

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM  
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG  
KHOA CÔNG NGHỆ THÔNG TIN



NGUYỄN VĂN KHÁNH ÂN - 51900475

**THIẾT KẾ, XÂY DỰNG HỆ  
THỐNG MẠNG NỘI BỘ CHO  
CÔNG TY CỔ PHẦN VIỄN  
THÔNG ACT**

**DỰ ÁN CÔNG NGHỆ THÔNG TIN 1**

**MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG  
DỮ LIỆU**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2024**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM  
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG  
KHOA CÔNG NGHỆ THÔNG TIN



NGUYỄN VĂN KHÁNH ÂN - 51900475

**THIẾT KẾ, XÂY DỰNG HỆ THỐNG  
MẠNG NỘI BỘ CHO CÔNG TY CỔ  
PHẦN VIỄN THÔNG ACT**

**DỰ ÁN CÔNG NGHỆ THÔNG TIN 1**

**MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG DỮ  
LIỆU**

Người hướng dẫn  
**ThS. Dương Hữu Phúc**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2024**

## LỜI CẢM ƠN

Sau khi đã hoàn thành bài báo cáo này, em muốn gửi những lời cảm ơn chân thành đến các thầy, cô trong khoa công nghệ thông tin trường đại học Tôn Đức Thắng đã tạo điều kiện cho em được đi thực tập tại công ty để em có thể áp dụng những kiến thức đã học vào thực tế. Ngoài ra, em xin gửi lời cảm ơn đến anh Trần Khắc Hưng và các anh chị trong phòng có định băng rộng đã giúp đỡ em trong suốt quá trình thực tập tại công ty. Và đặc biệt, em muốn gửi lời cảm ơn sâu sắc nhất đến thầy Dương Hữu Phúc, người đã hỗ trợ và hướng dẫn cho em rất nhiều trong suốt quá trình thực tập này và anh Trần Khắc Hưng, người đã không ngại thời gian mà hướng dẫn cho em rất tận tình, đưa ra những nhận xét, góp ý để cho đài tài được hoàn thiện hơn và là người đã chỉ cho em rất nhiều các kiến thức bổ ích và thực tiễn về ngành mạng máy tính và truyền thông để em có thêm được góc nhìn rộng hơn về ngành này, qua đó, phát hiện được những điểm còn thiếu ở bản thân cần phải khắc phục để giúp ích trên con đường nghề nghiệp của mình sau này. Vì bản thân còn thiếu kinh nghiệm nên đài tài không thể tránh khỏi những sai sót, nên em rất mong sẽ nhận được những ý kiến đóng góp quý báu từ quý thầy cô. Em xin chân thành cảm ơn mọi người

TP. Hồ Chí Minh, ngày ... tháng ... năm 20..

Tác giả

(Ký tên và ghi rõ họ tên)

Nguyễn Văn Khánh Ân

## CÔNG TRÌNH ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi và được sự hướng dẫn khoa học của ThS. Dương Hữu Phúc. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong Dự án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung Dự án của mình.** Trường Đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

TP. Hồ Chí Minh, ngày ... tháng ... năm 20..

Tác giả

(Ký tên và ghi rõ họ tên)

# THIẾT KẾ, XÂY DỰNG HỆ THỐNG MẠNG NỘI BỘ CHO CÔNG TY CỔ PHẦN VIỄN THÔNG ACT

## TÓM TẮT

Đề tài xây dựng hệ thống mạng nội bộ cho công ty cổ phần viễn thông ACT gồm: 3 khu vực văn phòng, phòng máy NOC và khu vực máy chủ (ZONE-SERVER) và đề tài này sẽ được thực hiện trên môi trường giả lập mạng ảo EVE-NG (Emulated Virtual Environment – Next Generation). Em sẽ xây dựng mô hình hệ thống mạng nội bộ cho công ty trên môi trường mạng ảo EVE-NG, cấu hình các thiết bị mạng ảo và các dịch vụ mạng để cho các thiết bị trong công ty có thể ra được bên ngoài mạng thật internet. Hệ thống mạng sẽ được cấu hình các công nghệ như VLAN, VTP, định tuyến động OSPF, cấu hình các thiết bị Wifi để tạo các vùng kết nối mạng không dây và cấu hình NAT để hệ thống mạng có thể kết nối ra ngoài mạng internet một cách an toàn. Về vấn đề bảo mật em sẽ sử dụng thiết bị tường lửa ASA, cấu hình các tập luật (Rules) để cho phép các lưu lượng mạng hợp pháp ngăn chặn các truy cập trái phép cố gắng xâm nhập vào hệ thống mạng để đánh cắp các thông tin, dữ liệu nội bộ của công ty

# **DESIGNING AND BUILDING AN INTERNAL NETWORK SYSTEM FOR ACT TELECOMMUNICATIONS JOINT STOCK COMPANY**

## **ABSTRACT**

The project of building an internal network system for ACT telecommunication joint stock company includes: 3 office areas, NOC (Network Operation Center) room and the server area (ZONE-SERVER). This project will be carried out in the EVE-NG (Emulated Virtual Environment – Next Generation) virtual network environment. I will construct the internal network system model for the company in the EVE-NG virtual network environment, configure the virtual network device and network services so that the devices within the company can connect to the real external internet. The network system will be configured with technologies such as VLAN, VTP, dynamic routing OSPF, configuring Wifi modems to create wireless network connection areas and configuring NAT (Network Address Translation) to allow the network system to connect to the internet safely. For the security problems, I will use ASA firewall and configure rule to allow legitimate network traffic and prevent unauthorized access attempts to infiltrate the network system to steal the company's internal information and data

## MỤC LỤC

<b>DANH MỤC HÌNH VẼ.....</b>	<b>viii</b>
<b>DANH MỤC BẢNG BIỂU.....</b>	<b>x</b>
<b>DANH MỤC CÁC CHỮ VIẾT TẮT.....</b>	<b>xi</b>
<b>CHƯƠNG 1. MỞ ĐẦU VÀ TỔNG QUAN ĐỀ TÀI.....</b>	<b>1</b>
1.1 Lý do chọn đề tài .....	1
1.2 Mục tiêu thực hiện đề tài .....	1
1.3 Đối tượng nghiên cứu:.....	2
<b>CHƯƠNG 2. CƠ SỞ LÝ THUYẾT.....</b>	<b>3</b>
2.1 Mạng nội bộ là gì:.....	3
2.2 Mạng diện rộng là gì:.....	4
2.3 Mô hình OSI và mô hình TCP/IP:.....	5
2.3.1 <i>Mô hình OSI (Open System Interconnection):.....</i>	5
2.3.2 <i>Mô hình TCP/IP: .....</i>	8
2.3.3 <i>So sánh giữa mô hình OSI và mô hình TCP/IP: .....</i>	12
2.4 Các thành phần trong mạng nội bộ:.....	13
2.4.1 <i>Router: .....</i>	13
2.4.2 <i>Switch Layer 3:.....</i>	16
2.4.3 <i>Switch layer 2: .....</i>	18
2.4.4 <i>Access point: .....</i>	21
2.4.5 <i>Tường lửa (Firewall):.....</i>	24
2.4.6 <i>Server: .....</i>	26
2.4.7 <i>Các thiết bị đầu cuối: .....</i>	27

2.4.8 Cáp mạng (Network cables): .....	28
2.4.9 Tủ Rack: .....	29
2.4.10 Nguồn điện dự phòng: .....	30
2.5 Các công nghệ cấu hình trong hệ thống mạng nội bộ: .....	31
2.5.1 Tổng quan về EVE-NG: .....	31
2.5.2 Tổng quan về VLAN: .....	31
2.5.3 Tổng quan về VTP: .....	34
2.5.4 OSPF (Open Shortest Path First): .....	36
<b>CHƯƠNG 3. THIẾT KẾ, CẤU HÌNH HỆ THỐNG .....</b>	<b>39</b>
3.1 Mô tả hệ thống:.....	39
3.2 Mô hình hệ thống: .....	40
3.3 Thông tin cài đặt cấu hình hệ thống: .....	40
3.3.1 Thông tin VLAN và inter-vlan trong hệ thống: .....	40
3.3.2 Thông tin về địa chỉ IP: .....	41
3.3.3 Thông tin ip trên các thiết bị:.....	41
3.3.4 Thông tin ip trên Server:.....	42
3.4 Cấu hình hệ thống:.....	42
3.4.1 Cấu hình VLAN: .....	42
3.4.2 Cấu hình VTP (Virtual Trunking Protocol):.....	43
3.4.3 Cấu hình định tuyến động OSPF: .....	47
3.4.4 Cấu hình bảo mật trên thiết bị tường lửa ASA: .....	54
3.4.5 Cấu hình DHCP Server: .....	58
3.4.6 Cấu hình Access-list: .....	60

3.4.7 Cấu hình NAT ra internet: .....	61
3.4.8 Cấu hình WiFi: .....	63
3.4.9 Kiểm thử hệ thống: .....	69
<b>CHƯƠNG 4. KẾT LUẬN .....</b>	<b>74</b>
4.1 Kết luận .....	74
4.2 Hướng phát triển.....	75
<b>TÀI LIỆU THAM KHẢO.....</b>	<b>76</b>

## **DANH MỤC HÌNH VẼ**

Hình 2.1 Mô hình mạng nội bộ .....	3
Hình 2.2 Mô hình mạng diện rộng (WAN) .....	5
Hình 2.3 Mô hình OSI .....	8
Hình 2.4 Thông tin gói tin trong giao thức TCP và UDP .....	11
Hình 2.5 Mô hình TCP/IP .....	12
Hình 2.6 So sánh giữa mô hình OSI và TCP/IP .....	13
Hình 2.7 Thiết bị router DrayTek .....	15
Hình 2.8 Thiết bị switch layer 3 .....	18
Hình 2.9 Thiết bị Switch layer 2 .....	20
Hình 2.10 Access point công nghệ Wifi 6 của Huawei .....	23
Hình 2.11 Tường lửa ASA 5506-x của cisco .....	25
Hình 2.12 Hệ thống máy chủ .....	27
Hình 2.13 Tủ rack mạng .....	30
Hình 2.14 Các Vlan trong hệ thống mạng nội bộ .....	33
Hình 2.15 Nguyên lý hoạt động của VTP .....	36
Hình 2.16 Mô hình hệ thống mạng sử dụng OSPF .....	38
Hình 3.1 Mô hình hệ thống mạng nội bộ công ty ACT .....	40
Hình 3.2 Đường định tuyến trên SWL3_2 .....	49
Hình 3.3 Các đường định tuyến trên SWL3_1 .....	50
Hình 3.4 Các đường định tuyến học được của SW_1LVH .....	51
Hình 3.5 Các đường định tuyến trên DrayTek 3220 .....	52
Hình 3.6 Các đường định tuyến trên router 7206XR2 .....	53

Hình 3.7 Máy tính từ các phòng ban của mạng nội bộ có thể ping thông đến văn phòng các trung tâm khu vực.....	69
Hình 3.8 Máy tính từ các phòng ban của mạng nội bộ có thể ping thông đến văn phòng chi nhánh số 1 Lê Văn Huân .....	70
Hình 3.9 Máy tính từ các phòng ban có thể ping thông đến các server của công ty để sử dụng các dịch vụ mạng.....	71
Hình 3.10 Các máy tính trong hệ thống mạng nội bộ đã có thể ra được mạng thật internet .....	72
Hình 3.11 Các máy kết nối với thiết bị không dây ACT_Guest dành cho khách không thể kết nối và giao tiếp với các máy trong hệ thống mạng nội bộ .....	73
Hình 3.12 Các máy kết nối với thiết bị không dây ACT_Guest dành cho khách chỉ có thể kết nối ra ngoài mạng internet .....	73

## DANH MỤC BẢNG BIỂU

Bảng 4.1: Thông kê kiểu thực thể trong tập VLSP 2016 .....Error! Bookmark not defined.

## DANH MỤC CÁC CHỮ VIẾT TẮT

BERT	Bidirectional Encoder Representations from Transformers
GEC	Grammatical Error Correction
MLM	Masked Language Model
NLP	Natural Language Processing
NSP	Next Sentence Prediction

## **CHƯƠNG 1. MỞ ĐẦU VÀ TỔNG QUAN ĐỀ TÀI**

### **1.1 Lý do chọn đề tài**

Trong thời đại 4.0 ngày nay, với sự phát triển vượt bậc của công nghệ chúng ta có thể truyền gửi những tài liệu, thư từ quan trọng chỉ bằng những cái click chuột mà không phải thông qua những phương pháp gửi thư truyền thống và rườm rà, nhờ vào sự phát triển của mạng internet mà chúng ta có thể gửi những dữ liệu từ máy tính dưới dạng số hóa thông qua môi trường mạng mà có thể đến với điểm đến với tốc độ cực kỳ nhanh mà không cần tốn nhiều chi phí và thời gian. Chính vì sự tiện lợi của internet mà ngày nay, các doanh nghiệp đang ra sức đầu tư để xây dựng và phát triển các hệ thống mạng nội bộ máy tính cho công ty để đảm bảo tốc độ truyền và nhận dữ liệu nhanh chóng và đảm bảo cho việc truy cập vào mạng internet một cách an toàn.

Hệ thống mạng máy tính là sự kết hợp các máy tính lại với nhau thông qua các thiết bị mạng như switch và router và các dây cáp mạng tạo thành một hệ thống mạng trao đổi thông tin qua lại với nhau bên cạnh việc truyền dữ liệu trong nội bộ mạng mà chúng còn có thể truy cập vào internet để có thể tương tác và kết nối với các vùng mạng khác ngoài vùng mạng nội bộ. Bên cạnh đó, để một hệ thống mạng nội bộ có thể hoạt động trơn tru và an toàn thì ta phải tiến hành bảo mật cho hệ thống mạng nội bộ ấy để ngăn chặn các xâm nhập mạng trái phép tấn công vào hệ thống mạng.

Chính vì vậy, để có thể tiếp cận được các hệ thống mạng nội bộ của các doanh nghiệp cũng như có thêm kiến thức và hiểu biết cách hoạt động của các thiết bị có trong hệ thống mạng ngoài thực tế, em sẽ thực hiện đề tài: “Xây dựng, thiết kế hệ thống mạng nội bộ cho công ty cổ phần viễn thông ACT” qua đó, có thể hiểu được cách các luồng dữ liệu trong hệ thống chạy như thế nào và các thiết bị khi cấu hình ngoài thực tế có các dịch vụ gì để từ đó có thêm kiến thức phục vụ cho công việc quản trị hệ thống mạng của bản thân.

### **1.2 Mục tiêu thực hiện đề tài**

Đề tài “Thiết kế và xây dựng hệ thống mạng nội bộ” được thực hiện với mục tiêu có thể tiếp xúc với mô hình hệ thống mạng của doanh nghiệp ngoài thực tế, hiểu

được các kiến thức tổng quan về mạng dành cho doanh nghiệp, nắm được các luồng dữ liệu trong hệ thống mạng nội bộ, cách ước lượng và phân chia ip hợp lý và cách bảo mật hệ thống mạng nội bộ một cách an toàn. Bên cạnh đó, hệ thống mạng này cần phải được thiết kế để có thể mở rộng mạng trong tương lai tùy theo nhu cầu của công ty và doanh nghiệp.

### **1.3 Đối tượng nghiên cứu:**

Đề tài nghiên cứu mô hình hệ thống mạng nội bộ của công ty cổ phần viễn thông ACT từ đó tiến hành mô phỏng lại hệ thống mạng đó lên phần mềm giả lập mạng qua đó hiểu được các loại công nghệ mạng mà doanh nghiệp cấu hình cho các thiết bị.

Đề tài sẽ được thực hiện trên phần mềm giả lập mạng EVE-NG, bằng cách xây dựng lại hệ thống mạng nội bộ của công ty ACT trên môi trường mạng ảo EVE-NG, ta có thể cấu hình cho hệ thống mạng chạy được những dịch vụ mà các phần mềm giả lập khác không thể chạy được nhờ vào tính năng NAT ra mạng của EVE-NG mà sau khi ta cấu hình và thiết kế hệ thống mạng ta có thể cho hệ thống mạng nội bộ này kết nối ra ngoài internet và cho chạy các dịch vụ mạng nhờ vậy ta sẽ có thể kiểm tra được hệ thống mạng hoạt động như thế nào, có tron tru hay không và các cấu hình bảo mật có hoạt động hay không.

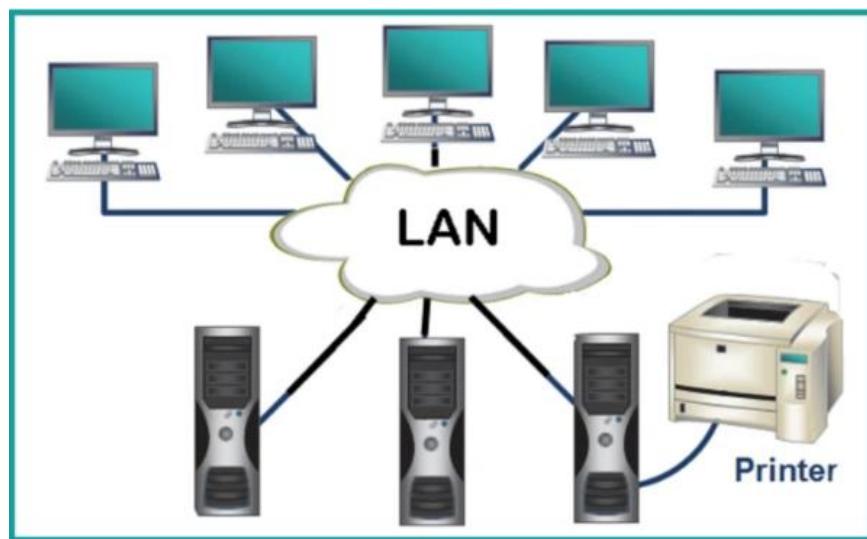
## CHƯƠNG 2. CƠ SỞ LÝ THUYẾT

### 2.1 Mạng nội bộ là gì:

Mạng nội bộ (mạng LAN) là hệ thống mạng dùng để kết nối các máy tính trong một phạm vi nội bộ như công ty, tòa nhà, trường học. Từ đó, các máy tính trong mạng LAN nội bộ có thể tương tác được với nhau và chia sẻ thông tin với nhau. Ngày nay, mạng nội bộ (Local Area Network) đang ngày càng trở nên thông dụng và phổ biến vì nó cho phép nhiều các thiết bị mạng có thể sử dụng chung các tài nguyên như máy in, ổ đĩa, server truyền tập tin và các dữ liệu dùng chung khác.

Các thiết bị như máy in khi được kết nối vào cùng một mạng LAN sẽ làm cho không chỉ các thao tác trở nên dễ dàng hơn mà còn giúp giảm chi phí phát sinh cho doanh nghiệp. Ví dụ khi một doanh nghiệp thay vì mua cho mỗi nhân viên một máy in thì khi kết nối máy in đó vào mạng LAN và chia sẻ máy in đó vào toàn bộ mạng thì cả toàn bộ nhân viên đã có thể sử dụng chung một máy in duy nhất.

Mạng nội bộ là một bộ phận của mạng diện rộng, thông qua việc cung cấp cho mạng nội bộ một đường dây (có thể là cáp quang hoặc cáp đồng trục) mà mạng nội bộ có thể kết nối internet và qua đó có thể tương tác với các máy chủ thuộc mạng nội bộ khác.



Hình 2.1 Mô hình mạng nội bộ

## 2.2 Mạng diện rộng là gì:

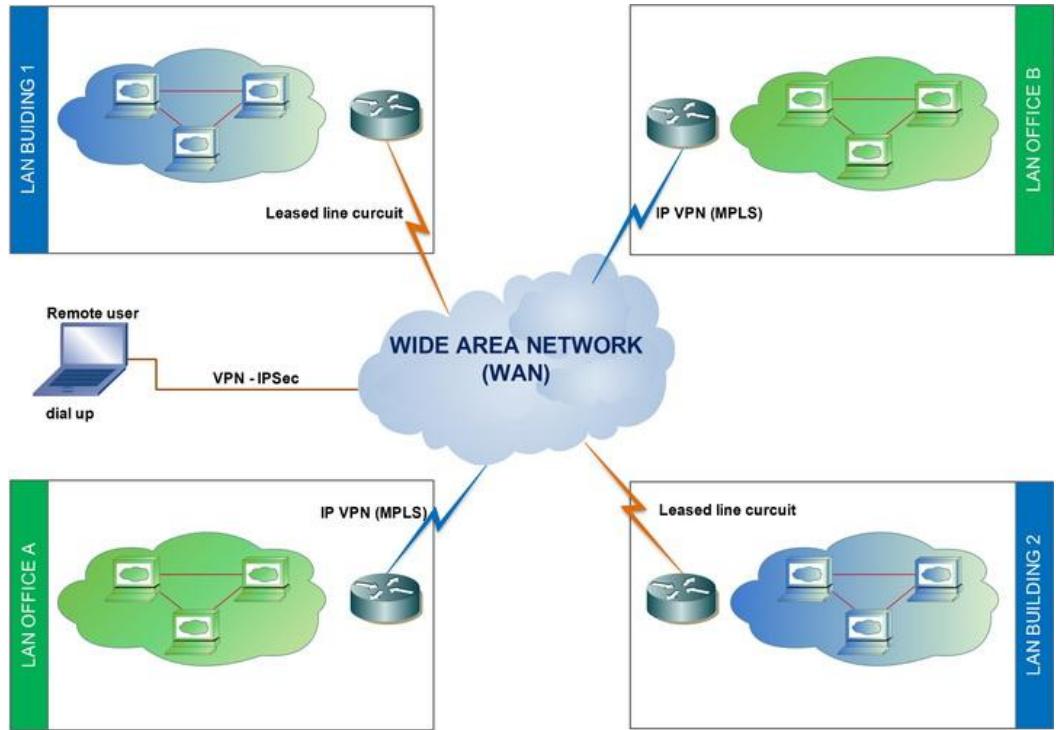
Mạng diện rộng (WAN) là mạng internet hệ thống thông tin liên lạc toàn cầu dùng để kết nối nhiều mạng cục bộ (LAN) lại với nhau. Thông qua việc kết nối các mạng nội bộ bằng đường cáp quang hoặc cáp đồng trục được cung cấp bởi các nhà cung cấp dịch vụ mạng từ đó hình thành một mạng lưới internet toàn cầu giúp mọi người ở xa nhau bởi khoảng cách địa lý có thể tương tác với nhau một cách nhanh chóng vượt qua mọi khó khăn về mặt khoảng cách.

Mạng internet đã trở nên vô cùng quen thuộc và phổ biến thậm chí đã và đang trở thành một phần không thể thiếu trong cuộc sống của mỗi người. Các ứng dụng mạng xã hội, các ứng dụng mail đều phải có kết nối internet thì mới có thể sử dụng để chia sẻ thông tin với nhau tạo thành một mạng lưới người dùng trên toàn thế giới.

Bên cạnh đó những lợi ích giúp nhiều người dùng có thể tương tác với nhau bất chấp khoảng cách về mặt địa lý thì mạng internet cũng tồn tại nhiều rủi ro bởi thông tin được chia sẻ rộng rãi trên internet rất khó để có thể kiểm duyệt được toàn bộ nội dung, nên đòi hỏi người dùng cần cẩn trọng xem xét và chọn lọc tránh những nội dung phản động và độc hại. Các doanh nghiệp muốn kết nối mạng nội bộ của công ty mình ra bên ngoài internet thì cần phải liên hệ với nhà cung cấp dịch vụ có một đường dây để có thể đi ra ngoài mạng internet điều này sẽ dẫn đến xảy ra độ trễ cao do dữ liệu phải được truyền tải giữa khoảng cách quá xa và qua nhiều các thiết bị và nhà trạm trung gian nên để đảm bảo được tốc độ mạng và giảm độ trễ thì các doanh nghiệp cần phải tốn thêm chi phí để đăng các gói cước có băng thông mạng dài hơn của các nhà cung cấp dịch vụ mạng đồng thời còn phải tốn thêm chi phí để bảo trì các thiết bị và nâng cấp hệ thống. Bên cạnh vấn đề chi phí thì vấn đề bảo mật cũng cần phải được chú trọng khi mà các tội phạm mạng sẽ tiến hành các cuộc xâm nhập mạng trái phép vào hệ thống mạng nội bộ của doanh nghiệp bằng các cuộc tấn công như DDoS, fishing và malware để nhắm vào các điểm yếu trong mạng từ đó phá hoại hệ thống mạng và đánh cắp những dữ liệu nhạy cảm.

Mặc dù mạng diện rộng đem lại nhiều lợi ích cũng như là chìa khóa cho sự phát triển vững mạnh của doanh nghiệp, tuy nhiên khi lắp đặt và xây dựng hệ

thống thì doanh nghiệp và các tổ chức cần cân nhắc kỹ lưỡng các tác hại tiềm ẩn này và đề ra các biện pháp quản lý, các chính sách bảo mật và tối ưu hóa để đảm bảo hệ thống mạng nội bộ có thể hoạt động trơn tru và an toàn trên môi trường internet.



Hình 2.2 Mô hình mạng diện rộng (WAN)

### 2.3 Mô hình OSI và mô hình TCP/IP:

#### 2.3.1 Mô hình OSI (*Open System Interconnection*):

Mô hình OSI là mô hình tiêu chuẩn chung của các hệ thống mạng máy tính, các hệ thống mạng máy tính đều phải được thiết kế theo dạng mô hình này để các hệ thống khác nhau có thể liên kết và truyền thông được với nhau. Mô hình này chia quá trình giao tiếp mạng thành 7 phần riêng biệt, mỗi tầng có các chức năng và nhiệm vụ riêng biệt:

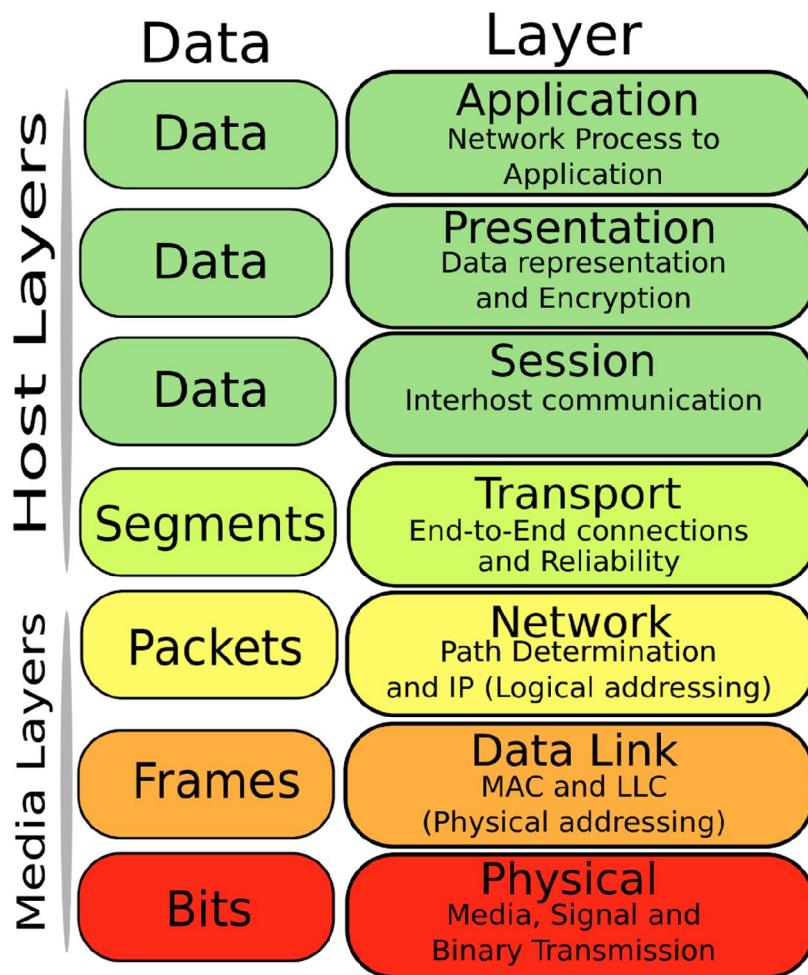
- Tầng vật lý (Physical Layer): tầng này có chức năng truyền tải các bit dữ liệu giữa các thiết bị trong hệ thống mạng bằng các đường truyền vật lý, cung cấp các phương tiện truyền dẫn về điện nhằm mục đích kết

nối các phần tử của mạng máy tính thành một hệ thống mạng hoàn chỉnh như dây cáp, sóng radio hoặc các tín hiệu quang học.

- Tầng liên kết dữ liệu (Data Link Layer): tầng này có nhiệm vụ đảm bảo dữ liệu khi truyền tải phải giữa các thiết bị không bị lỗi. Nó sẽ chia dữ liệu thành các frame, truyền các khung tuần tự và xử lý các thông điệp xác nhận (Acknowledgement frame) từ bên máy thu gửi về. Khi dữ liệu được truyền từ máy tính đến các thiết bị mạng thông qua các đường dây cáp thì các dữ liệu ấy có khả năng bị lỗi và gây ra thiếu sót dữ liệu nên tầng này phải giải quyết các vấn đề để kiểm soát lỗi, kiểm soát lưu lượng ngăn không gây ra tình trạng ngập lụt dữ liệu cho bên thu có tốc độ truyền thấp hơn. Các thiết bị sử dụng cho tầng này: Switch, bridge.
- Tầng mạng (Network): tầng này có nhiệm vụ quản lý việc định tuyến các gói tin giữa các mạng khác nhau. Đường đi có thể được định nghĩa cố định từ đầu (Static route) hoặc cũng có thể được định nghĩa khi bắt đầu các phiên giao tiếp giữa các mạng là đường đi động (Dynamic route) và có thể thay đổi tùy theo tình trạng tải dữ liệu của hệ thống mạng hiện tại.
- Tầng vận chuyển (Transport layer): Tầng này có chức năng đảm bảo dữ liệu khi được truyền tải đáng tin cậy và không bị lỗi giữa các điểm cuối (end-to-end), tầng vận chuyển sẽ chia các gói tin lớn thành các gói tin nhỏ hơn (segment) trước khi gửi đi để quản lý việc kiểm soát lỗi và luồng dữ liệu và thực hiện việc đánh số thứ tự trên các gói segment để những gói tin ấy được chuyển đi theo đúng thứ tự và bên nhận có thể sắp xếp dữ liệu vừa nhận được một cách nhanh chóng. Giao thức được sử dụng ở tầng này gồm: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
- Tầng phiên (Session Layer): tầng này có chức năng quản lý các phiên trò chuyện (Session) giữa các ứng dụng. Nó thiết lập, duy trì và kết thúc các phiên giao tiếp. Dịch vụ phiên cung cấp một liên kết giữa các đầu

cuối đảm bảo cuộc trao đổi dữ liệu được diễn ra một cách đồng bộ và khi kết thúc thì liên kết này sẽ được giải phóng. Cả quá trình giao tiếp này sẽ sử dụng token để truyền dữ liệu, đồng bộ hóa và hủy bỏ liên kết. Bên cạnh đó, khi xảy ra sự cố bất ngờ, 2 đầu cuối có thể bắt đầu lại từ phiên giao tiếp trước đó đã được đồng bộ.

- Tầng trình bày (Presentation Layer): tầng này chịu trách nhiệm về việc định dạng, mã hóa và giải nén dữ liệu, nó chuyển đổi và định dạng dữ liệu được gửi trên mạng sang dạng dữ liệu mà các hệ thống mạng cục bộ có thể đọc được. Giao thức được sử dụng ở tầng này gồm: SSL/TLS (Secure Sockets Layer/Transport Layer Security),
- Tầng ứng dụng (Application Layer): tầng này có chức năng xác nhận dịch vụ mà người dùng sử dụng khi kết nối với mô hình OSI. Gồm nhiều giao thức ứng dụng cung cấp các phương diện để cho người dùng truy cập vào môi trường mạng và các dịch vụ phân tán như email, lướt web và truyền tệp. Khi các ứng dụng của người dùng (Application Element) được sử dụng nó sẽ gọi đến các phần tử dịch vụ ứng dụng ASE (Application Service Element) trong hệ thống mạng. Mỗi ứng dụng mà người dùng sử dụng có rất nhiều các phần tử dịch vụ ứng dụng. Các phần tử dịch vụ ứng dụng trong hệ thống mạng được kết nối phôi hợp với nhau thông qua các liên kết đơn SAO (Single Association Object). SAO điều khiển điều khiển việc truyền thông và cho phép tuân tự hóa các truyền thông dịch vụ trong hệ thống mạng.



Hình 2.3 Mô hình OSI

### 2.3.2 Mô hình TCP/IP:

Mô hình TCP/IP, viết tắt của Transmission Control Protocol/Internet Protocol là một tập hợp các giao thức trao đổi thông tin được sử dụng rộng rãi để kết nối các thiết bị trong mạng internet. Đây là mô hình được sử dụng rất nhiều trong việc xây dựng các hệ thống mạng ngoài thực tế hiện nay với khả năng phục hồi tự động

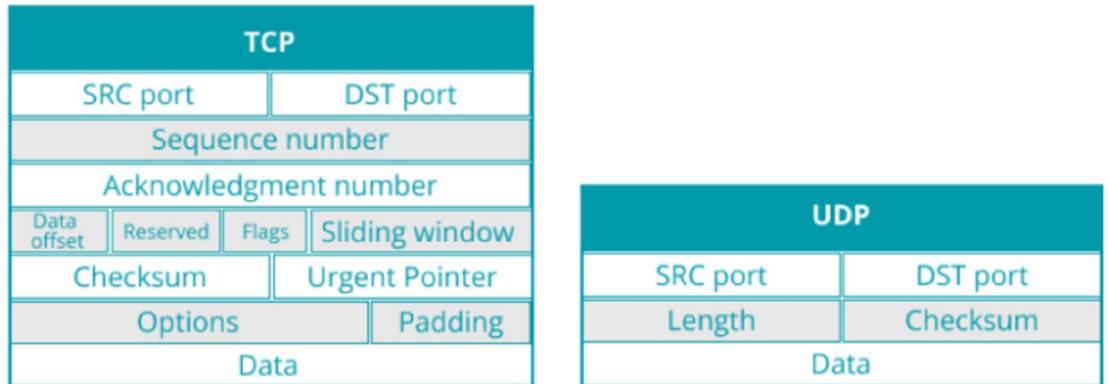
TCP/IP là sự kết hợp giữa 2 giao thức, IP (Internet Protocol) đây là giao thức mạng với tính năng định tuyến gói tin đến các đích đến đã được định nghĩa sẵn thông qua việc gán các thông tin về đường đi để các gói tin đến đúng được địa chỉ đã được

định sẵn ban đầu. Giao thức TCP (Transmission Control Protocol) đây là giao thức đảm bảo các gói tin khi được truyền đến các trạm vẫn còn nguyên vẹn và khi phát hiện gói tin bị thiết sót trong quá trình truyền tải thì giao thức này sẽ gửi tín hiệu về và yêu cầu hệ thống gửi lại một gói tin khác.

Mô hình OSI được thiết kế gồm 4 tầng từ thấp lên cao gồm: tầng liên kết (Link Layer), tầng mạng (Internet Layer), tầng giao vận (Transport Layer) và tầng ứng dụng (Application Layer).

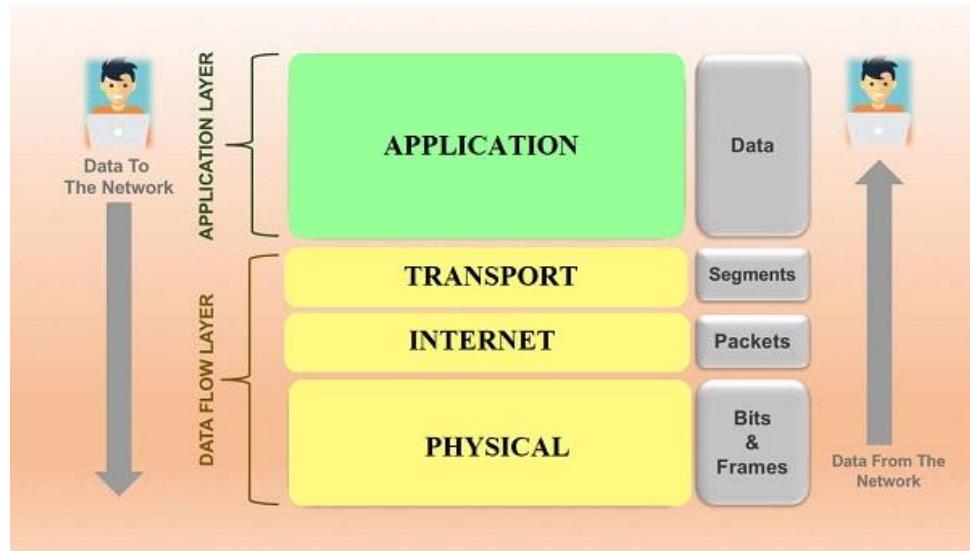
- Tầng liên kết (Link Layer): là tầng có nhiệm vụ truyền tải dữ liệu giữa 2 thiết bị trong cùng một mạng vật lý. Nó quản lý các kết nối và giao tiếp giữa các thiết bị mạng như máy tính, router, switch, đảm bảo các kết nối vật lý và quản lý địa chỉ MAC. Tại đây dữ liệu được chia thành các khung (frame) sau đó dữ liệu sẽ được truyền đến các đích sẽ được truyền đến các đích đến được chỉ định. Các giao thức được sử dụng gồm:
  - Ethernet: công nghệ công được gắn trên các thiết bị switch để kết nối các thiết bị trong mạng cục bộ lại với nhau, sử dụng các cáp đồng và cáp quang để kết nối.
  - Wifi: Công nghệ mạng không dây cho phép các thiết bị trong cùng một mạng nội bộ có thể kết nối mạng với nhau mà không cần sử dụng các đường dây cáp vật lý
- Tầng mạng (Internet Layer): tầng chịu trách nhiệm định tuyến và truyền tải dữ liệu đến các mạng khác nhau. Nó đóng gói các phân đoạn dữ liệu thành các gói tin (packets) với kích thước mỗi gói phù hợp với dung lượng của mạng chuyển mạch mà nó sử dụng để truyền tải dữ liệu, sau đó các gói tin được gán thêm phần header chứa thông tin của tầng mạng sau đó chúng được chuyển đến các tầng mạng tiếp theo. Các giao thức được sử dụng tại tầng này bao gồm:
  - IP (Internet Protocol): đây là giao thức chính của tầng này chịu trách nhiệm xác định địa chỉ và định tuyến gói dữ liệu

- ICMP (Internet Control Message Protocol): Giao thức này được sử dụng để gửi về các thiết bị nguồn các thông báo lỗi khi mà gói tin từ các thiết bị này gửi đi có lỗi xảy ra, hoặc được sử dụng để theo dõi và quản lý quá trình hoạt động của mạng
- IGMP (Internet Group Management Protocol): Quản lý việc truyền dữ liệu đa hướng (multicast) cho các nhóm thiết bị.
- Tầng giao vận (Transport Layer): chức năng của tầng này là chịu trách nhiệm xử lý các vấn đề giao tiếp giữa các máy trong một mạng nội bộ hoặc truyền tải dữ liệu qua các mạng khác nhau thông qua các thiết bị định tuyến đảm bảo dữ liệu được truyền đi một cách đáng tin cậy và theo đúng thứ tự. Tại đây, dữ liệu sẽ được chia thành các phân đoạn (Segment) và kích thước của mỗi Segment phải nhỏ hơn 64KB. Lúc này đây, bên trong Segment sẽ gồm các thành phần: Header sẽ chứa thông tin định tuyến và cuối cùng là dữ liệu. Tại tầng này, các giao thức được sử dụng chủ yếu gồm:
  - TCP (Transmission Control Protocol): Giao thức này cung cấp khả năng truyền tải đáng tin cậy với việc kiểm tra các dữ liệu được gửi theo đúng thứ tự nhằm đảm bảo chất lượng của các gói tin và kiểm soát tắc nghẽn khi truyền tải liên tục các lưu lượng dữ liệu lớn
  - UDP (User Datagram Protocol): Giao thức này đảm bảo về mặt tốc độ với việc cho phép dữ liệu được truyền tải một cách nhanh chóng tuy nhiên, trái ngược với TCP thì UDP không đảm bảo được chất lượng dữ liệu được truyền đi



Hình 2.4 Thông tin gói tin trong giao thức TCP và UDP

- Tầng ứng dụng (Application Layer): tầng này cung cấp các dịch vụ mạng cho phép các máy sử dụng các ứng dụng mạng giao tiếp với nhau sử dụng các dịch vụ mạng như lướt web, nhắn tin, email, truyền file, SSH, SMTP,... dữ liệu khi đến tầng này sẽ được chuyển thành kiểu Byte-to-Byte và được gán thêm thông tin định tuyến để đảm bảo dữ liệu được truyền đến đúng đích đến. Các giao thức được sử dụng chủ yếu trong tầng này:
  - HTTP (Hypertext Transfer Protocol): giao thức nền tảng World Wide Web cho phép truy cập các máy chủ (Web server) để tải về các trang web.
  - FTP (File Transfer Protocol): giao thức cho phép truyền và lưu trữ file giữa các thiết bị
  - SMTP (Simple Mail Transfer Protocol): Giao thức được sử dụng cho các dịch vụ mail dùng để gửi và nhận email.
  - DNS (Domain Name System): Hệ thống phân giải tên miền thành địa chỉ ip
  - SSH (Secure Shell): Giao thức cho phép điều khiển thiết bị từ xa và truyền tải dữ liệu



Hình 2.5 Mô hình TCP/IP

### 2.3.3 So sánh giữa mô hình OSI và mô hình TCP/IP:

Hiện nay, mô hình OSI và mô hình TCP/IP là 2 mô hình được sử dụng phổ biến và rộng rãi để có thể hiểu được cách thức hoạt động của hệ thống mạng. Với mô hình OSI là mô hình khái niệm, cung cấp khung lý thuyết chi tiết để có thể hiểu rõ các khía cạnh khác nhau của mạng máy tính, còn mô hình TCP/IP cung cấp thông tin về các giao thức thực tế và phương thức hoạt động của các hệ thống mạng hiện đại ngày nay nên các hệ thống mạng thực tế thường được thiết kế áp dụng theo mô hình TCP/IP. Bên cạnh đó, 2 mô hình này còn có những điểm khác biệt:

- Cả 2 mô hình đều có tầng ứng dụng, tuy nhiên tầng ứng dụng trong mô hình OSI được chia nhỏ hơn với 3 tầng (Application, Presentation, Session), còn mô hình TCP/IP chỉ có duy nhất tầng ứng dụng xử lý các chức năng như tầng ứng dụng của mô hình OSI
- Tầng Network trong mô hình OSI và tầng Internet trong mô hình TCP/IP đều có chức năng định tuyến gói tin đi đến đích
- Mô hình OSI có 2 tầng riêng biệt là tầng liên kết dữ liệu (Data link) và tầng vật lý (Physical Layer) để có thể truyền dữ liệu giữa các thiết bị

trong hệ thống mạng, trong khi tại mô hình TCP/IP chỉ có duy nhất một tầng liên kết dữ liệu (Data Link) đảm nhận chức năng này.

Điểm so sánh	Mô hình OSI	Mô hình TCP/IP
Cách giao tiếp ở các tầng	Mỗi tầng một nhiệm vụ riêng biệt	Kết hợp để thực hiện nhiệm vụ
Sự phụ thuộc	Độc lập hoàn toàn	Phụ thuộc vào giao thức
Sự phát triển	Xây dựng mô hình trước, phát triển giao thức sau	Giao thức được phát triển trước, xây dựng mô hình sau
Số lớp	7	4
Truyền thông	Hỗ trợ kết nối định tuyến và kết nối không dây	Chỉ hỗ trợ truyền thông không kết nối từ tầng mạng
Phương pháp tiếp cận	Chiều dọc	Chiều ngang

Hình 2.6 So sánh giữa mô hình OSI và TCP/IP

## 2.4 Các thành phần trong mạng nội bộ:

### 2.4.1 Router:

Router là thiết bị định tuyến trong mạng máy tính dùng để kết nối và chuyên tiếp các gói dữ liệu đi qua các vùng mạng khác nhau. Router thường có nhiều loại và đa dạng từ các router sử dụng để kết nối các thiết bị trong nhà ra internet với quy mô nhỏ cho tới các router lớn chịu được tải trọng cao được sử dụng cho các doanh nghiệp như các công ty, trường học, bệnh viện. Một số hãng cung cấp thiết bị router: Huawei, Cisco,...

#### 2.4.1.1 Chức năng của router:

Các chức năng của router bao gồm:

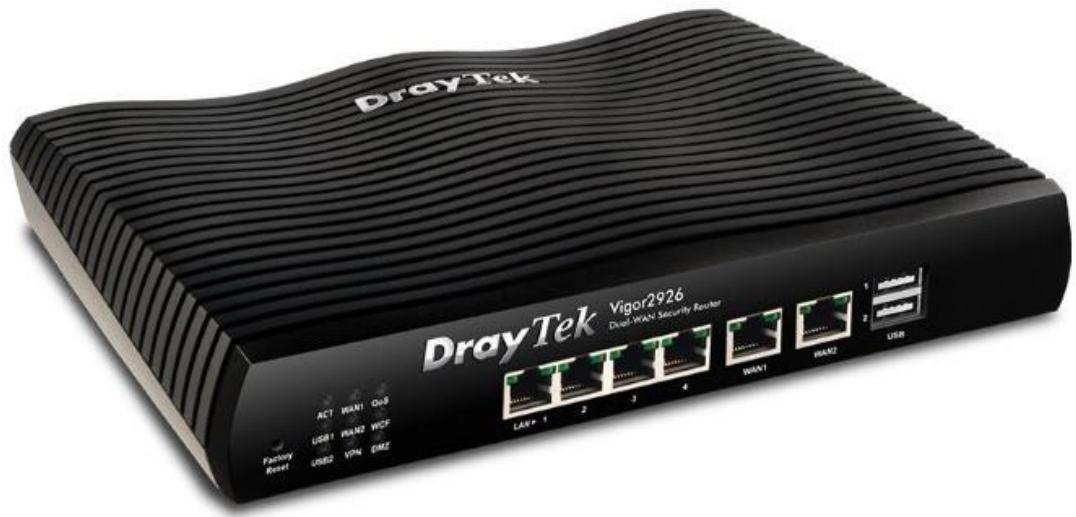
- Định tuyến gói tin:
  - Với tính năng này, router sẽ xác định đường đi ngắn nhất để gói tin có thể đến được đích đến thông qua việc đi qua các mạng con của các nhà trạm khác nhau, bằng việc sử dụng địa chỉ IP nguồn và địa chỉ IP đích sau đó gán vào gói tin để gói tin có thể được truyền đi tới đúng đích đến
  - Router sẽ sử dụng bảng định tuyến (routing table) và các giao thức định tuyến như (OSPF, BGP) từ đó xác định được tuyến đường đi ngắn nhất để đưa gói tin đến được đích đến.
- Kết nối các vùng mạng khác nhau:
  - Router sẽ kết nối các mạng LAN với nhau hoặc có thể kết nối tới nhà cung cấp dịch vụ mạng từ đó có thể kết nối tới các vùng mạng khác nhau để hình thành nên kết nối WAN tạo nên một mạng lưới Internet toàn cầu.
- Tính năng bảo mật:
  - Các router ngày nay thường tích hợp với một số tính năng bảo mật như Access-list và Zone-based firewall để lọc ra các lưu lượng cho phép đi vào hệ thống mạng và ngăn chặn các truy cập trái phép không mong muốn.
  - Các kỹ thuật NAT (Network Address Translation) có chức năng chuyển đổi địa chỉ IP public thành địa chỉ IP private nhằm che giấu địa chỉ IP trong hệ thống mạng nội bộ

#### 2.4.1.2 Nguyên lý vận hành của router:

- Xây dựng bảng định tuyến:
  - Đầu tiên, router sẽ thu thập thông tin của các vùng mạng lân cận thông qua các giao thức định tuyến như RIP, OSPF, EIGRP hay

các đường định tuyến tĩnh từ đó sẽ tự động xây dựng nên bảng định tuyến, dựa vào đó router sẽ chọn cho mình đường đi ngắn nhất để chuyển gói tin đến đích đến.

- Quá trình định tuyến gói tin:
  - Khi router nhận được một gói tin, nó sẽ kiểm tra địa chỉ ip đích của gói tin
  - Sau đó, nó sẽ dựa vào bảng định tuyến để xác định tuyến đường đi tốt nhất đưa gói tin đến đích
  - Sau đó, router sẽ đưa gói tin đến cổng interface và chuyển tiếp gói tin để cho nó tiếp tục cuộc hành trình của mình.
- Xử lý và chuyển tiếp gói tin:
  - Router đưa gói tin vào cổng interface, kiểm tra lại địa chỉ đích đến trên header của gói tin, xác nhận đường đi ngắn nhất đến đích sau đó tiến hành chuyển tiếp gói tin đi đến đích đến.



Hình 2.7 Thiết bị router DrayTek

### **2.4.2 Switch Layer 3:**

Switch layer 3 là thiết bị mạng tích hợp giữa tính năng của switch (tầng 2) và router (tầng 3) trong mô hình OSI. Nó không chỉ có thể sắp xếp và chuyển mạch các khung dữ liệu (frame) dựa trên địa chỉ MAC như switch layer 2 mà còn có thể định tuyến gói tin như router dựa trên địa chỉ ip.

#### **2.4.2.1 Chức năng của switch layer 3**

- **Chức năng chuyển mạch:** switch layer 3 có khả năng chuyển mạch các khung dữ liệu của các thiết bị trong cùng một mạng nội bộ (LAN) dựa trên địa chỉ MAC của các thiết bị đã kết nối với nó đồng thời đảm bảo được tốc độ đường truyền
- **Chức năng định tuyến:**
  - Switch layer 3 còn được tích hợp thêm khả năng định tuyến của router với việc dựa vào địa chỉ ip nguồn và đích của gói tin mà có thể định tuyến gói tin đến các vùng mạng khác hoặc các vlan khác nhau trong cùng một mạng nội bộ.
  - Bên cạnh đó, Switch layer 3 còn được kết hợp thêm các giao thức định tuyến động như OSPF, EIGRP,... để có thể định tuyến gói tin đến các vùng mạng lớn hơn và chia sẻ các bảng định tuyến giữa các thiết bị định tuyến trong cùng một khu vực nên ta có thể để việc cấu hình các đường default route dành cho việc định tuyến đến các thiết bị router và firewall
  - Tạo VLAN: Switch layer 3 vẫn giữ nguyên tính năng tạo vlan của switch layer 2 cho phép tạo ra các mạng riêng ảo riêng biệt nhằm tăng cường bảo mật, quản lý lưu lượng và giảm tắc nghẽn mạng.

#### 2.4.2.2 Nguyên lý hoạt động của Switch layer 3:

- Nguyên tắc hoạt động của chức năng chuyển mạch: khi switch Layer 3 nhận được một gói tin, nó sẽ kiểm tra địa chỉ IP đích của gói tin, nếu địa chỉ nó nằm trong cùng một mạng thì switch sẽ chuyển trực tiếp gói tin đó đến địa chỉ của thiết bị đích.
- Nguyên tắc hoạt động của chức năng định tuyến: Khi địa chỉ IP đích của gói tin nằm ngoài vùng mạng LAN của Switch thì thiết bị này sẽ sử dụng bảng định tuyến để xác định đường đi ngắn nhất để có thể đưa gói tin đến được đích đến cuối cùng.
- Nguyên tắc hoạt động của chức năng định tuyến giữa các VLAN: thiết bị switch layer 3 có thể gán các cổng vào các VLAN khác nhau để tạo ra các mạng ảo riêng biệt. Khi một gói tin được truyền đến, nó sẽ kiểm tra ID VLAN trên gói tin đó và định tuyến các gói tin vào cùng một VLAN hoặc đến các VLAN khác.
- Access control list: trên thiết bị Switch layer 3 ta có thể tạo ra các access-list để lọc ra những truy cập được phép đi vào hệ thống mạng nội bộ. Khi một gói tin đến Switch thì nó sẽ cho phép hoặc từ chối các gói tin đó dựa vào giao thức, cổng và địa chỉ IP của gói tin.

Switch layer 3 là một thiết bị mạng vượt trội với sự kết hợp giữa switch layer 2 và router cung cấp khả năng chuyển mạch và định tuyến hiệu quả trong hệ thống mạng nội bộ. Thiết bị này giúp cho hệ thống mạng được tối ưu hóa hiệu suất, bảo mật và quản lý lưu lượng trong mạng LAN, làm cho việc quản trị hệ thống mạng được hiệu quả hơn.



Hình 2.8 Thiết bị switch layer 3

#### **2.4.3 Switch layer 2:**

Switch layer 2 là thiết bị hoạt động ở tầng liên kết dữ liệu (Data Link) trong mô hình OSI, là một thiết bị mạng có khả năng chuyển tiếp các khung dữ liệu dựa trên địa chỉ MAC (Media Access Control). Switch layer 2 là một thành phần cơ bản trong hệ thống mạng LAN (Local Area Network) giúp kết nối các thiết bị như máy tính, máy in và các thiết bị khác trong cùng một mạng nội bộ.

##### **2.4.3.1 Chức năng của Switch layer 2:**

- **Chuyển mạch dữ liệu:** chức năng cho phép switch layer 2 chuyển tiếp các khung dữ liệu dựa trên địa chỉ MAC nguồn và đích, điều này cho

phép các thiết bị trong cùng mạng LAN có thể kết nối và giao tiếp được với nhau

- Học địa chỉ MAC: Chức năng này cho phép các thiết bị switch layer 2 có thể lưu lại các địa chỉ MAC của các thiết bị kết nối tới cổng của nó, điều này sẽ làm tối ưu hóa quá trình chuyển tiếp dữ liệu bằng cách ghi nhớ và tạo nên bảng địa chỉ MAC của các thiết bị với cổng tương ứng
- Phân mảnh và chuyển tiếp dữ liệu: Switch layer 2 sẽ phân mảnh dữ liệu mà nó nhận được thành các frame sau đó chuyển chúng đến đích.
- Tạo vlan (Virtual Local Area Network): trên switch layer 2 còn có chức năng cho phép tạo ra các mạng ảo (vlan) sau đó gán các cổng vật lý vào các vlan riêng biệt nhằm tăng cường khả năng bảo mật và quản lý lưu lượng mạng.

#### 2.4.3.2 Nguyên lý hoạt động của switch layer 2:

- Khám phá và học các địa chỉ MAC:
  - Khi switch layer 2 nhận được một khung dữ liệu, nó sẽ kiểm tra địa chỉ MAC nguồn. Nếu địa chỉ MAC nguồn này chưa được switch lưu lại thì nó sẽ tiến hành lưu lại địa chỉ MAC này cùng với cổng kết nối tương ứng. Điều này sẽ giúp switch biết được thiết bị nào được nối với cổng nào nhằm giúp cho việc chuyển tiếp dữ liệu diễn ra một cách tối ưu
- Chuyển tiếp dữ liệu:
  - Khi switch layer 2 nhận được một khung dữ liệu đến nó sẽ kiểm tra địa chỉ MAC đích của dữ liệu. Nếu như địa chỉ MAC đó đã được switch lưu lại thì nó sẽ chuyển tiếp gói tin đến cổng kết nối tương ứng với địa chỉ MAC đó. Còn nếu switch chưa lưu địa chỉ MAC đó thì nó sẽ gửi các gói broadcast đến các thiết bị kết nối đến nó sau đó các thiết bị sẽ phản hồi lại switch và nhờ vậy

switch đã có thể lưu lại địa chỉ MAC của các thiết bị đó cùng với cổng tương ứng, sau đó, switch sẽ chuyển tiếp gói tin đến đúng với thiết bị có địa chỉ MAC đích. Điều này xảy ra nhằm mục đích đảm bảo các gói tin được truyền tới đúng đích đến.

- Quản lý bảng địa chỉ MAC: Bảng địa chỉ MAC được switch cập nhật liên tục với các địa chỉ MAC mới và cổng tương ứng khi có thiết bị mới kết nối tới switch. Các thông tin địa chỉ MAC trong bảng sẽ được tự động xóa đi khi thiết bị sau một thời gian dài không được sử dụng nhằm mục đích cho bảng thông tin luôn luôn được cập nhật mới, đảm bảo các địa chỉ MAC luôn được cập nhật chính xác và hiệu quả.

Switch layer 2 là một thiết bị quan trọng trong mạng LAN, với chức năng chính là chuyển mạch dựa trên địa chỉ MAC của các thiết bị. Nó cung cấp hiệu suất cao, bảo mật tốt cùng với khả năng mở rộng linh hoạt các phân đoạn mạng. Nhưng vì không có khả năng định tuyến qua các vùng mạng khác nhau nên switch layer 2 chỉ có thể hoạt động trong một mạng nội bộ cụ thể. Nếu dữ liệu cần được chuyển tới một mạng khác nó sẽ định tuyến gói tin đến các thiết bị như router hoặc switch layer 3 để cho gói tin tiếp tục cuộc hành trình đi đến đích.



Hình 2.9 Thiết bị Switch layer 2

#### **2.4.4 Access point:**

Access point (AP) hay điểm truy cập, là một thiết bị mạng cho phép các thiết bị không dây như laptop, điện thoại thông minh, máy tính bảng,... có thể kết nối không dây (wireless) đến các mạng có dây (wired network) thông qua các công nghệ wifi. Access point hoạt động như một cầu nối giữa mạng không dây và mạng có dây, cho phép mở rộng phạm vi kết nối của các mạng không dây nhằm tăng thêm số lượng thiết bị có thể kết nối vào hệ thống mạng.

##### **2.4.4.1 Chức năng của Access point:**

- Kết nối không dây: Access point cung cấp khả năng kết nối không dây cho các thiết bị sử dụng các công nghệ kết nối internet không dây để truy cập vào internet và sử dụng các dịch vụ mạng mà không cần sử dụng các dây cáp để kết nối một cách rườm rà.
- Truyền dữ liệu: Các thiết bị access point có khả năng truyền tải dữ liệu và định tuyến gói tin đến các vùng mạng khác, chúng hoạt động như một thiết bị định tuyến nhưng có thêm khả năng định tuyến giữa các vùng mạng có dây và các vùng mạng không dây.
- Tính năng bảo mật: Các thiết bị access point cung cấp khả năng bảo mật sử dụng các phương thức như WPA2 và WPA3 yêu cầu xác thực trước khi kết nối để phòng tránh các tác nhân có ý đồ phá hoại xâm nhập vào hệ thống mạng không dây.
- Vì là các điểm truy cập mạng không dây nên Access point cung cấp khả năng mở rộng hệ thống mạng một cách dễ dàng mà không cần phải lắp đặt thêm dây cáp khi kết nối thêm các thiết bị khác vào hệ thống mạng

#### 2.4.4.2 Nguyên lý hoạt động của access point:

- Access point khi được kết nối vào hệ thống mạng nội bộ và được cấp nguồn để khởi động thì nó sẽ bắt đầu đi phát tán các sóng wifi để tạo điểm truy cập cá nhân cho các thiết bị không dây.
- Sau đó các thiết bị không dây khi muốn kết nối trực tiếp vào các điểm truy cập cá nhân này thì chúng sẽ phải quét để tìm kiếm SSID (Service Set Identifier) của access point và nhấp chọn SSID đó để yêu cầu kết nối. Tiếp đó, access point sẽ yêu cầu người dùng xác thực bằng cách nhập mật khẩu để tiến hành truy cập. Nếu như xác thực thành công thì access point sẽ cung cấp quyền truy cập vào hệ thống mạng không dây cho các thiết bị.
- Truyền dữ liệu: trong quá trình truyền tải dữ liệu giữa các vùng mạng khác nhau, access point sẽ nhận dữ liệu được gửi đến từ các thiết bị không dây sau đó định tuyến các dữ liệu này đến các vùng mạng có dây hoặc ngược lại, đảm bảo việc truyền tải giữa hệ thống mạng không dây và hệ thống mạng có dây luôn diễn ra ổn định và không bị gián đoạn.
- Lựa chọn kênh và băng tầng: trong quá trình hoạt động, các access point sẽ xét đến tình trạng băng tần tín hiệu tại địa điểm đó có ổn định không mà sẽ tự động lựa chọn kênh có tần số ít bị nhiễu nhất để kết nối thiết bị của người dùng. Hoặc xem xét các chuẩn kết nối không dây của thiết bị người dùng là chuẩn nào mà sẽ tự động chuyển sang loại công nghệ kết nối đó để tiến hành kết nối với thiết bị.
- Bảo mật: các access point sử dụng các phương thức mã hóa để tiến hành bảo mật dữ liệu trong suốt quá trình truyền tải dữ liệu của hệ thống mạng không dây. Các phương thức mã hóa phổ biến bao gồm WEP (Wired Equivalent Privacy), WPA (Wifi Protected Access) và WPA2.
- Công nghệ Mesh của các access point: đây là công nghệ cho phép các thiết bị access point phủ sóng wifi khắp cả một khu vực khiến cho việc kết nối internet của các thiết bị không dây và các dịch vụ của người

dùng không bị gián đoạn. Công nghệ Mesh cho phép thực hiện kết nối các access point lại với nhau để tạo ra một vùng phủ sóng wifi lớn hơn. Đây là công nghệ được áp dụng tại các tòa nhà lớn, công ty, trường học, ví dụ khi người dùng di chuyển thiết bị không dây của mình di chuyển đến một vị trí mà access point hiện tại không thể phủ sóng tới được thì lúc này công nghệ mesh sẽ tiến hành tìm các thiết bị access point khác gần với vị trí của người dùng nhất sau đó tiến hành kết nối không dây đến thiết bị của người dùng một cách nhanh chóng mà không gây bất tiện cho người dùng.

Access point cung cấp khả năng truy cập không dây linh hoạt và thuận tiện cho người dùng. Cung cấp các khả năng kết nối không dây và có dây đến với các thiết bị của người dùng tạo sự thuận tiện cho người dùng khi muốn kết nối internet một cách nhanh chóng nhưng vẫn đảm bảo tính bảo mật và an toàn cho dữ liệu của người dùng.



Hình 2.10 Access point công nghệ Wifi 6 của Huawei

### 2.4.5 Tường lửa (Firewall):

Tường lửa (firewall) là một thiết bị cực kỳ quan trọng trong hệ thống mạng nội bộ. Nó giúp bảo vệ cả hệ thống mạng khỏi các tác nhân có ý đồ gây hại, đánh cắp thông tin và làm sụp đổ hệ thống bằng cách chặn các lưu lượng gói tin xuất phát từ các địa chỉ ip nguồn không mong muốn. Tường lửa có thể là các thiết bị phần cứng hoặc cũng có thể là phần mềm được cài vào máy tính với chức năng chính là giám sát, kiểm soát lưu lượng mạng dựa trên các chính sách bảo mật được soạn ra bởi các quản trị viên hệ thống mạng.

#### 2.4.5.1 Chức năng của tường lửa:

- Lọc gói tin (Packet filtering): Firewall cung cấp khả năng lọc gói tin dựa trên việc kiểm tra các thông tin của gói tin như địa chỉ ip nguồn, ip đích, giao thức được sử dụng kết hợp với các chính sách bảo mật được thiết lập mà có thể cho phép hoặc từ chối các lưu lượng gói tin đó vào hệ thống mạng.
- Kiểm soát truy cập (Access Control): Firewall cung cấp khả năng cho phép các quản trị viên tạo ra các chính sách và tập luật từ đó dựa trên các chính sách vừa mới tạo ra mà tiến hành kiểm soát các lưu lượng gói tin đi vào hệ thống mạng.
- Bảo vệ và phòng chống xâm nhập: khi phát hiện ra các hành vi có可疑 xâm nhập mạng trái phép từ bên ngoài thì firewall sẽ tiến hành ngăn chặn và gửi thông báo đến cho quản trị viên hệ thống mạng nhằm phát hiện sớm các cuộc tấn công và xâm nhập bất thường vào hệ thống mạng.
- Chức năng quan sát lưu lượng mạng (Traffic monitoring): Bên cạnh đó, firewall còn có chức năng theo dõi và ghi lại nhật ký lưu lượng mạng nhằm hỗ trợ quản trị viên trong quá trình phân tích và khắc phục sự cố mạng, phát hiện sớm các nguy cơ tiềm ẩn đối với hệ thống mạng.

- NAT (Network Address Translation): Firewall có thể sử dụng tính năng NAT để chuyển đổi địa chỉ IP private của mạng nội bộ thành địa chỉ IP public để có thể che giấu địa chỉ IP của thiết bị khi đi ra ngoài mạng internet

#### 2.4.5.2 Nguyên lý hoạt động của tường lửa:

Khi một gói tin từ bên ngoài vùng mạng nội bộ đi đến thiết bị tường lửa, thì tường lửa sẽ dựa trên các chính sách bảo mật và tập luật được quản trị viên tạo ra để tiến hành kiểm tra các thông tin của gói tin. Các thông tin được kiểm tra bao gồm: địa chỉ IP nguồn, địa chỉ IP đích, giao thức được sử dụng để từ đó nếu như gói tin đáp ứng được các điều kiện của các tập luật thì các gói tin đó sẽ được cho phép định tuyến vào các thiết bị trong mạng nội bộ, còn nếu như không thì những gói tin đó sẽ bị chặn lại không cho phép đi vào hệ thống của mạng nội bộ.

Tường lửa là một phần không thể thiếu trong hệ thống mạng nội bộ, với khả năng giám sát và kiểm soát lưu lượng mạng, tường lửa bảo vệ mạng khỏi các mối đe dọa từ bên ngoài nhằm đảm bảo an ninh và sự ổn định của toàn bộ hệ thống mạng.



Hình 2.11 Tường lửa ASA 5506-x của cisco

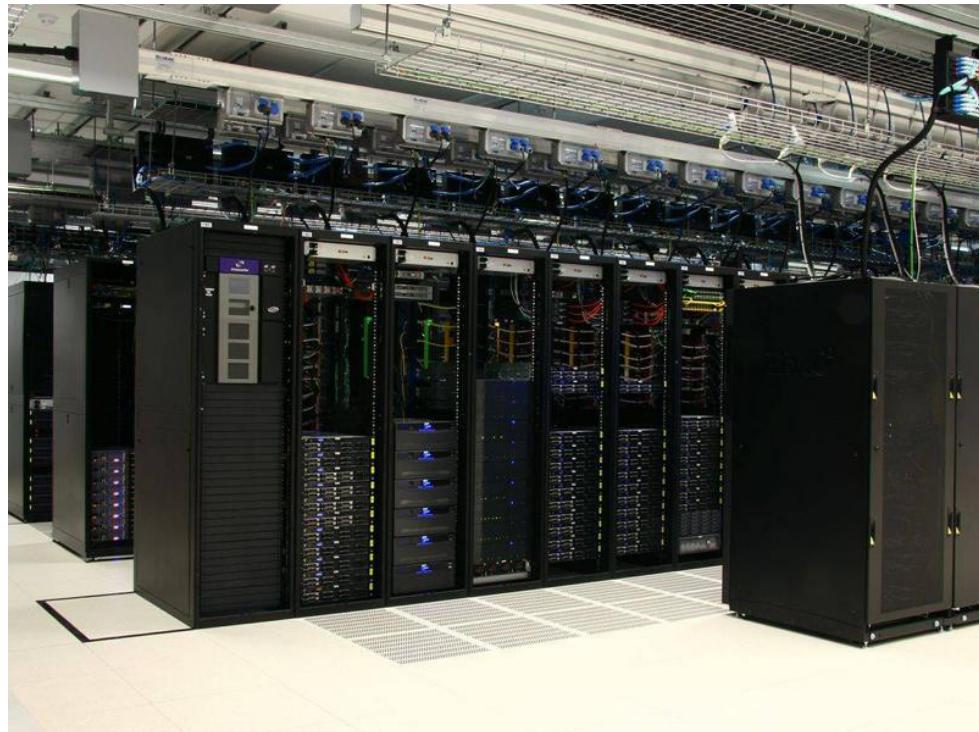
#### **2.4.6 Server:**

Server (máy chủ) là một hệ thống máy tính được kết nối internet nhằm cung cấp các dịch vụ cho các máy tính khách (client) khác trên môi trường internet. Nó là một máy tính nhưng có khả năng xử lý và lưu trữ vượt trội hơn so với các máy tính thông thường, server cho phép các máy khách kết nối tới nó để truy cập đến các dịch vụ đáp ứng nhu cầu sử dụng của người dùng. Ta có thể nói rằng máy chủ là nền tảng của mọi loại dịch vụ và ứng dụng trên môi trường internet.

Các dịch vụ của máy chủ bao gồm:

- Web Server (Máy chủ web): Máy chủ này có chức năng lưu trữ các trang web và cung cấp các giao thức HTTP và HTTPS để các máy khách có thể truy cập đến máy chủ và sử dụng các dịch vụ lướt web.
- Database Server (Máy chủ cơ sở dữ liệu): đây là loại máy chủ có chức năng lưu trữ và quản lý cơ sở dữ liệu, máy chủ này cung cấp khả năng truy cập bằng các câu lệnh truy vấn để các ứng dụng từ máy khách có thể truy cập và lấy về các thông tin cá nhân của mình.
- Email Server (Máy chủ mail): đây là máy chủ phục vụ cho các nền tảng dịch vụ gửi thư điện tử. Cung cấp và phân phối email đến với các tài khoản của người dùng, máy chủ này hỗ trợ các giao thức như SMTP, IMAP và POP3
- DNS Server (Máy chủ phân giải tên miền): DNS (Domain name Server) là máy chủ có chức năng phân giải tên miền, máy chủ này sẽ chứa toàn bộ thông tin về tên miền và địa chỉ ip tương ứng của các máy chủ web server và các máy chủ dịch vụ khác. Khi một máy khách nhập địa chỉ website của 1 trang web thì hệ thống mạng sẽ gửi gói tin đó đến địa chỉ của DNS Server để phân giải tên miền đó thành địa chỉ ip sau đó sẽ trả về và thiết bị định tuyến từ phía mạng của máy khách sẽ gửi gói tin đó đến đúng địa chỉ ip đích đến đó.
- FTP Server: đây là máy chủ có chức năng lưu trữ và truyền file thường được sử dụng trong nội bộ mạng của công ty để có thể tạo nên một hệ

cơ sở dữ liệu riêng trong nội bộ công ty và chỉ có thể truy cập được bởi các nhân viên trong công ty đó.



Hình 2.12 Hệ thống máy chủ

#### **2.4.7 Các thiết bị đầu cuối:**

- PC: là máy tính cá nhân được sử dụng để xử lý thông tin, lưu trữ dữ liệu và thực hiện các dịch vụ ứng dụng của người dùng như duyệt web, gửi mail và xem video.
- Laptop: Là thiết bị máy tính cá nhân nhưng có khả năng kết nối mạng không dây vào hệ thống mạng có dây giúp người dùng thuận tiện hơn trong việc kết nối internet để xử lý các công việc từ xa, truy cập vào tài nguyên mạng ở bất kỳ đâu trong phạm vi mạng nội bộ.
- Máy in: Là thiết bị phục vụ nhu cầu in dữ liệu thành bảng cứng, có thể chia sẻ và dùng chung bởi bất kỳ các thiết bị nào trong hệ thống mạng nội bộ.

- Điện thoại thông minh: Là thiết bị thuận tiện nhất đối với người dùng với khả năng truy cập internet không dây vào hệ thống mạng ở bất kỳ đâu đi kèm với một số chức năng như nhắn tin, video call xem video và chạy các ứng dụng di động.

#### **2.4.8 Cáp mạng (Network cables):**

Là thiết bị đảm bảo kết nối vật lý giữa các thiết bị trong hệ thống mạng LAN với chức năng truyền tải dữ liệu giữa các thiết bị trong nội bộ mạng. Người quản trị mạng có thể sử dụng dây cáp mạng để kết nối các thiết bị mạng lại với nhau để tạo thành một hệ thống mạng như PC với các thiết bị switch, router hay modem để có thể truy cập vào hệ thống mạng và sử dụng internet. Cáp ethernet (Cáp đồng) trong mạng nội bộ gồm các loại: Cat5e, Cat6, Cat6a, Cat7 và Cat8

- Cat5e (Category 5 Enhanced):
  - Cấu trúc: gồm 4 dây cáp xoắn, không có lớp che chắn chống nhiễu
  - Tốc độ truyền tải: 1Gbps
  - Bandwidth: lên đến 100 MHz
  - Thường được sử dụng trong các mạng gia đình và văn phòng nhỏ
- Cat6 (Category 6):
  - Cấu trúc: Bao gồm 4 cặp dây xoắn, có lớp che chắn chống nhiễu hoặc không
  - Tốc độ truyền tải: lên đến 10 Gbps ở khoảng cách 70m-100m
  - Bandwidth: Lên đến 250 MHz
  - Sử dụng trong các mạng văn phòng, trường học và doanh nghiệp có quy mô vừa
- Cat6a (Category 6 augmented):
  - Cấu trúc: Gồm 4 cặp dây xoắn với lớp che chắn chống nhiễu

- Tốc độ truyền tải: lên đến 10Gbps ở khoảng cách 100m
- Băng thông: lên đến 500 MHz
- Sử dụng trong các môi trường yêu cầu hiệu suất cao như trung tâm dữ liệu và mạng doanh nghiệp quy mô lớn
- Cat7 (Category 7):
  - Cấu trúc: Gồm 4 cặp dây xoắn với lớp che chắn chống nhiễu cho từng cặp và toàn bộ cáp
  - Tốc độ truyền tải: 10Gbps với khoảng cách tối đa 100m
  - Băng thông: lên đến 600 MHz
  - Sử dụng trong các môi trường công nghiệp và trung tâm dữ liệu cao cấp
- Cat8 (Category 8):
  - Cấu trúc: Bao gồm 4 cặp dây xoắn với lớp che chắn chống nhiễu cho từng cặp và toàn bộ cáp
  - Tốc độ truyền tải: 40Gbps ở khoảng cách 30m
  - Băng thông: lên đến 2000 MHz
  - Sử dụng trong các trung tâm dữ liệu và môi trường yêu cầu tốc độ truyền tải dữ liệu cao

#### **2.4.9 Tủ Rack:**

Tủ rack là một thành phần quan trọng của hạ tầng mạng, nó được dùng để tổ chức, quản lý và bảo vệ các thiết bị core quan trọng trong hệ thống mạng như switch, router và các thiết bị viễn thông khác khỏi các tác động đến từ môi trường bên ngoài.

Tủ rack mạng có các chức năng như:

- Tổ chức và quản lý: tủ rack có thể chứa nhiều thiết bị trong hệ thống mạng một cách khoa học, nhờ vậy mà các thiết bị phần cứng sẽ được sắp xếp một cách có tổ chức gọn gàng, dễ dàng quản lý và truy cập.

- Quản lý dây cáp: Thông qua các khe rãnh và giá đỡ trong tủ rack, ta có thể đặt và bố trí các dây cáp mạng một cách gọn gàng và an toàn giảm thiểu rủi ro hư hỏng cáp do cáp lỏng hoặc bị chèo chéo
- Khả năng làm mát: tủ rack cung cấp khả năng làm mát và tản nhiệt hiệu quả nhờ vào thiết kế thông thoáng giúp cho luồng khí dễ dàng lưu thông vào tủ, đồng thời còn tích hợp thêm các hệ thống làm mát đảm bảo các thiết bị được đặt trong tủ luôn ở trạng thái mát mẻ, nâng cao hiệu suất khi sử dụng



Hình 2.13 Tủ rack mạng

#### **2.4.10 Nguồn điện dự phòng:**

Nguồn điện dự phòng UPS (Uninterruptible Power Supply), là bộ nguồn cung cấp điện cho các hệ thống mạng chạy bằng pin được sử dụng khi có sự cố về điện trong hệ thống mạng. Nó có thể cung cấp điện cho các thiết bị mạng trong một khoảng thời gian khi hệ thống mạng bị mất điện, đảm bảo không làm gián đoạn các dịch vụ mạng.

## **2.5 Các công nghệ cấu hình trong hệ thống mạng nội bộ:**

### **2.5.1 Tổng quan về EVE-NG:**

EVE-NG (Emulated Virtual Environment – Next Generation) là một trong các công cụ giả lập mạng mạnh nhất hiện nay, đây là một nền tảng ảo hóa mạng cho phép xây dựng, mô phỏng và thử nghiệm các mô hình mạng phức tạp với các thiết bị mạng ảo như: switch và router, firewall cho đến các thiết bị đầu cuối như máy tính và các ứng dụng.

EVE-NG có thể được chạy trên các máy tính sử dụng những hệ điều hành thông dụng hiện nay như Windows, Linux và MacOS thông qua các công cụ ảo hóa như Vmware Workstation, Qemu và KVM

Với việc sử dụng giao diện web để tiến hành thao tác cũng như thiết kế và xây dựng mô hình mạng nên EVE-NG rất thân thiện về dễ dàng tiếp cận với đại đa số người dùng là các kỹ sư mạng muốn kiểm thử hệ thống mạng trước khi triển khai ngoài thực tế.

EVE-NG cung cấp môi trường mạng an toàn hỗ trợ cho các kỹ sư mạng và quản trị viên giả lập các thiết bị mạng ảo như switch và router để xây dựng nên các hệ thống mạng trong môi trường đó. Kết hợp với đặc điểm của EVE-NG đó là cho phép các mô hình hệ thống mạng ấy có thể kết nối ra bên ngoài mạng internet để sử dụng các dịch vụ mạng từ đó, hỗ trợ kiểm thử hệ thống mạng khi chạy các ứng dụng ngoài thực tế giúp cho các quản trị viên và kỹ sư hệ thống mạng có thể sớm phát hiện được những lỗi có thể xảy ra trước khi triển khai hệ thống đó cho các doanh nghiệp ngoài thực tế hoặc cũng để có thể cập nhật các chức năng và công nghệ mới cho các hệ thống mạng sẵn có của doanh nghiệp.

### **2.5.2 Tổng quan về VLAN:**

VLAN (Virtual Local Area Network) là một kỹ thuật cho phép chia mạng vật lý thành các các mạng logic riêng biệt trên thiết bị switch với mỗi mạng logic hoạt động như một mạng riêng biệt nhằm cải thiện tính bảo mật, hiệu suất và khả năng quản lý mạng

### 2.5.2.1 Các tính năng của VLAN:

- Bảo mật: VLAN cho phép cô lập lưu lượng giữa các nhóm người dùng với nhau, giúp tăng cường khả năng bảo mật và riêng tư giữa các phòng ban trong hệ thống mạng nội bộ. Ví dụ như dữ liệu của VLAN thuộc phòng tài chính không thể được truy cập bởi các máy thuộc VLAN của phòng khai thác.
- Quản lý: nhờ có VLAN mà các quản trị viên hệ thống mạng có thể phân chia các thiết bị và nhóm người dùng trong hệ thống mạng nội bộ vào các Vlan theo từng chức năng khác nhau làm cho việc quản lý trở nên đơn giản và dễ dàng hơn.
- Tăng hiệu suất của hệ thống: VLAN giúp giảm lưu lượng của các gói broadcast từ đó làm tăng hiệu suất của hệ thống mạng. Nếu không có VLAN, một broadcast được gửi đi từ một host có thể dễ dàng đi đến mọi thiết bị mạng, khi đó các thiết bị nhận được broadcast đều phải xử lý những gói tin đó khiến cho CPU của các thiết bị phải làm nhiều việc hơn gây ra hao phí. Vì vậy, khi có VLAN các thiết bị thuộc chung VLAN chỉ cần nhận và xử lý các gói broadcast thuộc Vlan đó từ đó làm giảm hao phí các thiết bị trong hệ thống mạng.

### 2.5.2.2 Nguyên lý hoạt động của VLAN:

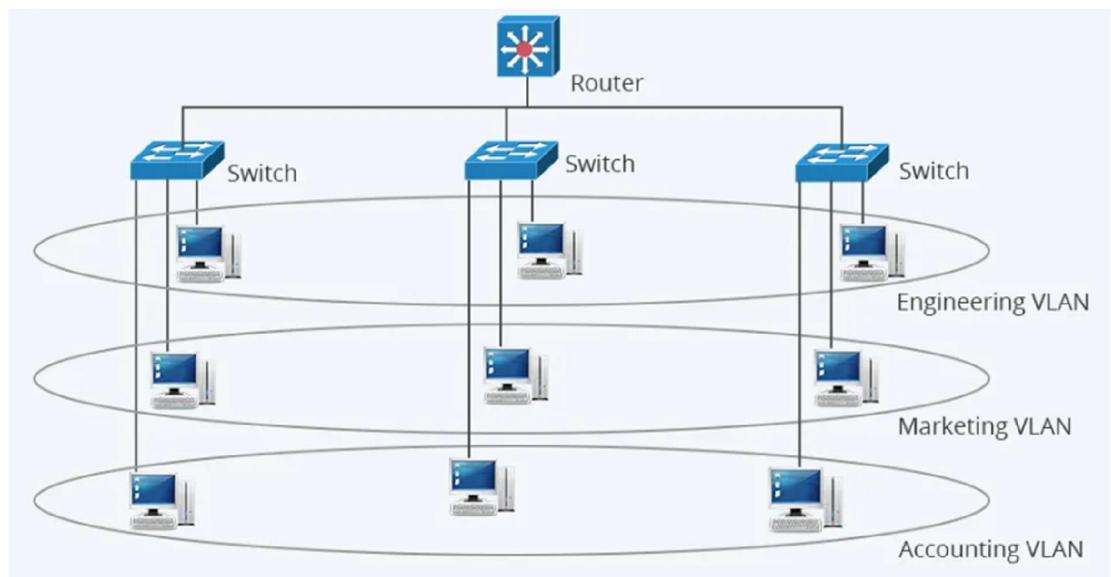
Vlan hoạt động bằng cách đánh dấu (tagging) lên header của các khung dữ liệu (frame). Các khung dữ liệu khi đi qua switch sẽ được thêm vào một tag chứa thông tin VLAN ID, tag này sẽ giúp xác định gói tin này thuộc về VLAN nào từ đó chuyển tiếp gói tin tới đúng với các thiết bị thuộc VLAN đó. Các bước chuyển mạch trong vlan bao gồm:

- Gửi khung dữ liệu: Khi một thiết bị gửi khung dữ liệu, nó sẽ thêm mã vlan vào header của khung nhằm xác định Vlan mà khung này thuộc về
- Chuyển khung đến bộ chuyển mạch (Switch): dữ liệu được chuyển đến bộ chuyển mạch thông qua các đường dây cáp mạng nối với nhau.

- Switch chuyển dữ liệu đến cổng tương ứng: Sau khi nhận được khung dữ liệu được chuyển tới, thiết bị switch sẽ đọc mã VLAN của gói tin nhằm xác định gói tin này thuộc VLAN nào sau đó sẽ chuyển gói tin này đến với cổng tương ứng với VLAN đó
- Thiết bị đầu cuối nhận được khung dữ liệu: thiết bị đầu cuối nhận được gói tin được chuyển đến từ switch

#### 2.5.2.3 Các loại cổng sử dụng trong VLAN:

- Access port: Kết nối các thiết bị đầu cuối như máy tính, máy in với các thiết bị switch và mỗi port access chỉ thuộc về 1 VLAN duy nhất
- Trunk ports: Được sử dụng cho các kết nối giữa các thiết bị switch với nhau hoặc giữa switch và router, đây là cổng cho phép các gói tin thuộc các VLAN khác nhau có thể đi qua đường trunking này để đến đích đến.



Hình 2.14 Các VLAN trong hệ thống mạng nội bộ

### **2.5.3 *Tổng quan về VTP:***

VTP (VLAN Trunking Protocol) là giao thức độc quyền của các thiết bị mạng Cisco, cho phép đồng bộ hóa VLAN giữa các thiết bị switch với nhau, khiến cho việc cấu hình VLAN trên các thiết bị switch trở nên dễ dàng và ít tốn thời gian hơn. Bằng việc tạo một domain trên thiết bị switch có chức năng làm VTP Server và cấu hình các thiết bị switch khác với vai trò là VTP Client và cho các VTP Client “join” cùng domain với thiết bị làm VTP Server thì các VLAN khi đã cấu hình trên VTP Server sẽ tự động chuyển xuống và đồng bộ với các switch làm VTP Client. Điều này sẽ làm cho việc quản lý của quản trị viên trở nên đơn giản hơn khi chỉ cần thay đổi hay chỉnh sửa các VLAN trên Switch làm VTP Server thì các VTP Client cũng sẽ tự động cập nhật và đồng bộ với nhau.

#### **2.5.3.1 Các chế độ hoạt động của VTP:**

VTP hỗ trợ 3 chế độ hoạt động chính gồm:

- Chế độ Server:
  - Switch trong chế độ này có thể tạo, xóa, sửa các VLAN
  - Thông tin VLAN được truyền đến các Switch khác trong cùng domain VTP
  - Đây là chế độ mặc định khi ta cấu hình VTP trên các thiết bị.
- Chế độ Client:
  - Switch trong chế độ này không thể tạo, xóa và sửa đổi các VLAN
  - Thiết bị chạy chế độ này chỉ có thể nhận, cập nhật và đồng bộ các VLAN từ các VTP Server trong cùng domain
- Chế độ Transparent:
  - Switch trong chế độ này không tham gia và quá trình đồng bộ hóa VLAN
  - Nó không thể truyền thông tin VLAN đến các switch khác nhưng vẫn có thể tạo, xóa sửa các VLAN trên Switch đó.

- Gửi các thông điệp VTP mà không làm thay đổi chúng

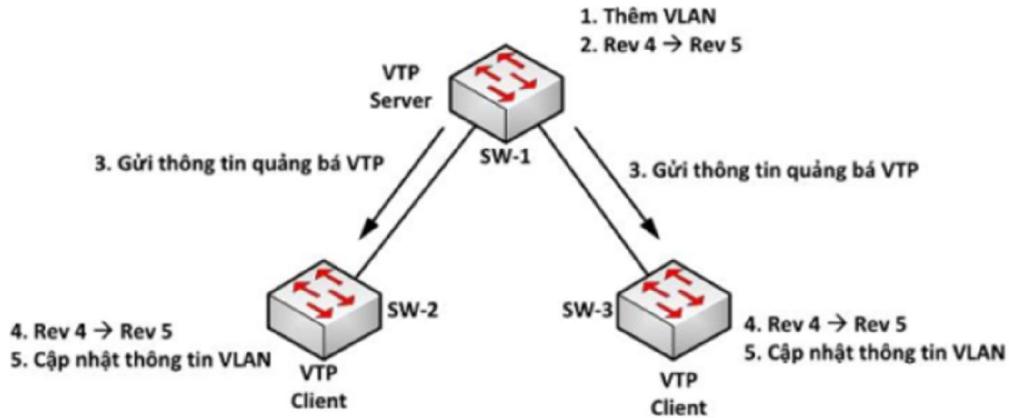
#### 2.5.3.2 Các phiên bản VTP:

- VTP version 1: Phiên bản đầu tiên của VTP, hỗ trợ các tính năng cơ bản
- VTP version 2: Được cải thiện thêm vào tính năng hỗ trợ cho Token Ring VLAN
- VTP version 3: Bổ sung nhiều tính năng như hỗ trợ MST (Multiple Spanning Tree), bảo mật VTP và quản lý vlan private

#### 2.5.3.3 Nguyên lý hoạt động của VTP:

- Quảng bá:
  - Switch khi chạy chế độ VTP Server sẽ gửi thông điệp quảng bá (VTP advertisement) mỗi 5 phút một lần hay khi có sự thay đổi trong quá trình cấu hình VLAN.
  - Các thông tin của gói quảng bá bao gồm: revision number, VLAN ID, tên VLAN và trạng thái
- Revision number:
  - Trong mỗi thông điệp quảng bá đều chứa một revision number
  - Mỗi khi các thông tin cấu hình VLAN trên các VTP Server được thay đổi thì nó sẽ tăng số revision number này lên 1 rồi sau đó sẽ quảng bá gói tin này đi. Khi 1 VTP Client nhận được gói quảng bá và thấy được chỉ số revision number được tăng lên, nó sẽ ngay lập tức cập nhật lại thông tin VLAN đồng bộ với các VTP Server
- Đồng bộ:
  - Switch trong chế độ VTP Client sẽ nhận và đồng bộ thông tin cấu hình VLAN của các switch chạy chế độ VTP Server

- Switch trong chế độ Transparent sẽ không đồng bộ thông tin VLAN nhưng sẽ có nhiệm vụ chuyển đi các thông điệp VTP từ VTP Server.



Hình 2.15 Nguyên lý hoạt động của VTP

#### **2.5.4 OSPF (*Open Shortest Path First*):**

OSPF là một giao thức định tuyến được sử dụng để định tuyến gói tin trong hệ thống mạng nội bộ có quy mô lớn như doanh nghiệp, trường học và bệnh viện. OSPF cho phép các thiết bị trong hệ thống mạng trao đổi thông tin định tuyến với nhau để tìm ra đường đi ngắn nhất đến với các mạng đích.

OSPF sử dụng thuật toán tìm đường đi ngắn nhất (Shortest Path First algorithm) để tính toán đường đi tốt nhất để chuyển gói tin đến với các mạng khác, bên cạnh đó giao thức OSPF còn hỗ trợ cho phép chia nhỏ các mạng xung quanh router thành các khu vực (Area) để giảm tải bớt cho các thiết bị định tuyến.

##### **2.5.4.1 Nguyên tắc hoạt động của OSPF:**

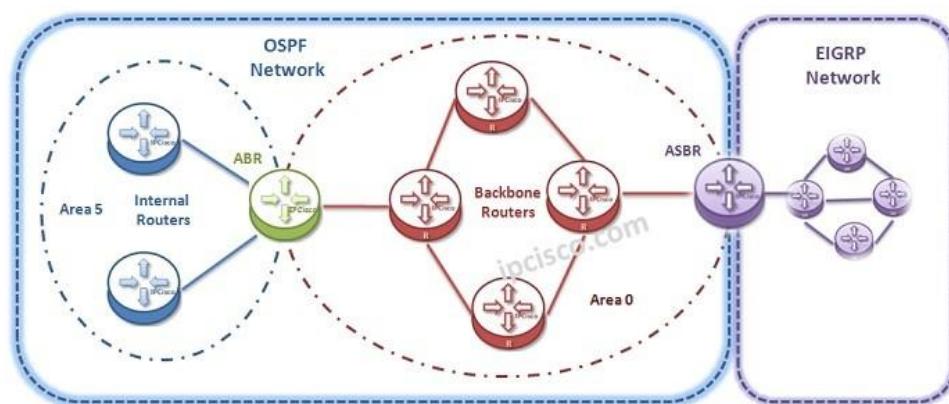
- Phát hiện thiết bị:

- Khi một thiết bị định tuyến chạy giao thức định tuyến động OSPF, nó sẽ gửi các gói tin Hello đến các thiết bị định tuyến chạy giao thức OSPF khác để khám phá các router láng giềng (Neighbors)
- Các router láng giềng sau khi nhận dữ liệu sẽ phản hồi lại bằng gói hello từ đó hình thành nên mối quan hệ láng giềng
- Trao đổi thông tin định tuyến:
  - Các thiết bị router chạy giao thức định tuyến OSPF sẽ trao đổi thông tin định tuyến với nhau thông qua gói LSA. LSA (Link-state Advertisement) là giao thức trao đổi trạng thái liên kết chứa thông tin về bộ định tuyến, các mạng kết nối xung quanh bộ định tuyến, và các thông tin khác.
- Xây dựng cơ sở dữ liệu trạng thái liên kết (LSDB):
  - Thông qua việc trao đổi các gói LSA mà mỗi router sẽ tiến hành xây dựng các LSDB (Link-state Database) bằng việc lưu trữ các thông tin trong gói LSA mà router nhận được.
- Xây dựng bảng định tuyến dựa trên thuật toán SPF:
  - Giao thức OSPF sẽ sử dụng thuật toán shortest path first để tính toán các đường đi ngắn nhất đến các mạng đích dựa trên các thông tin trong cơ sở dữ liệu (Link-state Database).
  - Kết quả cuối cùng mà ta nhận được là bảng định tuyến (ip routing) dựa trên kết quả của thuật toán SPF.

#### 2.5.4.2 Ưu và nhược điểm của OSPF:

- Ưu điểm:
  - Hiệu suất: OSPF sử dụng thuật toán tìm đường đi ngắn nhất nên phù hợp với môi trường mạng lớn cho phép phát hiện và chọn ra đường đi tốt nhất để định tuyến gói tin đến với các mạng đích

- Mở rộng dễ dàng: OSPF tạo điều kiện cho việc mở rộng thêm các mạng con khác một cách dễ dàng và chia sẻ vùng mạng con đó vào miền định tuyến động OSPF.
- Linh hoạt: OSPF cho phép chia các mạng xung quanh bộ định tuyến thành các khu vực (area) nhằm giảm tải bớt gánh nặng cho các thiết bị định tuyến
- Hỗ trợ lựa chọn đường đi dự phòng: OSPF hỗ trợ trong việc tự động lựa chọn định tuyến sang đường đi dự phòng khi có sự cố mạng xảy ra
- Tối ưu hóa đường đi: OSPF sẽ dựa vào thuật toán shortest path first mà lựa chọn đường đi tốt nhất đến với các mạng khác.
- Nhược điểm:
  - Phức tạp khi triển khai: vì là định tuyến động nên khi cấu hình OSPF người quản trị có thể không nắm bắt được hướng đi của các luồng dữ liệu trong hệ thống.
  - Tiêu tốn tài nguyên: Việc triển khai OSPF ngoài thực tế yêu cầu tài nguyên xử lý (CPU) của các thiết bị là cực kỳ lớn để duy trì thông tin trong bảng trạng thái liên kết Link-state database và thực hiện thuật toán shortest path first



Hình 2.16 Mô hình hệ thống mạng sử dụng OSPF

## CHƯƠNG 3. THIẾT KẾ, CẤU HÌNH HỆ THỐNG

### 3.1 Mô tả hệ thống:

Hệ thống mạng nội bộ của công ty cổ phần viễn thông ACT bao gồm 2 khu vực văn phòng gồm Văn phòng công ty số 8 Lê Văn Huân và văn phòng số 1 Lê Văn Huân, phòng máy NOC chứa các thiết bị chính là phần core của cả hệ thống mạng và phòng máy chủ Zone-Server là nơi đặt các hệ thống máy chủ, là nơi lưu trữ dữ liệu nội bộ của công ty và là máy chủ của các mạng internet.

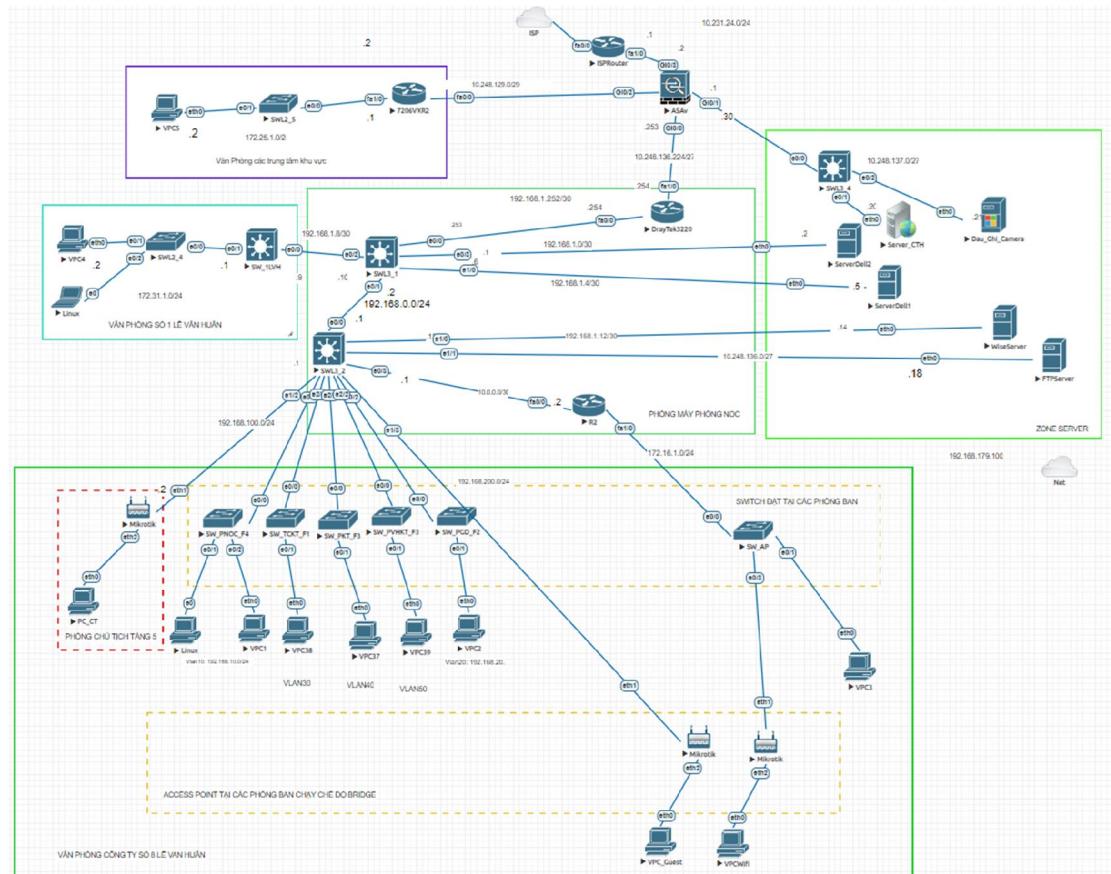
Với văn phòng công ty số 8 Lê Văn Huân bao gồm 5 tầng và có 6 khu vực văn phòng:

- Tầng 1: phòng phó giám đốc công ty,
- Tầng 2: phòng TCKT với 225 nhân viên
- Tầng 3: phòng kế toán với 200 nhân viên, phòng vận hành khai thác với 230 nhân viên
- Tầng 4: phòng NOC,
- Tầng 5: phòng chủ tịch

Hệ thống mạng nội bộ của công ty khi cấu hình cần phải có các thành phần:

- Nhà cung cấp dịch vụ internet (ISP): cung cấp đường mạng internet để hệ thống mạng nội bộ có thể truy cập và sử dụng các dịch vụ internet
- Các tiêu chuẩn bảo mật: Sử dụng tường lửa ASA để tiến hành bảo mật hệ thống mạng, ngăn chặn các tác nhân xâm nhập từ bên ngoài. Cấu hình các Access-list để ngăn chặn các lưu lượng trong nội bộ hệ thống mạng dành cho khách hàng có thể truy cập vào mạng nội bộ.
- Các thiết bị switch: Switch layer 3, Switch Layer 2 của Cisco
- Các thiết bị máy tính.
- Các thiết bị router của cisco: sử dụng để định tuyến các gói tin dữ liệu

### 3.2 Mô hình hệ thống:



Hình 3.1 Mô hình hệ thống mạng nội bộ công ty ACT

### 3.3 Thông tin cài đặt cấu hình hệ thống:

#### 3.3.1 Thông tin VLAN và inter-vlan trong hệ thống:

Bảng 3.1 Thông tin VLAN của hệ thống

Tên SW	VLAN	Port	IP
SW_TCKT_F1	30	e0/1	192.168.30.1/24
SW_PGD_F2	20	e0/1	192.168.20.1/24
SW_PKT_F3	40	e0/1	192.168.40.1/24
SW_PVHKT_F3	50	e0/1	192.168.50.1/24
SW_PNOC_F4	10	e0/1	192.168.10.1/24

### **3.3.2 Thông tin về địa chỉ IP:**

Bảng 3.2 Thông tin IP management

VLAN	Network	Subnet mask	Dải địa chỉ ip
NOC	192.168.10.0	/24	192.168.10.1- 192.168.10.254
VICE- CHAIRMAN	192.168.20.0	/24	192.168.20.1- 192.168.20.254
TCKT	192.168.30.0	/24	192.168.30.1- 192.168.30.254
KETOAN	192.168.40.0	/24	192.168.40.1- 192.168.40.254
VHKT	192.168.50.0	/24	192.168.50.1- 192.168.50.254

### **3.3.3 Thông tin ip trên các thiết bị:**

Thiết bị	Port	Địa chỉ IP
Router ISP	fa0/0	DHCP
	fa1/0	10.231.24.1/24
Firewall ASA V	G0/3	10.231.24.2/24
	G0/0	10.248.136.253/27
	G0/1	10.248.137.1/27
	G0/2	10.248.129.1/29
DrayTek3220	F1/0	10.248.136.254/27
	F0/0	192.168.1.254/30
SWL3_1	e0/0	192.168.1.253/30
	e0/3	192.168.1.1/30
	e1/0	192.168.1.6/30

	e0/2	192.168.1.10/30
	e0/1	192.168.0.2/24
SWL3_2	e0/0	192.168.0.1/24
	e1/0	192.168.1.13/30
	e1/1	10.248.136.1/27
	e0/3	10.0.0.1/30
	e1/3	192.168.200.1/24
	e1/2	192.168.100.1/24
R2	fa0/0	10.0.0.2/30
	fa1/0	172.16.1.1/30
SW_1LVH	e0/0	192.168.1.9/30
	e0/1	172.31.1.1/24
7206VXR2	fa0/0	10.248.129.2/29
	fa1/0	172.25.1.1/24

### 3.3.4 Thông tin ip trên Server:

Máy chủ	Địa chỉ ip
Server Cầu truyền hình	10.248.137.20/27
Server Đầu ghi Camera	10.248.137.21/27
Server Dell2	192.168.1.2/30
Server Dell1	192.168.1.5/30
Wise Server (Server máy chấm công)	192.168.1.14/30
FTP Server	10.248.136.18/27

## 3.4 Cấu hình hệ thống:

### 3.4.1 Cấu hình VLAN:

Ta sẽ cấu hình tạo VLAN trên Switch SWL3\_2 và chia đều cho các phòng ban:

- Vlan 10: Phòng NOC
- Vlan 20: Phòng phó chủ tịch
- Vlan 30: Phòng kỹ thuật
- Vlan 40: Phòng kế toán
- Vlan 50: Phòng vận hành khai thác

#### **Switch SWL3\_2:**

VLAN	Name	Status	Ports
1	default	active	Et2/3
10	NOC	active	
20	VICE-CHAIRMAN	active	
30	TCKT	active	
40	KETOAN	active	
50	VHKT	active	
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
50	enet	100050	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0

--More--

#### **3.4.2 Cấu hình VTP (Virtual Trunking Protocol):**

Tiếp đến ta sẽ cấu hình VTP cho thiết bị Switch layer 3 SWL3\_2 chạy chế độ VTP mode server để có thể đồng bộ hóa VLAN với các switch layer 2 chạy chế độ VTP Client

#### **Switch SWL3\_2:**

```
vtp domain act.vn
vtp mode server
vtp version 2
```

```

SWL3_2
Switch#show vtp status
VTP Version capable          : 1 to 3
VTP version running          : 2
VTP Domain Name              : act.vn
VTP Pruning Mode             : Disabled
VTP Traps Generation         : Disabled
Device ID                    : aabb.cc80.2000
Configuration last modified by 192.168.10.1 at 5-27-24 15:33:18
Local updater ID is 192.168.10.1 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN:
-----
VTP Operating Mode           : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs      : 10
Configuration Revision        : 10
MD5 digest                   : 0x5E 0xA6 0xB9 0x48 0x14 0xF3 0x2B 0x34
                                0x76 0xD6 0x0C 0xCA 0xE3 0x63 0x37 0x9A
Switch#
Switch#
*May 27 17:30:27.874: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ether
net0/3 (not full duplex), with Router FastEthernet0/0 (full duplex).
Switch#

```

Sau đó, ta sẽ cấu hình port trunk trên các thiết bị để các lưu lượng mạng từ các VLAN khác có thể đi qua đoạn đường này.

### **Switch SWL3\_2**

```

interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk

interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk

interface Ethernet2/1
switchport trunk encapsulation dot1q
switchport mode trunk
!

interface Ethernet2/1
switchport trunk encapsulation dot1q

```

```
switchport mode trunk
!
interface Ethernet2/2
    switchport trunk encapsulation dot1q
    switchport mode trunk
!
SW_PNOC_F4
interface Ethernet0/0
    switchport trunk encapsulation dot1q
    switchport mode trunk
```

```
SW_TCKT_F1
interface Ethernet0/0
    switchport trunk encapsulation dot1q
    switchport mode trunk
```

```
SW_PKT_F3
interface Ethernet0/0
    switchport trunk encapsulation dot1q
    switchport mode trunk
```

```
SW_PVHKT_F3
interface Ethernet0/0
    switchport trunk encapsulation dot1q
    switchport mode trunk
```

```
SW_PGD_F2
interface Ethernet0/0
    switchport trunk encapsulation dot1q
```

*switchport mode trunk*

Sau đó ta sẽ cấu hình các thiết bị Switch layer 2 đặt tại các phòng ban chạy chế độ VTP mode client để có thể đồng bộ hóa VLAN với VTP Server

```

SW_TCKT_F1

Switch>
Switch>ENA
Switch#show vtp st
Switch#show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 2
VTP Domain Name          : act.vn
VTP Pruning Mode         : Disabled
VTP Traps Generation    : Disabled
Device ID                : aabb.cc82.2000
Configuration last modified by 192.168.10.1 at 5-27-24 15:33:18

Feature VLAN:
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 10
Configuration Revision    : 10
MD5 digest               : 0x5E 0xA6 0xB9 0x48 0x14 0xF3 0x2B 0x34
                           0x76 0xD6 0x0C 0xCA 0xE3 0x63 0x37 0x9A
Switch#

```

3.4.2.1 Gán port vào VLAN tại các switch layer 2:

#### **SW\_PNOC\_L4:**

*interface Ethernet0/1*

*switchport access vlan 10*

*switchport mode access*

#### **SW\_TCKT\_F1:**

*interface Ethernet0/1*

*switchport access vlan 30*

*switchport mode access*

**SW\_PKT\_F3:**

*interface Ethernet0/1  
switchport access vlan 40  
switchport mode access*

**SW\_PVHKT\_F3:**

*interface Ethernet0/1  
switchport access vlan 50  
switchport mode access*

**SW\_PGD\_F2**

*interface Ethernet0/1  
switchport access vlan 20  
switchport mode access*

Việc gán các cổng vào VLAN nhằm nhóm các thiết bị nối với các cổng đó vào cùng một VLAN để tăng khả năng bảo mật dữ liệu cho mỗi phòng ban.

### **3.4.3 Cấu hình định tuyến động OSPF:**

Cấu hình OSPF trong hệ thống mạng nội bộ của công ty ACT sẽ giúp cho các gói tin mạng có thể tự động định tuyến đến các mạng khác nhau bằng các tuyến đường đi tốt nhất.

Để cấu hình OSPF ta sẽ quảng bá các mạng con xung quanh nối trực tiếp với thiết bị định tuyến sau đó để để các thiết bị định tuyến chia sẻ thông tin định tuyến với nhau để có thể xây dựng bảng định tuyến gồm các đường đi tốt nhất đến các mạng

con khác nhau trong khu vực mạng nội bộ. Bên cạnh đó, ta sẽ cấu hình định tuyến một đường default route đó trên các thiết bị định tuyến và quảng bá đường default-route đó vào vùng định tuyến động để cho các thiết bị có thể định tuyến gói tin ra bên ngoài mạng internet để có thể sử dụng các dịch vụ mạng internet.

### **SWL3\_2:**

```

router ospf 1
network 10.0.0.0 0.0.0.3 area 0
network 10.248.136.0 0.0.0.31 area 0
network 192.168.0.0 0.0.0.255 area 0
network 192.168.1.12 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
default-information originate
ip route 0.0.0.0 0.0.0.0 192.168.0.2
ip route 192.168.100.0 255.255.255.0 10.0.0.2

```

```

S*   0.0.0.0/0 [1/0] via 192.168.0.2
      10.0.0.0/8 is variably subnetted, 8 subnets, 5 masks
C       10.0.0.0/30 is directly connected, Ethernet0/3
L       10.0.0.1/32 is directly connected, Ethernet0/3
O       10.231.24.0/24 [110/31] via 192.168.0.2, 00:37:59, Ethernet0/0
O       10.248.129.0/29 [110/31] via 192.168.0.2, 00:37:59, Ethernet0/0
C       10.248.136.0/27 is directly connected, Ethernet1/1
L       10.248.136.1/32 is directly connected, Ethernet1/1
O       10.248.136.224/27 [110/21] via 192.168.0.2, 00:38:09, Ethernet0/0
O       10.248.137.0/27 [110/31] via 192.168.0.2, 00:37:59, Ethernet0/0
      172.16.0.0/24 is subnetted, 1 subnets
O         172.16.1.0 [110/11] via 10.0.0.2, 00:38:09, Ethernet0/3
      172.25.0.0/24 is subnetted, 1 subnets
O         172.25.1.0 [110/32] via 192.168.0.2, 00:37:59, Ethernet0/0
      172.31.0.0/24 is subnetted, 1 subnets
O         172.31.1.0 [110/30] via 192.168.0.2, 00:38:09, Ethernet0/0
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.0.0/24 is directly connected, Ethernet0/0
L         192.168.0.1/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
O         192.168.1.0/30 [110/20] via 192.168.0.2, 00:38:09, Ethernet0/0
O         192.168.1.4/30 [110/20] via 192.168.0.2, 00:38:09, Ethernet0/0
O         192.168.1.8/30 [110/20] via 192.168.0.2, 00:38:09, Ethernet0/0

```

Hình 3.2 Đường định tuyến trên SWL3\_2

### **SWL3\_1:**

```

router ospf 1
  network 192.168.0.0 0.0.0.255 area 0
  network 192.168.1.0 0.0.0.3 area 0
  network 192.168.1.4 0.0.0.3 area 0
  network 192.168.1.8 0.0.0.3 area 0
  network 192.168.1.252 0.0.0.3 area 0
  default-information originate
  ip route 0.0.0.0 0.0.0.0 192.168.1.254

```

```

SWL3_1
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
a - application route
+ - replicated route, % - next hop override

Gateway of last resort is 192.168.1.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.1.254
      10.0.0.0/8 is variably subnetted, 6 subnets, 4 masks
O        10.0.0.0/30 [110/20] via 192.168.0.1, 00:46:59, Ethernet0/1
O        10.231.24.0/24 [110/21] via 192.168.1.254, 00:46:49, Ethernet0/0
O        10.248.129.0/29 [110/21] via 192.168.1.254, 00:46:49, Ethernet0/0
O        10.248.136.0/27 [110/20] via 192.168.0.1, 00:46:59, Ethernet0/1
O        10.248.136.224/27 [110/11] via 192.168.1.254, 00:47:24, Ethernet0/0
O        10.248.137.0/27 [110/21] via 192.168.1.254, 00:46:49, Ethernet0/0
      172.16.0.0/24 is subnetted, 1 subnets
O        172.16.1.0 [110/21] via 192.168.0.1, 00:46:49, Ethernet0/1
      172.25.0.0/24 is subnetted, 1 subnets
O        172.25.1.0 [110/22] via 192.168.1.254, 00:46:39, Ethernet0/0
      172.31.0.0/24 is subnetted, 1 subnets

SWL3_2
C      10.248.136.0/27 is directly connected, Ethernet1/1
L      10.248.136.1/32 is directly connected, Ethernet1/1
O      10.248.136.224/27 [110/21] via 192.168.0.2, 00:48:17, Ethernet0/0
O      10.248.137.0/27 [110/31] via 192.168.0.2, 00:48:07, Ethernet0/0
      172.16.0.0/24 is subnetted, 1 subnets
O        172.16.1.0 [110/11] via 10.0.0.2, 00:48:17, Ethernet0/3
      172.25.0.0/24 is subnetted, 1 subnets
O        172.25.1.0 [110/32] via 192.168.0.2, 00:48:07, Ethernet0/0
      172.31.0.0/24 is subnetted, 1 subnets
O        172.31.1.0 [110/30] via 192.168.0.2, 00:48:17, Ethernet0/0
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.0.0/24 is directly connected, Ethernet0/0
L          192.168.0.1/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
O        192.168.1.0/30 [110/20] via 192.168.0.2, 00:48:17, Ethernet0/0
O        192.168.1.4/30 [110/20] via 192.168.0.2, 00:48:17, Ethernet0/0
O        192.168.1.8/30 [110/20] via 192.168.0.2, 00:48:17, Ethernet0/0
C          192.168.1.12/30 is directly connected, Ethernet1/0
L          192.168.1.13/32 is directly connected, Ethernet1/0
O        192.168.1.252/30 [110/20] via 192.168.0.2, 00:48:17, Ethernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.10.0/24 is directly connected, Vlan10
L          192.168.10.1/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks

```

Hình 3.3 Các đường định tuyến trên SWL3\_1

**SW\_1LVH:**

```
router ospf 1
network 172.31.1.0 0.0.0.255 area 0
network 192.168.1.8 0.0.0.3 area 0
ip route 0.0.0.0 0.0.0.0 192.168.1.10
```

The image shows two terminal windows for the switch SW\_1LVH. The top window displays the output of the command `Switch#show ip route`, which lists various network routes and their details. The bottom window displays the output of the command `Switch#show ip route`, which lists more network routes and their details.

```
SW_1LVH
Switch#show ip route
Codes: L - local, C - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
      a - application route
      + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

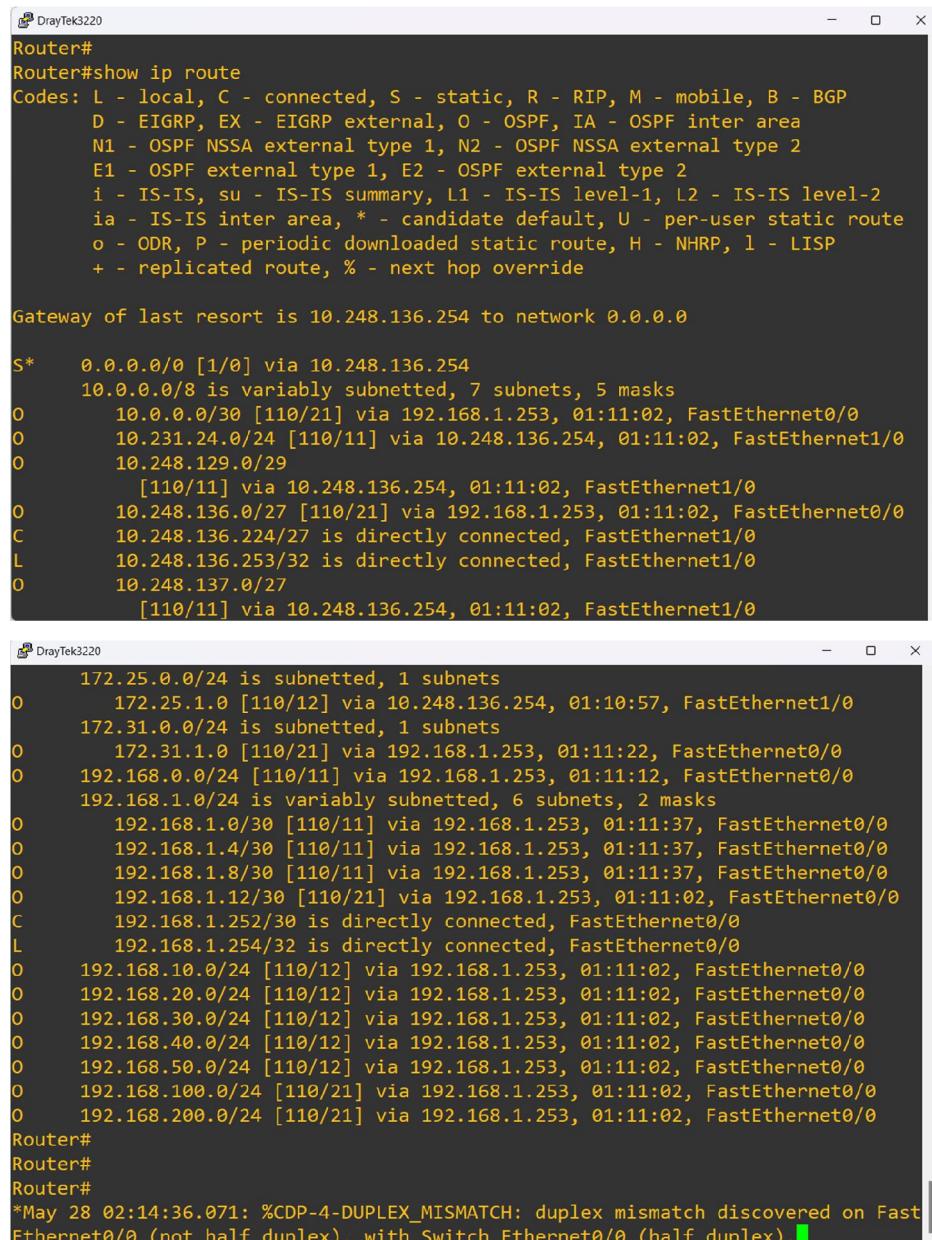
S*   0.0.0.0/0 [1/0] via 192.168.1.10
    10.0.0.0/8 is variably subnetted, 6 subnets, 4 masks
O     10.0.0.0/30 [110/30] via 192.168.1.10, 01:06:22, Ethernet0/0
O     10.231.24.0/24 [110/31] via 192.168.1.10, 01:06:22, Ethernet0/0
O     10.248.129.0/29 [110/31] via 192.168.1.10, 01:06:22, Ethernet0/0
O     10.248.136.0/27 [110/30] via 192.168.1.10, 01:06:22, Ethernet0/0
O     10.248.136.224/27 [110/21] via 192.168.1.10, 01:06:52, Ethernet0/0
O     10.248.137.0/27 [110/31] via 192.168.1.10, 01:06:22, Ethernet0/0
O     172.16.0.0/24 is subnetted, 1 subnets
O       172.16.1.0 [110/31] via 192.168.1.10, 01:06:22, Ethernet0/0
O     172.25.0.0/24 is subnetted, 1 subnets

SW_1LVH
Switch#show ip route
O     172.25.1.0 [110/32] via 192.168.1.10, 01:06:12, Ethernet0/0
    172.31.0.0/16 is variably subnetted, 2 subnets, 2 masks
C     172.31.1.0/24 is directly connected, Ethernet0/1
L     172.31.1.1/32 is directly connected, Ethernet0/1
O     192.168.0.0/24 [110/20] via 192.168.1.10, 01:06:32, Ethernet0/0
    192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
O       192.168.1.0/30 [110/20] via 192.168.1.10, 01:06:52, Ethernet0/0
O       192.168.1.4/30 [110/20] via 192.168.1.10, 01:06:52, Ethernet0/0
C       192.168.1.8/30 is directly connected, Ethernet0/0
L       192.168.1.9/32 is directly connected, Ethernet0/0
O       192.168.1.12/30 [110/30] via 192.168.1.10, 01:06:22, Ethernet0/0
O       192.168.1.252/30 [110/20] via 192.168.1.10, 01:06:52, Ethernet0/0
O       192.168.10.0/24 [110/21] via 192.168.1.10, 01:06:22, Ethernet0/0
O       192.168.20.0/24 [110/21] via 192.168.1.10, 01:06:22, Ethernet0/0
O       192.168.30.0/24 [110/21] via 192.168.1.10, 01:06:22, Ethernet0/0
O       192.168.40.0/24 [110/21] via 192.168.1.10, 01:06:22, Ethernet0/0
O       192.168.50.0/24 [110/21] via 192.168.1.10, 01:06:22, Ethernet0/0
O       192.168.100.0/24 [110/30] via 192.168.1.10, 01:06:22, Ethernet0/0
O       192.168.200.0/24 [110/30] via 192.168.1.10, 01:06:22, Ethernet0/0
Switch#
Switch#
Switch#
Switch#
Switch#
```

Hình 3.4 Các đường định tuyến học được của SW\_1LVH

### DrayTek3220:

```
router ospf 1
network 10.248.136.224 0.0.0.31 area 0
network 192.168.1.252 0.0.0.3 area 0
default-information originate
```



The screenshot shows two terminal windows for the DrayTek3220 router. The top window displays the output of the command `show ip route`, listing various network routes with their metrics and interfaces. The bottom window shows the output of `show ip route` for a specific subnet (172.25.0.0/24) and then ends with an error message about a duplex mismatch.

```
Router# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      + - replicated route, % - next hop override

Gateway of last resort is 10.248.136.254 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 10.248.136.254
      10.0.0.0/8 is variably subnetted, 7 subnets, 5 masks
O     10.0.0.0/30 [110/21] via 192.168.1.253, 01:11:02, FastEthernet0/0
O     10.231.24.0/24 [110/11] via 10.248.136.254, 01:11:02, FastEthernet1/0
O     10.248.129.0/29
          [110/11] via 10.248.136.254, 01:11:02, FastEthernet1/0
O     10.248.136.0/27 [110/21] via 192.168.1.253, 01:11:02, FastEthernet0/0
C     10.248.136.224/27 is directly connected, FastEthernet1/0
L     10.248.136.253/32 is directly connected, FastEthernet1/0
O     10.248.137.0/27
          [110/11] via 10.248.136.254, 01:11:02, FastEthernet1/0

Router# show ip route 172.25.0.0/24
172.25.0.0/24 is subnetted, 1 subnets
O     172.25.1.0 [110/12] via 10.248.136.254, 01:10:57, FastEthernet1/0
172.31.0.0/24 is subnetted, 1 subnets
O     172.31.1.0 [110/21] via 192.168.1.253, 01:11:22, FastEthernet0/0
O     192.168.0.0/24 [110/11] via 192.168.1.253, 01:11:12, FastEthernet0/0
192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
O     192.168.1.0/30 [110/11] via 192.168.1.253, 01:11:37, FastEthernet0/0
O     192.168.1.4/30 [110/11] via 192.168.1.253, 01:11:37, FastEthernet0/0
O     192.168.1.8/30 [110/11] via 192.168.1.253, 01:11:37, FastEthernet0/0
O     192.168.1.12/30 [110/21] via 192.168.1.253, 01:11:02, FastEthernet0/0
C     192.168.1.252/30 is directly connected, FastEthernet0/0
L     192.168.1.254/32 is directly connected, FastEthernet0/0
O     192.168.10.0/24 [110/12] via 192.168.1.253, 01:11:02, FastEthernet0/0
O     192.168.20.0/24 [110/12] via 192.168.1.253, 01:11:02, FastEthernet0/0
O     192.168.30.0/24 [110/12] via 192.168.1.253, 01:11:02, FastEthernet0/0
O     192.168.40.0/24 [110/12] via 192.168.1.253, 01:11:02, FastEthernet0/0
O     192.168.50.0/24 [110/12] via 192.168.1.253, 01:11:02, FastEthernet0/0
O     192.168.100.0/24 [110/21] via 192.168.1.253, 01:11:02, FastEthernet0/0
O     192.168.200.0/24 [110/21] via 192.168.1.253, 01:11:02, FastEthernet0/0

Router#
Router#
Router#
*May 28 02:14:36.071: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Fast
Ethernet0/0 (not half duplex), with Switch Ethernet0/0 (half duplex).*
```

Hình 3.5 Các đường định tuyến trên DrayTek 3220

**7206XR2:**

```
router ospf 1
network 10.248.129.0 0.0.0.7 area 0
network 172.25.1.0 0.0.0.255 area 0
default-information originate
ip route 0.0.0.0 0.0.0.0 10.248.129.1
```

```

7206VXR2
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.248.129.1 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 10.248.129.1
      10.0.0.0/8 is variably subnetted, 7 subnets, 5 masks
O     10.0.0.0/30 [110/32] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     10.231.24.0/24 [110/11] via 10.248.129.1, 01:18:06, FastEthernet0/0
C     10.248.129.0/29 is directly connected, FastEthernet0/0
L     10.248.129.2/32 is directly connected, FastEthernet0/0
O     10.248.136.0/27 [110/32] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     10.248.136.224/27
          [110/11] via 10.248.129.1, 01:18:06, FastEthernet0/0
O     10.248.137.0/27 [110/11] via 10.248.129.1, 01:18:06, FastEthernet0/0
      172.16.0.0/24 is subnetted, 1 subnets
O     172.16.1.0 [110/33] via 10.248.129.1, 01:18:01, FastEthernet0/0
      172.25.0.0/16 is variably subnetted, 2 subnets, 2 masks
C     172.25.1.0/24 is directly connected, FastEthernet1/0
L     172.25.1.1/32 is directly connected, FastEthernet1/0
      172.31.0.0/24 is subnetted, 1 subnets
O     172.31.1.0 [110/32] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.0.0/24 [110/22] via 10.248.129.1, 01:18:01, FastEthernet0/0
      192.168.1.0/30 is subnetted, 5 subnets
O     192.168.1.0 [110/22] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.1.4 [110/22] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.1.8 [110/22] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.1.12 [110/32] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.1.252 [110/12] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.10.0/24 [110/23] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.20.0/24 [110/23] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.30.0/24 [110/23] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.40.0/24 [110/23] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.50.0/24 [110/23] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.100.0/24 [110/32] via 10.248.129.1, 01:18:01, FastEthernet0/0
O     192.168.200.0/24 [110/32] via 10.248.129.1, 01:18:01, FastEthernet0/0

```

Hình 3.6 Các đường định tuyến trên router 7206XR2

Cấu hình định tuyến động trên tường lửa ASA:

**ASAv:**

```

router ospf 1
  network 10.231.24.0 255.255.255.0 area 0
  network 10.248.129.0 255.255.255.248 area 0
  network 10.248.136.224 255.255.255.224 area 0
  network 10.248.137.0 255.255.255.224 area 0
  log-adj-changes
  default-information originate
!
route internet 0.0.0.0 0.0.0.0 10.231.24.1 1
route inside 172.16.1.0 255.255.255.0 10.248.136.253 1
route inside 172.31.1.0 255.255.255.0 10.248.136.253 1
route inside 192.168.0.0 255.255.0.0 10.248.136.253 1
route inside 192.168.100.0 255.255.255.0 10.248.136.253 1

```

### **3.4.4 Cấu hình bảo mật trên thiết bị tường lửa ASA:**

Việc cấu hình tường lửa nhằm mục đích chặn những lưu lượng mạng không mong muốn có thể xâm nhập vào các cơ sở dữ liệu và hệ thống máy chủ của công ty ACT. Bằng cách viết các tập luật Access-list ta sẽ ngăn chặn hoặc cho phép các lưu lượng mạng vào hệ thống mạng nội bộ, ta sẽ chia khu vực mạng xung quanh tường lửa ra làm 4 khu vực:

- INSDIE: khu vực mạng nội bộ
- OUTSIDE: khu vực mạng của các trung tâm khu vực
- DMZ: khu vực máy chủ của công ty ACT
- INTERNET: khu vực mạng bên ngoài internet

Đầu tiên, ta sẽ cấu hình đặt tên các vùng mạng xung quanh tường lửa trên các interface của tường lửa và cấu hình mức độ bảo mật cho từng vùng:

```

interface GigabitEthernet0/0
  nameif inside
  security-level 100
  ip address 10.248.136.254 255.255.255.224
!

interface GigabitEthernet0/1
  nameif dmz
  security-level 70
  ip address 10.248.137.30 255.255.255.224
!

interface GigabitEthernet0/2
  nameif outside
  security-level 0
  ip address 10.248.129.1 255.255.255.248
!

interface GigabitEthernet0/3
  nameif internet
  security-level 0
  ip address 10.231.24.2 255.255.255.0
!

```

Sau đó ta sẽ cấu hình NAT cho vùng DMZ:

```

object network DMZ-INTERNET
  nat (dmz,outside) dynamic interface

```

Tiếp đến, ta sẽ cấu hình viết các tập luật cho phép các lưu lượng mạng của các trung tâm khu vực có thể giao tiếp được với các phòng ban của mạng nội bộ nhưng không cho phép kết nối tới các khu vực máy chủ chứa các thông tin nhạy cảm và dịch vụ của công ty:

```
access-list INSIDE-OUTSIDE extended permit tcp any any eq www  
access-list INSIDE-OUTSIDE extended permit udp any any eq bootps  
access-list INSIDE-OUTSIDE extended permit udp any any eq bootpc  
access-list INSIDE-OUTSIDE extended permit icmp any 172.31.1.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit icmp any 172.16.1.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit icmp any 192.168.10.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit icmp any 192.168.20.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit icmp any 192.168.30.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit icmp any 192.168.40.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit icmp any 192.168.50.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit icmp any 192.168.100.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit icmp any 192.168.200.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit ip any 172.31.1.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit ip any 172.16.1.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit ip any 192.168.10.0  
255.255.255.0  
access-list INSIDE-OUTSIDE extended permit ip any 192.168.20.0  
255.255.255.0
```

```

access-list INSIDE-OUTSIDE extended permit ip any 192.168.30.0
255.255.255.0
access-list INSIDE-OUTSIDE extended permit ip any 192.168.40.0
255.255.255.0
access-list INSIDE-OUTSIDE extended permit ip any 192.168.50.0
255.255.255.0
access-list INSIDE-OUTSIDE extended permit ip any 192.168.100.0
255.255.255.0
access-list INSIDE-OUTSIDE extended permit ip any 192.168.200.0
255.255.255.0

```

Tiếp đó, ta sẽ cấu hình access-list cho phép các thiết bị thuộc vùng mạng DMZ là vùng chứa máy chủ của công ty có thể tương tác với các thiết bị thuộc hệ thống mạng nội bộ:

```

access-list INSIDE-DMZ extended permit icmp any any
access-list INSIDE-DMZ extended permit tcp any any eq www
access-list INSIDE-DMZ extended permit udp any any eq bootps
access-list INSIDE-DMZ extended permit udp any any eq bootpc

```

Sau đó, ta sẽ cấu hình Access-list cho phép các thiết bị trong hệ thống mạng nội bộ có thể ra ngoài internet và sử dụng các dịch vụ mạng gồm lướt web và gửi mail và ngăn chặn từ chối các dịch vụ khác vào hệ thống mạng

```

access-list INSIDE-INTERNET extended permit tcp any any
access-list INSIDE-INTERNET extended permit tcp any any eq www
access-list INSIDE-INTERNET extended permit udp any any eq bootps
access-list INSIDE-INTERNET extended permit udp any any eq bootpc
access-list INSIDE-INTERNET extended permit icmp any any

```

Cuối cùng ta sẽ đặt các tập luật vừa cấu hình lên các cổng trên tường lửa để các tập luật được thực thi tiến hành bảo mật cho hệ thống mạng nội bộ

*access-group INSIDE-DMZ in interface dmz  
 access-group INSIDE-OUTSIDE in interface outside  
 access-group INSIDE-INTERNET in interface internet*

### **3.4.5 Cấu hình DHCP Server:**

Ta sẽ cấu hình cho thiết bị router DrayTek 3220 làm DHCP-Server để cấp địa chỉ ip cho các thiết bị máy tính của các phòng ban trong mạng nội bộ

#### **DrayTek3220:**

```
ip dhcp pool Vlan10_IT
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8
!
ip dhcp pool Vlan20_OFFICE
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
dns-server 8.8.8.8
!
ip dhcp pool Vlan10_It
!
ip dhcp pool Chairman_AP
network 192.168.100.0 255.255.255.0
default-router 192.168.100.1
dns-server 8.8.8.8
!
ip dhcp pool TCKT
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 8.8.8.8
```

```

!
ip dhcp pool KETOAN
network 192.168.40.0 255.255.255.0
default-router 192.168.40.1
dns-server 8.8.8.8
!
ip dhcp pool VHKT
network 192.168.50.0 255.255.255.0
default-router 192.168.50.1
dns-server 8.8.8.8
!
```

Sau đó ta sẽ cấu hình ip-helper address lên VLAN của các phòng ban trên

### SWL3\_2

#### **SWL3\_2:**

```

interface Vlan10
ip address 192.168.10.1 255.255.255.0
ip access-group 1 out
ip helper-address 192.168.1.254
!
interface Vlan20
ip address 192.168.20.1 255.255.255.0
ip access-group 1 out
ip helper-address 192.168.1.254
!
interface Vlan30
ip address 192.168.30.1 255.255.255.0
ip access-group 1 out
ip helper-address 192.168.1.254
!
```

```

interface Vlan40
ip address 192.168.40.1 255.255.255.0
ip access-group 1 out
ip helper-address 192.168.1.254
!
interface Vlan50
ip address 192.168.50.1 255.255.255.0
ip access-group 1 out
ip helper-address 192.168.1.254
!
```

### **3.4.6 Cấu hình Access-list:**

Ta sẽ cấu hình access-list để ngăn chặn lưu lượng mạng wifi ACT\_Guest không thể kết nối tới mạng nội bộ mà chỉ có thể đi ra được internet

#### **SWL3\_2:**

```
access-list 1 deny 192.168.200.0 0.0.0.255
```

```
access-list 1 permit any
```

```
interface Vlan10
```

```
ip address 192.168.10.1 255.255.255.0
```

```
ip access-group 1 out
```

```
ip helper-address 192.168.1.254
```

```
!
```

```
interface Vlan20
```

```
ip address 192.168.20.1 255.255.255.0
```

```
ip access-group 1 out
```

```
ip helper-address 192.168.1.254
```

```
!
```

```
interface Vlan30
```

```
ip address 192.168.30.1 255.255.255.0
```

```
ip access-group 1 out
```

```

ip helper-address 192.168.1.254
!
interface Vlan40
  ip address 192.168.40.1 255.255.255.0
  ip access-group 1 out
  ip helper-address 192.168.1.254
!
interface Vlan50
  ip address 192.168.50.1 255.255.255.0
  ip access-group 1 out
  ip helper-address 192.168.1.254
!
```

**SWL3\_1:**

```

access-list 1 deny 192.168.200.0 0.0.0.255
access-list 1 permit any
interface Ethernet0/2
  no switchport
  ip address 192.168.1.10 255.255.255.252
  ip access-group 1 out
```

**7206XRV2:**

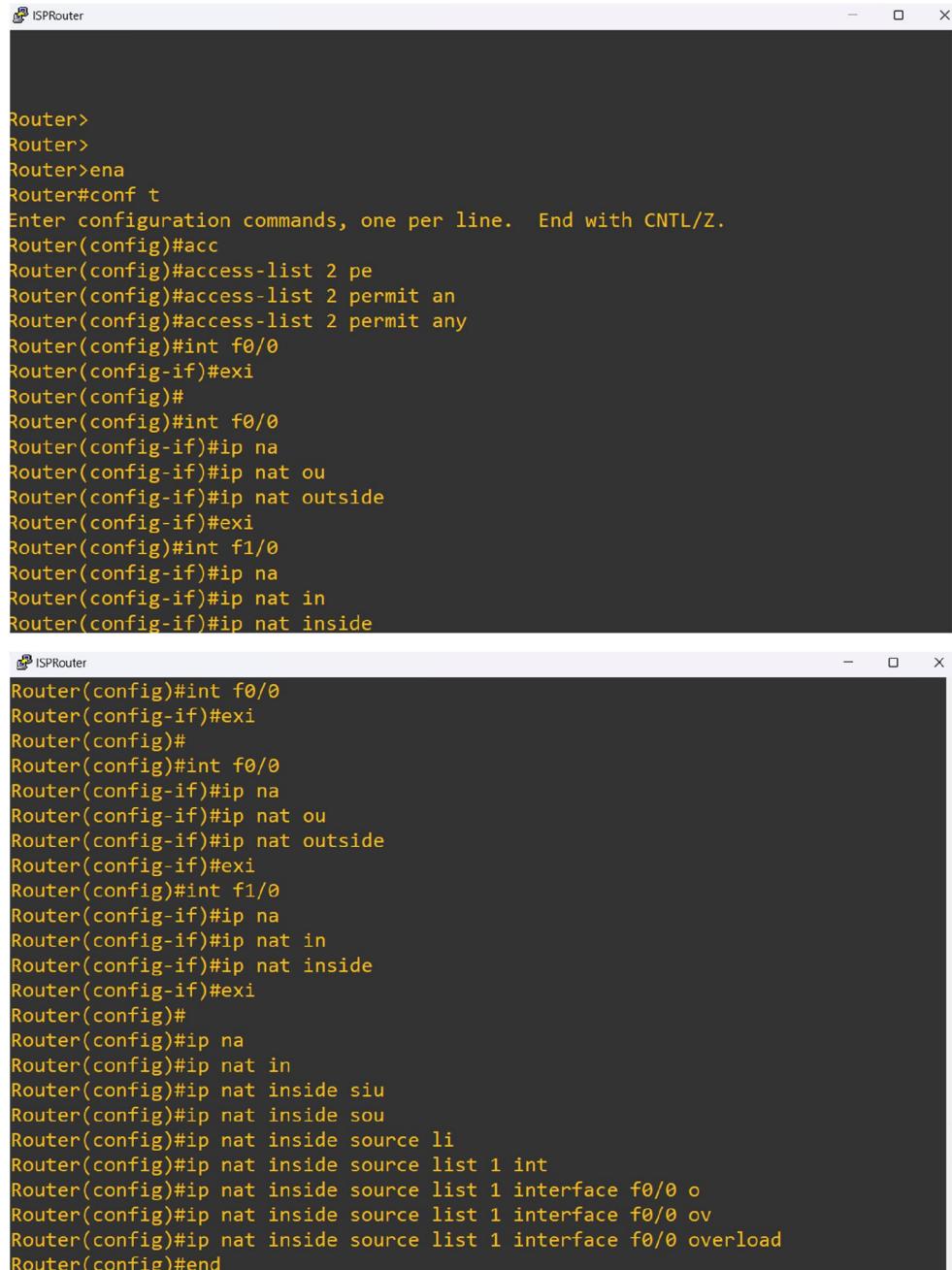
```

access-list 1 deny 192.168.200.0 0.0.0.255
access-list 1 permit any
interface FastEthernet0/0
  ip address 10.248.129.2 255.255.255.248
  ip access-group 1 in
```

***3.4.7 Cấu hình NAT ra internet:***

Trên thiết bị router ISP em sẽ kết nối trực tiếp thiết bị này với router của nhà cung cấp dịch vụ sau đó sẽ cấu hình NAT trên router này để cho các thiết bị trong

mạng nội bộ có thể ra được internet một cách an toàn thông qua việc chuyển đổi các địa chỉ ip private thành địa chỉ ip public



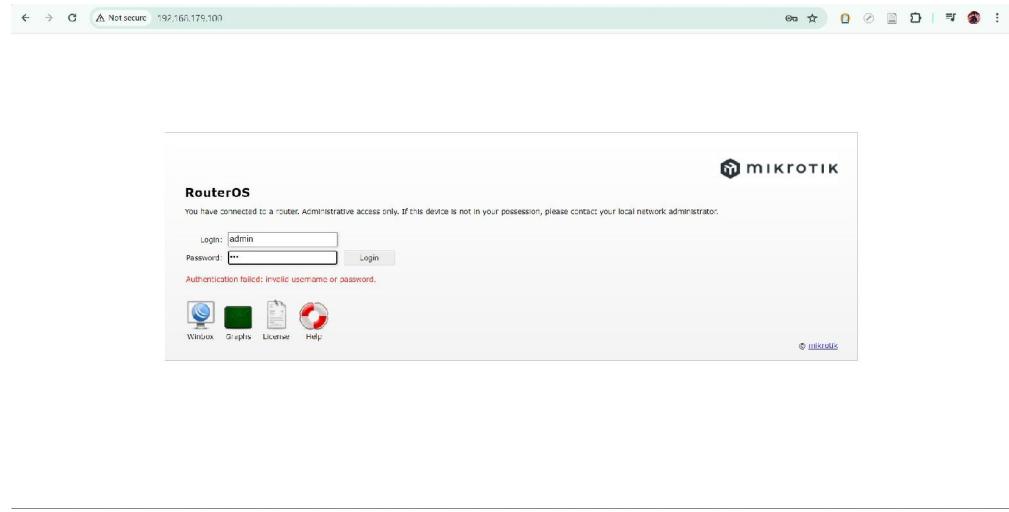
```
Router>
Router>
Router>ena
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#acc
Router(config)#access-list 2 pe
Router(config)#access-list 2 permit an
Router(config)#access-list 2 permit any
Router(config)#int f0/0
Router(config-if)#exi
Router(config)#
Router(config)#int f0/0
Router(config-if)#ip na
Router(config-if)#ip nat ou
Router(config-if)#ip nat outside
Router(config-if)#exi
Router(config)#int f1/0
Router(config-if)#ip na
Router(config-if)#ip nat in
Router(config-if)#ip nat inside

Router(config)#int f0/0
Router(config-if)#exi
Router(config)#
Router(config)#int f0/0
Router(config-if)#ip na
Router(config-if)#ip nat ou
Router(config-if)#ip nat outside
Router(config-if)#exi
Router(config)#int f1/0
Router(config-if)#ip na
Router(config-if)#ip nat in
Router(config-if)#ip nat inside
Router(config-if)#exi
Router(config)#
Router(config)#ip na
Router(config)#ip nat in
Router(config)#ip nat inside siu
Router(config)#ip nat inside sou
Router(config)#ip nat inside source li
Router(config)#ip nat inside source list 1 int
Router(config)#ip nat inside source list 1 interface f0/0 o
Router(config)#ip nat inside source list 1 interface f0/0 ov
Router(config)#ip nat inside source list 1 interface f0/0 overload
Router(config)#end
```

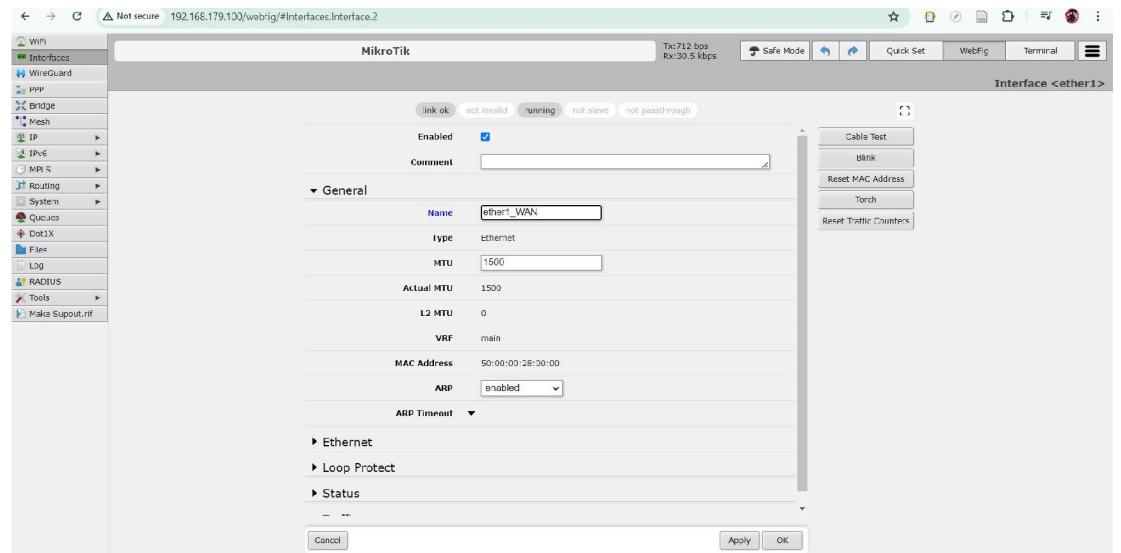
### 3.4.8 Cấu hình WiFi:

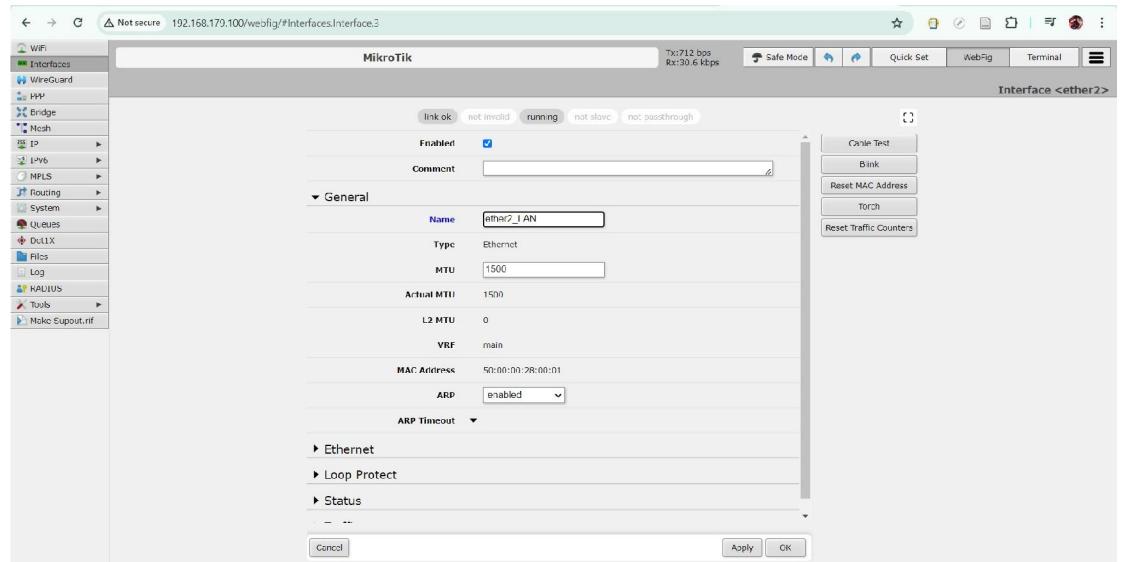
Trong mô hình này em sẽ sử dụng các thiết bị WiFi của Mikrotik

Đầu tiên ta sẽ đăng nhập vào giao diện cấu hình của wifi mikrotik:

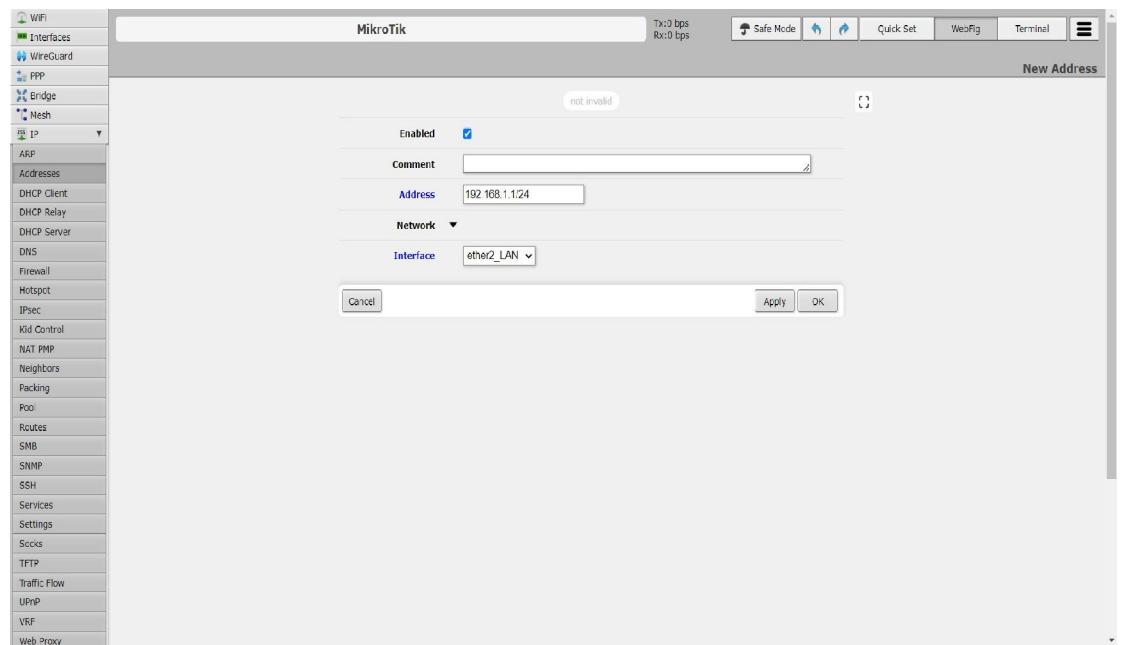


Sau khi vào giao diện đăng nhập ta sẽ đổi tên các interface của WiFi Mikrotik:

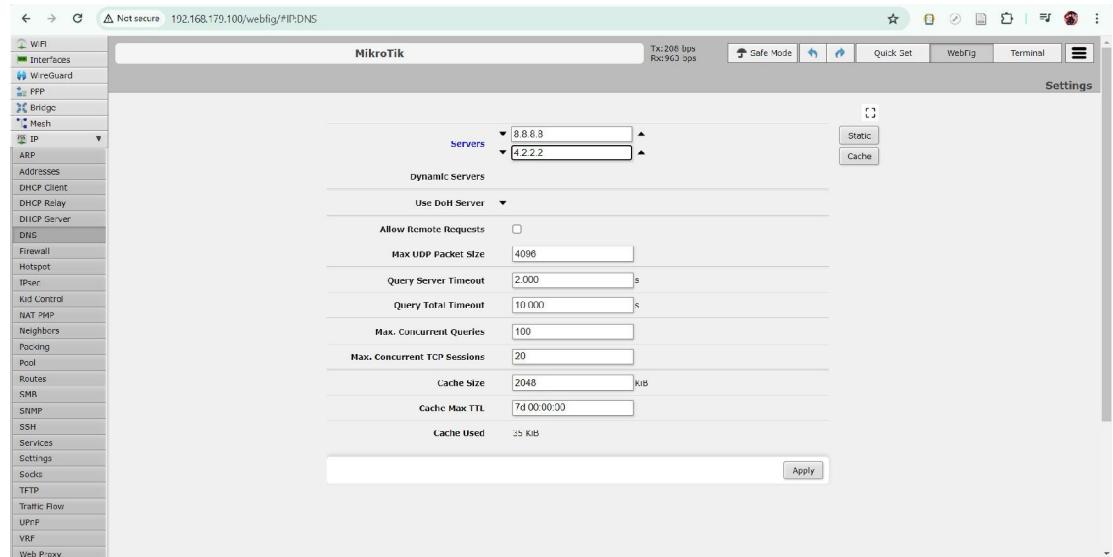




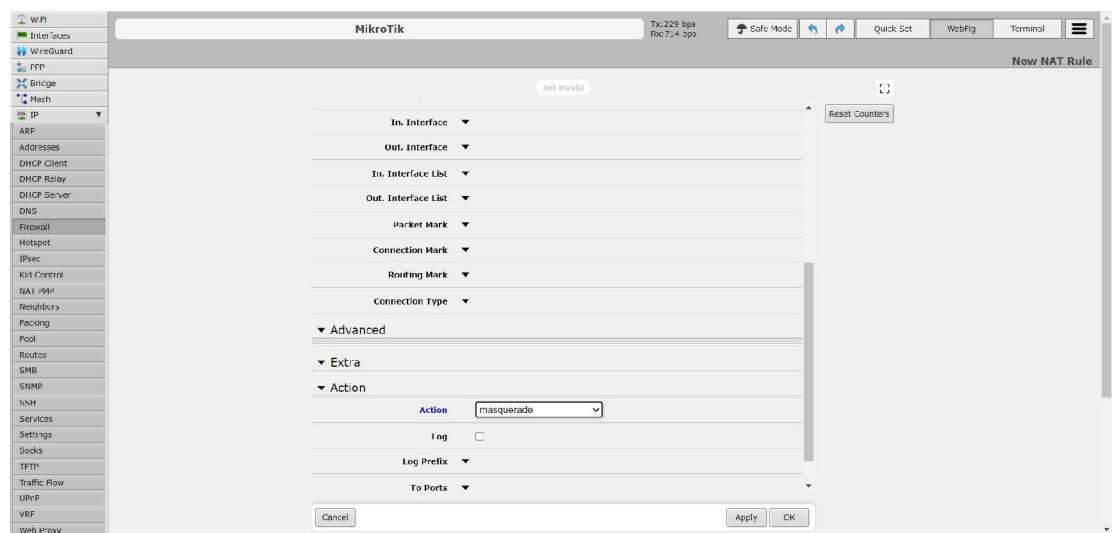
Sau đó ta sẽ đặt địa chỉ ip cho các cổng trên interface:



Sau đó ta sẽ cấu hình DNS Server trên thiết bị wifi:

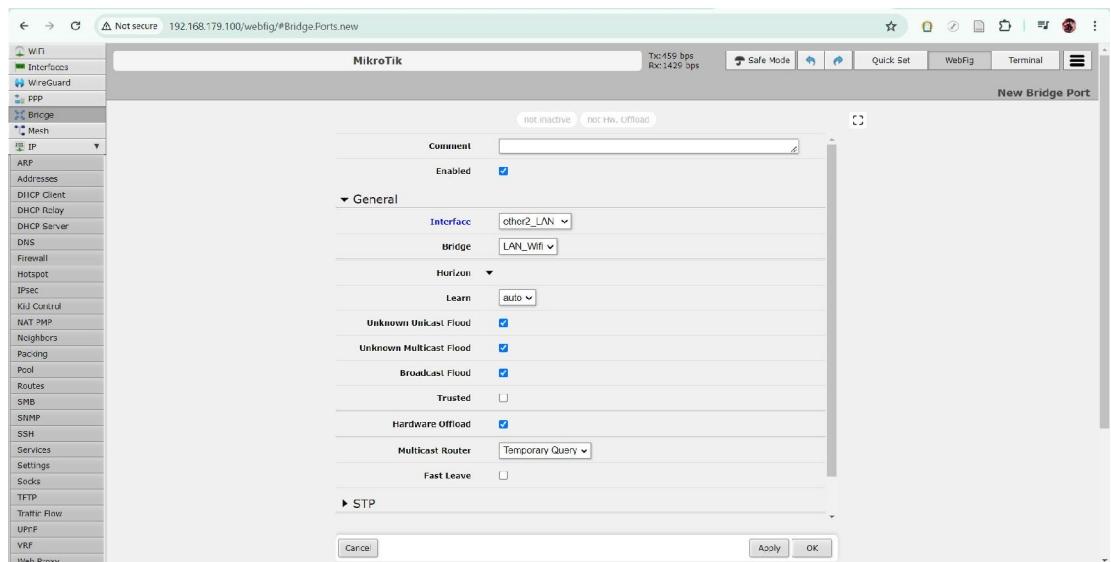
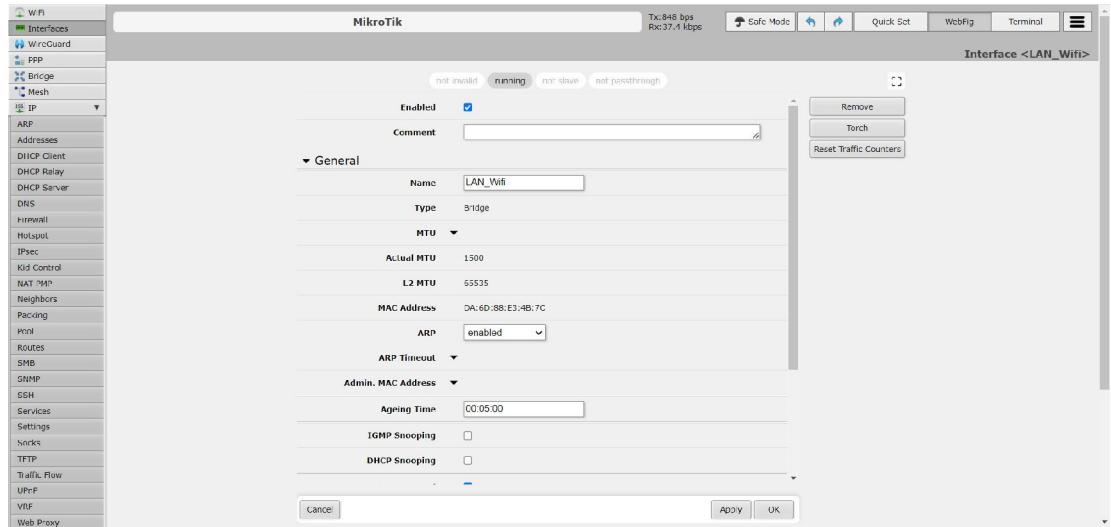


Tiếp theo ta sẽ cấu hình NAT cho Wifi để che giấu địa chỉ ip của thiết bị khi đi ra các khu vực mạng khác



Tiếp đến, ta sẽ cấu hình default route để cho thiết bị router WiFi có thể định tuyến gói tin ra ngoài mạng internet cũng như có thể đi vào mạng nội bộ.

Sau đó, em sẽ cấu hình bridge trên thiết bị wifi để có tránh xung đột với các địa chỉ dhcp mà thiết bị wifi cấp phát với các địa chỉ ip có trong mạng nội bộ



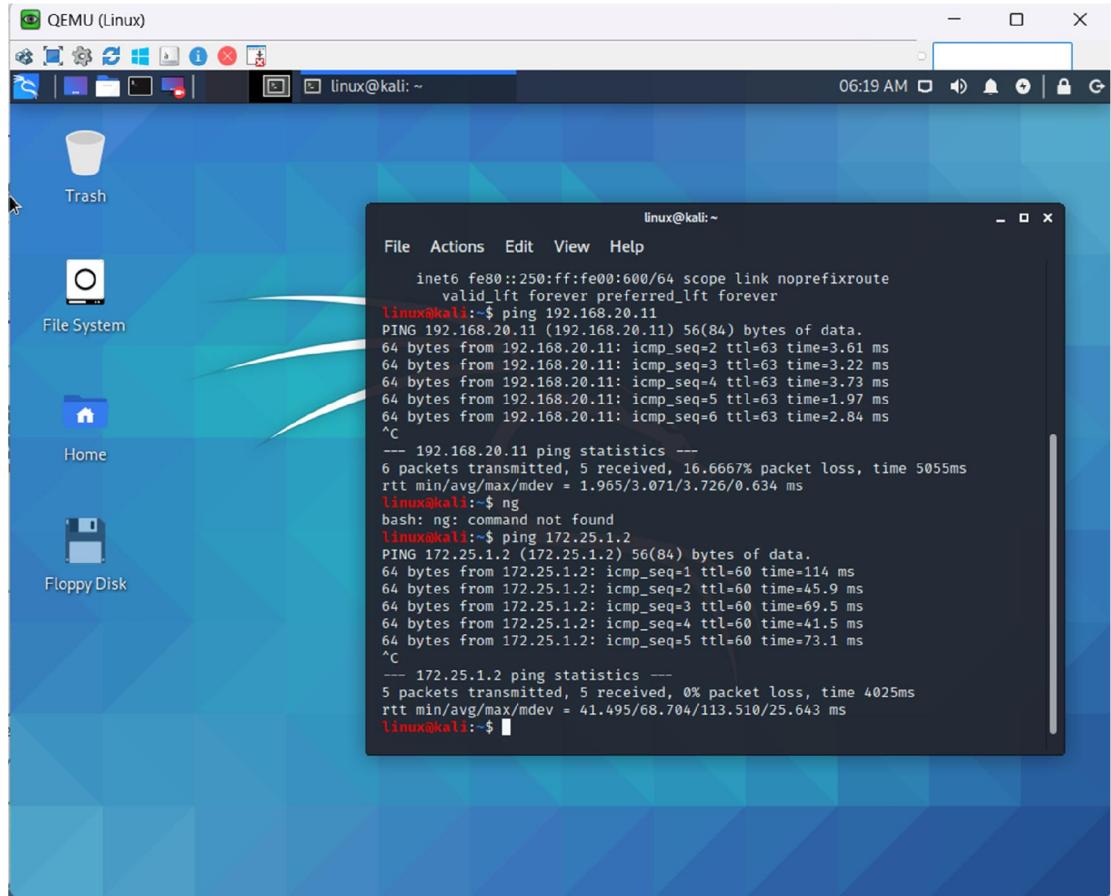
#	Comment	Interface	Bridge	Horiz...	Trust...	Priority (hex)	PVID
0		ether2_LAN	LAN_Wifi		no	80	1
1		ether3	LAN_Wifi		no	80	1

Cuối cùng ta sẽ cấu hình dhcp để cho thiết bị cấp địa chỉ ip động xuống cho các thiết bị không dây

Comment	Name	Interface	Relay	Lease Time	Address Pool	Add Max For Leases
dhcp1		LAN_Wifi		02:00:00	dhcp_pool0	no

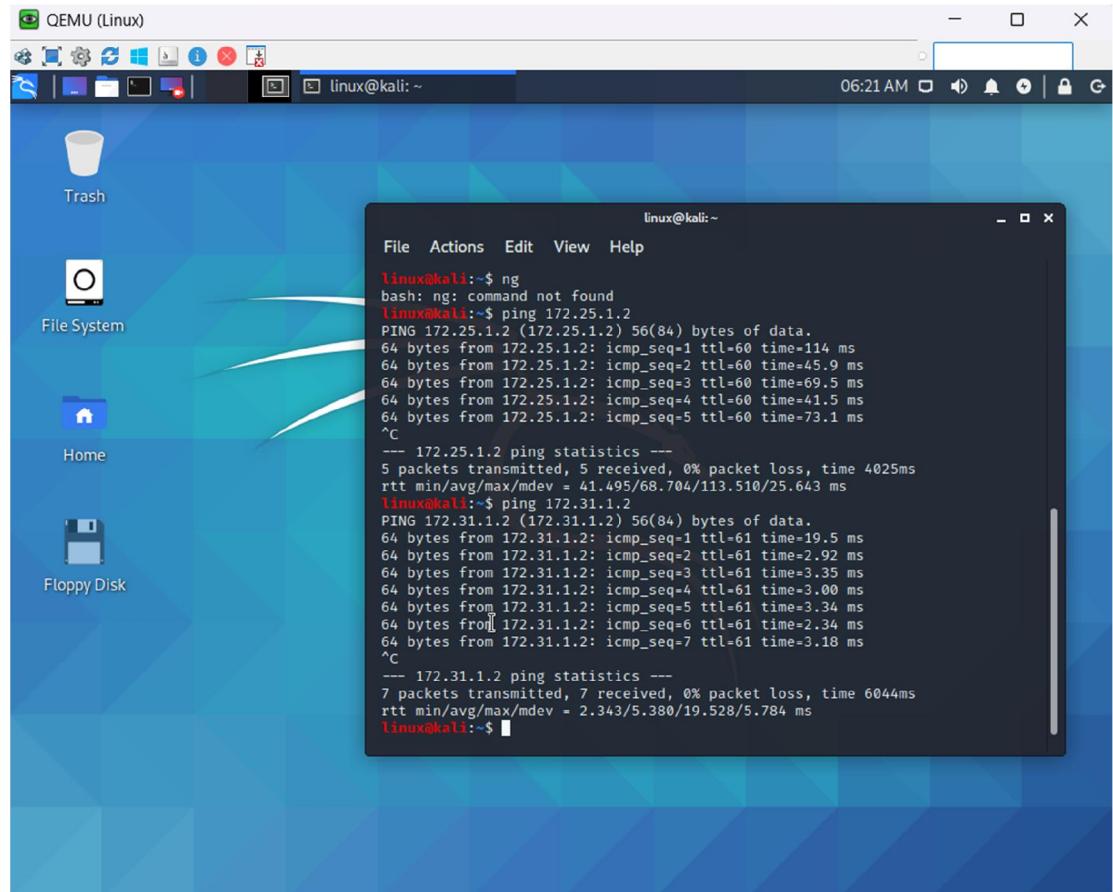
### 3.4.9 Kiểm thử hệ thống:

#### 3.4.9.1 Máy tính từ các phòng ban



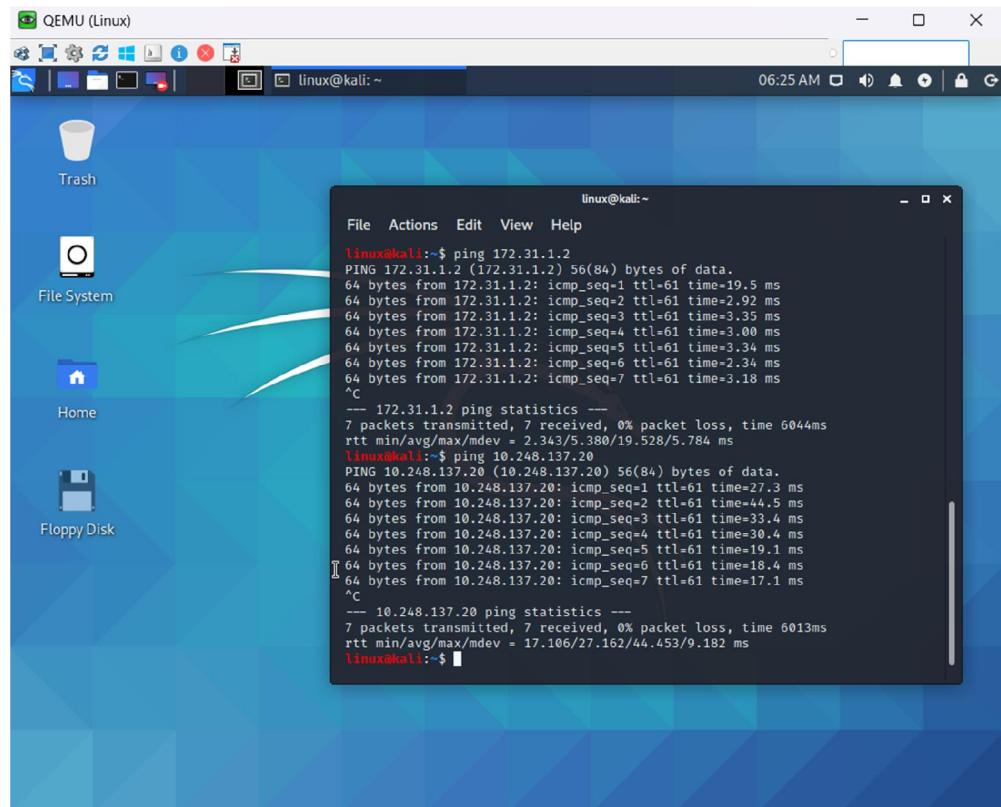
Hình 3.7 Máy tính từ các phòng ban của mạng nội bộ có thể ping thông đến văn phòng các trung tâm khu vực

Máy tính từ các phòng ban đã của văn phòng công ty số 8 Lê Văn Huân đã có thể tiến hành giao tiếp mạng với các máy thuộc các trung tâm khu vực với ip 172.25.1.2.



Hình 3.8 Máy tính từ các phòng ban của mạng nội bộ có thể ping thông đến văn phòng chi nhánh số 1 Lê Văn Huân

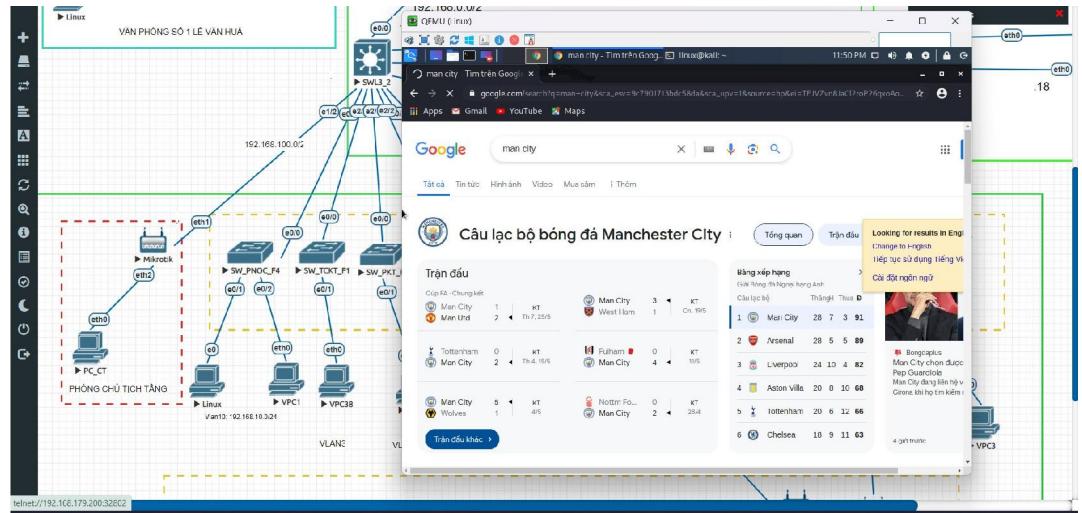
Máy tính từ các phòng ban đã của văn phòng công ty số 8 Lê Văn Huân đã có thể tiến hành giao tiếp mạng với các máy thuộc khu vực tòa nhà văn phòng số 1 Lê Văn Huân với ip 172.31.1.2



Hình 3.9 Máy tính từ các phòng ban có thể ping thông đến các server của công ty để sử dụng các dịch vụ mạng.

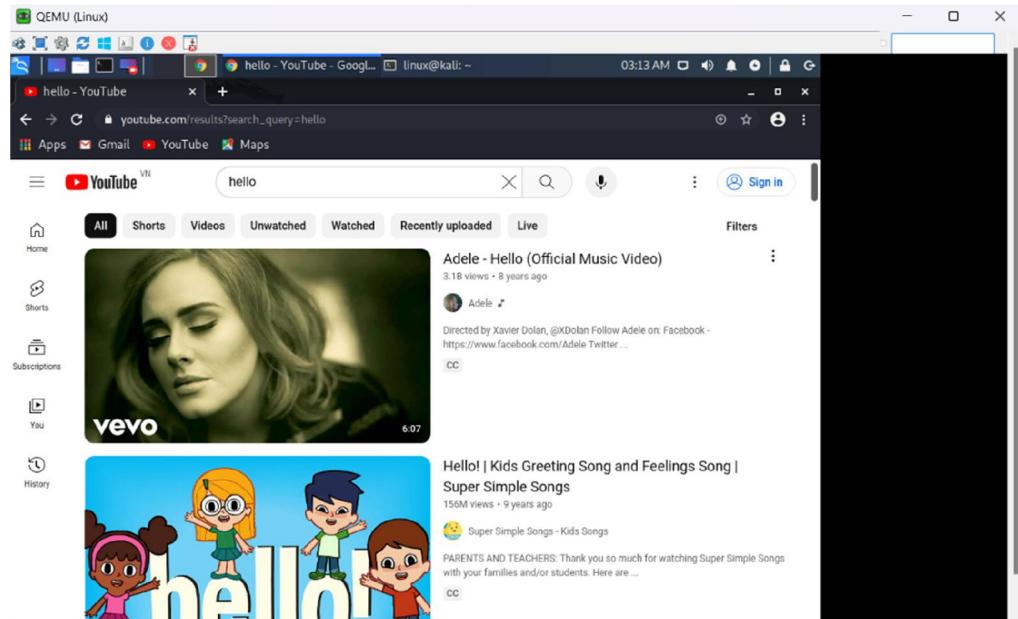
Các máy từ phòng ban của hệ thống mạng nội bộ đã có thể kết nối với các máy chủ thuộc khu vực ZONE-Server với ip 10.248.137 để có thể truy cập vào cơ sở dữ liệu nội bộ của công ty

### 3.4.9.2 Kiểm thử đường internet:



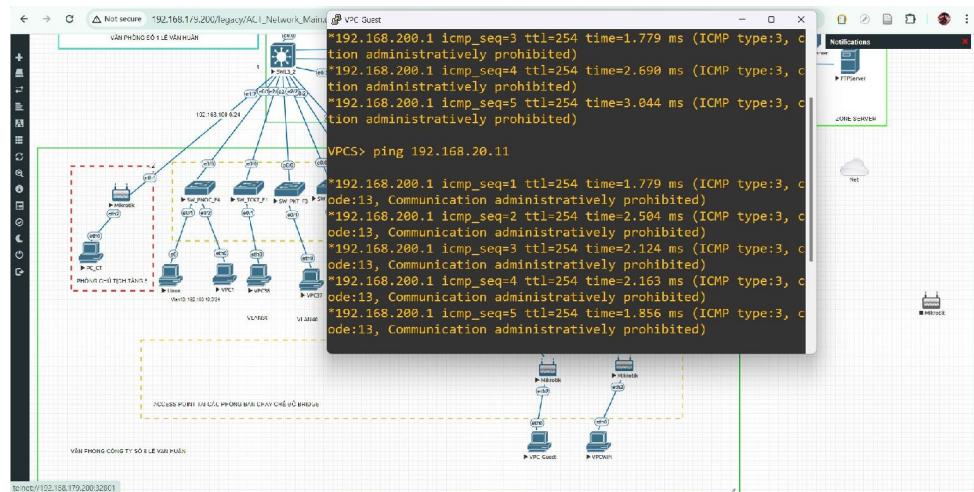
Hình 3.10 Các máy tính trong hệ thống mạng nội bộ đã có thể ra được mạng thật internet

Các máy tính trong nội bộ công ty ACT đã có thể kết nối ra bên ngoài internet để sử dụng các dịch vụ mạng. Ở đây em sẽ sử dụng máy ảo Linux mà em đã cấu hình trong mô hình mạng nội bộ này để kết nối ra ngoài mạng thật bằng cách sử dụng trình duyệt web của máy ảo này đến trang web của google và tìm kiếm với từ khóa “*Man City*” và đã thành công.

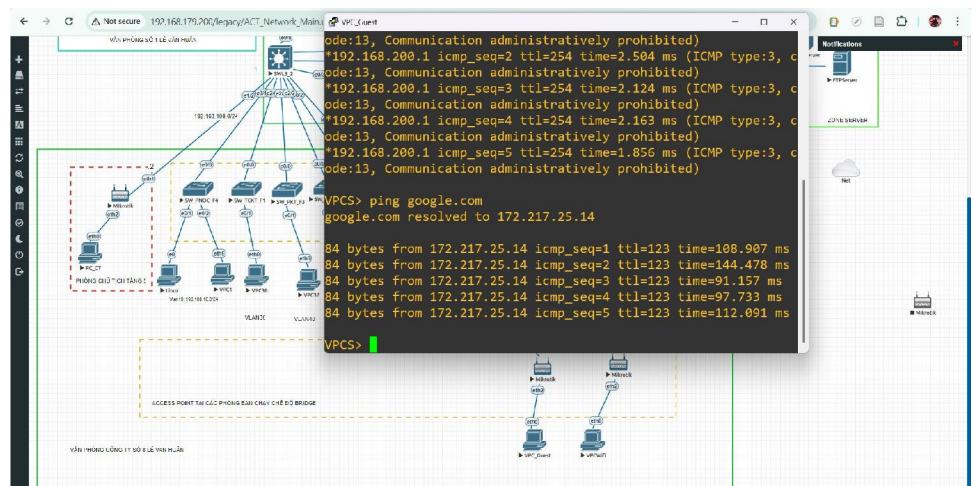


Sau đó em đã sử dụng máy ảo trong mạng nội bộ này để truy cập vào trang web youtube để xem video và đã thành công

### 3.4.9.3 Kiểm tra Wifi:



Hình 3.11 Các máy kết nối với thiết bị không dây ACT\_Guest dành cho khách không thể kết nối và giao tiếp với các máy trong hệ thống mạng nội bộ



Hình 3.12 Các máy kết nối với thiết bị không dây ACT\_Guest dành cho khách chỉ có thể kết nối ra ngoài mạng internet

Em đã sử dụng máy tính khách để kết nối với hệ thống mạng wifi ACT\_Guest dành cho khách sử dụng trong hệ thống mạng nội bộ. Và theo như mong muốn khi thiết kế thì máy tính của khách hàng không thể kết nối với mạng nội bộ nhưng vẫn có thể kết nối ra ngoài internet khi vẫn có thể ping được tới trang web của google.com

## CHƯƠNG 4. KẾT LUẬN

### 4.1 Kết luận

Trong quá trình nghiên cứu, thực hiện đề tài “Xây dựng, thiết kế hệ thống mạng nội bộ cho công ty cổ phần Viễn thông ACT”, em đã đạt được nhiều kết quả quan trọng góp phần nâng cao các kỹ năng cũng như thêm được những kiến thức mới để có thể góp phần phát triển cho công việc quản trị hệ thống mạng của mình.

Trước hết, để thực hiện đề tài này, em đã xây dựng và thiết kế mô hình hệ thống mạng này lên phần mềm giả lập mạng EVE-NG (Emulated Virtual Environment – Next Generation), đây là phần mềm cho phép kiểm thử các mô hình mạng trước khi triển khai vào thực tế. Nó cho phép các thiết bị trong mô hình mạng có thể hoạt động như các thiết bị thật ngoài thực tế với những tính năng như các thiết bị mạng của các hãng nổi tiếng như Cisco, DrayTek, và Huawei,... thêm vào đó là những máy tính với các giao diện đồ họa và các tính năng như một máy tính thật. Và quan trọng nhất, nó hỗ trợ cho phép các thiết bị trong mô hình mạng có thể kết nối ra ngoài mạng internet thật, giúp cho các mô hình có thể kiểm thử các chức năng đã được cấu hình một cách chính xác và toàn diện hơn.

Qua việc thực hiện đề tài này, em đã có cơ hội có thể tiếp xúc với mô hình mạng ngoài thực tế, tiếp xúc và trực tiếp thực hiện các kỹ thuật cấu hình các thiết bị phù hợp với yêu cầu của mô hình mạng. Thiết lập các chính sách bảo mật phù hợp và thỏa mãn với yêu cầu của công ty. Cấu hình các thiết bị Wifi trong mô hình mạng một cách trực quang thông qua các giao diện cấu hình của thiết bị, được cấu hình thêm các tính năng khác của các thiết bị thật mà trong quá trình học tại trường em không thể học được. Bên cạnh đó, em cũng học thêm được nhiều kiến thức về tìm kiếm và phát hiện lỗi trong quá trình cấu hình và kiểm thử các mô hình mạng.

Tuy nhiên, trong mô hình hệ thống vẫn còn nhiều thiếu sót, khi EVE-NG hỗ trợ rất nhiều các tính năng nhưng các thiết bị ảo như router hay switch thì lại không có sẵn mà phải đi tìm kiếm ở các nguồn trên mạng hoặc là mua license của các hãng

thiết bị bởi vì các thiết bị chạy trên môi trường EVE-NG đều có các tính năng giống hầu hết các tính năng của các thiết bị thật để có thể kết nối mô hình mạng mà mình thiết kế ra ngoài mạng internet ngoài thực tế. Thêm vào đó, để các mô hình mạng với nhiều các thiết bị ảo như vậy hoạt động trên một chiếc máy tính thì máy tính cần rất nhiều các yêu cầu cao về phần cứng và bộ nhớ RAM để mô hình có thể hoạt động bình thường nên mô hình em thiết kế không có quá nhiều các thiết bị nhưng vẫn đảm bảo đầy đủ các tính năng quan trọng của hệ thống mạng.

## 4.2 Hướng phát triển

Trong tương lai, em sẽ phát triển và mở rộng mô hình hệ thống này bằng việc kết nối thêm với các mô hình mạng nội bộ khác để làm cho hệ thống mạng này rộng hơn. Áp dụng thêm các công nghệ của các thiết bị mạng mới nhằm xây dựng một hệ thống mạng hiện đại và tân tiến hơn. Bên cạnh đó việc phát triển các chính sách và các công nghệ bảo mật mới là điều không thể thiếu khi mà việc đầu tư vào các vấn đề về bảo mật này sẽ giúp ngăn chặn những tội phạm mạng với lối suy nghĩ thông minh sử dụng các công cụ tiên tiến có thể vượt qua được hết các tầng lớp bảo mật để đánh cắp và bán các thông tin nhạy cảm của công ty

## TÀI LIỆU THAM KHẢO

Tiếng Việt

[2024] Tường lửa là gì | Tổng hợp thông tin [A-Z] về Firewall. (n.d.).

Retrieved May 29, 2024, from <https://vinahost.vn/tuong-lua-la-gi/>

Đông, C. ty C. phần T. G. D. (2020a, August 28). Access Point là gì? Nên dùng Access Point, Router hay Modem? Retrieved May 29, 2024, from Thegioididong.com website: <https://www.thegioididong.com/hoi-dap/access-point-la-gi-dung-de-lam-gi-khi-nao-can-dung-den-1284585>

Đông, C. ty C. phần T. G. D. (2020b, December 12). Mesh WiFi là gì? Hoạt động như thế nào? Ưu nhược điểm của WiFi Mesh. Retrieved May 29, 2024, from Thegioididong.com website: <https://www.thegioididong.com/hoi-dap/wifi-mesh-la-gi-he-thong-wifi-mesh-hoat-dong-ra-sao-co-nen-1313383>

Đông, C. ty C. phần T. G. D. (2021, March 15). Máy chủ (Server) là gì? Có mấy loại? Có vai trò như thế nào? Retrieved May 29, 2024, from Thegioididong.com website: <https://www.thegioididong.com/hoi-dap/may-chu-server-la-gi-co-may-loai-co-vai-tro-nhu-the-nao-1335540>

Hưng N. (2024, April 16). VLAN là gì? Giải thích chi tiết về mạng LAN ảo. Retrieved May 29, 2024, from <https://vietnix.vn/vlan/>

Huy Đ. V. (n.d.). Điểm giống và khác nhau khi so sánh mô hình OSI và TCP/IP. Retrieved May 29, 2024, from <https://suncloud.vn/so-sanh-mo-hinh-osi-va-tcp-ip>

JSC, A. T., & Atalink. (2022, March 30). Tủ rack là gì? Ứng dụng và tiêu chí lựa chọn các dòng tủ rack. Retrieved May 29, 2024, from ATALINK's Blog website: <https://vietnam.atalink.com/blog/tu-rack-la-gi-ung-dung-va-tieu-chi-lua-chon-cac-dong-tu-rack/>

Mô hình OSI là gì? Chức năng của các tầng giao thức trong mô hình OSI. (2019, May 14). Retrieved May 29, 2024, from TOTOLINK Việt Nam website: <https://www.totolink.vn/article/136-mo-hinh-osi-la-gi-chuc-nang-cua-cac-tang-giao-thuc-trong-mo-hinh-osi.html>

Mô hình TCP/IP là gì? Chức năng của các tầng trong mô hình TCP/IP. (2019, June 4). Retrieved May 29, 2024, from TOTOLINK Việt Nam website: <https://www.totolink.vn/article/149-mo-hinh-tcp-ip-la-gi-chuc-nang-cuacac-tang-trong-mo-hinh-tcp-ip.html>

VietTuanS. (n.d.). Switch Layer 3 là gì? Đặc điểm, chức năng của Switch Layer 3. Retrieved May 29, 2024, from Việt Tuấn—Phân Phối Thiết Bị Mạng, Wifi, Thiết Bị Lưu Trữ NAS website: <https://viettuans.vn/switch-layer-3-la-gi>

VTP là gì? VLAN TRUNKING PROTOCOL là gì? (2019, April 8). Retrieved May 29, 2024, from TOTOLINK Việt Nam website: <https://www.totolink.vn/article/97-vtp-la-gi-vlan-trunking-protocol-la-gi.html>