu hóa lưu lượng mạng: Giảm độ trễ và tăng hiệu suất tổng thể bằng cách định tuyến dữ liệu qua các đường đi tối ưu.
* Khả năng mở rộng tốt: Phù hợp với mạng có quy mô từ trung bình đến lớn.
* Tự động cập nhật: Các router tự động trao đổi và cập nhật thông tin định tuyến mà không cần quản lý thủ công.

### Xây dựng hệ thống mạng đầy đủ

Mô Tả: Xây dựng một hệ thống mạng đầy đủ tối ưu bằng cách sử dụng các thiết bị cùng hang, tích hợp tất cả các thành phần mạng, bao gồm router, switchlayer3, sw , wireless router và server, đảm bảo chúng hoạt động cùng nhau một cách hiệu quả.

Lợi ích: Tất cả thiết bị hoạt động hài hòa, giảm thiểu xung đột và tối ưu hóa hiệu suất.

### Cấu hình NAT để ra Internet

Mô tả: Network Address Translation (NAT) đã được cấu hình giữa core router và isp, thực hiện chuyển đổi giữa địa chỉ IP nội bộ trong công ty và địa chỉ mạng công cộng.

Lợi ích :

* Bảo mật: Giấu địa chỉ IP nội bộ, ngăn chặn truy cập từ bên ngoài.
* Tiết kiệm IP: Cho phép nhiều thiết bị sử dụng chung một địa chỉ IP công cộng.
* Quản lý dễ dàng: Giảm thiểu yêu cầu thay đổi cấu trúc mạng khi kết nối Internet.
* Mở rộng linh hoạt: Dễ dàng mở rộng mạng mà không cần thêm địa chỉ IP công cộng.
* Tăng hiệu quả: Giúp tối ưu hóa việc sử dụng các địa chỉ IP công cộng.

### Cấu hình ACL

Mô tả: ACL đã được cấu hình đã được cấu hình và áp dụng trên các interface vlan, mục đích là chỉ cho phép trao đổi nội bộ giữa các phòng ban với nhau, ngoài ra dev bên chi nhánh có thể giao tiếp tới dev bên trụ sở, tester bên chi nhánh cũng có thể giao tiếp với tester bên trụ sở. Tất cả developer và tester được truy cập đến hệ thông cloud và datacenter.

Lợi ích :

* Bảo mật: Hạn chế lưu lượng không cần thiết hạn chế truy cập trái phép.
* Hiệu quả mạng: Giảm thiểu xung đột lưu lượng không liên quan, tối ưu hóa tài nguyên mạng.
* Bảo vệ tài nguyên: Giới hạn quyền truy cập đến cloud và datacenter, chỉ cho phép các đối tượng đã xác định truy cập.

# Thiếu sót trong hệ thống:

* **Giám sát và quản lý mạng**

Hiện tại, hệ thống đang thiếu công cụ giám sát hiệu suất mạng, vì vậy cần triển khai một hệ thống giám sát tự động toàn diện để phát hiện kịp thời các sự cố, tối ưu hóa hoạt động mạng và đảm bảo hiệu suất liên tục cho người dùng.

* **Bảo mật cho VPN**

Hệ thống chưa được cấu hình mã hóa mạnh mẽ cho VPN, điều này làm tăng nguy cơ rò rỉ thông tin nhạy cảm, do đó cần thiết lập các giao thức bảo mật như IPSec hoặc SSL để bảo vệ dữ liệu khi truyền qua Internet và đảm bảo an toàn cho các kết nối từ xa.

* **Đường mạng internet nội bộ**

Thiếu kết nối internet nội bộ cho từng phòng ban thuộc các tầng nhà, theo như kế hoạch đường internet sẽ phát ra các kết nối thuộc các VLAN của các phòng ban, thiết bị kết nối tới internet nội bộ của phòng ban có thể giao tiếp với các thiết bị khác cùng phòng ban.

Trong bài làm đã thiết kế hệ thống AP phát ra mạng nhưng không thể phát ra đúng theo mong đợi.

## Chi phí cho toàn hệ thống

### 4.2.1 Chi phí cho thiết bị

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Loại thiết bị | Mẫu sản phẩm | Số lượng thiết bị | Đơn giá, ước tính | Thành tiền |
| Router | [Router Integrated ISR 4331 Cisco ISR4331/K9](https://www.sieuthivienthong.com/router-integrated-isr-4331-cisco-isr4331k9-31359.html) | 4 | 40.000.000 đ | 160.000.000 đ |
|  |
|  |
| Switch Layer 2 | [Switch CISCO Catalyst 2960 WS-C2960X-24TS-L](https://www.sieuthivienthong.com/switch-cisco-catalyst-2960-ws-c2960x-24ts-l-12401.html) | 15 | 39.000.000 đ | 585.000.000 đ |  |
|  |
|  |
|  |
|  |
|  |
| Switch Layer 3 | [Data Switch Cisco C9200-24P-E](https://www.sieuthivienthong.com/24-port-poe-data-switch-cisco-c9200-24p-e-42295.html) | 4 | 80.000.000 đ | 320.000.000 đ |  |
|  |
|  |
| Acess Point | [Wi-Fi 6 Access Point CISCO CBW150AX-S](https://www.sieuthivienthong.com/150ax-wi-fi-6-access-point-cisco-cbw150ax-s-86206.html) | 6 | 4.000.000 đ | 24.000.000 đ |  |
|  |
|  |
| Tổng cộng | | | | 1.089.000.000 đ |  |

### 4.2.2 Chi phí cho dịch vụ:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| STT | Dịch vụ | Đơn giá | Số lượng | Băng thông trong nước/ quốc tế | Thành tiền |
| 1 | [Gói cước F300 PLUS](https://internetviettel.vn/goi-cuoc-f300-plus-internet-viettel.html) | 9.900.000 đ /tháng | 1 | 600Mbps /  30Mbps | 6.600.000 đ/tháng |
| 2 | [Gói cước VIP200 Internet Viettel cho khách](https://internetviettel.vn/goi-cuoc-f90-plus-internet-viettel.html) | 800.000 đ/tháng | 2 | 200Mbps/  5Mbps | 1.600.000 đ/tháng |
| 3 | [Microsoft Azure Virtual Machines: Standard F4s\_v2](https://cloudprice.net/vm/Standard_F4s_v2) | 2.500.000 đ/tháng | 1 | -- | 3.000.000 đ/tháng |
| **Thành tiền** | | | | | 11.200.000 đ/tháng |

# Kết luận

Báo cáo đồ án này đã trình bày một cách chi tiết về quy trình thiết kế, cài đặt và triển khai hệ thống mạng cho tổ chức. Qua từng giai đoạn, từ khảo sát hiện trạng đến thực hiện và đánh giá. Kết quả đã xây dựng hệ thống ổn định đạt được các mục tiêu đề ra ban đầu.

Hệ thống mạng đã được thiết kế và triển khai thành công, đáp ứng gần như đầy đủ các yêu cầu của công ty Outsource O-UIT. Tuy nhiên, để nâng cao hiệu suất và bảo mật, cần triển khai thêm công cụ giám sát mạng và cải thiện bảo mật VPN. Hệ thống này đã tạo nền tảng vững chắc cho sự phát triển trong tương lai.

# Các nguồn tài liệu tham khảo

[1] CNTT SHOP, “Hướng dẫn cấu hình GRE VPN Tunnel over IPSEC Trên Router Cisco,” *YouTube*, Jan. 13, 2022. https://www.youtube.com/watch?v=qW0B5ueOPGw (accessed Dec. 01, 2024).

[2] Gurutech Networking Training, “CCNA DAY 49: Configure HSRP with Multiple VLANs | HSRP with Inter-VLAN Routing Configuration,” *YouTube*, Jun. 21, 2023. https://www.youtube.com/watch?v=9-JY\_On0-vY (accessed Jun. 02, 2024).

[3] Có chắc yêu là đây, “Tự thực hành Wireless miễn phí với Cisco Packet Tracer,” *Quantrimang.com*, Dec. 09, 2011. https://quantrimang.com/cong-nghe/tu-thuc-hanh-wireless-mien-phi-84141

[4] “Configuring a LAN with DHCP and VLANs  [Support],” *Cisco*. <https://www.cisco.com/en/US/docs/routers/access/800/850/software/configuration/guide/dhcpvlan.htm>

[5] cnttshop, “Lê Văn Tuấn,” *Cnttshop.vn*, 2023. https://cnttshop.vn/blogs/cisco/huong-dan-cau-hinh-access-list-tren-cisco-voi-lab-cu-the (accessed Dec. 10, 2024).

‌

‌