

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



ĐỒ ÁN MÔN AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG

**Đề Tài: Xây Dựng Và Bảo Mật Hệ Thống
Mạng Không Dây Cho Công Ty TNHH
Giải Pháp Thương Hiệu**

Người hướng dẫn: TS. BÙI QUY ANH

Người thực hiện: DUƠNG THANH QUÝ – 52000591

Lớp : 20050401

Khoá : 24

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023

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



ĐỒ ÁN MÔN AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG

**Đề Tài: Xây Dựng Và Bảo Mật Hệ Thống
Mạng Không Dây Cho Công Ty TNHH
Giải Pháp Thương Hiệu**

Người hướng dẫn: TS. BÙI QUY ANH

Người thực hiện: ĐƯƠNG THANH QUÝ – 52000591

Lớp : 20050401

Khoá : 24

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023

LỜI CẢM ƠN

Để hoàn thành bài báo cáo này, chúng em xin cảm ơn đến TS Bùi Quy Anh đã hướng dẫn cho em đi từ những cái cơ bản nhất của môn An toàn mạng không dây và di động để chúng em có thể có đủ kiến thức hoàn thành bài cáo cáo cuối kỳ này, chúng em xin cảm ơn!

TP. Hồ Chí Minh, ngày 9 tháng 05 năm 2023

Tác giả

(Ký tên và ghi rõ họ tên)

BÁO CÁO ĐƯỢC HOÀN THÀNH

TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Tôi xin cam đoan đây là báo cáo của riêng tôi và được sự hướng dẫn khoa học của thầy Bùi Quy Anh. Các nội dung báo cáo, kết quả trong đề tài này là trung thực. 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 báo cáo 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 chúng tôi xin hoàn toàn chịu trách nhiệm về nội dung báo cáo 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 9 tháng 05 năm 2023

Tác giả

(Ký tên và ghi rõ họ tên)

MỤC LỤC

LỜI CẢM ƠN	i
MỤC LỤC.....	iii
DANH MỤC HÌNH VẼ	viii
DANH MỤC BẢNG BIỂU	xii
DANH MỤC CÁC CHỮ VIẾT TẮT.....	xiv
PHẦN 1 GIỚI THIỆU ĐỀ TÀI	1
1.1 Tính cấp thiết của đề tài	1
1.2 Đối tượng nghiên cứu.....	1
1.4 Phạm vi nghiên cứu.....	2
1.5 Phương pháp nghiên cứu.....	3
1.6 Mô tả công ty	4
1.6 Chi tiết yêu cầu của khách hàng cho việc xây dựng hệ thống mạng cho công ty.....	7
1.7 Xác định các ứng dụng mạng của khách hàng.....	8
1.8 Phân tích các ràng buộc của hệ thống mạng	10
1.9 Phân tích mục tiêu kỹ thuật	13
1.9.1 <i>Khả năng mở rộng</i>	13
1.9.2 <i>Khả năng bảo mật.....</i>	14
1.9.3 <i>Khả năng quản lý</i>	15
1.9.4 <i>Khả năng sử dụng</i>	15
1.9.5 <i>Hiệu quả chi phí.....</i>	15
PHẦN 2 CƠ SỞ LÝ THUYẾT.....	16
2.1 Thiết kế mạng phân cấp (Hierarchical Network Design).....	16
2.2 Virtual LAN (VLAN).....	18
2.2.1 <i>Giới thiệu về VLAN.....</i>	18
2.2.2 <i>Các loại VLAN</i>	19
2.2.3 <i>Cách thức hoạt động</i>	23
2.3 Inter - VLAN Routing (Switch Virtual Interface SVI).....	24

2.3.1 Giới thiệu về Inter-VLAN Routing	24
2.3.2 Giới thiệu về SVI	26
2.3.3 Các loại SVI	28
2.3.4 Cách thức hoạt động	29
2.4 Internet Service Providers (ISPs)	30
2.4.1 Giới thiệu về ISPs	30
2.4.2 Các loại ISPs	32
2.4.3 Cách thức hoạt động	33
2.5 Port-Security	34
2.5.1 Giới thiệu về Port-Security	34
2.5.2 Cách thức hoạt động	35
2.5.3 Các phương pháp cấu hình Port-Security	36
2.6 EtherChannel	37
2.6.1 Giới thiệu về EtherChannel	37
2.6.2 Điều kiện cấu hình EtherChannel	39
2.6.3 Cách thức hoạt động	39
2.7 Dynamic Host Configuration Protocol (DHCP)	40
2.7.1 Giới thiệu về DHCP	40
2.7.2 Các bước để lấy một địa chỉ từ DHCP	42
2.8 Spanning Tree Protocol (STP)	43
2.8.1 Giới thiệu về STP	43
2.8.2 Các khái niệm liên quan	45
2.8.3 Cách thức hoạt động	49
2.9 Access Controller Lists (ACLs)	50
2.9.1 Giới thiệu về ACLs	50
2.9.2 Các loại ACLs	51
2.9.3 Cách thức hoạt động	52
2.10 Secure Shell (SSH)	53
2.10.1 Giới thiệu về SSH	53

2.10.2 Các loại mã hóa SSH.....	55
2.10.3 Các tính năng của SSH	56
2.10.4 Cách thức hoạt động.....	57
2.11 Subnetting and IP Addressing	58
2.11.1 Giới thiệu về IP Address	58
2.11.2 Giới thiệu về Subnetting	60
2.11.3 Phương pháp Variable Length Subnet Mask (VLSM)	61
2.12 Open Shortest Path First (OSPF)	62
2.12.1 Giới thiệu về OSPF	62
2.12.2 Cách thức hoạt động.....	64
2.13 Wireless Network (WLAN)	65
2.13.1 Giới thiệu về WLAN	65
2.13.2 Các chuẩn của WLAN.....	67
2.13.3 Các kỹ thuật bảo mật WLAN	69
2.13.4 Cách thức hoạt động.....	70
2.14 Default/ Static Route	71
2.14.1 Giới thiệu về Default/ Static Route	71
2.14.2 Cách thức hoạt động.....	72
2.15 Site-to-site IPSec VPN (Virtual Private Network)	73
2.15.1 Giới thiệu về VPN	73
2.15.2 Các giao thức trong IPSec.....	74
2.15.3 Cách thức hoạt động.....	75
2.16 Port Address Translation (PAT - NAT Overload).....	77
2.16.1 Giới thiệu về PAT	77
2.16.2 Các loại PAT.....	78
2.16.3 Cách thức hoạt động.....	79
2.17 NTP và Syslog.....	80
PHẦN 3 THIẾT KẾ MẠNG LUẬN LÝ	81
3.1 Sơ đồ mạng logic.....	81

3.2 Phân chia địa chỉ IP cho các thiết bị.....	81
3.3 Thiết kế an ninh mạng	82
PHẦN 4 THIẾT KẾ MẠNG VẬT LÝ	83
4.1 Sơ đồ mạng vật lý	83
4.2 Bảng thống kê hàng hóa	83
4.3 Sơ đồ Rack	92
4.4 Thông tin kết nối Port trong hệ thống mạng	95
4.5 Thông tin VLAN, Inter-VLAN, IP trong hệ thống mạng	101
4.6 Thông tin chi tiết quy hoạch địa chỉ IP trong hệ thống mạng	102
PHẦN 5 THỰC NGHIỆM	113
5.1 Sơ đồ hệ thống mạng trên Cisco Packet Tracer	113
5.2 Cấu hình bảo mật cơ bản trên thiết bị	114
5.3 Cấu hình VLANs và Trunking trên các thiết bị.....	116
<i>5.3.1 Tạo các VLANs</i>	116
<i>5.3.2 Cấu hình Port-Security cho Server.....</i>	118
<i>5.3.3 Cấu hình Inter-VLANs</i>	118
5.4 Cấu hình dịch vụ tại Server	124
<i>5.4.1 Tạo DHCP Server.....</i>	124
<i>5.4.2 Tạo WEB Server.....</i>	125
<i>5.4.3 Tạo DNS Server</i>	127
<i>5.4.4 Tạo Email Server</i>	128
<i>5.4.5 Dịch vụ FTP</i>	130
5.5 Subnetting và gán địa chỉ IP	134
5.6 Cấu hình OSPF.....	139
5.7 Cấu hình Wireless Network	142
5.8 Cấu hình PAT	172
5.9 Cấu hình Access Control List	176
5.10 Cấu hình bảo mật Site-to-site IPSec VPN.....	177
5.11 Cấu hình Default/Static Route	179

5.12 Cấu hình Spanning Tree (STP).....	180
TÀI LIỆU THAM KHẢO	183

DANH MỤC HÌNH VẼ

No table of figures entries found.

Hình 2.2.1. 1 Giới thiệu mô hình VLAN	19
Hình 2.2.2. 1 Mô hình Static VLAN	20
Hình 2.2.2. 2 Mô hình Port-Based VLAN	21
Hình 2.2.2. 3 Mô hình Subnet-Based VLAN.....	21
Hình 2.2.2. 4 Mô hình Protocol-based VLAN.....	22
Hình 2.3.1. 1 Mô hình Inter-VLAN Routing	25
Hình 2.3.2. 1 Mô hình SVI.....	26
Hình 2.4.1. 1 Mô hình ISP	31
Hình 2.5.1. 1 Port-Security	35
Hình 2.6.1. 1 Mô hình EtherChannel	37
Hình 2.6.1. 2 Mô hình Etherchannel giữa các Switch.....	38
Hình 2.7.1. 1 Mô hình cấp phát địa chỉ bằng DHCP	41
Hình 2.8.1. 1 Mô hình STP	44
Hình 2.8.2. 1 Mô hình RSTP	46
Hình 2.8.2. 2 Mô hình MSTP	47
Hình 2.8.2. 3 Mô hình BPDU.....	47
Hình 2.8.2. 4 Mô hình Root Bridge.....	48
Hình 2.8.2. 5 Mô hình Blocked Port	49
Hình 2.9.1. 1 Mô hình ACLs.....	51
Hình 2.10.1. 1 Mô hình SSH	54

Hình 2.11.1. 1 Cấp phát IP Address cho các thiết bị	59
Hình 2.11.2. 1 Mô hình kỹ thuật Subnetting	60
Hình 2.12.1. 1 Mô hình định tuyến hệ thống mạng bằng OSPF	63
Hình 2.13.1. 1 Mô hình mạng Wireless LAN	66
Hình 2.15.1. 1 Mô hình ứng dụng công nghệ VPN trong hệ thống mạng	74
Hình 2.16.1. 1 Mô hình hệ thống định tuyến PAT	77
Hình 3.1. 1 Sơ đồ mạng logic	81
Hình 4.1. 1 Sơ đồ mạng vật lý	83
Hình 4.3. 1 Sơ đồ RACK trong tòa nhà chính	92
Hình 4.3. 2 Sơ đồ RACK trong tòa nhà chính	93
Hình 4.3. 3 Sơ đồ RACK trong chi nhánh	94
Hình 5.1. 1 Sơ đồ hệ thống mạng trong Cisco Packet Tracer	114
Hình 5.4.1. 1 Tạo các Pool DHCP	125
Hình 5.4.1. 2 Cập nhật danh sách các Pool DHCP	125
Hình 5.4.2. 1 Đặt IP tĩnh cho Web Server.....	126
Hình 5.4.2. 2 Truy cập dịch vụ bằng IP	126
Hình 5.4.2. 3 Truy cập dịch vụ bằng tên miền.....	126
Hình 5.4.3. 1 Đặt IP tĩnh cho DNS Server.....	127
Hình 5.4.3. 2 Đăng ký dịch vụ DNS	127
Hình 5.4.4. 1 Đặt IP tĩnh cho Email Server	128
Hình 5.4.4. 2 Tạo các tài khoản trên Email Server	129

Hình 5.4.4. 3 Đăng ký tài khoản tại PC, Laptop	129
Hình 5.4.4. 4 Gửi Email đến một tài khoản khác	130
Hình 5.4.4. 5 Thông báo gửi Email thành công	130
Hình 5.4.4. 6 Phản hồi lại thành công.....	130
Hình 5.4.5. 1 Tạo các user trên Server	131
Hình 5.4.5. 2 Tạo file .txt và đẩy lên Server.....	131
Hình 5.4.5. 3 Cập nhật file thành công trên Server	132
Hình 5.4.5. 4 Truyền file đến các thiết bị khác	133
Hình 5.4.5. 5 Truyền file thành công	134
Hình 5.7. 1 Đăng nhập vào dịch vụ WLAN	143
Hình 5.7. 2 Nhập Username và Passwork.....	143
Hình 5.7. 3 Kiểm tra các kết nối đến Light Weight Access Point.....	144
Hình 5.7. 4 Danh sách các Interface đã tạo trên Controller	144
Hình 5.7. 5 Chi tiết Interface VLAN 10	145
Hình 5.7. 6 Chi tiết Interface VLAN 12	145
Hình 5.7. 7 Chi tiết Interface VLAN 30	146
Hình 5.7. 8 Chi tiết Interface VLAN 40	146
Hình 5.7. 9 Chi tiết Interface VLAN 50	147
Hình 5.7. 10 Chi tiết Interface VLAN 60	147
Hình 5.7. 11 Chi tiết Interface management.....	148
Hình 5.7. 12 Danh sách các WLANs đã đăng ký.....	148
Hình 5.7. 13 Chi tiết đăng ký WLAN và VLAN 10.....	149
Hình 5.7. 14 Chi tiết đăng ký WLAN và VLAN 10.....	149
Hình 5.7. 15 Chi tiết đăng ký WLAN và VLAN 10.....	150
Hình 5.7. 16 Danh sách Groups đã tạo theo từng VLAN cho WLAN	150
Hình 5.7. 17 Chi tiết tạo Group cho WLAN BRM.....	151
Hình 5.7. 18 Chi tiết tạo Group cho WLAN BRM.....	151
Hình 5.7. 19 Chi tiết tạo Group cho WLAN BRM.....	152

Hình 5.7. 20 Gắn Card mạng cho LAPTOP	153
Hình 5.7. 21 Refresh để tìm kiếm WLAN tương ứng theo từng VLAN	154
Hình 5.7. 22 Chọn WLAN phù hợp theo từng VLAN	154
Hình 5.7. 23 Kết nối đến WLAN	155
Hình 5.7. 24 Kết nối thành công	155
Hình 5.7. 25 Ping thành công thiết bị kết nối WLAN đến các thiết bị khác....	156

DANH MỤC BẢNG BIỂU

Bảng 1.7. 1 các ứng dụng mạng của khách hàng	10
Bảng 1.8. 1 Bảng chi tiết thi công công việc trong 2 tháng.....	12
Bảng 1.9.1. 1 Khả năng mở rộng của hệ thống trong 2 năm tới	13
Bảng 2.14.2. 1 So sánh Default và Static Route.....	73
Bảng 4.2. 1 Bảng thống kê hàng hóa	92
Bảng 4.4. 1 Bảng thông tin kết nối port	95
Bảng 4.4. 2 Bảng thông tin kết nối port	96
Bảng 4.4. 3 Bảng thông tin kết nối port	97
Bảng 4.4. 4 Bảng thông tin kết nối port	98
Bảng 4.4. 5 Bảng thông tin kết nối port	99
Bảng 4.4. 6 Bảng thông tin kết nối port	100
Bảng 4.4. 7 Bảng thông tin kết nối port	101
Bảng 4.5. 1 Bảng thông tin VLAN, Inter-VLAN, IP trong hệ thống mạng	102
Bảng 4.6. 1 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	103
Bảng 4.6. 2 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	104
Bảng 4.6. 3 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	104
Bảng 4.6. 4 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	105
Bảng 4.6. 5 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	106
Bảng 4.6. 6 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	107
Bảng 4.6. 7 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	108
Bảng 4.6. 8 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	109
Bảng 4.6. 9 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	110
Bảng 4.6. 10 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	111

Bảng 4.6. 11 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	112
Bảng 4.6. 12 Bảng thông tin chi tiết quy hoạch địa chỉ IP.....	113

DANH MỤC CÁC CHỮ VIẾT TẮT

CSDL	:	Cơ sở dữ liệu
HTTP	:	HyperText Transfer Protocol
AJAX	:	Asynchronous Javascript and XML
XML	:	Extensible Markup Language
URL	:	Uniform Resource Locator
API	:	Application Programming Interface
CSS	:	Cascading Style Sheets
SQL	:	Structured Query Language
JS	:	Java Script
RDBMS	:	Relational Database Management System

PHẦN 1 GIỚI THIỆU ĐỀ TÀI

1.1 Tính cấp thiết của đề tài

Việc xây dựng và bảo mật hệ thống mạng không dây là một vấn đề cực kỳ cấp thiết trong thời đại công nghệ số hiện nay. Công ty TNHH Giải pháp Thương hiệu Sao Kim cần tập trung vào xây dựng một hệ thống mạng không dây với các tiêu chuẩn bảo mật cao nhằm đảm bảo an toàn cho dữ liệu và thông tin quan trọng của công ty.

Tính cấp thiết của đề tài này nằm ở việc đảm bảo sự bảo mật và ổn định của hệ thống mạng không dây. Với sự phát triển nhanh chóng của công nghệ, cũng tương đương với việc tăng cường các mối đe dọa về an ninh mạng. Nếu công ty không đầu tư vào các biện pháp bảo mật chặt chẽ, họ sẽ dễ dàng trở thành mục tiêu tấn công của các hacker hay virus gây hại. Điều này có thể dẫn đến mất mát dữ liệu và ảnh hưởng xấu đến uy tín của công ty.

Để đảm bảo an toàn cho hệ thống mạng không dây, công ty cần triển khai các biện pháp bảo mật như cấu hình bảo mật trên các thiết bị mạng, thiết lập mạng riêng ảo VPN, sử dụng phần mềm chống virus và thiết lập các Access Control List (ACLs) để kiểm soát quyền truy cập vào hệ thống. Tuy nhiên, việc triển khai và duy trì các biện pháp bảo mật này là một quá trình liên tục và đòi hỏi sự tập trung và kiên trì để đảm bảo rằng hệ thống mạng không dây của công ty luôn được bảo mật và an toàn.

1.2 Đối tượng nghiên cứu

Đề tài Xây dựng và bảo mật hệ thống mạng không dây cho Công ty TNHH Giải pháp Thương hiệu Sao Kim tập trung vào nghiên cứu và thực hiện các giải pháp để tăng cường bảo mật hệ thống mạng không dây của công ty. Đối tượng nghiên cứu của đề tài này sẽ bao gồm các thành phần chính của hệ thống mạng không dây của công ty Sao Kim.

Các thành phần chính của hệ thống mạng không dây của công ty Sao Kim bao gồm:

1. Các thiết bị mạng: Router, Access Point, Switch, Wireless LAN, các thiết bị IoT,...được sử dụng để thiết lập và kết nối mạng không dây trong công ty.
2. Phần mềm quản lý mạng: Các phần mềm được sử dụng để quản lý, giám sát và điều khiển các thiết bị mạng, cũng như các hoạt động trong hệ thống mạng không dây.
3. Các ứng dụng và dịch vụ trên mạng: Email, web server, file server, database server, VPN, Remote Desktop Protocol,...được sử dụng để cung cấp dịch vụ và hỗ trợ cho các hoạt động kinh doanh của công ty.
4. Nhân viên và người dùng: Các nhân viên và người dùng sử dụng các thiết bị và ứng dụng để làm việc, truy cập thông tin và thực hiện các hoạt động kinh doanh.

Vì vậy, để xây dựng và bảo mật hệ thống mạng không dây cho Công ty TNHH Giải pháp Thương hiệu Sao Kim, đề tài sẽ tập trung vào phân tích và đánh giá các yếu tố liên quan đến các thành phần trên. Nghiên cứu sẽ tập trung vào việc xây dựng các giải pháp để tăng cường bảo mật hệ thống mạng không dây và đảm bảo rằng nó đáp ứng được nhu cầu kinh doanh của công ty.

1.4 Phạm vi nghiên cứu

Đầu tiên, để xây dựng và bảo mật hệ thống mạng không dây phù hợp với nhu cầu kinh doanh của Sao Kim, đề tài sẽ tìm hiểu và phân tích các yêu cầu và nhu cầu kinh doanh của công ty. Điều này sẽ giúp xác định các yêu cầu về hiệu suất, bảo mật và khả năng mở rộng của hệ thống mạng không dây của công ty.

Thứ hai, đề tài sẽ phân tích các rủi ro bảo mật mạng không dây nhằm đảm bảo an toàn và bảo mật cho hệ thống mạng không dây của Sao Kim. Việc này bao gồm phân tích các mối đe dọa, lỗ hổng và các kỹ thuật tấn công thường gặp. Sau đó, đề tài sẽ đưa ra các giải pháp để xây dựng và bảo mật hệ thống mạng không dây.

Thứ ba, đề tài sẽ đưa ra các giải pháp để thiết lập hệ thống mạng không dây cho công ty Sao Kim. Các giải pháp này sẽ bao gồm thiết kế và triển khai hệ thống mạng không dây, cấu hình và quản lý các thiết bị mạng và phần mềm quản lý mạng.

Tiếp theo, đề tài sẽ đưa ra các giải pháp bảo mật mạng không dây để đảm bảo an toàn và bảo mật cho hệ thống mạng không dây của Sao Kim. Các giải pháp này bao gồm xác thực và phân quyền người dùng, mã hóa dữ liệu, giám sát mạng và phát hiện xâm nhập.

Cuối cùng, đề tài sẽ đánh giá hiệu suất và độ tin cậy của hệ thống mạng không dây của Sao Kim. Đánh giá này sẽ được thực hiện sau khi triển khai các giải pháp bảo mật để đảm bảo hiệu suất và độ tin cậy của hệ thống mạng không dây.

1.5 Phương pháp nghiên cứu

Phương pháp nghiên cứu của đề tài Xây Dựng và Bảo Mật Hệ Thống Mạng Không Dây Cho Công ty TNHH Giải pháp Thương hiệu Sao Kim sẽ sử dụng phương pháp nghiên cứu kết hợp giữa phương pháp nghiên cứu lý thuyết và phương pháp nghiên cứu thực nghiệm.

Phương pháp nghiên cứu lý thuyết sẽ được sử dụng để tìm hiểu và phân tích các kiến thức cơ bản liên quan đến hệ thống mạng không dây, bao gồm các khái niệm, nguyên tắc và các giải pháp bảo mật mạng không dây. Nghiên cứu lý thuyết cũng sẽ được sử dụng để xác định các phương pháp đánh giá hiệu suất và độ tin cậy của hệ thống mạng không dây.

Phương pháp nghiên cứu thực nghiệm sẽ được sử dụng để xác định các yêu cầu và nhu cầu kinh doanh của công ty Sao Kim, phân tích các rủi ro bảo mật mạng không dây và xây dựng các giải pháp bảo mật mạng không dây. Nghiên cứu thực nghiệm cũng sẽ được sử dụng để thiết lập hệ thống mạng không dây cho công ty Sao Kim và đánh giá hiệu suất và độ tin cậy của hệ thống mạng không dây sau khi triển khai các giải pháp bảo mật.

1.6 Mô tả công ty

Công ty TNHH Giải pháp Thương hiệu Sao Kim là một công ty hoạt động trong lĩnh vực cung cấp các giải pháp và dịch vụ thương hiệu cho khách hàng của mình. Công ty có trụ sở chính và một chi nhánh, nằm trong cùng một khu vực đô thị.

Trụ sở chính của công ty Sao Kim có các bộ phận sau:

1. Bộ phận Dịch vụ Tư vấn & Vận hành Giải pháp Thương hiệu (COSB): Đây là bộ phận chuyên cung cấp dịch vụ tư vấn và vận hành giải pháp thương hiệu cho khách hàng của công ty. Bộ phận này sẽ giúp khách hàng đưa ra các quyết định chiến lược liên quan đến thương hiệu và đảm bảo rằng các giải pháp được triển khai đáp ứng được các mục tiêu kinh doanh và đem lại lợi ích tối đa cho khách hàng.
2. Bộ Phận Báo cáo và Quản lý Hồ sơ Thương hiệu (BRM): Đây là bộ phận chịu trách nhiệm quản lý và lưu trữ hồ sơ thương hiệu của công ty. Bộ phận này sẽ đảm bảo rằng các thông tin liên quan đến thương hiệu được lưu trữ và bảo mật một cách an toàn, đồng thời cung cấp các báo cáo về thương hiệu để hỗ trợ các quyết định kinh doanh.
3. Bộ Phận Điều hành & Sản xuất (OP): Bộ phận này chịu trách nhiệm quản lý và điều hành quá trình sản xuất và cung cấp dịch vụ của công ty. Bộ phận này sẽ đảm bảo rằng các sản phẩm và dịch vụ được sản xuất và cung

cấp đáp ứng được các tiêu chuẩn chất lượng và đáp ứng nhu cầu của khách hàng.

4. Bộ Phận Tư vấn & Chăm sóc khách hàng (CCA): Đây là bộ phận chịu trách nhiệm tư vấn và hỗ trợ khách hàng của công ty. Bộ phận này sẽ giúp đỡ khách hàng giải quyết các thắc mắc liên quan đến sản phẩm và dịch vụ của công ty, đồng thời cung cấp các giải pháp để nâng cao trải nghiệm của khách hàng.
5. Bộ Phận Công nghệ thông tin (IT): Đây là bộ phận chịu trách nhiệm quản lý và vận hành các hệ thống công nghệ thông tin của công ty. Bộ phận này sẽ đảm bảo rằng các hệ thống công nghệ thông tin được vận hành hiệu quả và đáp ứng được nhu cầu của các bộ phận khác trong công ty.
6. Khu vực Dành cho Khách/Đợi (CWA1): Đây là khu vực đón tiếp khách hàng của COSB. Khu vực này được thiết kế thoải mái và hiện đại để tạo cảm giác thoải mái cho khách hàng khi đến công ty. Ngoài ra, khu vực còn cung cấp các tiện ích như wifi miễn phí, trà, cà phê để khách hàng có thể sử dụng trong quá trình đợi.

Chi nhánh của công ty Sao Kim được thiết kế để chia sẻ khối lượng công việc với trụ sở chính, do đó nó bao gồm các bộ phận sau:

1. Nghiên cứu và Phát triển Thương hiệu (MD): Đây là bộ phận chịu trách nhiệm về nghiên cứu, phát triển và tạo ra các giải pháp cho các thương hiệu của công ty. Các nhân viên trong bộ phận này sẽ thực hiện các hoạt động tìm hiểu thị trường, phân tích cạnh tranh, đưa ra các phân tích SWOT và đề xuất các chiến lược tiếp thị để phát triển và tăng cường thương hiệu của công ty.

2. Phòng Tiếp thị (MK): Bộ phận này chịu trách nhiệm về quản lý và triển khai các chiến dịch quảng cáo, truyền thông và tiếp thị của công ty. Các nhân viên trong phòng Tiếp thị sẽ phối hợp với bộ phận Nghiên cứu và Phát triển Thương hiệu để xây dựng các chiến lược tiếp thị hiệu quả cho các sản phẩm và dịch vụ của công ty.
3. Phòng Nhân sự (HR): Bộ phận này chịu trách nhiệm về tuyển dụng, đào tạo và quản lý nhân viên trong công ty. Các nhân viên trong phòng Nhân sự sẽ thực hiện các hoạt động như phân tích nhu cầu nhân sự, quản lý chính sách nhân sự, tuyển dụng và đào tạo nhân viên.
4. Phòng Tài chính (FIN): Bộ phận này chịu trách nhiệm về quản lý tài chính và kế toán của công ty. Các nhân viên trong phòng Tài chính sẽ thực hiện các hoạt động như lập kế hoạch tài chính, quản lý kế toán, kiểm toán và báo cáo tài chính cho ban lãnh đạo.
5. Phòng Thiết kế & Sáng tạo (DC): Bộ phận này chịu trách nhiệm về thiết kế và phát triển các sản phẩm, dịch vụ của công ty. Các nhân viên trong phòng Thiết kế & Sáng tạo sẽ thực hiện các hoạt động thiết kế, phát triển sản phẩm và đưa ra các ý tưởng sáng tạo để cải thiện sản phẩm và dịch vụ của công ty.
6. Khu vực Dành cho Khách/Đợi (CWA2): Đây là khu vực đón tiếp khách hàng của COSB. Khu vực này được thiết kế thoải mái và hiện đại để tạo cảm giác thoải mái cho khách hàng khi đến công ty. Ngoài ra, khu vực còn cung cấp các tiện ích như wifi miễn phí, trà, cà phê để khách hàng có thể sử dụng trong quá trình đợi.

Công ty Sao Kim hiện tại đang dùng mạng của một bên thứ ba để duy trì các dịch vụ công nghệ thông tin (CNTT) của mình. Tuy nhiên, để đảm bảo tính bảo mật và toàn vẹn thông tin, ban lãnh đạo cấp cao của công ty đã quyết định sẽ tự xây dựng

và sở hữu cơ sở hạ tầng mạng của mình, bao gồm LAN, WAN và một Server-Side site.

Trang web phía máy chủ sẽ lưu trữ các máy chủ DHCP, Máy chủ DNS, Máy chủ Web và Máy chủ Email. Điều này giúp cho việc quản lý và triển khai các dịch vụ trở nên thuận tiện và hiệu quả hơn.

Mạng của công ty Sao Kim sẽ được thiết kế theo mô hình phân cấp, với hai bộ định tuyến Lõi đã mua, một tại trụ sở chính và một tại chi nhánh. Các bộ định tuyến này sẽ kết nối với hai nhà cung cấp dịch vụ internet (ISP) đã đăng ký để đảm bảo tính khả dụng và ổn định của kết nối mạng.

Nhằm đảm bảo tính bảo mật và tránh rủi ro từ bên ngoài, công ty Sao Kim sẽ áp dụng chính sách phân đoạn mạng riêng biệt cho các phòng ban. Tức là, mỗi phòng ban sẽ được đặt trên một phân đoạn mạng LAN riêng biệt nhau, giúp tránh được sự truy cập trái phép từ các nguồn bên ngoài và tăng tính bảo mật của hệ thống mạng.

Đồng thời, công ty cũng sẽ triển khai hệ thống IPSec VPN để kết nối mạng giữa các chi nhánh và trụ sở chính với nhau, giúp cho việc truy cập tài nguyên mạng trở nên dễ dàng và thuận tiện hơn.

Tóm lại, việc tự xây dựng cơ sở hạ tầng mạng của công ty Sao Kim sẽ đem lại nhiều lợi ích về mặt an ninh thông tin, quản lý và triển khai dịch vụ CNTT, đồng thời cũng cải thiện hiệu suất và tính khả dụng của hệ thống mạng.

1.6 Chi tiết yêu cầu của khách hàng cho việc xây dựng hệ thống mạng cho công ty

Em sẽ công tác như một kỹ sư an ninh mạng để thiết kế mạng đáp ứng yêu cầu của cấp quản lý cao. Mạng sẽ được thiết kế theo mô hình phân cấp với hai bộ định tuyến lõi (một tại Trụ sở chính và một tại Chi nhánh), mỗi bộ kết nối với hai nhà cung cấp dịch vụ Internet để đảm bảo tính sẵn sàng và dự phòng. Vì lý do bảo mật, mỗi bộ

phận sẽ được đặt trong một mạng cục bộ riêng biệt. Em sẽ triển khai danh sách kiểm soát truy cập và mạng riêng ảo (VPN) để đảm bảo tính bảo mật, toàn vẹn và khả dụng của dữ liệu và thông tin liên lạc. Chính sách an ninh mạng sẽ được thực hiện bằng danh sách kiểm soát truy cập (ACL) để quản lý quyền truy cập của người dùng trên từng trang web. Cisco Packet Tracer sẽ được lựa chọn để thiết kế và triển khai giải pháp mạng, sử dụng mô hình phân cấp để đảm bảo tính dự phòng trong mạng và cũng sẽ cấu hình bảo mật cho Wireless LAN cấp phát IP từ xa. Mỗi bộ phận sẽ có một mạng không dây riêng biệt và được đặt trong một VLAN và một mạng con riêng biệt. Địa chỉ cung cấp cho cơ sở là 192.168.100.0 và phân bổ địa chỉ IP cho từng bộ phận. Các thiết bị trong mạng đều được định cấu hình để giao tiếp với nhau bằng bộ chuyển mạch đa lớp và sử dụng OSPF làm giao thức định tuyến. Bạn sẽ định cấu hình SSH, bảo mật cổng, quy tắc ACL và VPN site-to-site để đảm bảo tính bảo mật và mã hóa giao tiếp giữa các địa điểm. Em cũng sẽ triển khai PAT và đảm bảo rằng tất cả các thiết bị trong mạng đều hoạt động như mong đợi bằng cách kiểm tra giao tiếp.

1.7 Xác định các ứng dụng mạng của khách hàng

Ứng dụng mạng	Loại ứng dụng	Mô tả	Quan trọng hay không?
Dịch vụ email	Email	Lưu trữ và truyền thông qua email	Quan trọng
DHCP server	DHCP	Cung cấp địa chỉ IP động cho các máy trong LAN	Quan trọng
DNS server	DNS	Chuyển đổi tên miền sang địa chỉ IP	Quan trọng
Web Server	Web	Lưu trữ trang web và phục vụ yêu cầu HTTP	Quan trọng

FTP Server	File Transfer Protocol	Lưu trữ và phục vụ các file qua giao thức FTP	Quan trọng
VPN site-to-site	VPN	Kết nối mạng giữa các địa điểm khác nhau	Quan trọng
IPSec VPN	VPN	Mã hóa giao tiếp giữa các địa điểm	Quan trọng
ACL	Quản lý truy cập	Quản lý truy cập	Quan trọng
OSPF	Giao thức định tuyến	Định tuyến và chuyển tiếp dữ liệu trên mạng	Quan trọng
PAT	NAT	Chuyển đổi địa chỉ IP và cổng để kết nối với Internet	Quan trọng
Port-Security	Bảo mật	Giới hạn truy cập vào các cổng của thiết bị mạng	Quan trọng
SSH	Bảo mật	Đăng nhập an toàn vào các thiết bị mạng từ xa	Quan trọng
Wireless LAN	Mạng không dây	Kết nối thiết bị không dây trong mạng	Quan trọng
VLAN	Mạng ảo	Phân chia mạng vật lý thành nhiều mạng logic khác nhau	Quan trọng
Quản lý băng thông	Quản lý mạng	Quản lý băng thông và sử dụng Internet	Quan trọng

Hệ thống giám sát mạng	Giám sát mạng	Giám sát hiệu suất và tính khả dụng của mạng	Quan trọng
------------------------	---------------	--	------------

Bảng 1.7. Các ứng dụng mạng của khách hàng

1.8 Phân tích các ràng buộc của hệ thống mạng

Hệ thống mạng được thiết kế cho công ty Sao Kim bao gồm cơ sở hạ tầng mạng với LAN, WAN và một Server-Side site. Thiết kế này giúp cho việc quản lý và triển khai các dịch vụ trở nên thuận tiện và hiệu quả hơn. Tuy nhiên, để đảm bảo tính bảo mật và toàn vẹn thông tin, công ty quyết định tự xây dựng và sở hữu cơ sở hạ tầng mạng của mình thay vì sử dụng mạng của một bên thứ ba như hiện tại.

Điều này đặt ra ràng buộc về chi phí, thời gian, và nguồn lực để thiết kế, triển khai, và duy trì hệ thống mạng mới. Các bộ định tuyến lõi đã mua tại trụ sở chính và chi nhánh, mỗi bộ kết nối với hai nhà cung cấp dịch vụ Internet nhằm đảm bảo tính sẵn sàng và dự phòng. Điều này đảm bảo rằng nếu một nhà cung cấp dịch vụ Internet gặp sự cố, hệ thống mạng vẫn có thể hoạt động thông qua nhà cung cấp dịch vụ Internet thứ hai. Việc này cũng đòi hỏi công ty phải có đủ ngân sách để mua và duy trì các thiết bị và dịch vụ Internet từ hai nhà cung cấp.

Ngoài ra, sự phân đoạn mạng riêng biệt cho các phòng ban cũng là một ràng buộc về cấu trúc của hệ thống mạng. Các phòng ban sẽ được đặt trên một phân đoạn mạng LAN riêng biệt nhau để tránh được sự truy cập trái phép từ các nguồn bên ngoài và tăng tính bảo mật của hệ thống mạng. Điều này yêu cầu công ty phải có kế hoạch phân bổ địa chỉ IP cho từng phân đoạn mạng và đảm bảo rằng các phân đoạn mạng này không gây xung đột khi giao tiếp với nhau.

Hệ thống IPSec VPN cũng là một giải pháp quan trọng để kết nối mạng giữa các chi nhánh và trụ sở chính với nhau, giúp cho việc truy cập tài nguyên mạng trở nên dễ dàng và thuận tiện hơn. Mặc dù giải pháp này có thể ảnh hưởng đến hiệu suất mạng, nhưng nó là cần thiết để đảm bảo tính khả dụng và bảo mật cho thông tin liên lạc giữa các địa điểm.

Việc áp dụng chính sách phân đoạn mạng riêng biệt cho các phòng ban cũng đặt ra ràng buộc về quản lý người dùng và phân quyền truy cập. Chính sách an ninh mạng sẽ được thực hiện bằng danh sách kiểm soát truy cập (ACL) để quản lý quyền truy cập của người dùng trên từng trang web.

Ngoài ra, việc định cấu hình SSH, bảo mật cổng, quy tắc ACL và VPN site-to-site cũng là những ràng buộc về tính bảo mật của hệ thống mạng. Việc triển khai PAT và kiểm tra giao tiếp giữa các thiết bị trong mạng cũng đòi hỏi công ty phải có kế hoạch và quản lý nhằm đảm bảo tính khả dụng

Ngân sách: 9.000,000,000 (tám tỷ đồng)

Thời gian bảo hành: tùy theo thiết bị, đã được liệt kê ở bảng

Thời gian thi công: 2 tháng (01/05/2023 - 01/06/2023)

Tháng 1	
Thiết kế mô hình mạng (4 ngày)	<ul style="list-style-type: none"> - Phân tích yêu cầu và tài nguyên của mạng - Xác định các thiết bị mạng cần thiết - Thiết kế mô hình mạng với 2 bộ định tuyến lõi, mỗi bộ kết nối với 2 ISP, và các bộ phận mạng riêng biệt.
Cấu hình các thiết bị mạng (12 ngày)	<ul style="list-style-type: none"> - Cấu hình IP cho các interface trên các thiết bị. - Cấu hình OSPF để định tuyến giữa các thiết bị mạng. - Cấu hình SSH và bảo mật cổng để đảm bảo tính bảo mật của mạng.

Triển khai danh sách kiểm soát truy cập (ACL) (4 ngày)	<ul style="list-style-type: none"> - Thiết lập quy tắc ACL để quản lý quyền truy cập của người dùng trên từng trang web.
Triển khai mạng riêng ảo (VPN) (4 ngày)	<ul style="list-style-type: none"> - Thiết lập VPN site-to-site giữa trụ sở chính và chi nhánh.
Tháng 2	
Cấu hình các máy chủ (8 ngày)	<ul style="list-style-type: none"> - Cấu hình các máy chủ DHCP, DNS, Email và Web.
Triển khai Wireless LAN (4 ngày)	<ul style="list-style-type: none"> - Thiết lập VLAN và mạng con cho mỗi bộ phận. - Cấu hình bảo mật cho Wireless LAN cấp phát IP từ xa.
Kiểm tra và thử nghiệm (8 ngày)	<ul style="list-style-type: none"> - Kiểm tra tính bảo mật và tính khả dụng của mạng. - Kiểm tra giao tiếp giữa các thiết bị trong mạng. - Kiểm tra tính năng của các máy chủ.
Đào tạo và triển khai (4 ngày)	<ul style="list-style-type: none"> - Đào tạo nhân viên về cách sử dụng mạng mới. <p>Triển khai hệ thống vào hoạt động thực tế.</p>
<p>Tổng cộng, thời gian thi công là 2 tháng với tổng số công việc là 44 ngày. Việc phân bổ công việc theo thời gian sẽ giúp đảm bảo tiến độ và chất lượng công việc được thực hiện đúng và đầy đủ. Bên cạnh đó, các công việc sẽ được phân bổ hợp lý để đảm bảo tính hiệu quả và tiết kiệm thời gian và nguồn lực. Sự kết hợp giữa kiến thức chuyên môn về an ninh mạng, kỹ năng quản trị mạng và sử dụng công cụ Packet Tracer sẽ giúp cho quá trình triển khai mạng được thực hiện thành công.</p>	

Bảng 1.8. 1 Bảng chi tiết thi công công việc trong 2 tháng

1.9 Phân tích mục tiêu kỹ thuật

1.9.1 *Khả năng mở rộng*

	% năm 1	% năm 2	Số lượng dự kiến
Thêm bộ phận mới	5%	10%	2-4 bộ phận
Tăng số lượng host trong các bộ phận hiện có	8%	12%	20-50 host/bộ phận
Thêm chi nhánh mới	3%	7%	1-2 chi nhánh
Mở rộng dung lượng lưu trữ	4%	8%	500 GB - 1 TB
Nâng cấp phần cứng (switch, router, server)	2%	5%	1-2 thiết bị/năm
Thêm dịch vụ CNTT mới	6%	10%	2-4 dịch vụ
Nâng cấp dịch vụ CNTT hiện có	4%	8%	1-2 dịch vụ/năm
Thêm mạng không dây mới	3%	6%	1-2 mạng/năm
Tăng số lượng thiết bị kết nối mạng hiện có	3%	9%	10-20 thiết bị

Bảng 1.9.1. 1 *Khả năng mở rộng của hệ thống trong 2 năm tới*

Giải thích:

Thêm bộ phận mới: Công ty Sao Kim dự kiến sẽ mở rộng quy mô và mở rộng các hoạt động của mình, do đó cần tuyển thêm nhân viên và mở rộng các bộ phận. Tuy nhiên, việc thêm bộ phận mới sẽ kéo theo chi phí cao về cơ sở hạ tầng, phần cứng và phần mềm.

Tăng số lượng host trong các bộ phận hiện có: Công ty sẽ tiếp tục phát triển các bộ phận hiện tại để đáp ứng nhu cầu kinh doanh và mở rộng quy mô. Điều này yêu cầu tăng số lượng host để đảm bảo tính khả dụng và hiệu suất của mạng.

Thêm chi nhánh mới: Với chiến lược mở rộng kinh doanh, công ty sẽ mở rộng hoạt động của mình sang các khu vực mới. Việc thêm chi nhánh mới sẽ giúp công ty tăng cường mạng lưới kinh doanh và tăng doanh thu.

Mở rộng dung lượng lưu trữ: Với việc lưu trữ thông tin kinh doanh ngày càng tăng, công ty cần mở rộng dung lượng lưu trữ để đáp ứng nhu cầu.

Nâng cấp phần cứng (switch, router, server): Các thiết bị mạng của công ty sẽ tiếp tục được nâng cấp để đảm bảo tính khả dụng và hiệu suất của hệ thống.

Thêm dịch vụ CNTT mới: Công ty sẽ tiếp tục cung cấp các dịch vụ mới để đáp ứng nhu cầu của khách hàng và mở rộng quy mô hoạt động kinh doanh. Các dịch vụ mới này có thể là các giải pháp lưu trữ đám mây, bảo mật mạng, dịch vụ internet vệ tinh, v.v.

Nâng cấp dịch vụ CNTT hiện có: Để đảm bảo tính khả dụng và hiệu suất của các dịch vụ CNTT hiện có, công ty sẽ tiếp tục nâng cấp các dịch vụ này để đáp ứng nhu cầu của khách hàng và tăng cường hiệu quả hoạt động.

Thêm mạng không dây mới: Với sự phát triển của công nghệ không dây, công ty sẽ tiếp tục mở rộng mạng không dây để đáp ứng nhu cầu sử dụng của nhân viên và khách hàng.

Tăng số lượng thiết bị kết nối mạng hiện có: Công ty sẽ tiếp tục tăng cường hệ thống kết nối mạng bằng cách thêm các thiết bị kết nối mạng để đáp ứng nhu cầu của nhân viên và khách hàng.

1.9.2 *Khả năng bảo mật*

Thiết kế phân đoạn mạng LAN riêng biệt cho các phòng ban giúp ngăn chặn sự truy cập trái phép từ các nguồn bên ngoài và tăng cường tính bảo mật của hệ thống mạng.

Sử dụng danh sách kiểm soát truy cập (ACL) để quản lý quyền truy cập của người dùng trên từng trang web, giúp kiểm soát và giới hạn quyền truy cập vào các tài nguyên trong mạng.

Triển khai mạng riêng ảo (VPN) để bảo vệ tính bảo mật, toàn vẹn và khả dụng của dữ liệu và thông tin liên lạc.

Áp dụng chính sách phân đoạn mạng riêng biệt cho các phòng ban giúp tăng tính bảo mật và tránh rủi ro từ bên ngoài.

1.9.3 *Khả năng quản lý*

Thiết kế mạng theo mô hình phân cấp với hai bộ định tuyến lõi (một tại Trụ sở chính và một tại Chi nhánh) giúp kiểm soát và quản lý mạng hiệu quả hơn.

Triển khai danh sách kiểm soát truy cập (ACL) để quản lý quyền truy cập của người dùng trên từng trang web.

Sử dụng Cisco Packet Tracer để thiết kế và triển khai giải pháp mạng, giúp quản lý và kiểm soát mạng hiệu quả.

1.9.4 *Khả năng sử dụng*

Thiết kế mạng theo mô hình phân cấp với hai bộ định tuyến lõi giúp cải thiện hiệu suất và tính khả dụng của hệ thống mạng.

Triển khai mạng riêng ảo (VPN) để kết nối mạng giữa các chi nhánh và trụ sở chính với nhau, giúp cho việc truy cập tài nguyên mạng trở nên dễ dàng và thuận tiện hơn.

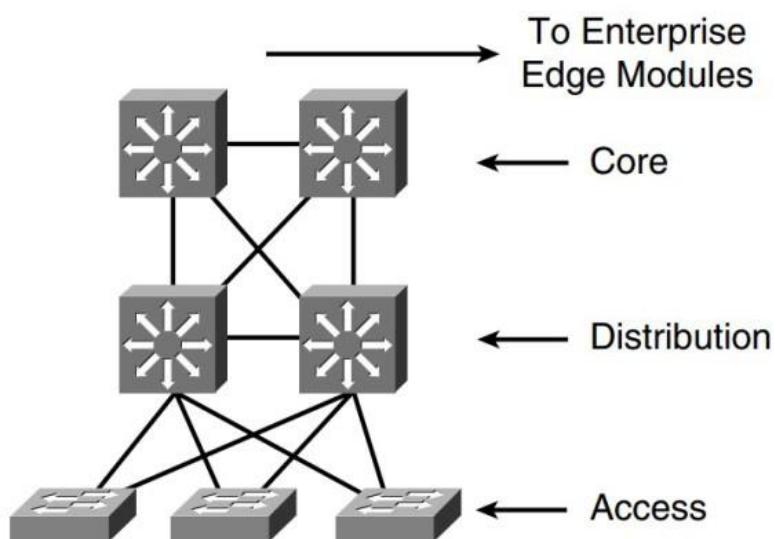
1.9.5 *Hiệu quả chi phí*

Thiết kế mạng theo mô hình phân cấp với hai bộ định tuyến lõi và triển khai danh sách kiểm soát truy cập (ACL) để quản lý quyền truy cập của người dùng trên từng trang web là cách tiết kiệm chi phí và hiệu quả để quản lý mạng.

PHẦN 2 CƠ SỞ LÝ THUYẾT

2.1 Thiết kế mạng phân cấp (Hierarchical Network Design)

Thiết kế mạng phân cấp (hierarchical network design) là một phương pháp thiết kế mạng máy tính được sử dụng để tạo ra các mạng có tính linh hoạt cao, dễ quản lý và mở rộng, đồng thời giảm thiểu chi phí vận hành và bảo trì. Phương pháp này dựa trên việc chia mạng thành các tầng khác nhau, mỗi tầng đóng vai trò khác nhau và có các đặc tính riêng.

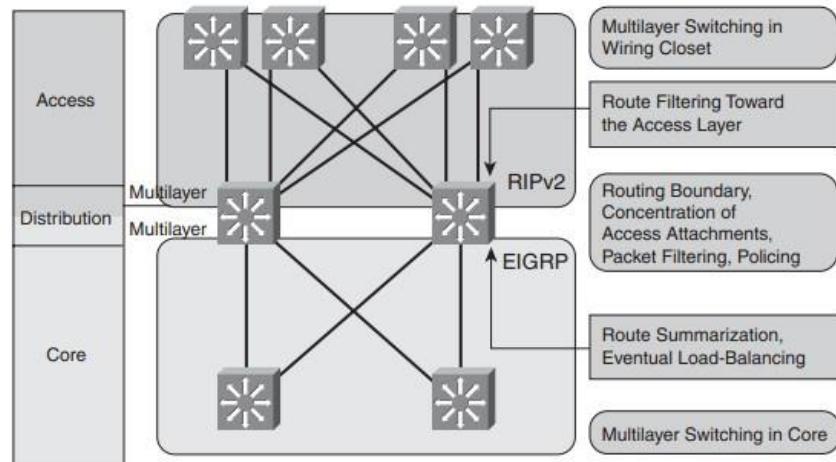


Hình 2.1. 1 Mô hình mạng phân cấp

Tầng Access Layer là tầng gần nhất với các thiết bị người dùng như máy tính cá nhân, điện thoại, máy in,... Nó là nơi kết nối các thiết bị này vào mạng, cung cấp các dịch vụ truy cập tới mạng như DHCP, NAT, Firewall, và định tuyến cục bộ. Tầng này còn chịu trách nhiệm cho việc phân phối dữ liệu giữa các thiết bị trong mạng nội bộ.

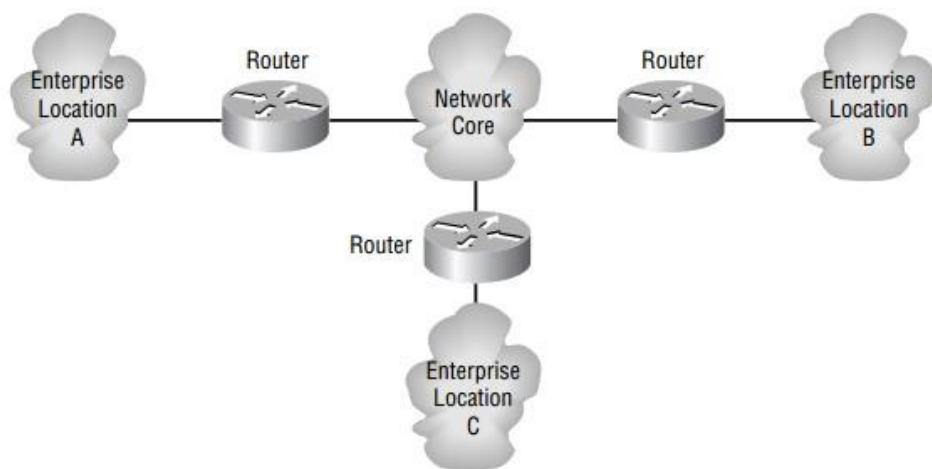
Tầng Distribution Layer là tầng trung gian, nó chịu trách nhiệm kết nối các tầng nhỏ hơn và lớn hơn nó trong mạng. Nó cũng thực hiện các chức năng chính như:

định tuyến, chuyển mạch, lọc dữ liệu, giảm tải cho mạng, và cung cấp các dịch vụ như QoS (Quality of Service), Policy-Based Routing.



Hình 2.1. 2 Mô hình tầng Distribution Layer

Tầng Core Layer là tầng cấp cao nhất, cung cấp kết nối cho tất cả các tầng trong mạng. Tầng này thường được thiết kế với mức độ độ tin cậy cao, tốc độ truyền dữ liệu nhanh và băng thông lớn. Các thiết bị trong tầng này thường không thực hiện các chức năng xử lý dữ liệu, mà chỉ đơn thuần là chuyển mạch dữ liệu.



Hình 2.1. 3 Mô hình tầng Core Layer

Thiết kế mạng phân cấp cho phép các nhà quản trị mạng phân biệt và quản lý các phân đoạn khác nhau của mạng một cách hiệu quả. Họ có thể dễ dàng kiểm soát một phần của mạng mà không ảnh hưởng đến các khu vực khác, đồng thời giảm thiểu các lỗi và vấn đề về hiệu suất. Các phân đoạn cũng có thể được mở rộng độc lập với nhau, tạo điều kiện thuận lợi cho việc mở rộng và nâng cấp mạng trong tương lai.

2.2 Virtual LAN (VLAN)

2.2.1 Giới thiệu về VLAN

Virtual LAN (VLAN) là một công nghệ được sử dụng để phân chia một mạng vật lý thành nhiều mạng logic độc lập, mỗi mạng có thể có các thiết bị và người dùng khác nhau, tạo ra sự linh hoạt và quản lý mạng hiệu quả hơn. Điều này giúp tăng cường bảo mật và hiệu suất của mạng, đồng thời giảm thiểu lưu lượng truyền tải trên mạng.

Một trong những ứng dụng phổ biến của VLAN là phân chia mạng giữa các phòng ban và các khu vực khác nhau trong một tổ chức. Ví dụ, một tổ chức có thể tạo ra các VLAN cho các bộ phận khác nhau như kế toán, marketing và phát triển sản phẩm. Mỗi VLAN sẽ có một số lượng thiết bị và người dùng nhất định, được giới hạn truy cập vào các thiết bị và tài nguyên của chính VLAN đó. Điều này giúp giảm thiểu rủi ro an ninh mạng, vì một người dùng ở một phòng ban không thể truy cập vào tài nguyên của phòng ban khác.

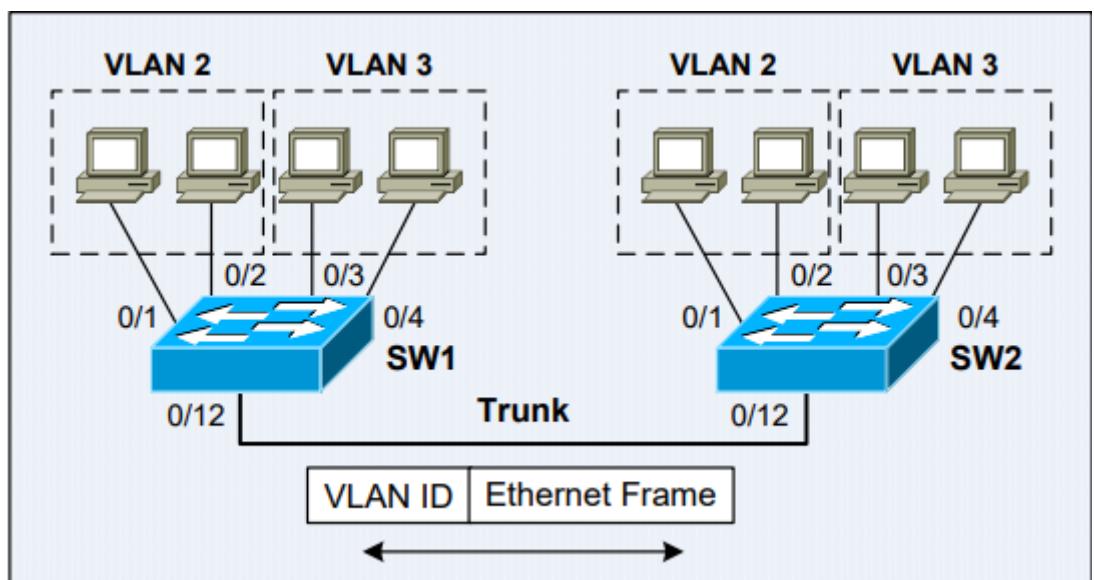
Tất cả các thiết bị trong cùng một mạng LAN đều nằm trong cùng một miền phát sóng. Tuy nhiên, công nghệ VLAN cho phép switch tạo ra nhiều miền phát sóng khác nhau.

Một Virtual LAN (VLAN) là một miền phát sóng được tạo ra bởi một hoặc nhiều switch. Switch tạo ra các VLAN bằng cách gán các giao diện của nó vào các VLAN khác nhau.

Dưới đây là một số lợi ích của việc triển khai VLAN:

- Cho phép nhóm logic người dùng hoặc thiết bị dựa trên chức năng hoặc bộ phận của họ thay vì vị trí vật lý của họ.
- Giảm chi phí mạng bằng cách giới hạn kích thước của mỗi miền phát sóng.
- Cung cấp bảo mật mạng nâng cao bằng cách giữ các thiết bị nhạy cảm trên một VLAN riêng biệt.

Trunking VLAN được sử dụng khi một VLAN trải dài qua nhiều switch. Khi switch nhận được khung từ switch khác, nó sử dụng thẻ khung được tạo ra bởi switch khác để xác định thành viên của khung VLAN và chuyển tiếp nó ra các cổng được liên kết với VLAN tương ứng.

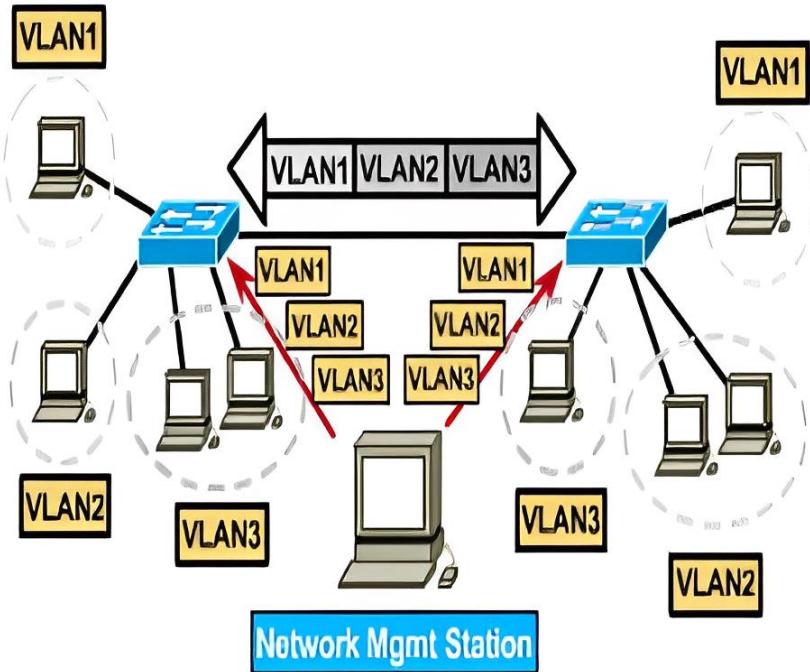


Hình 2.2.1. 1 Giới thiệu mô hình VLAN

2.2.2 Các loại VLAN

- VLAN đối tượng (Static VLAN) là loại VLAN được cấu hình tĩnh và phân chia theo đối tượng sử dụng, ví dụ như VLAN cho phòng kế toán hoặc

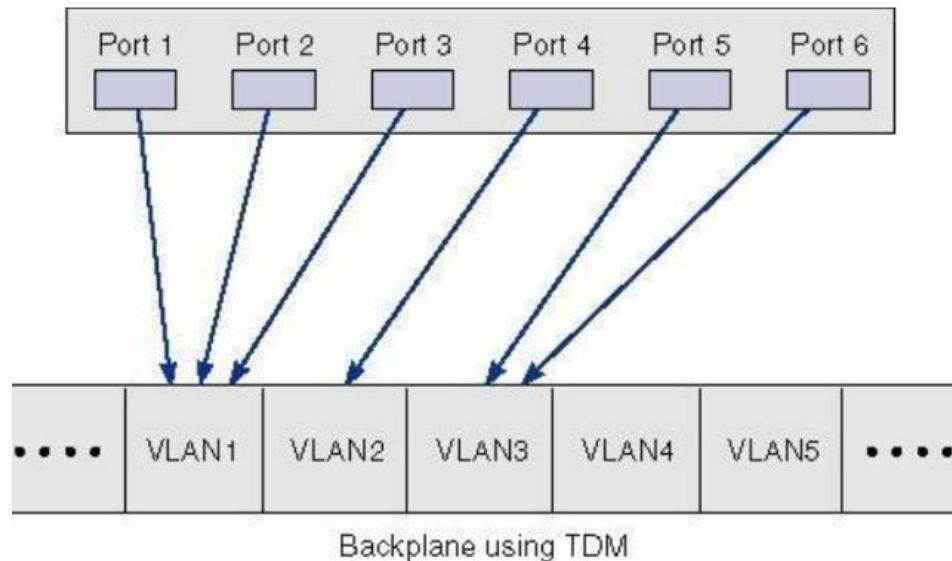
VLAN cho phòng nhân sự. Người quản trị mạng có thể cấu hình VLAN này trên switch hoặc router để ngăn chặn sự truy cập trái phép trong mạng vật lý.



Hình 2.2.2. 1 Mô hình Static VLAN

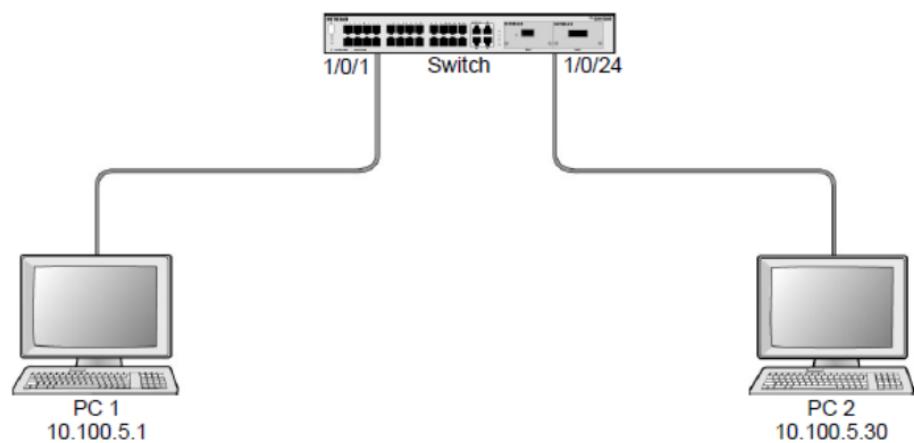
- VLAN cổng (Port-based VLAN) là loại VLAN được phân chia theo cổng kết nối trên switch hoặc router, có nghĩa là các thiết bị kết nối vào cùng một cổng sẽ thuộc cùng một VLAN. Loại VLAN này phù hợp cho các mạng có nhiều thiết bị kết nối vào một switch và muốn phân chia chúng vào các mạng ảo khác nhau.

Port-Based VLANs



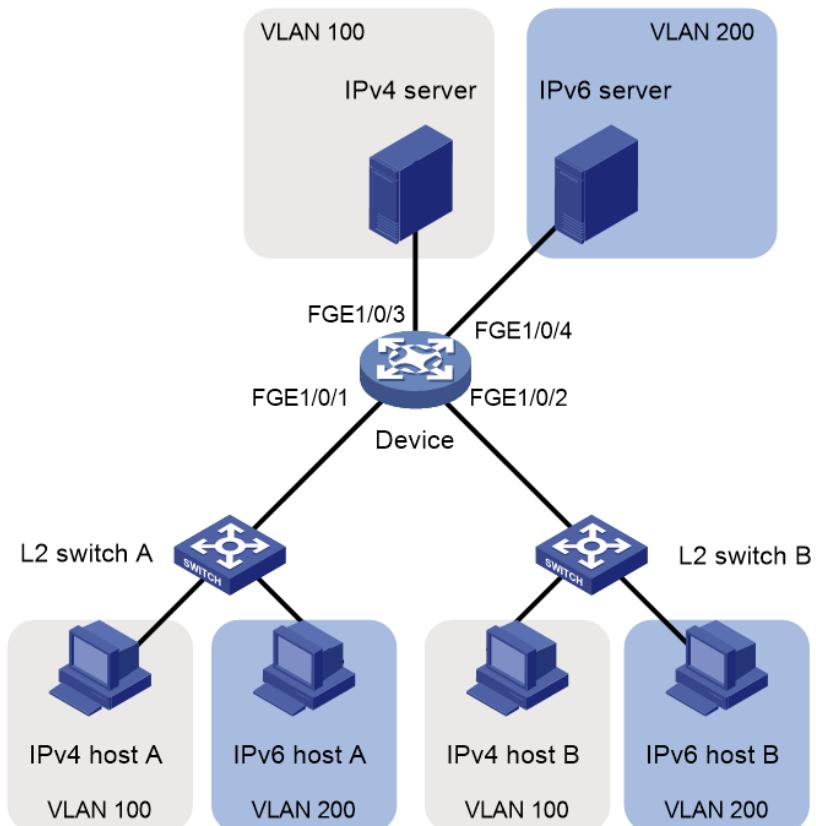
Hình 2.2.2. 2 Mô hình Port-Based VLAN

- VLAN IP (Subnet-based VLAN) là loại VLAN được phân chia theo địa chỉ IP của các thiết bị trong mạng. Người quản trị mạng có thể tạo VLAN dựa trên các địa chỉ IP thuộc cùng một mạng con (subnet), giúp cho các thiết bị trong cùng một VLAN có thể truy cập trực tiếp vào nhau mà không cần thông qua router.



Hình 2.2.2. 3 Mô hình Subnet-Based VLAN

- VLAN vùng (Protocol-based VLAN) là loại VLAN được phân chia dựa trên giao thức mạng, ví dụ như VLAN cho giao thức VoIP hoặc VLAN cho giao thức video. Loại VLAN này giúp tối ưu hóa hiệu suất mạng cho các ứng dụng cụ thể.



Hình 2.2.2. 4 Mô hình Protocol-based VLAN

- VLAN phiên bản (Voice VLAN) là loại VLAN được sử dụng cho các hệ thống thoại IP, giúp tách riêng dữ liệu thoại và dữ liệu thông thường trong mạng. Với loại VLAN này, các thiết bị thoại IP được đưa vào một VLAN riêng biệt và được ưu tiên truy cập để đảm bảo chất lượng thoại tốt nhất.

Tóm lại, VLAN là công nghệ cho phép phân chia một mạng vật lý thành nhiều mạng ảo độc lập nhau. Các loại VLAN khác nhau được sử dụng tùy thuộc vào nhu cầu sử dụng mạng của từng công ty hoặc tổ chức. Tuy nhiên, sử dụng

VLAN đúng cách có thể giúp tăng hiệu quả sử dụng mạng, cải thiện bảo mật và quản lý dễ dàng hơn.

2.2.3 *Cách thức hoạt động*

Cách thức hoạt động của VLAN bao gồm các bước sau:

Bước 1: Xác định các port

Trong một switch, các cổng được sử dụng để kết nối các thiết bị mạng vào mạng LAN. Để tạo ra các VLAN, các cổng này được phân loại và xác định là thuộc về VLAN nào. Các cổng này được gán cho một VLAN cụ thể và chỉ có thể truy cập các thiết bị trong cùng VLAN đó.

Bước 2: Tạo ra các VLAN

Sau khi các cổng được xác định, các VLAN sẽ được tạo ra. Các VLAN được tạo ra với mục đích phân tách mạng vật lý thành các mạng logic khác nhau. Các VLAN này có thể được đặt tên và số hiệu để dễ dàng quản lý về sau.

Bước 3: Thiết lập các cấu hình VLAN

Một số cấu hình VLAN có thể được thiết lập theo nhu cầu của người quản trị mạng. Ví dụ, các giá trị như địa chỉ IP, subnet mask, default gateway và DNS server có thể được thiết lập cho mỗi VLAN.

Bước 4: Liên kết VLAN

Các VLAN có thể được liên kết với nhau để cho phép các thiết bị trong các VLAN khác nhau có thể truy cập vào nhau. Điều này có thể được thực hiện bằng cách tạo ra các VLAN trunk, là các kết nối mạng giữa các switch hoặc router.

Bước 5: Quản lý VLAN

Việc quản lý VLAN gồm việc thêm hoặc xóa các VLAN cụ thể, chỉnh sửa cấu hình của các VLAN và đảm bảo rằng các cổng và VLAN được gán đúng.

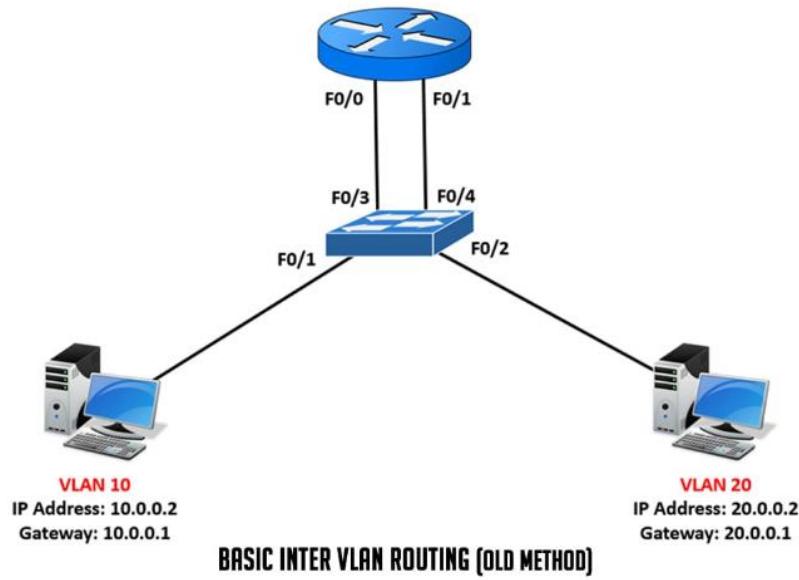
Tóm lại, VLAN là một công nghệ mạng cho phép phân chia một mạng vật lý thành các mạng logic khác nhau. Các VLAN được tạo ra bằng cách xác định các cổng và thiết lập các cấu hình phù hợp. Các VLAN có thể được liên kết để cho phép truy cập giữa các VLAN khác nhau. Việc quản lý VLAN bao gồm thêm, xóa và chỉnh sửa các VLAN cụ thể cũng như đảm bảo rằng các cổng được gán đúng và các VLAN được quản lý một cách hiệu quả.

2.3 Inter - VLAN Routing (Switch Virtual Interface SVI)

2.3.1 Giới thiệu về Inter-VLAN Routing

Inter-VLAN Routing là một kỹ thuật quan trọng trong mạng máy tính, cho phép các thiết bị trong các VLAN (Virtual Local Area Network) khác nhau có thể giao tiếp với nhau. Nó cho phép các thiết bị trong các VLAN khác nhau truy cập vào các tài nguyên và dịch vụ trên một mạng chung. Inter-VLAN Routing được sử dụng rộng rãi trong các tổ chức, doanh nghiệp và trường học để cung cấp truy cập mạng an toàn và hiệu quả.

Trong một mạng LAN, các thiết bị nằm trong cùng một VLAN sẽ có thể giao tiếp với nhau thông qua một switch hoặc bridge. Tuy nhiên, khi các thiết bị nằm trong các VLAN khác nhau, chúng sẽ không thể giao tiếp trực tiếp với nhau. Để giải quyết vấn đề này, Inter-VLAN Routing được sử dụng. Trong Inter-VLAN Routing, một router được sử dụng để kết nối các VLAN khác nhau và cho phép các thiết bị trong các VLAN khác nhau giao tiếp với nhau thông qua router.



Hình 2.3.1. 1 Mô hình Inter-VLAN Routing

Có hai phương pháp chính để triển khai Inter-VLAN Routing: đó là sử dụng Router on a Stick và sử dụng Layer 3 Switch. Trong phương pháp Router on a Stick, một router được sử dụng để kết nối tất cả các VLAN và cho phép các thiết bị trong các VLAN khác nhau giao tiếp với nhau thông qua router. Khi sử dụng phương pháp này, toàn bộ lưu lượng truy cập giữa các VLAN sẽ đi qua router, làm giảm hiệu suất mạng.

Phương pháp thứ hai là sử dụng Layer 3 Switch. Layer 3 Switch có thể đóng vai trò như một router, được thiết kế để hỗ trợ Inter-VLAN Routing. Với phương pháp này, các switch đầu cuối được kết nối trực tiếp với Layer 3 Switch và không cần phải đi qua router. Điều này làm giảm thiểu lưu lượng mạng, đồng thời cải thiện hiệu suất mạng.

Một số lợi ích của Inter-VLAN Routing bao gồm:

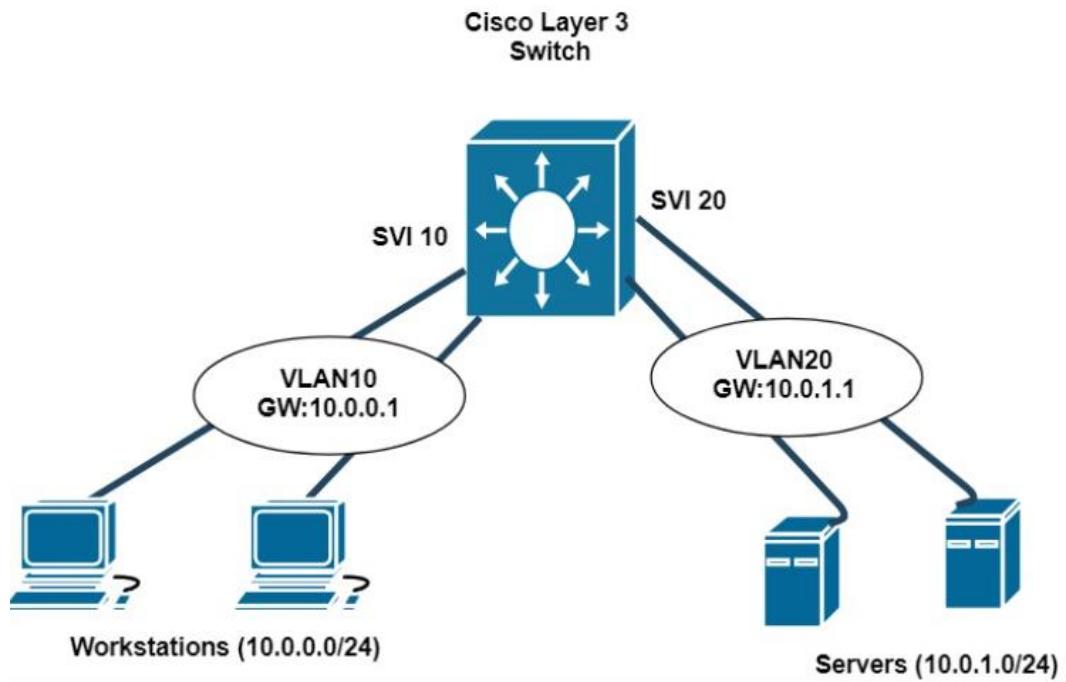
Tăng tính bảo mật: Inter-VLAN Routing cho phép các VLAN khác nhau duy trì tính riêng tư và an toàn. Nó cung cấp một lớp bảo vệ bổ sung bằng cách ngăn chặn các thiết bị không thuộc cùng VLAN truy cập vào tài nguyên mạng.

Cải thiện hiệu suất mạng: Inter-VLAN Routing giúp tối ưu hóa lưu lượng mạng vì nó cho phép các thiết bị trong các VLAN khác nhau giao tiếp trực tiếp với nhau mà không cần đi qua router.

Quản lý dễ dàng: Inter-VLAN Routing giúp quản lý mạng dễ dàng hơn bởi vì nó cho phép chia nhỏ mạng thành các VLAN khác nhau và tạo ra các chính sách riêng để quản lý các VLAN đó.

2.3.2 Giới thiệu về SVI

Switch Virtual Interface (SVI) là một khái niệm quan trọng trong kỹ thuật mạng, và nó liên quan đến việc triển khai các mạng VLAN (Virtual Local Area Network). SVI cho phép chúng ta tạo ra một địa chỉ IP ảo cho mỗi VLAN, giúp các thiết bị trong một VLAN có thể giao tiếp với các thiết bị trong một VLAN khác thông qua một router hoặc switch có tính năng định tuyến.



Hình 2.3.2. 1 Mô hình SVI

Khi triển khai các mạng VLAN, mỗi VLAN sẽ được xem như một mạng LAN riêng biệt và các thiết bị trong cùng VLAN sẽ có thể giao tiếp với nhau mà không cần

đến bất kỳ thiết bị nào khác. Tuy nhiên, để cho phép các thiết bị trong các VLAN khác nhau giao tiếp với nhau, chúng ta cần sử dụng một router hoặc switch định tuyến.

Có hai cách để triển khai việc giao tiếp giữa các VLAN khác nhau: sử dụng router-on-a-stick hoặc sử dụng SVI. Trong phương pháp router-on-a-stick, một router được kết nối với một switch thông qua một cổng trunk. Các sub-interface được cấu hình trên router, để cho phép các gói dữ liệu được chuyển tiếp giữa các VLAN khác nhau thông qua cổng trunk. Tuy nhiên, phương pháp này có thể gây ra tình trạng đám mây lưu lượng mạng.

Trong khi đó, SVI là giải pháp cho vấn đề này bằng cách cho phép chúng ta tạo một địa chỉ IP ảo cho mỗi VLAN trên switch. Địa chỉ IP ảo này sẽ trở thành default gateway của mỗi thiết bị trong VLAN tương ứng. Vì vậy, khi một thiết bị trong một VLAN muốn truy cập đến một thiết bị trong một VLAN khác, nó sẽ gửi gói tin đến địa chỉ IP ảo của VLAN đích. Switch sẽ sau đó định tuyến gói tin đến VLAN đích dựa trên địa chỉ IP ảo của VLAN.

Việc triển khai SVI mang lại một số lợi ích cho các mạng VLAN:

- Hiệu suất mạng cao hơn: Khi sử dụng SVI, các gói dữ liệu được chuyển tiếp trực tiếp từ switch đến switch mà không cần router hoặc switch định tuyến, giảm tình trạng đám mây lưu lượng mạng và cải thiện hiệu suất.
- Tối ưu hóa sử dụng tài nguyên: Với SVI, chúng ta không cần phải triển khai một số lượng lớn các router vật lý để định tuyến gói tin giữa các VLAN khác nhau. Điều này giúp tiết kiệm chi phí và tối ưu hóa sử dụng tài nguyên.
- Quản lý dễ dàng: SVI cho phép quản lý các VLAN dễ dàng hơn bằng cách chỉ cần quản lý một switch duy nhất thay vì nhiều router hay switch định tuyến khác nhau.

2.3.3 Các loại SVI

Có nhiều loại của SVI được hỗ trợ trên các switch hiện nay, và trong bài viết này, chúng ta sẽ điểm qua các loại thông dụng nhất.

- Basic SVI: Đây là loại SVI cơ bản nhất, chỉ cần tạo một interface ảo và gán một địa chỉ IP vào đó. Basic SVI thường được sử dụng để cung cấp dịch vụ định tuyến và điều khiển truy cập mạng cho các thiết bị khác kết nối tới switch.
- Routed SVI: Loại SVI này có thể được sử dụng để thực hiện các chức năng định tuyến Layer 3 trên switch. Routed SVI được cấu hình với một mạng con (subnet) cụ thể và thường được sử dụng để định tuyến giữa các VLAN trên switch hoặc với các mạng ngoài.
- Management SVI: Loại SVI này được sử dụng để quản lý từ xa switch. Nó được thiết lập trên một VLAN riêng biệt, và được truy cập từ xa thông qua một địa chỉ IP. Management SVI thường được sử dụng để quản lý switch khi không có kết nối console hoặc telnet.
- VRF-aware SVI: Đây là loại SVI có khả năng hỗ trợ các Virtual Routing and Forwarding (VRF) khác nhau. Khi VRF-aware SVI được sử dụng, mỗi VRF sẽ có một SVI tương ứng trên switch. Loại SVI này cho phép chúng ta thiết lập các mạng con khác nhau trên các VRF khác nhau, giúp quản lý tốt hơn các mạng con trên switch.
- Private-VLAN SVI: Loại SVI này được sử dụng để triển khai các Private VLAN trên switch. Các Private VLANs cung cấp một cơ chế bảo mật hiệu quả bằng cách giới hạn sự truy cập giữa các máy tính trong cùng một VLAN. Với Private-VLAN SVI, chúng ta có thể tạo ra một gateway cho các VLAN private.

- Transparent SVI: Loại SVI này cho phép chúng ta tạo ra một interface ảo trên switch, mà không cần cấu hình địa chỉ IP. Transparent SVI được sử dụng để kết nối các switch Layer 2 với nhau để tạo thành một switch Layer 2 lớn hơn.
- Layer 2 SVI: Loại SVI này sử dụng để giải quyết các vấn đề liên quan đến STP (Spanning Tree Protocol). Khi một switch Layer 3 được cấu hình với một Layer 2 SVI, interface SVI sẽ tham gia vào tiến trình STP của switch và giúp loại bỏ các loop trên mạng.

2.3.4 Cách thức hoạt động

Inter-VLAN Routing là một kỹ thuật cho phép truyền thông giữa các VLAN trên cùng một switch hoặc giữa các switch khác nhau trong mạng. Để thực hiện Inter-VLAN Routing, chúng ta sử dụng Switch Virtual Interface (SVI).

Bước 1: Cấu hình SVI trên switch

Đầu tiên, chúng ta cần tạo ra các VLAN trên switch và gán các cổng vào VLAN tương ứng. Sau đó, chúng ta cấu hình Switch Virtual Interface (SVI) trên switch để cho phép các VLAN trên switch có thể giao tiếp với nhau. SVI được tạo ra bằng cách chỉ định một địa chỉ IP trong subnet của mỗi VLAN.

Bước 2: Tạo đường đi giữa các VLAN

Sau khi đã cấu hình SVI, chúng ta cần tạo ra đường đi giữa các VLAN để có thể truyền thông giữa chúng. Để làm điều này, chúng ta có hai phương pháp:

Sử dụng Router-on-a-Stick: Phương pháp này sử dụng một router ngoài để định tuyến giữa các VLAN trên switch. Các VLAN được kết nối với router thông qua một cổng duy nhất trên switch (thường là cổng trunk). Router sẽ xử lý các gói tin được gửi giữa các VLAN và định tuyến chúng đến đích.

Sử dụng Layer 3 switch: Một số switch hiện đại hỗ trợ khả năng định tuyến Layer 3, cho phép chúng ta định tuyến giữa các VLAN trên cùng một switch. Trong trường hợp này, SVI được sử dụng để định tuyến giữa các VLAN trên switch.

Bước 3: Cấu hình định tuyến

Sau khi đã tạo ra đường đi giữa các VLAN, chúng ta cần cấu hình định tuyến trên switch hoặc router để cho phép các VLAN giao tiếp với nhau thông qua đường đi này. Đối với phương pháp Router-on-a-Stick, chúng ta cấu hình router để cho phép định tuyến giữa các VLAN trên switch. Đối với phương pháp Layer 3 switch, chúng ta cấu hình switch để định tuyến giữa các VLAN.

Bước 4: Kiểm tra kết nối

Cuối cùng, chúng ta cần kiểm tra tính đúng đắn của kết nối giữa các VLAN bằng cách ping từ một thiết bị trong một VLAN đến một thiết bị trong VLAN khác. Nếu kết quả trả về là thành công, nghĩa là Inter-VLAN Routing đã được cấu hình đúng và hoạt động tốt.

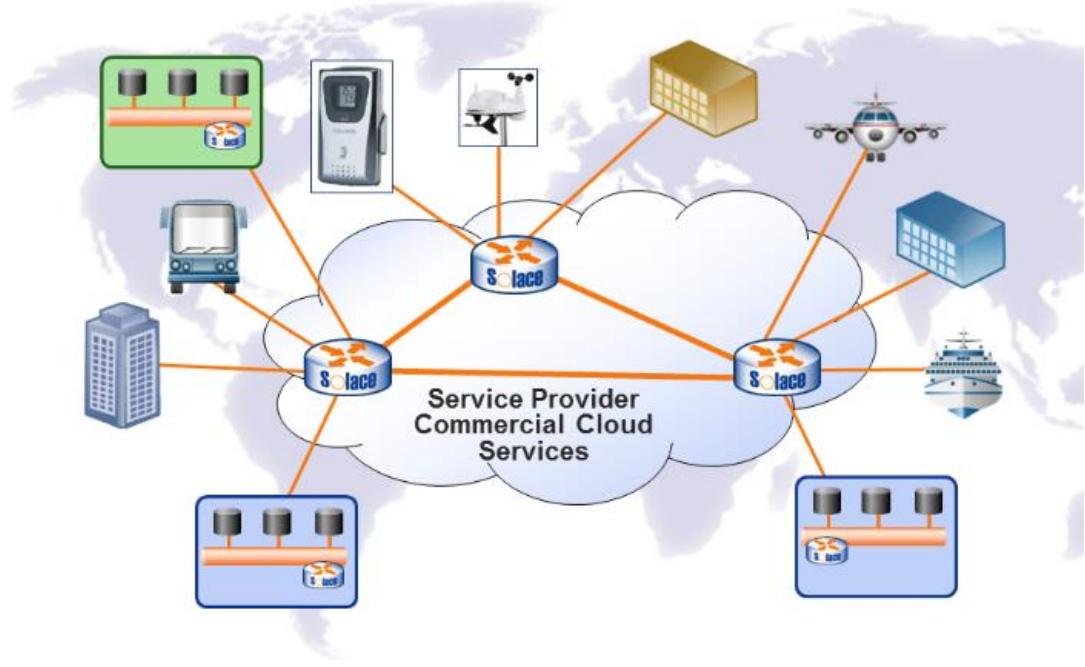
2.4 Internet Service Providers (ISPs)

2.4.1 Giới thiệu về ISPs

Internet Service Providers (ISPs) là các tổ chức cung cấp kết nối mạng Internet cho người dùng. Các ISP có thể là các doanh nghiệp tư nhân, tổ chức phi lợi nhuận hoặc cơ quan chính phủ. Với sự phát triển của công nghệ và nhu cầu sử dụng Internet ngày càng tăng cao, vai trò của các ISP trở nên quan trọng hơn bao giờ hết.

Công việc chính của các ISP là cung cấp kết nối Internet cho khách hàng của họ. Để đảm bảo việc này, các ISP cần đầu tư vào cơ sở hạ tầng để cung cấp kết nối mạng cho khách hàng của họ, bao gồm cả việc xây dựng và bảo trì các đường truyền và thiết bị. Các ISP phải tính toán cẩn thận để đảm bảo rằng họ có thể đáp ứng được

nhu cầu ngày càng tăng của khách hàng và đáp ứng được các yêu cầu về băng thông và tốc độ truy cập.



Hình 2.4.1. 1 Mô hình ISP

Các ISP cung cấp nhiều loại dịch vụ khác nhau. Một số dịch vụ phổ biến bao gồm:

Truy cập Internet: Đây là dịch vụ cơ bản mà các ISP cung cấp. Truy cập Internet cho phép người dùng truy cập vào các trang web và các ứng dụng khác thông qua mạng Internet.

Hosting: Dịch vụ hosting cho phép người dùng lưu trữ các trang web của họ trên máy chủ của các ISP.

Email hosting: Một số ISP cung cấp dịch vụ email hosting để người dùng có thể gửi và nhận email.

Domain Name Registration: Các ISP cung cấp dịch vụ đăng ký tên miền cho người dùng của họ.

Virtual Private Network (VPN): Dịch vụ VPN cho phép người dùng kết nối với mạng internet một cách an toàn và bảo mật hơn.

Dịch vụ điện thoại: Một số ISP cung cấp dịch vụ điện thoại bằng cách sử dụng giao thức Voice over IP (VoIP).

Ngoài ra, các ISP còn có thể cung cấp các dịch vụ khác như quản lý và bảo trì hệ thống, bảo mật mạng và giám sát băng thông.

Các ISP thường phải tuân theo các quy định của chính phủ và các tổ chức quốc tế liên quan đến việc hoạt động của họ. Nhiều quốc gia đã thiết lập các quy định về net neutrality (tức là nguyên tắc không phân biệt đối xử) để đảm bảo rằng các ISP không giới hạn truy cập vào nội dung trên Internet hoặc ưu tiên một số dịch vụ Internet hơn các dịch vụ khác.

2.4.2 Các loại ISPs

Internet Service Providers (ISPs) là các tổ chức cung cấp kết nối mạng Internet cho người dùng. Các ISP có thể được phân loại theo nhiều cách khác nhau, bao gồm:

- Các ISP truyền thống: Đây là các công ty cung cấp dịch vụ truyền hình cáp hoặc dịch vụ điện thoại di động có thêm dịch vụ truy cập Internet.
- Các ISP qua đường dây điện thoại: Các ISP sử dụng đường dây điện thoại để cung cấp kết nối Internet cho khách hàng của họ. Một số ISP sử dụng công nghệ ADSL (Asymmetric Digital Subscriber Line) để truyền tải dữ liệu qua đường dây điện thoại.
- Các ISP qua cáp quang: Các ISP này sử dụng cáp quang để truyền tải dữ liệu và cung cấp kết nối Internet cho khách hàng của họ. Kết nối cáp quang thường cung cấp băng thông cao hơn so với các công nghệ truyền tải khác.

- Các ISP qua vệ tinh: Các ISP sử dụng truyền thông vệ tinh để cung cấp kết nối Internet cho khách hàng của họ. Điều này đặc biệt hữu ích cho những vùng khó tiếp cận hoặc nơi mà hạ tầng truyền thông không phát triển.
- Các ISP qua Wi-Fi công cộng: Đây là các ISP cung cấp kết nối Internet thông qua các điểm phát sóng Wi-Fi công cộng. Người dùng có thể truy cập Internet bằng cách kết nối với điểm phát sóng trên điện thoại di động, máy tính bảng hoặc laptop của mình.
- Các ISP qua mạng di động: Các ISP này cung cấp kết nối Internet thông qua mạng di động. Người dùng có thể truy cập Internet bằng cách sử dụng điện thoại di động hoặc các thiết bị khác kết nối với mạng di động của ISP.

2.4.3 *Cách thức hoạt động*

Internet Service Providers (ISPs) là các tổ chức cung cấp kết nối mạng Internet cho người dùng. Để cung cấp dịch vụ này, các ISP phải hoạt động theo một quá trình phức tạp bao gồm:

- Tạo ra một mạng truyền thông: Các ISP cần xây dựng và bảo trì hạ tầng để cung cấp kết nối mạng cho khách hàng của họ. Điều này bao gồm việc xây dựng và bảo trì các đường truyền và thiết bị để đảm bảo rằng khách hàng có thể truy cập Internet một cách nhanh chóng và hiệu quả.
- Kết nối với các nhà cung cấp Internet khác: Để cung cấp khả năng truy cập tốt nhất cho khách hàng của họ, các ISP sẽ kết nối với các nhà cung cấp Internet khác. Điều này giúp cho các ISP có thể truyền tải dữ liệu giữa các mạng khác nhau và cung cấp kết nối mạng toàn cầu cho khách hàng của họ.
- Cung cấp dịch vụ cho khách hàng: Sau khi đã xây dựng mạng truyền thông và kết nối với các nhà cung cấp Internet khác, các ISP sẽ cung cấp dịch vụ

cho khách hàng của họ. Điều này bao gồm việc đảm bảo rằng khách hàng có thể truy cập Internet một cách nhanh chóng và hiệu quả, và cung cấp các dịch vụ khác như email, hosting và VPN.

- Quản lý kết nối mạng: Các ISP phải quản lý kết nối mạng của khách hàng của họ để đảm bảo rằng các kết nối được duy trì ổn định và có sức mạnh tín hiệu đủ để truy cập Internet.

Các ISP cũng phải tuân theo các quy định của chính phủ và các tổ chức quốc tế liên quan đến việc hoạt động của họ. Nhiều quốc gia đã thiết lập các quy định về net neutrality (tức là nguyên tắc không phân biệt đối xử) để đảm bảo rằng các ISP không giới hạn truy cập vào nội dung trên Internet hoặc ưu tiên một số dịch vụ Internet hơn các dịch vụ khác.

Các ISP thường sẽ cung cấp cho khách hàng một loạt các gói dịch vụ khác nhau để đáp ứng nhu cầu của từng khách hàng. Những gói dịch vụ này sẽ có giá cả và tính năng khác nhau tùy vào loại dịch vụ và mức độ băng thông, tốc độ truy cập và các tính năng bổ sung.

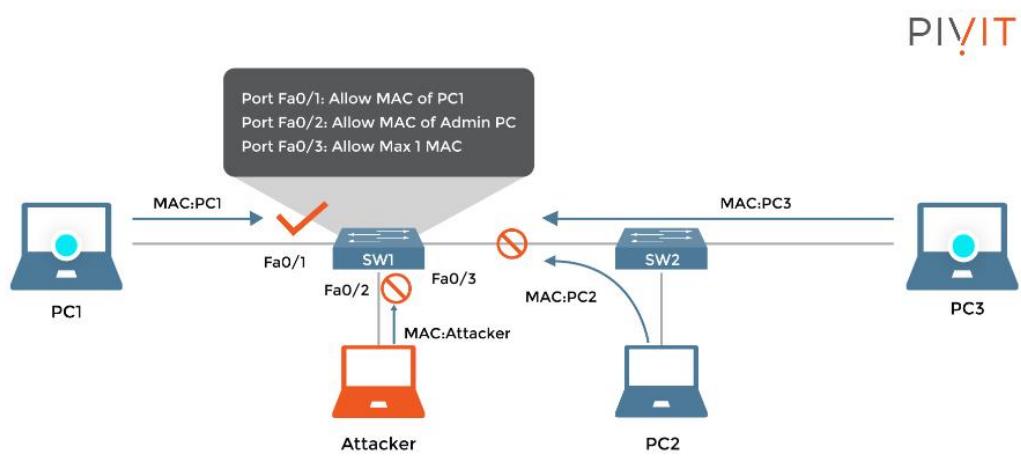
Thường thì, khách hàng sẽ phải ký hợp đồng với ISP để có thể sử dụng được dịch vụ của họ. Hợp đồng này sẽ ghi rõ các điều khoản và điều kiện sử dụng dịch vụ, các yêu cầu về bảo mật và quyền riêng tư và chi phí sử dụng dịch vụ.

2.5 Port-Security

2.5.1 Giới thiệu về Port-Security

Port-Security là một tính năng trong hệ thống mạng Cisco, được thiết kế để bảo vệ lớp 2 trên mạng Ethernet. Port-Security giúp ngăn chặn các cuộc tấn công từ bên ngoài như MAC flooding hoặc ARP poisoning, cũng như giảm thiểu các rủi ro an ninh liên quan đến việc sử dụng các thiết bị không được cho phép truy cập vào mạng.

Tính năng Port-Security cũng có khả năng phát hiện các cuộc tấn công từ bên ngoài và ngăn chặn chúng. Ví dụ, khi một hacker cố gắng phá vỡ bảo mật của một mạng bằng cách gửi nhiều thông điệp Ethernet với các địa chỉ MAC giả mạo, Port-Security sẽ phát hiện ra và chặn lại những thông điệp này. Nó cũng có thể giúp ngăn chặn việc ARP poisoning bằng cách theo dõi giao thức ARP và từ chối bất kỳ yêu cầu ARP nào từ các thiết bị không được cho phép.



Hình 2.5.1. 1 Port-Security

Port-Security cho phép quản trị viên mạng tăng cường bảo mật của hệ thống mạng bằng cách giới hạn số lượng thiết bị được phép truy cập vào mạng và chặn các cuộc tấn công từ bên ngoài. Tính năng này cũng cho phép quản trị viên tìm hiểu chính xác hơn về các thiết bị được kết nối vào mạng, cũng như làm giảm rủi ro an ninh liên quan đến việc sử dụng các thiết bị không được cho phép.

Những điểm cần lưu ý khi triển khai Port-Security là về khả năng ảnh hưởng đến tính khả dụng của mạng. Khi một số thiết bị không đăng ký được kết nối vào cổng switch, chúng sẽ bị loại bỏ khỏi mạng. Điều này có thể gây ra sự cố không đáng có nếu các thiết bị bị loại bỏ là các thiết bị quan trọng, hoặc nếu số lượng thiết bị được cho phép truy cập vào mạng không đủ.

2.5.2 Cách thức hoạt động

Port-Security hoạt động dựa trên việc giới hạn số lượng thiết bị được phép kết nối với mạng thông qua một cổng Ethernet trên switch. Điều này được thực hiện bằng cách xác định danh sách các địa chỉ MAC của các thiết bị được cho phép sử dụng cổng Ethernet đó. Khi một thiết bị mới được kết nối vào cổng Ethernet đó, Port-Security sẽ kiểm tra xem địa chỉ MAC của thiết bị đó có nằm trong danh sách được phép hay không. Nếu địa chỉ MAC của thiết bị không được liệt kê trong danh sách, thiết bị sẽ không được phép truy cập vào mạng.

Port-Security cũng có khả năng phát hiện và ngăn chặn các cuộc tấn công từ bên ngoài. Ví dụ, khi một hacker cố gắng phá vỡ bảo mật của một mạng bằng cách gửi nhiều thông điệp Ethernet với các địa chỉ MAC giả mạo, Port-Security sẽ phát hiện ra và chặn lại những thông điệp này. Nó cũng có thể giúp ngăn chặn việc ARP poisoning bằng cách theo dõi giao thức ARP và từ chối bất kỳ yêu cầu ARP nào từ các thiết bị không được cho phép.

2.5.3 Các phương pháp cấu hình Port-Security

Phương pháp cấu hình Port-Security

Port-Security có thể được cấu hình trên các cổng Ethernet trên switch Cisco để giới hạn số lượng thiết bị được phép sử dụng cổng đó. Quý vị có thể cấu hình Port-Security trực tiếp trên switch hoặc thông qua giao diện dòng lệnh (CLI).

Bước 1: Kích hoạt tính năng Port-Security trên switch

Trước khi bắt đầu cấu hình Port-Security, quý vị cần kích hoạt tính năng này trên switch.

Bước 2: Thiết lập chính sách bảo mật

Sau khi kích hoạt tính năng Port-Security, cần thiết lập chính sách bảo mật để xác định danh sách các địa chỉ MAC được phép truy cập vào mạng. Các địa chỉ MAC này sẽ được đặt trong danh sách được phép.

Bước 3: Thiết lập hành động khi có sự vi phạm

Khi một thiết bị không được cho phép được kết nối vào cổng Ethernet đã cấu hình, Port-Security sẽ thực hiện một số hành động khác nhau

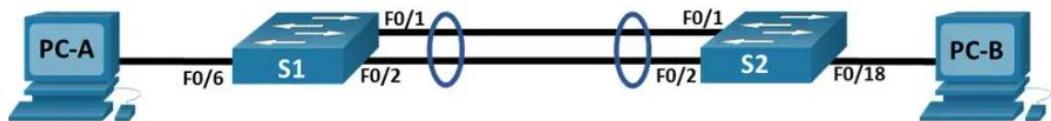
Bước 4: Lưu cấu hình

Sau khi hoàn thành việc cấu hình Port-Security, cần lưu cấu hình để switch có thể sử dụng cấu hình đã được thiết lập.

2.6 EtherChannel

2.6.1 Giới thiệu về EtherChannel

EtherChannel là một kỹ thuật được sử dụng để kết hợp nhiều đường truyền vật lý thành một liên kết logic duy nhất giữa các thiết bị mạng như switch và router. Kỹ thuật này còn được gọi là port-channeling.

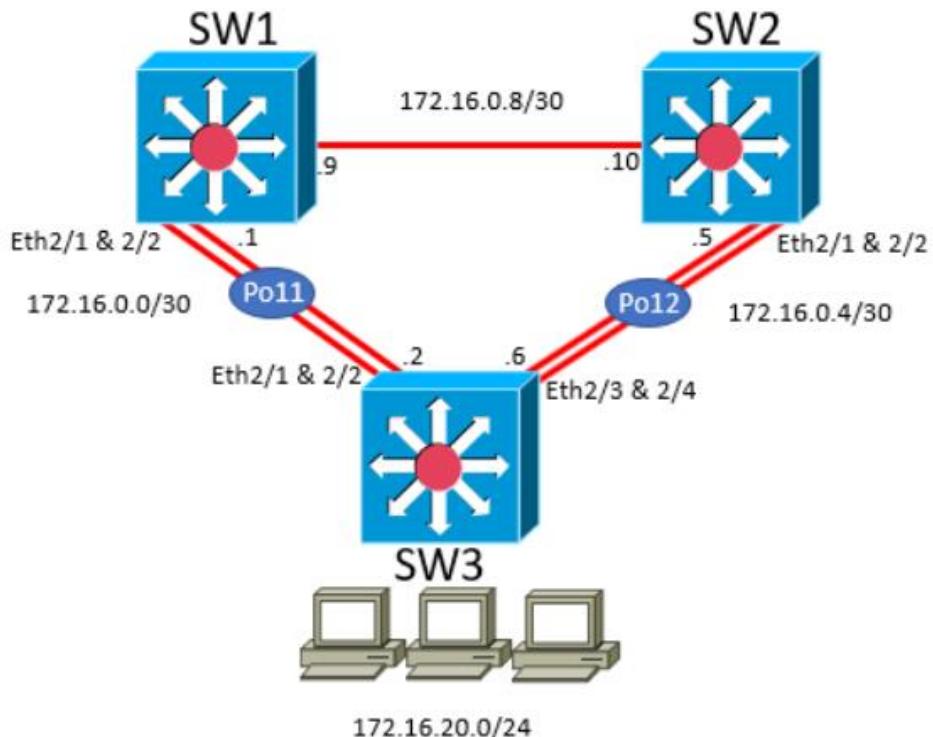


Hình 2.6.1. 1 Mô hình EtherChannel

Việc sử dụng EtherChannel có thể giúp tăng khả năng truyền tải dữ liệu của một mạng, đồng thời tăng tính sẵn sàng và độ tin cậy của mạng do có thêm các đường truyền phụ trợ. Ngoài ra, việc kết hợp nhiều đường truyền thành một liên kết logic cũng giúp tối ưu hóa tài nguyên mạng và giảm thiểu rủi ro trong trường hợp một đường truyền bị lỗi.

Có hai loại EtherChannel phổ biến: EtherChannel trên cùng một switch và EtherChannel giữa các switch khác nhau. Trong EtherChannel trên cùng một switch, các cổng trên switch được kết hợp lại thành một liên kết logic. Trong khi đó, trong

EtherChannel giữa các switch khác nhau, các liên kết vật lý giữa các switch được kết hợp lại thành một liên kết logic.



Hình 2.6.1. 2 Mô hình Etherchannel giữa các Switch

Trong quá trình hoạt động, các gói dữ liệu sẽ được chia thành các khối nhỏ và gửi trên các đường truyền khác nhau trên liên kết logic của EtherChannel. Để đảm bảo tính toàn vẹn dữ liệu, các khối này sẽ được kiểm tra lỗi CRC khi đến đích và sẽ được sắp xếp lại thành các khối gốc ban đầu trước khi được chuyển tiếp đến máy tính đích.

Tuy nhiên, việc triển khai EtherChannel cần được thực hiện cẩn thận và theo đúng hướng dẫn để tránh gặp phải các vấn đề về độ tin cậy và hiệu suất mạng. Ví dụ, không nên kết hợp các cổng kết nối đến các switch khác nhau trong cùng một EtherChannel do có rủi ro về loop. Ngoài ra, cũng cần chọn các giao thức EtherChannel phù hợp với các thiết bị mạng và cài đặt chính xác các thông số để đảm bảo tính sẵn sàng và độ tin cậy của mạng.

2.6.2 Điều kiện cấu hình EtherChannel

Điều kiện cấu hình EtherChannel là một trong những yếu tố quan trọng để đảm bảo tính sẵn sàng và độ tin cậy của mạng máy tính. Việc thực hiện cấu hình EtherChannel đúng cách giúp kết hợp các cổng vật lý thành một liên kết logic duy nhất, tăng khả năng truyền tải dữ liệu và giảm thiểu rủi ro do một đường truyền bị lỗi.

Trong quá trình cấu hình EtherChannel, có một số điều kiện cần phải được đáp ứng như sau:

- Tốc độ cổng: Các cổng được kết hợp lại trong EtherChannel phải có cùng tốc độ. Nếu không, sự khác biệt về tốc độ giữa các cổng sẽ gây ra sự chậm trễ và hiệu suất kém của mạng.
- Duplex mode: Các cổng phải hoạt động ở cùng chế độ duplex mode. Nếu một cổng hoạt động ở chế độ half-duplex trong khi cổng khác hoạt động ở chế độ full-duplex, tính toàn vẹn và độ tin cậy của mạng có thể bị ảnh hưởng.
- Địa chỉ MAC: Mỗi giao diện mạng phải có địa chỉ MAC riêng biệt. Điều này giúp giảm thiểu rủi ro gửi các gói dữ liệu trùng lặp và tăng cường tính sẵn sàng của mạng.
- Cấu hình EtherChannel: Mỗi giao diện mạng được sử dụng trong EtherChannel phải được cấu hình để hoạt động trong EtherChannel. Hai giao thức phổ biến được sử dụng để cấu hình EtherChannel là Port Aggregation Protocol (PAgP) của Cisco và Link Aggregation Control Protocol (LACP) chuẩn IEEE 802.3ad.

2.6.3 Cách thức hoạt động

Cách thức hoạt động của EtherChannel là quá trình kết hợp nhiều đường truyền vật lý thành một liên kết logic duy nhất giữa các thiết bị mạng như switch và router. Kỹ thuật này còn được gọi là link aggregation hoặc port-channeling.

Trong quá trình hoạt động, các gói dữ liệu sẽ được chia thành các khối nhỏ và gửi trên các đường truyền khác nhau trên liên kết logic của EtherChannel. Các khối dữ liệu này được gọi là frames trong giao thức Ethernet. Mỗi frame bao gồm tiêu đề và phần thân dữ liệu. Tiêu đề giúp định danh các frame và chỉ định các thông số quan trọng như địa chỉ nguồn và đích.

Các khối dữ liệu sẽ được gửi trên các đường truyền khác nhau trong EtherChannel theo cơ chế round-robin. Điều này có nghĩa là mỗi khối dữ liệu sẽ được gửi qua một đường truyền khác nhau trong liên kết logic. Khi các khối dữ liệu đến đích, chúng sẽ được kiểm tra lỗi CRC để đảm bảo tính toàn vẹn dữ liệu. Sau đó, các khối dữ liệu sẽ được sắp xếp lại theo thứ tự gốc ban đầu trước khi được chuyển tiếp đến máy tính đích.

Ngoài ra, cơ chế đòn hồi cũng là một phần quan trọng trong hoạt động của EtherChannel. Nếu một trong các cổng trên EtherChannel bị lỗi, cơ chế đòn hồi sẽ cho phép dữ liệu được chuyển tiếp qua các đường truyền khác trong liên kết logic. Điều này giúp tăng tính sẵn sàng và độ tin cậy của mạng.

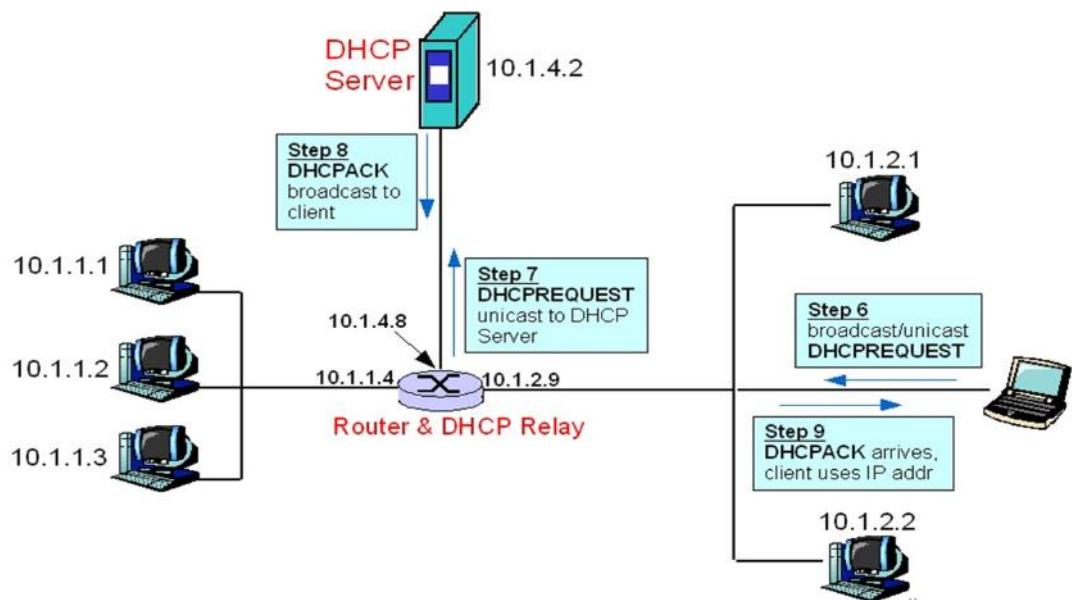
2.7 Dynamic Host Configuration Protocol (DHCP)

2.7.1 Giới thiệu về DHCP

Dynamic Host Configuration Protocol (DHCP) là một giao thức mạng được sử dụng để cấp phát địa chỉ IP và các thông số mạng khác cho các thiết bị trong một mạng. DHCP giúp cho quá trình quản lý địa chỉ IP trở nên đơn giản hơn và hiệu quả hơn, đặc biệt là trong các mạng có nhiều thiết bị kết nối.

DHCP hoạt động theo cơ chế client-server, với máy chủ DHCP cung cấp các địa chỉ IP và thông tin mạng khác cho các thiết bị yêu cầu. Khi một thiết bị mới được kết nối vào mạng, nó sẽ gửi yêu cầu đến máy chủ DHCP để yêu cầu một địa chỉ IP và các thông số mạng khác, như subnet mask, default gateway và DNS server.

Máy chủ DHCP sẽ nhận yêu cầu này và cung cấp một địa chỉ IP trong pool địa chỉ mà nó quản lý. Địa chỉ IP này được cấp cho thiết bị yêu cầu và các thông số mạng khác cũng được cung cấp kèm theo. Sau đó, thiết bị sẽ sử dụng các thông số này để thiết lập kết nối mạng của mình.



Hình 2.7.1. 1 Mô hình cấp phát địa chỉ bằng DHCP

Một trong những ưu điểm của DHCP là nó giúp cho việc quản lý địa chỉ IP trở nên dễ dàng hơn, đặc biệt là trong các mạng lớn với hàng trăm hoặc hàng ngàn thiết bị kết nối. Nếu không có DHCP, việc quản lý địa chỉ IP sẽ trở nên rất khó khăn và tốn nhiều thời gian.

Ngoài ra, DHCP cũng giúp cho quá trình cấu hình mạng trở nên tự động hóa hơn. Thay vì phải cấu hình thủ công các thông số mạng cho từng thiết bị, ta có thể sử dụng DHCP để tự động cấu hình các thông số này cho toàn bộ mạng.

Tuy nhiên, cũng cần lưu ý rằng việc sử dụng DHCP cũng có những hạn chế. Điển hình là khi máy chủ DHCP gặp sự cố hoặc bị tấn công, toàn bộ mạng sẽ bị ảnh hưởng và không thể kết nối được. Do đó, cần có các biện pháp bảo vệ và sao lưu để đảm bảo tính sẵn sàng và tin cậy cho mạng.

Trong các mạng lớn, DHCP còn được sử dụng để áp dụng các chính sách mạng, như giới hạn thời gian thuê địa chỉ IP hay cung cấp các thông tin khác cho các thiết bị trong mạng. Điều này giúp cho việc quản lý và bảo vệ mạng trở nên hiệu quả hơn.

2.7.2 Các bước để lấy một địa chỉ từ DHCP

Để lấy một địa chỉ IP từ DHCP, ta cần phải thực hiện một số bước nhất định. Dưới đây là các bước chi tiết để lấy một địa chỉ IP từ DHCP:

Bước 1: Thiết lập kết nối mạng

Trước khi có thể sử dụng DHCP để lấy địa chỉ IP, thiết bị của bạn phải đã được kết nối với mạng. Điều này có thể được thực hiện thông qua Wi-Fi hoặc cáp Ethernet. Nếu thiết bị của bạn chưa được kết nối với một mạng nào, bạn sẽ không thể lấy được địa chỉ IP từ DHCP.

Bước 2: Yêu cầu địa chỉ IP

Sau khi thiết lập kết nối mạng, thiết bị của bạn sẽ tự động gửi yêu cầu địa chỉ IP đến máy chủ DHCP trên mạng. Yêu cầu này sẽ bao gồm địa chỉ MAC của thiết bị của bạn và yêu cầu cho một địa chỉ IP mới.

Bước 3: Máy chủ DHCP nhận yêu cầu

Sau khi nhận được yêu cầu địa chỉ IP từ thiết bị của bạn, máy chủ DHCP sẽ kiểm tra vào danh sách các địa chỉ IP khả dụng và cung cấp một địa chỉ IP mới cho

thiết bị của bạn. Máy chủ DHCP cũng sẽ cung cấp các thông tin mạng đầy đủ, như subnet mask, default gateway và DNS server.

Bước 4: Thiết bị cập nhật cài đặt mạng

Sau khi máy chủ DHCP cung cấp địa chỉ IP và các thông tin mạng khác, thiết bị của bạn sẽ tự động cập nhật cài đặt mạng để sử dụng các giá trị này. Điều này bao gồm cập nhật địa chỉ IP cũng như các thông số mạng khác, như subnet mask, default gateway và DNS server.

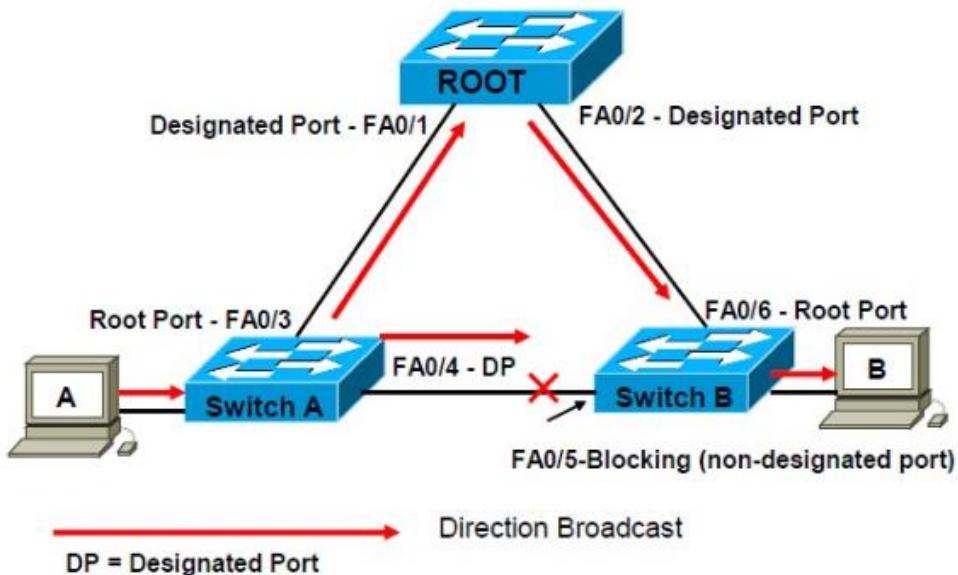
Bước 5: Kết nối mạng hoàn tất

Sau khi cài đặt mạng đã được cập nhật với các giá trị mới từ máy chủ DHCP, thiết bị của bạn sẽ kết nối thành công với mạng qua địa chỉ IP mới được cấp phát. Nếu có bất kỳ vấn đề gì xảy ra trong quá trình này, thiết bị của bạn không thể kết nối với mạng.

2.8 Spanning Tree Protocol (STP)

2.8.1 Giới thiệu về STP

Spanning Tree Protocol (STP) là một giao thức mạng được sử dụng để loại bỏ các vòng lặp trong mạng Ethernet. Khi có nhiều đường truyền giữa các switch hoặc bridge, các vòng lặp có thể xảy ra và gây ra sự cố mạng. STP là giải pháp cho việc này, giúp cho mạng trở nên ổn định hơn và tránh được các vòng lặp.



Hình 2.8.1. 1 Mô hình STP

STP hoạt động bằng cách chọn một số cổng trên một switch hoặc bridge để đóng vai trò là cổng chính, còn lại là các cổng dự phòng. Các cổng trên switch hoặc bridge sẽ được gán một độ ưu tiên riêng biệt, được tính toán bằng thuật toán STP. Cổng nào có độ ưu tiên cao nhất sẽ được chọn làm cổng chính, các cổng khác sẽ được đóng cửa để tránh sự cố mạng.

Các thông số liên quan đến STP bao gồm root bridge, đường link tốt nhất và đường link dự phòng. Root bridge là switch hoặc bridge có độ ưu tiên cao nhất trong mạng. Đường link tốt nhất là đường đi từ switch hoặc bridge trực tiếp kết nối với root bridge. Đường link dự phòng là các đường đi khác từ switch hoặc bridge, được sử dụng khi đường link tốt nhất bị gián đoạn.

STP có thể được cấu hình và tùy chỉnh để đáp ứng các yêu cầu cụ thể của mạng. Ví dụ, chúng ta có thể thiết lập độ ưu tiên hoặc sử dụng các giao thức khác để cải thiện hiệu suất hoặc tính sẵn sàng của mạng.

Một số ưu điểm của STP bao gồm:

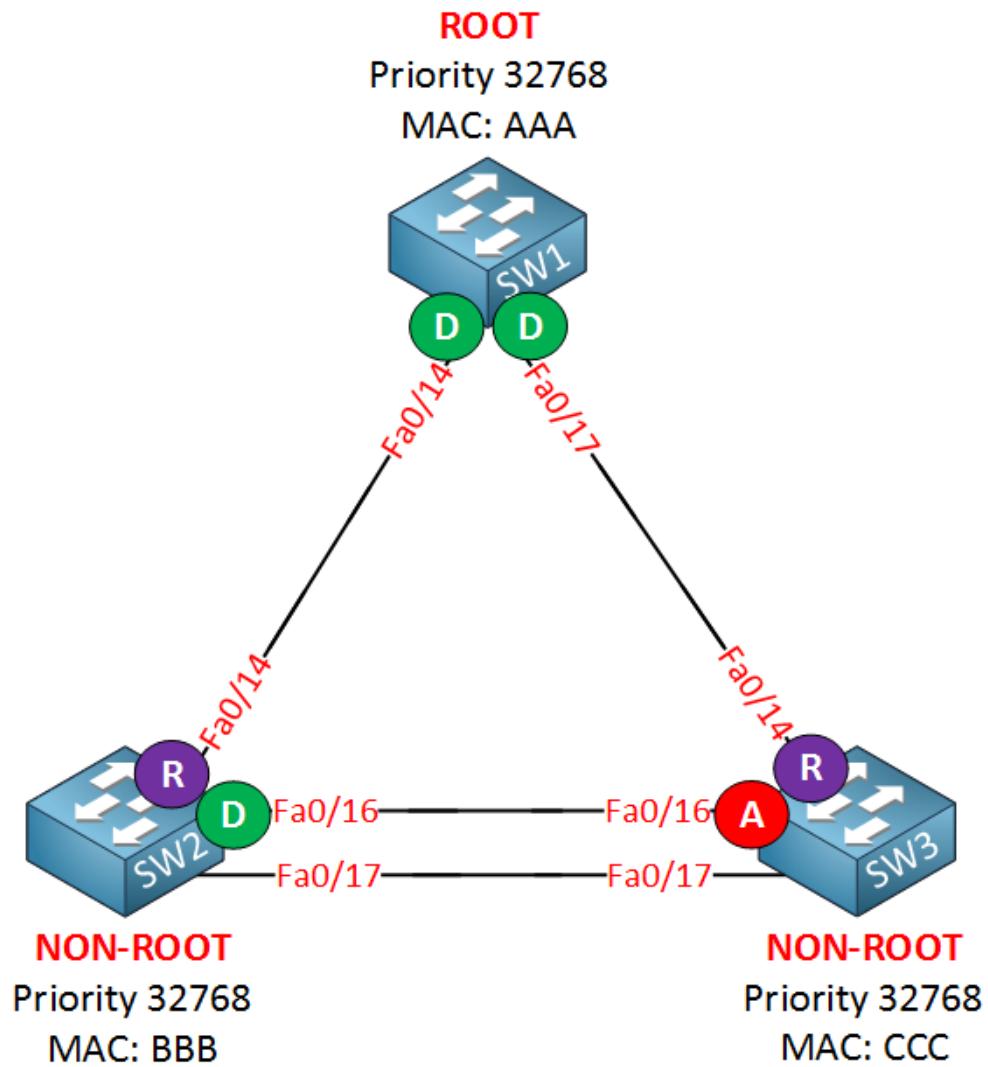
- Loại bỏ các vòng lặp: STP loại bỏ các vòng lặp trong mạng Ethernet, tránh tình trạng xung đột và mất dữ liệu.
- Tăng tính sẵn sàng: STP tự động chuyển đổi đường link nếu cổng chính bị lỗi, đảm bảo tính sẵn sàng của mạng.
- Giảm thiểu băng thông không cần thiết: STP giúp giảm thiểu sử dụng băng thông mạng bằng cách đóng cửa các cổng không cần thiết.

Tuy nhiên, STP cũng có một số hạn chế, bao gồm:

- Tốn tài nguyên mạng: STP yêu cầu các switch hoặc bridge phải liên tục giao tiếp để duy trì thông tin về mạng, điều này có thể tốn tài nguyên mạng.
- Chậm khi khởi động lại: Khi một switch hoặc bridge khởi động lại, chúng ta phải đợi STP tính toán lại trước khi chúng ta có thể sử dụng mạng.
- Không bảo vệ chính xác dữ liệu: STP không bảo vệ chính xác dữ liệu trong mạng, chỉ loại bỏ vòng lặp.

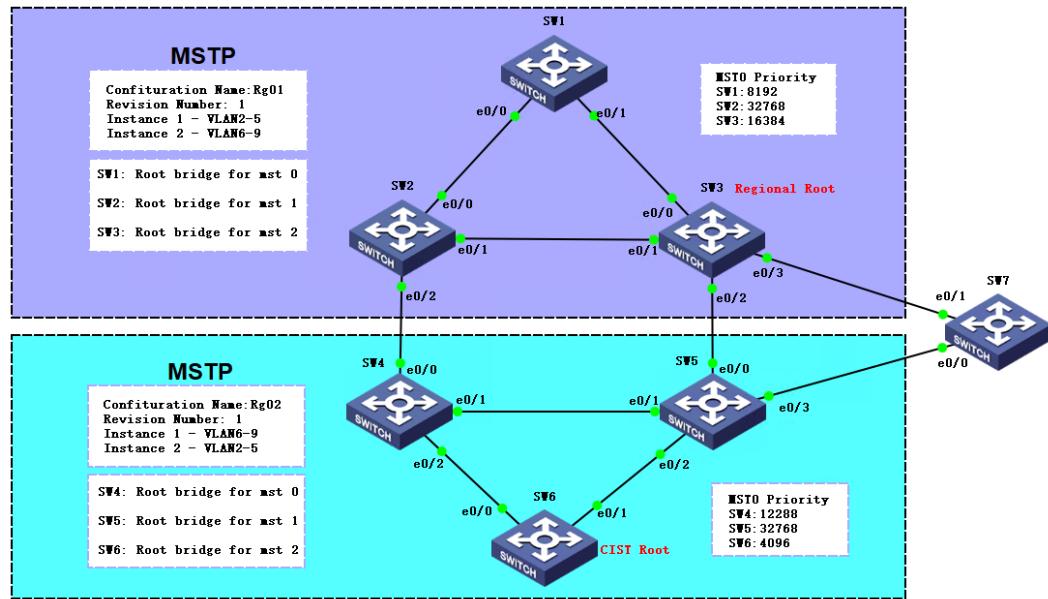
2.8.2 Các khái niệm liên quan

Rapid Spanning Tree Protocol (RSTP) là một phiên bản nhanh hơn của STP, được thiết kế để cải thiện tính sẵn sàng của mạng. RSTP hoạt động nhanh hơn so với STP vì nó sử dụng một số cơ chế tối ưu hóa, như PortFast và UplinkFast. PortFast là một tính năng cho phép cổng chuyển đổi trực tiếp sang trạng thái chuyển đổi khi nó được kích hoạt, giảm thời gian khởi động lại. UplinkFast là tính năng cho phép cổng chuyển đổi phụ cập nhật thông tin topology nếu cổng chính bị gián đoạn.



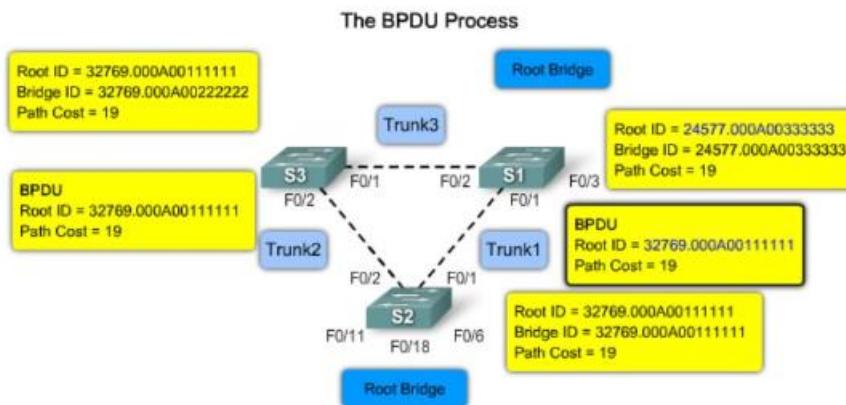
Hình 2.8.2. 1 Mô hình RSTP

Multiple Spanning Tree Protocol (MSTP) là một phiên bản mở rộng của STP, cho phép chia mạng Ethernet thành nhiều cây khung hình. Mỗi cây khung hình tương ứng với một VLAN cụ thể, giúp cải thiện hiệu suất và tính sẵn sàng trong các mạng lớn. MSTP cho phép giao thức STP hoạt động độc lập cho từng cây khung hình, giúp tối ưu hóa quản lý và bảo trì.



Hình 2.8.2. 2 Mô hình MSTP

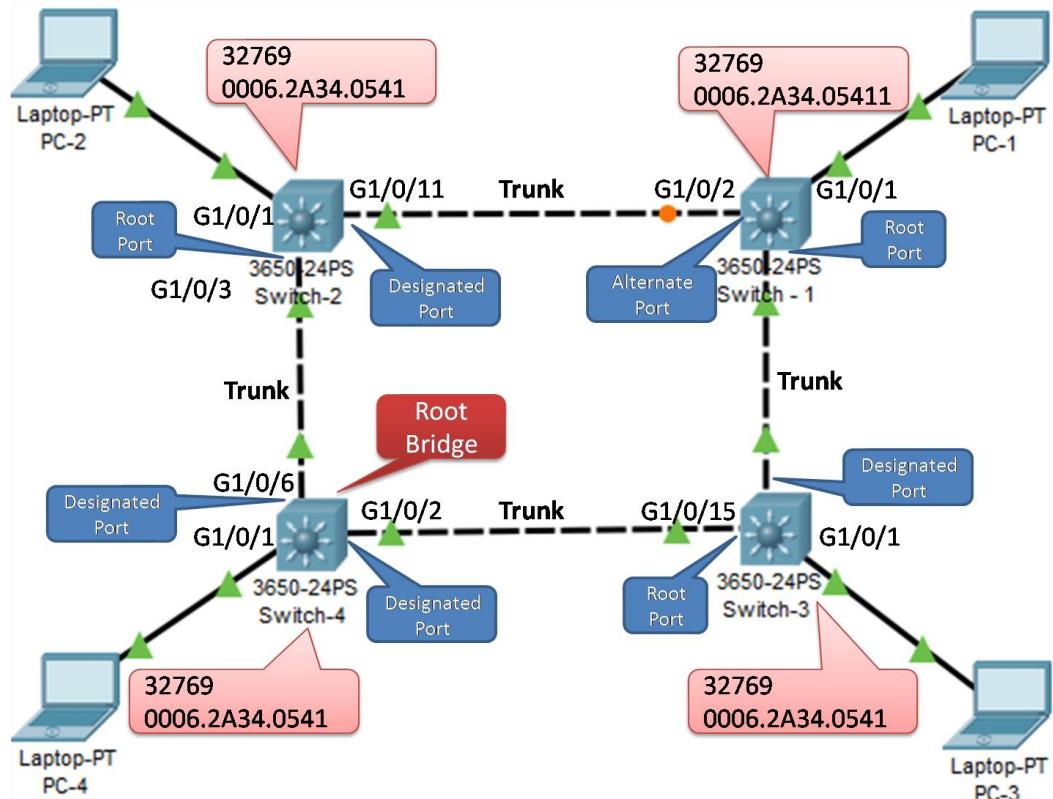
Bridge Protocol Data Unit (BPDU) là một loại gói tin được sử dụng để gửi thông tin mạng giữa các switch hoặc bridge trong mạng Ethernet. BPDU chứa thông tin về topology của mạng, bao gồm địa chỉ MAC, độ ưu tiên, danh sách các cổng và các thông số mạng khác. STP sử dụng BPDU để kiểm tra thông tin topology và chọn cổng chính cho mỗi switch hoặc bridge.



Hình 2.8.2. 3 Mô hình BPDU

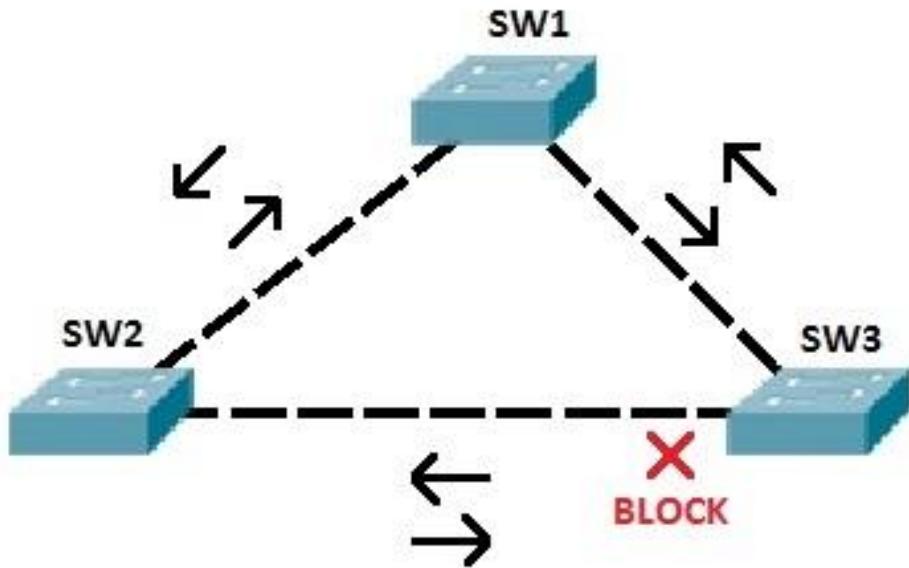
Root Bridge là switch hoặc bridge có độ ưu tiên cao nhất trong mạng, được sử dụng làm điểm tổng hợp cho toàn bộ mạng. Các switch hoặc bridge kết nối trực tiếp

với Root Bridge sẽ trở thành cổng chính, đảm bảo tính sẵn sàng và hiệu suất của mạng. Khi Root Bridge bị lỗi, STP sẽ chọn một switch hoặc bridge khác làm Root Bridge.



Hình 2.8.2. 4 Mô hình Root Bridge

Blocked Port là cổng được đóng cửa để tránh vòng lặp trong mạng Ethernet. Các switch hoặc bridge sử dụng STP để chọn một cổng chính và đóng cửa các cổng khác để tránh sự cố mạng. Các cổng bị đóng cửa được gọi là Blocked Port.



Hình 2.8.2. 5 Mô hình Blocked Port

2.8.3 Cách thức hoạt động

STP hoạt động theo các bước sau:

Bước 1: Khởi động quá trình

Khi STP được kích hoạt, switch hoặc bridge sẽ bắt đầu quá trình tìm kiếm Root Bridge. Mỗi switch hoặc bridge chọn cổng có độ ưu tiên cao nhất để gửi BPDU, chọn cổng này làm cổng gốc. Các switch hoặc bridge nhận BPDU từ các switch hoặc bridge khác và kiểm tra độ ưu tiên của chúng để tìm ra Root Bridge.

Bước 2: Tìm kiếm Root Bridge

Khi các switch hoặc bridge trong mạng Ethernet tìm được Root Bridge, chúng sẽ chọn cổng trực tiếp kết nối với Root Bridge làm cổng root. Các cổng khác sẽ được gán trạng thái Blocking, chỉ cho phép dữ liệu đi qua trên cổng root. STP sử dụng thuật toán Spanning Tree Algorithm (STA) để kiểm tra topology mạng và xác định cổng root cho từng switch hoặc bridge.

Bước 3: Chọn cổng chính

Mỗi switch hoặc bridge trong mạng Ethernet chọn một cổng chính để truyền dữ liệu. Cổng chính được chọn bởi switch hoặc bridge có đường link tốt nhất đến cổng root. Các cổng khác sẽ được gán trạng thái Blocking, giữ cho chúng không hoạt động, tránh các vòng lặp trong mạng.

Bước 4: Dự phòng cổng

Các switch hoặc bridge trong mạng Ethernet cũng chọn các cổng dự phòng, được sử dụng khi đường link tốt nhất bị gián đoạn. Khi đường link tốt nhất không hoạt động, switch hoặc bridge sẽ chuyển sang cổng dự phòng để truyền dữ liệu.

Khi một cổng mới được kích hoạt trong mạng Ethernet, nó sẽ bắt đầu quá trình STP lại từ đầu để tìm kiếm Root Bridge và chọn cổng chính. Quá trình này có thể tồn thời gian, khiến cho việc khởi động lại mạng Ethernet chậm hơn so với mạng không sử dụng STP.

2.9 Access Controller Lists (ACLs)

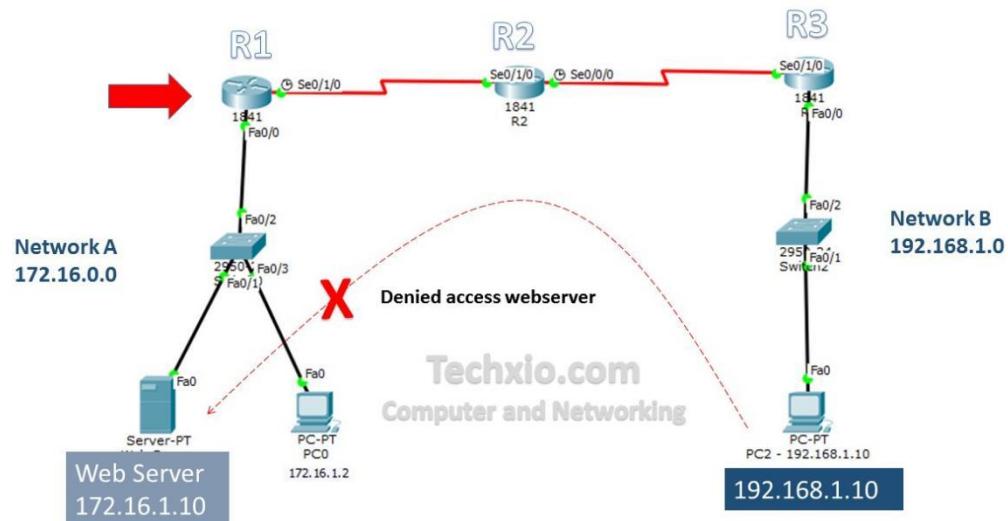
2.9.1 Giới thiệu về ACLs

Access Control List (ACLs) là công nghệ được sử dụng để kiểm soát quyền truy cập vào các tài nguyên mạng như file sharing, email servers, web servers và nhiều hơn nữa. ACLs cho phép quản trị viên mạng xác định ai được phép truy cập vào tài nguyên mạng nào, và trong thời gian bao lâu. Thông qua việc này, ACLs giúp đảm bảo rằng chỉ có những người được ủy quyền mới có thể truy cập vào các tài nguyên mạng đó.

Một danh sách điều khiển truy cập (ACL) trong mạng máy tính được sử dụng để áp dụng các quy tắc truy cập cho các giao thức khác nhau, cho phép hoặc từ chối truy cập vào tài nguyên mạng. Những quy tắc này có thể được xác định dựa trên địa chỉ IP, số cổng, tên miền và nhiều thông tin khác. Mỗi quy tắc trong danh sách điều

khiến truy cập (ACL) được áp dụng theo thứ tự, vì vậy nếu có mâu thuẫn giữa các quy tắc, quy tắc ưu tiên cao hơn sẽ được áp dụng.

Extended ACL Example



The above example, we are going to block the HTTP traffic from Network B by Applying extended ACL on R1 (Router)

Hình 2.9.1. 1 Mô hình ACLs

Ngoài việc giúp đảm bảo an ninh và tính bảo mật của mạng máy tính, ACLs cũng cung cấp cho quản trị viên mạng khả năng theo dõi và giám sát các hoạt động mạng. Bằng cách kiểm soát quyền truy cập vào các tài nguyên nhạy cảm, quản trị viên có thể theo dõi và phân tích các hoạt động của người dùng và ứng dụng để xác định những lỗ hổng bảo mật.

2.9.2 Các loại ACLs

Access Control List (ACLs) là công nghệ quan trọng trong mạng máy tính để kiểm soát quyền truy cập vào các tài nguyên mạng. Các loại của ACLs được sử dụng phổ biến trong mạng máy tính bao gồm Standard ACLs, Extended ACLs, VLAN ACLs và Time-based ACLs.

Standard ACLs là loại ACL đơn giản nhất trong mạng máy tính. Chúng chỉ cho phép hoặc từ chối truy cập dựa trên địa chỉ IP nguồn. Standard ACLs thường được sử dụng để cấm hoặc cho phép truy cập vào toàn bộ một mạng con hoặc subnet, hoặc ngược lại. Ví dụ, một quản trị viên có thể tạo ra một Standard ACL để từ chối truy cập tới một mạng con cụ thể.

Extended ACLs là loại ACL phức tạp hơn, cho phép quản trị viên mạng thiết lập các quy tắc truy cập dựa trên nhiều tiêu chí khác nhau, bao gồm địa chỉ IP nguồn, địa chỉ IP đích, số cổng và giao thức. Extended ACLs được sử dụng rộng rãi trong mạng máy tính để cấu hình các quy tắc truy cập phức tạp hơn, như giới hạn truy cập vào các dịch vụ mạng cụ thể.

VLAN ACLs là loại ACL được sử dụng để kiểm soát quyền truy cập vào các VLAN trong mạng. Chúng cho phép quản trị viên mạng áp dụng các quy tắc truy cập dựa trên địa chỉ MAC hoặc số cổng của thiết bị. VLAN ACLs được sử dụng để cấu hình truy cập cho các VLAN khác nhau và đảm bảo tính an toàn cho mạng.

Time-based ACLs là loại ACL được sử dụng để kiểm soát quyền truy cập vào các tài nguyên mạng dựa trên thời gian. Chúng cho phép quản trị viên thiết lập các quy tắc truy cập được kích hoạt hoặc vô hiệu hóa trong các khoảng thời gian cụ thể. Ví dụ, quản trị viên có thể thiết lập time-based ACLs để hạn chế truy cập vào một máy chủ nào đó trong giờ làm việc.

2.9.3 *Cách thức hoạt động*

Các quy tắc truy cập trong danh sách điều khiển truy cập (ACL) có thể được thiết lập theo nhiều cách khác nhau. Một số thông số quan trọng nhất được sử dụng để thiết lập các quy tắc truy cập bao gồm:

Bước 1: Địa chỉ IP nguồn và đích

Địa chỉ IP nguồn và đích là hai thông số chính được sử dụng để xác định người dùng được phép truy cập vào tài nguyên mạng nào. Quản trị viên mạng có thể áp dụng ACLs để cho phép hoặc từ chối truy cập dựa trên địa chỉ IP của người dùng.

Bước 2: Số cổng và giao thức

Số cổng và giao thức là các thông số được sử dụng để xác định loại dịch vụ mạng mà người dùng muốn truy cập. Quản trị viên mạng có thể áp dụng ACLs để giới hạn truy cập vào các dịch vụ mạng cụ thể, chẳng hạn như HTTP hoặc FTP.

Bước 3: Xác định thời gian

Thời gian là một thông số quan trọng trong ACLs, cho phép quản trị viên mạng thiết lập các quy tắc truy cập dựa trên thời gian. Time-based ACLs được sử dụng để kích hoạt hoặc vô hiệu hóa các quy tắc truy cập trong các khoảng thời gian cụ thể.

Khi thiết lập các quy tắc truy cập trong danh sách điều khiển truy cập (ACL), quản trị viên mạng có thể thiết lập chúng để cho phép hoặc từ chối truy cập của người dùng. Các quy tắc truy cập này được áp dụng trong thứ tự ưu tiên, vì vậy nếu có mâu thuẫn giữa các quy tắc, quy tắc ưu tiên cao hơn sẽ được áp dụng. Nếu không có quy tắc nào khớp với yêu cầu truy cập, hệ thống sẽ từ chối yêu cầu truy cập đó.

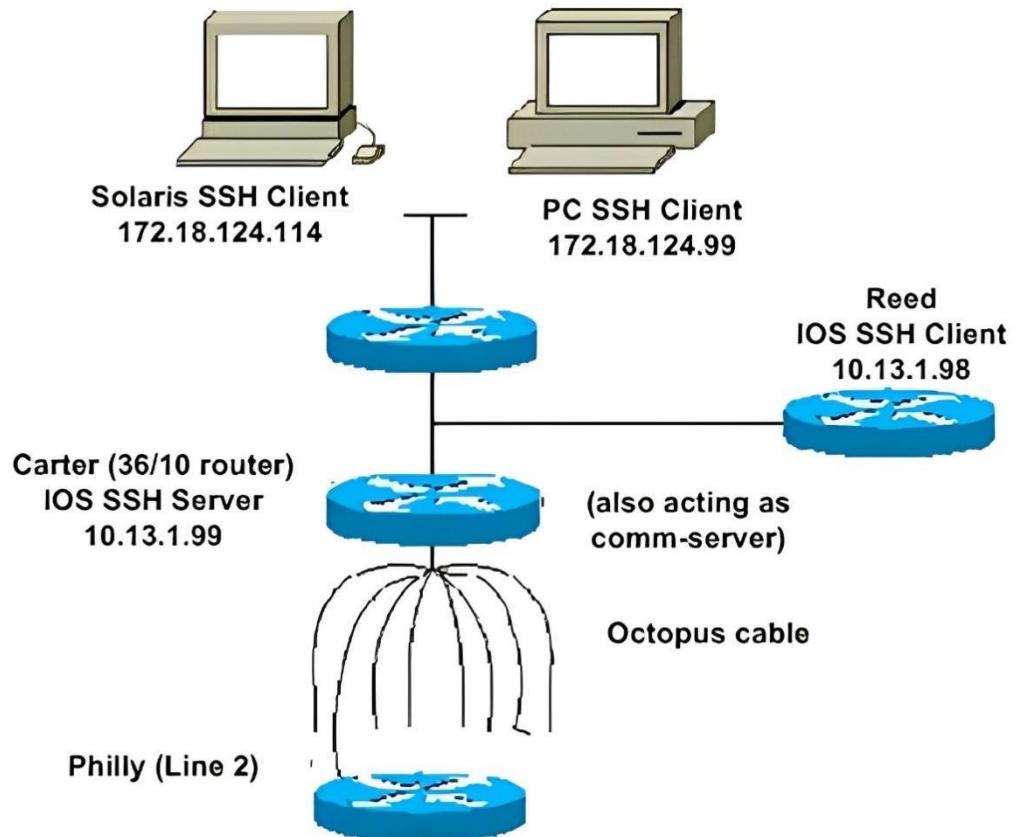
2.10 Secure Shell (SSH)

2.10.1 Giới thiệu về SSH

Secure Shell (SSH) là một giao thức dùng để thiết lập kết nối an toàn giữa hai máy tính và truyền tải dữ liệu qua mạng. Giao thức được phát triển từ năm 1995 bởi Tatu Ylönen và các đồng nghiệp của ông tại Đại học Teknillinen Korkeakoulu ở Phần Lan, trong bối cảnh những cuộc tấn công bảo mật ngày càng tinh vi trên Internet.

SSH cho phép người dùng truy cập, quản lý và điều khiển từ xa các thiết bị mà không cần đến một kết nối vật lý. Sử dụng SSH, người dùng có thể thiết lập các

kết nối mã hoá để bảo vệ dữ liệu đang truyền tải và xác thực người sử dụng để đảm bảo tính toàn vẹn của hệ thống.



Hình 2.10.1. 1 Mô hình SSH

Ứng dụng của SSH rất đa dạng và phổ biến trong các hệ thống Unix và Linux. Một trong những ứng dụng chính của SSH là quản lý máy chủ từ xa bằng cách sử dụng một terminal thông qua giao thức SSH. SSH cũng được sử dụng để sao lưu và phục hồi dữ liệu, chia sẻ file và thao tác với các máy tính khác trên mạng với một cách thức an toàn.

SSH hoạt động dựa trên một kiểu mã hoá đối xứng (symmetric encryption) và một cơ chế xác thực hai bước (two-factor authentication). Khi thiết lập kết nối, SSH sử dụng các thuật toán mã hoá để mã hóa dữ liệu gửi đi qua mạng. Các thuật toán này bao gồm AES (Advanced Encryption Standard), Blowfish, và 3DES (Triple Data Encryption Standard).

Một trong những cơ chế xác thực phổ biến nhất của SSH là việc sử dụng cặp khóa công khai và khóa bí mật. Trong quá trình xác thực, máy chủ sẽ yêu cầu người dùng cung cấp khóa bí mật tương ứng với khóa công khai được lưu trữ trên máy chủ. Nếu khóa bí mật được cung cấp chính xác, người dùng sẽ được cho phép truy cập vào hệ thống.

SSH cũng có thể được cấu hình để cho phép các kết nối từ xa thông qua một kết nối VPN (Virtual Private Network). Điều này cho phép các người dùng kết nối đến hệ thống từ bất kỳ đâu trên thế giới mà không cần phải truy cập trực tiếp vào mạng của tổ chức.

Trong kết luận, SSH là một giao thức quan trọng trong việc bảo vệ an ninh thông tin và quản lý các hệ thống từ xa. Nó cung cấp cho người dùng một giải pháp an toàn để thiết lập kết nối và truyền tải dữ liệu qua mạng. Bằng cách sử dụng SSH, ta có thể giảm thiểu rủi ro an ninh và đảm bảo tính toàn vẹn của hệ thống.

2.10.2 Các loại mã hóa SSH

Secure Shell (SSH) là một giao thức mã hóa được sử dụng để bảo mật kết nối đến máy chủ từ xa và truyền tải dữ liệu qua mạng một cách an toàn. SSH sử dụng nhiều loại mã hóa khác nhau để đảm bảo tính bảo mật của dữ liệu khi truyền tải.

Mã hóa đối称 (Symmetric Encryption) là phương pháp mã hóa bảo vệ dữ liệu bằng cách sử dụng một khoá để mã hóa và giải mã. Khoá này được chia sẻ giữa người gửi và người nhận, cho phép cả hai bên có thể truy cập vào dữ liệu. SSH sử dụng các thuật toán mã hóa đối称 như AES (Advanced Encryption Standard), Blowfish và 3DES (Triple Data Encryption Standard).

Mã hóa bất đối称 (Asymmetric Encryption) là phương pháp mã hóa thông tin bằng cách sử dụng hai khóa: khóa công khai và khóa bí mật. Khóa công khai được chia sẻ công khai trong khi khóa bí mật chỉ được giữ bởi chủ sở hữu của nó. Người gửi sử dụng khóa công khai để mã hóa thông tin trước khi gửi nó đi, và người nhận

sử dụng khóa bí mật để giải mã. SSH sử dụng các thuật toán mã hóa bất đối xứng như RSA (Rivest–Shamir–Adleman) và DSA (Digital Signature Algorithm).

Chữ ký số (Digital Signatures) là phương pháp thực hiện xác thực người gửi tin nhắn. Người gửi tạo ra một chữ ký số bằng cách sử dụng khóa bí mật của mình và sau đó gửi nó cùng với thông điệp cho người nhận. Người nhận sử dụng khóa công khai để xác thực chữ ký số. Nếu chữ ký số hợp lệ, người nhận có thể tin tưởng vào tính xác thực của thông điệp đã được gửi. SSH sử dụng các thuật toán chữ ký số như RSA và DSA.

Mã hóa tiền tố (Prefix Encryption) là một phương pháp mã hóa mà ta thêm một ký tự tiền tố vào trước thông điệp gốc trước khi mã hóa. Ký tự tiền tố này sẽ được giải mã trước khi thông điệp gốc được giải mã. Phương pháp này giúp đảm bảo tính bảo mật khi truyền tải thông tin qua kết nối SSH. Tuy nhiên, phương pháp này không được sử dụng phổ biến trong SSH.

Mã hóa khối (Block Ciphers) là một kiểu mã hóa đối xứng, nhưng thay vì mã hóa từng byte của dữ liệu, nó mã hóa dữ liệu theo từng khối. Kích thước khối thường là 64 bit hoặc 128 bit. SSH sử dụng các thuật toán mã hóa khối như AES và Blowfish.

Kỹ thuật Hashing cũng là phương thức mã hóa phổ biến trong giao thức Secure Shell. Để tạo ra một mật mã Hash rất đơn giản, chỉ qua một lần Input nhưng lại không thể Input qua chính lần Hash đó. Hiểu đơn giản là Client sẽ giữ Input và chỉ Client mới tạo ra được một Crypto-Graphic để hai bên có thể nhập Input. Giao thức Secure Shell sử dụng kỹ thuật Hashing để xác thực tin nhắn, đảm bảo lệnh không thể giả mạo dù dùng phương thức nào.

2.10.3 Các tính năng của SSH

Đây là một công nghệ quan trọng trong việc bảo vệ thông tin truyền tải trên mạng. Dưới đây là các tính năng của SSH:

Mã hóa dữ liệu: SSH sử dụng mã hóa để bảo vệ dữ liệu khi truyền qua mạng. Dữ liệu được mã hóa bằng các thuật toán mã hóa chắc chắn và chỉ có người được phép mới có thể giải mã.

Xác thực: SSH cung cấp các phương pháp xác thực để đảm bảo rằng chỉ những người được phép mới có thể truy cập vào hệ thống. Các phương pháp xác thực bao gồm mật khẩu, khóa công khai, chứng chỉ số, vân tay và xác thực hai yếu tố.

Tăng cường bảo mật: SSH cung cấp các tính năng bảo mật như chặn IP và giới hạn số lần đăng nhập không thành công. Nó cũng cho phép các quản trị viên thiết lập các quy tắc bảo mật để đảm bảo rằng chỉ những người được phép mới có thể truy cập vào hệ thống.

Điều khiển từ xa: SSH cho phép người dùng truy cập vào các dịch vụ mạng từ xa một cách an toàn và dễ dàng. Nó cho phép các quản trị viên truy cập vào các máy chủ từ xa và thực hiện các tác vụ quản lý hệ thống.

Đa nền tảng: SSH là một công nghệ đa nền tảng và có thể được sử dụng trên nhiều hệ điều hành, bao gồm Linux, Unix, Windows, macOS và các hệ thống khác.

2.10.4 Cách thức hoạt động

Đây là một công nghệ quan trọng trong việc bảo vệ thông tin truyền tải trên mạng. Dưới đây là cách hoạt động của SSH:

Thiết lập kết nối: Trước khi thiết lập kết nối SSH, máy chủ và máy khách phải xác định nhau. Điều này được thực hiện bằng cách sử dụng một tiến trình gọi là “handshake” để thiết lập kết nối an toàn.

Xác thực: Sau khi kết nối được thiết lập, quá trình xác thực sẽ bắt đầu. SSH cung cấp nhiều phương pháp xác thực như mật khẩu, khóa công khai và chứng chỉ số. Người dùng sẽ phải nhập thông tin xác thực để có thể truy cập vào hệ thống.

Mã hóa dữ liệu: Sau khi xác thực thành công, SSH sẽ bắt đầu mã hóa dữ liệu được truyền tải giữa hai máy tính. Dữ liệu sẽ được mã hóa bằng một thuật toán mã hóa chắc chắn, đảm bảo rằng chỉ có người được phép mới có thể giải mã.

Truyền tải dữ liệu: Dữ liệu được truyền tải giữa hai máy tính bằng các gói tin được mã hóa. SSH sẽ đảm bảo rằng các gói tin được truyền tải một cách an toàn và đảm bảo tính toàn vẹn của dữ liệu.

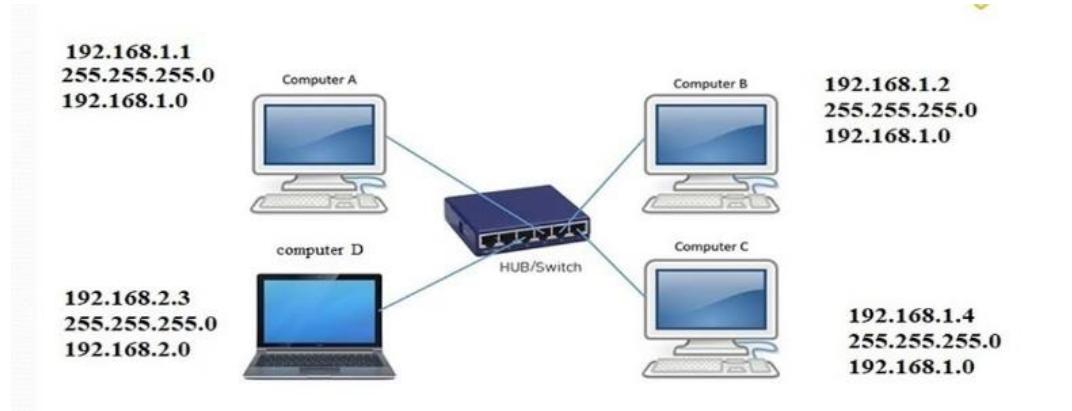
Kết thúc kết nối: Sau khi quá trình truyền tải dữ liệu hoàn tất, SSH sẽ kết thúc kết nối giữa hai máy tính. Trong trường hợp bị ngắt kết nối đột ngột, SSH cũng cung cấp khả năng tái kết nối và tiếp tục truyền tải dữ liệu.

2.11 Subnetting and IP Addressing

2.11.1 Giới thiệu về IP Address

IP address, hay còn gọi là địa chỉ IP, là một chuỗi các số được dùng để xác định và định vị một thiết bị trên mạng internet. IP address là yếu tố không thể thiếu trong việc kết nối các thiết bị với nhau và truyền tải dữ liệu giữa chúng trên mạng.

Mỗi thiết bị mạng đều có một địa chỉ IP riêng, còn được gọi là địa chỉ IP tĩnh, được cấp phát bởi các nhà cung cấp dịch vụ Internet (ISP) hoặc tự quản lý bởi doanh nghiệp, tổ chức. Địa chỉ IP này cho phép các thiết bị trao đổi thông tin và truy cập vào internet.



Hình 2.11.1. 1 Cấp phát IP Address cho các thiết bị

IP address là một chuỗi của các số ngăn cách bằng dấu chấm, ví dụ như 192.168.1.1. Tất cả các thiết bị trong mạng đều phải có một địa chỉ IP độc nhất để có thể nhận diện và trao đổi thông tin với nhau.

Có hai phiên bản của giao thức IP hiện tại đang được sử dụng phổ biến trên toàn cầu: IPv4 (Internet Protocol Version 4) và IPv6 (Internet Protocol Version 6). IPv4 là phiên bản đầu tiên và phổ biến nhất, được sử dụng trong hầu hết các thiết bị và mạng hiện nay. IPv6 là phiên bản mới hơn và cho phép địa chỉ IP tăng gấp đôi so với IPv4.

IPv4 sử dụng địa chỉ IP 32 bit, chia thành 4 cặp số từ 0 đến 255 (ví dụ: 192.168.1.1). Tuy nhiên, địa chỉ IPv4 có giới hạn, chỉ có thể cấp được khoảng 4 tỷ địa chỉ IP. Đây là lý do tại sao IPv6 được ra đời, để giải quyết vấn đề hạn chế này. IPv6 sử dụng 128 bit địa chỉ IP, cho phép tạo ra đến 340 undecillion địa chỉ, đủ để đáp ứng nhu cầu của toàn bộ internet trong tương lai.

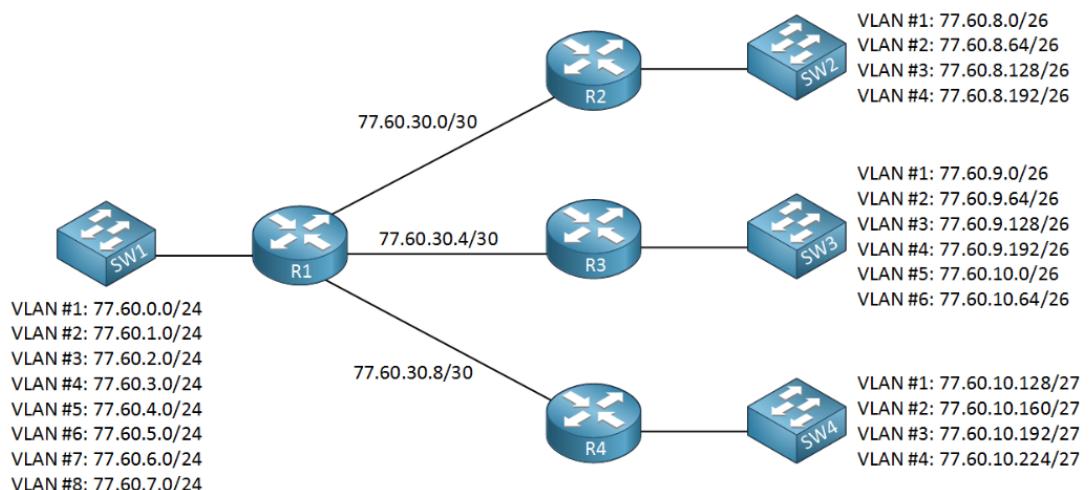
Có hai loại địa chỉ IP: địa chỉ IP tĩnh và địa chỉ IP động. Địa chỉ IP tĩnh là địa chỉ IP được cấp phát cho một thiết bị và không thay đổi theo thời gian. Trong khi đó, địa chỉ IP động không cố định và có thể thay đổi theo thời gian hoặc khi thiết bị kết nối lại vào mạng.

Địa chỉ IP cũng được sử dụng để giới hạn quyền truy cập vào các tài nguyên trên internet. Những địa chỉ IP được cho phép truy cập vào các tài nguyên nhất định, trong khi những địa chỉ IP khác bị từ chối hoặc bị giới hạn quyền truy cập.

Địa chỉ IP là một yếu tố quan trọng trong việc kết nối và truyền tải thông tin trên mạng Internet. Việc hiểu rõ về địa chỉ IP sẽ giúp chúng ta có thể hiểu và sử dụng các dịch vụ trên internet một cách hiệu quả và an toàn.

2.11.2 Giới thiệu về Subnetting

Subnetting là một kỹ thuật được sử dụng trong việc chia mạng máy tính thành các mạng con nhỏ hơn, hoặc còn gọi là subnet. Kỹ thuật này cho phép chia bớt áp lực trên mạng chính và giúp quản lý và điều khiển mạng dễ dàng hơn.



Hình 2.11.2. 1 Mô hình kỹ thuật Subnetting

Khi bạn thiết lập một mạng máy tính, mỗi thiết bị đều được cấp một địa chỉ IP để truyền tải thông tin qua lại với các thiết bị khác. Tuy nhiên, nếu mạng quá lớn, việc quản lý và điều khiển mạng sẽ trở nên khó khăn. Để giải quyết vấn đề này, ta có thể sử dụng kỹ thuật subnetting để chia mạng chính thành các mạng nhỏ hơn.

Khi áp dụng kỹ thuật subnetting, ta sẽ chia địa chỉ IP mạng ra thành hai phần: phần định danh mạng (network ID) và phần định danh thiết bị (host ID). Phần định

danh mạng sẽ xác định mạng con nào thiết bị đó thuộc về, trong khi phần định danh thiết bị sẽ chỉ ra địa chỉ của thiết bị trên mạng con đó.

Để chia mạng thành các subnet, ta sẽ tạo ra các mặt nạ mạng (subnet mask) để chỉ ra phần của địa chỉ IP nào thuộc về network ID và phần nào là host ID. Mặt nạ mạng sẽ có thể được xác định dựa trên số bit 1 trong binary representation của nó.

2.11.3 Phương pháp Variable Length Subnet Mask (VLSM)

Variable Length Subnet Mask (VLSM) là một phương pháp cho phép chia mạng thành các subnet có kích thước khác nhau. Với VLSM, ta có thể tùy chỉnh kích thước của các subnet để sử dụng địa chỉ IP một cách hiệu quả hơn và giúp giảm tải trên mạng.

Khi sử dụng phương pháp chia mạng thông thường, ta sẽ chia mạng ra thành các subnet có kích thước bằng nhau. Tuy nhiên, điều này không phải lúc nào cũng là hiệu quả nhất. Ví dụ, trong một mạng lớn, ta cần sử dụng nhiều địa chỉ IP cho các mạng con nhỏ hơn, trong khi lại chỉ cần ít địa chỉ IP cho các mạng lớn hơn.

Với VLSM, ta có thể tùy chỉnh kích thước của các subnet để sử dụng địa chỉ IP một cách hiệu quả hơn. Thay vì chia mạng ra thành các subnet có kích thước bằng nhau như phương pháp thông thường, ta có thể chia mạng thành các subnet có kích thước khác nhau tùy thuộc vào nhu cầu sử dụng địa chỉ IP của từng mạng con.

Ví dụ, nếu ta có một mạng lớn với địa chỉ IP là 192.168.1.0/24 và muốn chia thành các subnet có kích thước khác nhau để sử dụng hiệu quả hơn, ta có thể sử dụng phương pháp VLSM để tạo ra các subnet có kích thước khác nhau như sau:

Subnet 1: cần 10 địa chỉ IP - ta có thể sử dụng mặt nạ mạng /28 (255.255.255.240) để tạo ra 16 địa chỉ IP. Địa chỉ IP của subnet này sẽ là 192.168.1.0/28.

Subnet 2: cần 25 địa chỉ IP - ta có thể sử dụng mặt nạ mạng /27 (255.255.255.224) để tạo ra 32 địa chỉ IP. Địa chỉ IP của subnet này sẽ là 192.168.1.16/27.

Subnet 3: cần 5 địa chỉ IP - ta có thể sử dụng mặt nạ mạng /29 (255.255.255.248) để tạo ra 8 địa chỉ IP. Địa chỉ IP của subnet này sẽ là 192.168.1.48/29.

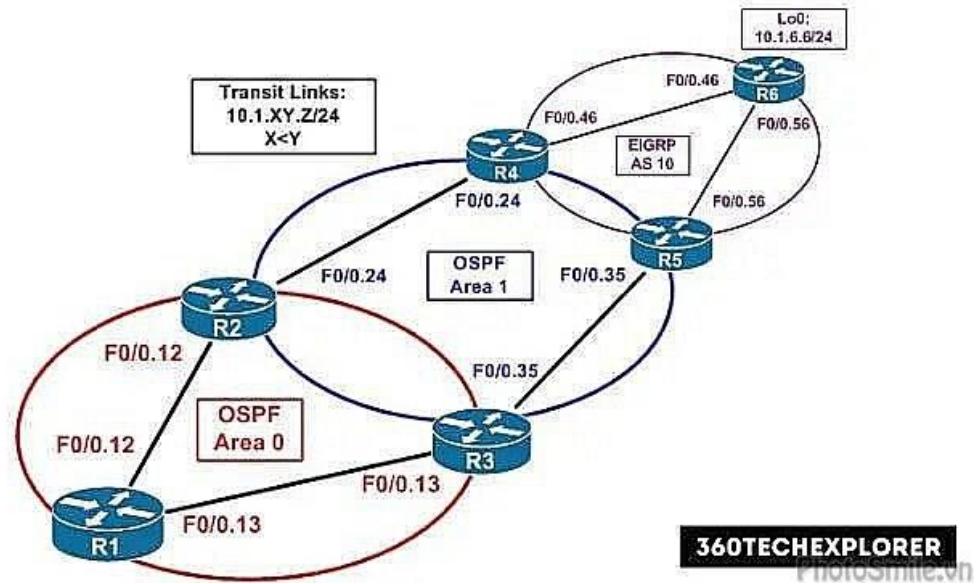
Subnet 4: cần 100 địa chỉ IP - ta có thể sử dụng mặt nạ mạng /25 (255.255.255.128) để tạo ra 128 địa chỉ IP. Địa chỉ IP của subnet này sẽ là 192.168.1.56/25.

Như vậy, ta đã chia mạng ra thành các subnet có kích thước khác nhau tùy thuộc vào nhu cầu sử dụng địa chỉ IP của từng mạng con. Qua đó, ta đã sử dụng địa chỉ IP một cách hiệu quả hơn và giảm tải trên mạng.

2.12 Open Shortest Path First (OSPF)

2.12.1 Giới thiệu về OSPF

Open Shortest Path First (OSPF) là một giao thức định tuyến trong mạng máy tính dựa trên tiêu chuẩn Open Standards. OSPF được sử dụng để xác định đường đi tốt nhất giữa các router trong một mạng lớn. Với OSPF, các router có thể cập nhật thông tin định tuyến với nhau một cách liên tục và động, giúp tối ưu hóa việc truyền tải dữ liệu giữa các thiết bị.



Hình 2.12.1. 1 Mô hình định tuyến hệ thống mạng bằng OSPF

OSPF được phát triển vào năm 1987 và hiện được sử dụng rộng rãi trong các mạng máy tính lớn và phức tạp. Giao thức này hoạt động trên layer 3 của mô hình OSI (Open Systems Interconnection), giúp định tuyến thông qua một số thuật toán định tuyến.

Một trong những ưu điểm chính của OSPF là tính linh hoạt cao trong việc quản lý mạng. Giao thức này cho phép chia mạng thành các area (vùng) riêng biệt, giúp giảm thiểu lưu lượng truyền tải thông tin định tuyến và tăng tính bảo mật. Mỗi area sẽ có một router core (trung tâm định tuyến) quản lý và các router chỉ trao đổi thông tin định tuyến với nhau trong cùng một area.

OSPF sử dụng thuật toán Dijkstra để tính toán đường đi tốt nhất giữa các router. Thuật toán này xác định đường đi dựa trên chi phí (cost) của mỗi kết nối giữa các router. Chi phí được tính bằng cách đo đặc khoảng cách, tốc độ truyền tải và băng thông của kết nối. OSPF cũng hỗ trợ chức năng equal-cost load balancing, cho phép chia đều lưu lượng truyền tải thông qua nhiều đường đi có chi phí bằng nhau.

OSPF cũng có thể được cấu hình để hoạt động với các giao thức định tuyến khác như RIP, EIGRP hoặc BGP. Giao thức này cũng hỗ trợ các tính năng như

authentication (xác thực), summarization (tóm tắt) và route redistribution (phân phối lại thông tin định tuyến).

Một số ứng dụng của OSPF bao gồm:

- Thiết kế và triển khai mạng máy tính lớn và phức tạp.
- Định tuyến giữa các data center và site của công ty.
- Tối ưu hóa việc truyền tải dữ liệu giữa các router và giảm thiểu độ trễ.
- Tăng tính tin cậy và bảo mật cho hệ thống mạng.

Tuy nhiên, việc cấu hình OSPF có thể khó khăn và phức tạp đối với những người mới bắt đầu trong lĩnh vực này. Vì vậy, việc sử dụng giao thức này nên được thực hiện bởi những người có kinh nghiệm và chuyên môn cao trong lĩnh vực mạng máy tính.

2.12.2 Cách thức hoạt động

OSPF hoạt động bằng cách trao đổi thông tin định tuyến giữa các router để xác định đường đi tốt nhất giữa chúng. Khi một thiết bị mới được thêm vào mạng, hoặc khi có sự thay đổi về cấu hình mạng, OSPF sẽ tự động cập nhật bảng định tuyến để đảm bảo các router có thông tin định tuyến mới nhất.

OSPF sử dụng thuật toán Dijkstra để tính toán đường đi tốt nhất giữa các router. Thuật toán này xác định đường đi dựa trên chi phí (cost) của mỗi kết nối giữa các router. Chi phí được tính bằng cách đo đặc khoảng cách, tốc độ truyền tải và băng thông của kết nối. Với OSPF, băng thông được tính dựa trên độ rộng của các kênh truyền tải dữ liệu (bandwidth) giữa các router.

Mỗi router trên mạng OSPF được gán một địa chỉ IP và một ID duy nhất, gọi là Router ID. Router ID được sử dụng để xác định router này trong bảng định tuyến và trong các giao thức khác. Thông tin định tuyến được lưu trữ trong bảng định tuyến

của mỗi router, bao gồm danh sách các subnet được kết nối đến router đó và các thuộc tính của chúng như cost, next hop, network mask, area ID, và router ID.

OSPF cho phép chia mạng thành các area riêng biệt, giúp giảm thiểu lưu lượng truyền tải thông tin định tuyến và tăng tính bảo mật. Mỗi area sẽ có một router core (trung tâm định tuyến) quản lý và các router chỉ trao đổi thông tin định tuyến với nhau trong cùng một area. Khi các thông tin định tuyến được cập nhật ở một area, các router border (biên giới định tuyến) sẽ truyền thông tin này qua các area khác.

2.13 Wireless Network (WLAN)

2.13.1 Giới thiệu về WLAN

Wireless Local Area Network (WLAN) là một công nghệ kết nối mạng không dây giữa các thiết bị điện tử như máy tính, điện thoại di động hay các thiết bị IoT. WLAN cho phép người dùng truy cập vào Internet hoặc mạng nội bộ từ bất kỳ đâu trong vùng phủ sóng của mạng WLAN.

Một mạng WLAN gồm các thành phần sau: bộ phát sóng (Access Point), các thiết bị kết nối (Client Devices), và hệ thống cáp kết nối giữa các Access Point để tạo nên mạng lưới. Các thiết bị Client sử dụng các chuẩn kết nối không dây như Wi-Fi để kết nối vào mạng WLAN thông qua Access Point.



Hình 2.13.1. 1 Mô hình mạng Wireless LAN

Mạng WLAN đang trở thành một phần không thể thiếu của cuộc sống hiện đại, đặc biệt là trong các nơi công cộng như quán cà phê, khách sạn, sân bay hay trường học. Nó cho phép người dùng kết nối mạng, trao đổi thông tin, xem video, lướt web hay chơi game trực tuyến một cách tiện lợi, nhanh chóng và linh hoạt.

Các chuẩn kết nối WLAN được phát triển theo từng giai đoạn, từ chuẩn 802.11a, 802.11b, 802.11g, và cuối cùng là 802.11n. Các chuẩn mới nhất hiện nay là 802.11ac và 802.11ax (hay còn gọi là Wi-Fi 5 và Wi-Fi 6) được đưa ra với nhiều cải tiến về tốc độ truyền dữ liệu, độ tin cậy và phạm vi hoạt động so với các chuẩn trước đó.

Một trong những ưu điểm của WLAN là tính di động cao, cho phép người dùng truy cập vào mạng từ bất kỳ đâu trong vùng phủ sóng của mạng WLAN. Điều này rất hữu ích cho người dùng di động như giáo viên, sinh viên, nhân viên công ty hay những người thường xuyên di chuyển trong quá trình làm việc.

Tuy nhiên, WLAN cũng có một số nhược điểm như khả năng bị nhiễu sóng từ các thiết bị khác, đặc biệt là các thiết bị sử dụng tần số giống như micrô sóng hoặc điện thoại không dây. Bên cạnh đó, tốc độ truyền dữ liệu của WLAN có thể bị giảm bởi những yếu tố như khoảng cách, vật cản, hay số lượng người dùng đồng thời kết nối vào mạng.

Ngoài ra, vấn đề bảo mật của WLAN cũng là một vấn đề cần được quan tâm. Sự phát triển của công nghệ hàng đầu, sản xuất các thiết bị không dây và các giải pháp bảo mật đã giúp nâng cao đáng kể bảo mật cho các mạng WLAN. Tuy nhiên, việc cài đặt, thiết lập chính sách bảo mật và giám sát cũng là yếu tố quan trọng để đảm bảo mạng WLAN hoạt động an toàn và hiệu quả.

2.13.2 Các chuẩn của WLAN

Wireless LAN (WLAN) là một công nghệ truyền thông không dây cho phép các thiết bị di động kết nối vào mạng thông qua sóng radio. WLAN được sử dụng rộng rãi trong nhiều môi trường khác nhau, từ các văn phòng và khách sạn đến các hộ gia đình và khu vực công cộng.

WLAN tuân theo một số chuẩn để đảm bảo tính tương thích giữa các thiết bị và quản lý tốt các kết nối. Các chuẩn này cũng định nghĩa tốc độ dữ liệu tối đa có thể đạt được trên các mạng WLAN.

Chuẩn đầu tiên của WLAN là IEEE 802.11, được giới thiệu vào năm 1997. Tuy nhiên, kể từ đó đã có nhiều phiên bản và bổ sung. Hiện nay, có ba chuẩn chính đang được sử dụng nhiều nhất:

- IEEE 802.11b: Chuẩn này được ra mắt vào năm 1999 và hoạt động trên băng tần 2,4 GHz. Tốc độ tối đa đạt được là 11 Mbps.
- IEEE 802.11g: Chuẩn này được giới thiệu vào năm 2003 và cũng hoạt động trên băng tần 2,4 GHz. Tuy nhiên, tốc độ dữ liệu đã được cải thiện lên đến 54 Mbps.
- IEEE 802.11n: Chuẩn này được phát triển vào năm 2009 và sử dụng cả băng tần 2,4 GHz và 5 GHz. Tốc độ truyền tải tối đa là 600 Mbps và có khả năng hoạt động trên khoảng cách xa hơn so với các chuẩn trước đó.

Một số thành phần quan trọng của WLAN bao gồm:

- Access point (AP): Thiết bị này là trung tâm của mạng WLAN và cung cấp kết nối không dây cho thiết bị di động.
- Network interface card (NIC): Thiết bị này cung cấp khả năng kết nối với mạng WLAN cho các thiết bị điện tử như laptop, smartphone hoặc máy tính bảng.
- Antenna: Một bộ phận quan trọng trong việc truyền tải sóng radio, giúp tăng cường tín hiệu và độ phủ sóng của mạng WLAN.
- Security protocols: Vì WLAN là một mạng không dây, do đó các giải pháp bảo mật là rất quan trọng để ngăn chặn các cuộc tấn công từ các hacker hay tin tặc. WEP, WPA và WPA2 là các giao thức bảo mật được sử dụng phổ biến.

Ngoài ra, để đảm bảo tính ổn định và hiệu quả của mạng WLAN, các chuẩn này cũng định nghĩa các tiêu chuẩn chất lượng tín hiệu như độ trễ (latency), độ rộng băng thông (bandwidth), độ ổn định tín hiệu (signal stability) và độ phủ sóng (coverage). Các tiêu chuẩn này giúp đảm bảo mạng WLAN hoạt động ổn định và cho

phép người dùng truy cập Internet và các ứng dụng trực tuyến một cách nhanh chóng và dễ dàng.

2.13.3 Các kỹ thuật bảo mật WLAN

WEP (Wired Equivalent Privacy) là một giao thức bảo mật cơ bản cho WLAN. Nó sử dụng mã hóa RC4 để bảo vệ dữ liệu gửi đi trên mạng. Tuy nhiên, WEP đã bị khai phá là có lỗ hổng bảo mật và dễ bị tấn công bởi hacker. Vì vậy, WEP không còn được sử dụng rộng rãi trong các mạng WLAN hiện đại.

WPA (Wi-Fi Protected Access) là một phiên bản nâng cấp của WEP. Nó cung cấp một số tính năng bảo mật mới, bao gồm mã hóa TKIP (Temporal Key Integrity Protocol), kiểm tra xác thực từ xa và quản lý khóa tốt hơn. WPA là một giao thức bảo mật tạm thời và đã được nâng cấp thành WPA2.

WPA2 (Wi-Fi Protected Access II) là phiên bản tiếp theo của WPA và hiện đang được sử dụng rộng rãi trong các mạng WLAN. Nó sử dụng mã hóa AES (Advanced Encryption Standard) để bảo vệ dữ liệu truyền qua mạng. Khi kết hợp với các tính năng khác như kiểm tra xác thực từ xa và quản lý khóa, WPA2 giúp bảo vệ dữ liệu truyền qua mạng một cách an toàn.

802.1X là một giao thức bảo mật mạng WLAN phổ biến, được sử dụng để xác thực người dùng và thiết bị trước khi cho phép truy cập vào mạng. Giao thức này yêu cầu người dùng cung cấp thông tin xác thực (tên người dùng và mật khẩu) để có thể kết nối vào mạng WLAN.

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) là một giao thức xác thực khác được sử dụng rộng rãi trong các mạng WLAN. Nó sử dụng chứng chỉ số để xác thực danh tính của người dùng và thiết bị trước khi cho phép truy cập vào mạng. EAP-TLS được coi là một trong những giao thức bảo mật WLAN mạnh nhất hiện nay.

VPN (Virtual Private Network) là một công nghệ bảo mật mạng khác được sử dụng để bảo vệ dữ liệu truyền qua mạng WLAN. Nó tạo ra một kết nối mạng an toàn giữa hai điểm cuối và mã hóa dữ liệu truyền qua mạng. VPN được sử dụng rộng rãi trong các tổ chức và doanh nghiệp để bảo vệ thông tin quan trọng và dữ liệu nhạy cảm.

2.13.4 Cách thức hoạt động

Cách thức hoạt động của WLAN bao gồm ba yếu tố chính: điểm truy cập (Access Point - AP), thiết bị kết nối và phần mềm quản lý mạng.

Điểm truy cập (AP) là trung tâm của một mạng không dây. Nó là thiết bị cơ sở cho phép các thiết bị khác kết nối vào mạng và truy cập các tài nguyên khác nhau. AP có thể kết nối với mạng có dây và cung cấp kết nối không dây cho các thiết bị khác. Mỗi AP có một địa chỉ MAC duy nhất để xác định nó trên mạng. Ngoài ra, mỗi AP còn có một tên mạng SSID (Service Set Identifier) để các thiết bị khác có thể tìm kiếm và kết nối vào mạng.

Thiết bị kết nối trong mạng WLAN là những thiết bị có khả năng kết nối vào mạng không dây, chẳng hạn như máy tính xách tay, điện thoại thông minh, máy tính bảng và các thiết bị IoT. Chúng sử dụng sóng vô tuyến để truyền và nhận dữ liệu từ AP.

Phần mềm quản lý mạng là một bộ phần mềm cho phép người quản trị mạng cấu hình và quản lý mạng WLAN. Nó cho phép định cấu hình các thiết bị kết nối vào mạng, giám sát trạng thái của các thiết bị và quản lý việc truy cập vào tài nguyên mạng.

Khi một thiết bị di động muốn kết nối vào mạng WLAN, nó sẽ quét các tín hiệu sóng vô tuyến trong khu vực và tìm kiếm các mạng có sẵn. Khi tìm thấy một mạng có sẵn, thiết bị sẽ yêu cầu kết nối vào mạng này bằng cách gửi yêu cầu đến AP. Sau đó, AP sẽ yêu cầu thiết bị cung cấp thông tin đăng nhập, chẳng hạn như mật khẩu,

để xác thực thiết bị. Nếu thông tin đăng nhập chính xác, AP sẽ cho phép thiết bị truy cập vào mạng.

Khi đã kết nối vào mạng WLAN, các thiết bị có thể giao tiếp với nhau và truy cập vào các tài nguyên khác như internet hoặc hệ thống tập tin trong mạng. Các tín hiệu sóng vô tuyến được mã hóa để đảm bảo tính riêng tư và an toàn của dữ liệu.

2.14 Default/ Static Route

2.14.1 Giới thiệu về Default/ Static Route

Default/Static Route là một phương thức dùng để định tuyến (routing) các gói tin trong mạng. Khi một thiết bị mạng muốn gửi dữ liệu đến một địa chỉ mà nó không biết cách đến, nó sẽ sử dụng route mặc định (default route) để chuyển tiếp gói tin đó đến một thiết bị khác để xử lý.

Để hiểu rõ hơn về cách hoạt động của Default/Static Route, ta hãy cùng điểm qua các thành phần chính của nó:

- Destination Network: Đây là địa chỉ IP của mạng đích mà chúng ta muốn gửi gói tin đến.
- Subnet Mask: Là số bit mà trong địa chỉ IP của mạng đích sẽ được sử dụng để xác định địa chỉ con mạng (subnet) và địa chỉ host.
- Gateway: Là địa chỉ IP của thiết bị mạng tiếp nhận gói tin và chuyển tiếp đến mạng đích.
- Interface: Là giao diện mạng mà gói tin sẽ được gửi ra để đến gateway.

Khi một gói tin được truyền trong mạng, thiết bị mạng sẽ kiểm tra xem địa chỉ IP đích của gói tin có nằm trong bảng định tuyến (routing table) của nó hay không. Nếu có, thiết bị sẽ xác định được gateway để chuyển tiếp gói tin đến đích. Nếu không, thiết bị sẽ sử dụng default route để gửi gói tin đến gateway mặc định để xử lý tiếp.

Việc sử dụng Default/Static Route có nhiều ưu điểm như giảm tốn chi phí vì không cần phải sử dụng các giao thức định tuyến phức tạp như OSPF hay BGP, đồng thời giúp cho việc quản lý mạng dễ dàng hơn bởi vì các thông số cấu hình được định nghĩa trực tiếp trên thiết bị mạng.

Tuy nhiên, việc sử dụng Default/Static Route cũng có những hạn chế nhất định. Chẳng hạn như nếu một thiết bị mạng cần gửi dữ liệu đến một địa chỉ IP mới mà không nằm trong bảng định tuyến của nó, thì gói tin sẽ không được chuyển tiếp đến đích. Đồng thời, việc quản lý và cấu hình cho các route tĩnh cũng có thể trở nên phức tạp nếu mạng lớn hoặc độ phân giải mạng lớn.

2.14.2 Cách thức hoạt động

Router là một thiết bị mạng có khả năng kết nối các mạng với nhau. Điều này nhờ vào tính năng định tuyến (routing). Tính năng này cho phép router có khả năng xử lý các gói tin dữ liệu và chuyển chúng từ một mạng sang mạng khác.

Khi một gói tin dữ liệu được gửi từ một thiết bị tới một địa chỉ đích, router sẽ tiếp nhận thông tin về gói tin đó và quyết định chuyển tiếp nó đến mạng nào. Việc quyết định này được thực hiện thông qua các tuyến đường (route) được cấu hình trên router.

Có hai loại tuyến đường chính: Default Route và Static Route.

Default Route	Static Route
Default Route là một tuyến đường mặc định cho phép chuyển tiếp các gói tin mà không có tuyến đường cụ thể nào được cấu hình trên router. Nó được sử dụng khi router không biết	Static Route là tuyến đường được cấu hình trực tiếp trên router, thường được sử dụng trong các mạng nhỏ hoặc trung bình. Các tuyến đường này được cấu hình bằng tay bởi người

<p>làm sao để đưa gói tin đến đích cuối cùng.</p> <p>Khi một gói tin được gửi từ một thiết bị, và không có tuyến đường cụ thể nào được cấu hình trên router, router sẽ sử dụng Default Route để gửi gói tin đó tiếp theo. Tuy nhiên, điều này chỉ xảy ra nếu không có tuyến đường cụ thể nào được cấu hình trên router.</p> <p>Default Route thường được cấu hình trên router thông qua các thông số như IP address và subnet mask.</p>	<p>quản trị mạng, và không thay đổi theo thời gian.</p> <p>Khi một gói tin được gửi từ một thiết bị, router sẽ kiểm tra các tuyến đường được cấu hình trên nó để quyết định làm sao để chuyển tiếp gói tin đến đích cuối cùng. Nếu router tìm thấy tuyến đường cụ thể cho địa chỉ đó, nó sẽ sử dụng tuyến đường đó để chuyển tiếp gói tin. Nếu không có tuyến đường nào được cấu hình cho địa chỉ đó, router sẽ tiếp tục kiểm tra các tuyến đường khác cho đến khi nó tìm ra một tuyến đường phù hợp.</p>
---	---

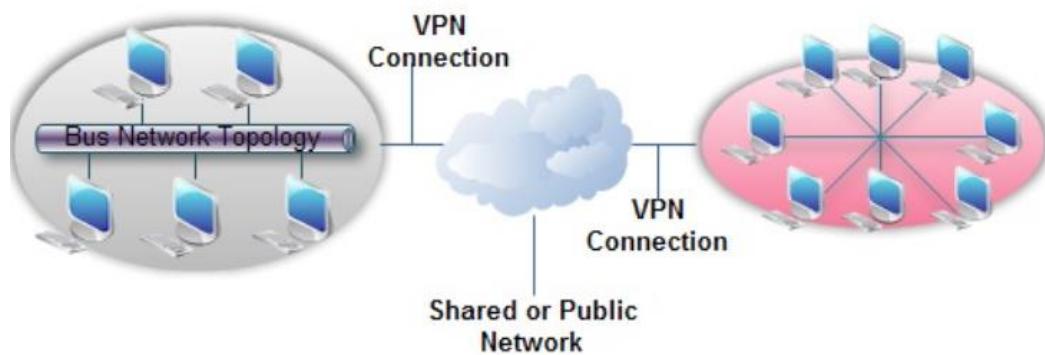
Bảng 2.14.2. 1 So sánh Default và Static Route

2.15 Site-to-site IPSec VPN (Virtual Private Network)

2.15.1 Giới thiệu về VPN

VPN (Virtual Private Network) là một công nghệ được sử dụng để tạo ra một kết nối an toàn và riêng tư giữa các thiết bị trong một mạng. VPN cho phép người dùng truy cập vào internet thông qua một máy chủ ẩn danh, giúp che giấu địa chỉ IP của người dùng và tăng tính bảo mật của dữ liệu truyền qua mạng.

Trong thời đại số hóa hiện nay, việc sử dụng VPN đã trở thành một phương tiện quan trọng để bảo vệ thông tin cá nhân và tăng tính riêng tư trên internet. VPN được sử dụng rộng rãi trong nhiều lĩnh vực khác nhau, từ doanh nghiệp đến người dùng cá nhân, để tăng cường tính bảo mật và tránh các cuộc tấn công mạng.



Hình 2.15.1. 1 Mô hình ứng dụng công nghệ VPN trong hệ thống mạng

Một trong những ứng dụng phổ biến của VPN là cho phép người dùng truy cập vào các trang web bị chặn hoặc cấm truy cập, bằng cách đổi địa chỉ IP của mình thành địa chỉ IP khác tại một quốc gia khác. Ví dụ, khi truy cập vào một trang web có nội dung bị kiểm duyệt bởi chính phủ Trung Quốc, người dùng có thể sử dụng VPN để giả mạo địa chỉ IP tại Mỹ hoặc một quốc gia khác, và truy cập vào trang web đó mà không bị giới hạn.

Ngoài ra, VPN cũng được sử dụng trong các doanh nghiệp để tạo ra một mạng riêng ảo (VPN) giữa các văn phòng hoặc giữa các nhân viên. Điều này giúp giảm thiểu rủi ro khi truyền tải dữ liệu giữa các thành viên trong mạng. Các doanh nghiệp cũng có thể sử dụng VPN để bảo vệ thông tin quan trọng, chẳng hạn như thông tin khách hàng, thông tin tài khoản và các dữ liệu nhạy cảm khác.

Trong quá trình sử dụng VPN, dữ liệu sẽ được mã hóa và giải mã khi đi qua máy chủ VPN. Điều này giúp ngăn chặn các cuộc tấn công mạng và giảm thiểu rủi ro bị đánh cắp thông tin cá nhân hoặc dữ liệu quan trọng.

Tuy nhiên, cần lưu ý rằng việc sử dụng VPN chỉ là một trong những biện pháp để tăng tính bảo mật và riêng tư trên internet, và không phải là giải pháp tuyệt đối. Thậm chí, một số người còn cho rằng việc sử dụng VPN có thể gây ảnh hưởng đến tốc độ kết nối internet của người dùng.

2.15.2 Các giao thức trong IPSec

IPSec (Internet Protocol Security) là một giao thức được sử dụng để tạo ra một kết nối an toàn và bảo mật giữa các thiết bị trong một mạng. Các giao thức được sử dụng trong IPSec bao gồm Authentication Header (AH), Encapsulating Security Payload (ESP) và Internet Key Exchange (IKE).

Authentication Header (AH) là một phương thức xác thực gói tin trên mạng thông qua việc thêm một trường mã hóa vào phần header của gói tin IP. Trong quá trình truyền tải dữ liệu, AH sẽ đảm bảo tính toàn vẹn của gói tin, ngăn chặn các cuộc tấn công Man-in-the-middle hoặc các cuộc tấn công khác nhằm thay đổi dữ liệu trên đường truyền.

Encapsulating Security Payload (ESP) là một giao thức cho phép mã hóa dữ liệu và tạo ra một kênh kết nối an toàn giữa hai thiết bị. ESP cung cấp tính riêng tư cho dữ liệu truyền tải giữa các thiết bị và ngăn chặn các cuộc tấn công từ bên ngoài.

Internet Key Exchange (IKE) là giao thức được sử dụng để thiết lập các kết nối IPSec giữa các thiết bị. IKE có hai phiên bản: IKEv1 và IKEv2. IKEv1 sử dụng pre-shared keys để thiết lập kết nối, trong khi IKEv2 sử dụng các chứng chỉ số để xác thực thiết bị.

Các giao thức trên đều được sử dụng để tăng cường tính bảo mật và riêng tư cho các kết nối trên internet. Với IPSec, các thiết bị có thể kết nối với nhau qua mạng Internet một cách an toàn và bảo mật hơn, ngăn chặn các cuộc tấn công từ bên ngoài và giảm thiểu rủi ro bị đánh cắp thông tin cá nhân hoặc dữ liệu quan trọng.

Ngoài ra, việc sử dụng IPSec cũng có thể ảnh hưởng đến tốc độ truyền tải dữ liệu của mạng. Tuy nhiên, điều này thường không ảnh hưởng đến hiệu suất của mạng cho đến khi mạng trở nên quá tải.

2.15.3 Cách thức hoạt động

Các thiết bị được sử dụng trong Site-to-site IPSec VPN bao gồm các cổng (gateway) VPN hoặc các thiết bị router có tính năng VPN. Các thiết bị này được cấu hình để thiết lập kết nối VPN giữa hai mạng khác nhau.

Quá trình thiết lập kết nối Site-to-site IPSec VPN bao gồm các bước sau:

Bước 1: Xác định các thông số kết nối: Điều này bao gồm việc xác định địa chỉ IP của các cổng VPN, loại mã hóa và các thông số khác liên quan đến kết nối.

Bước 2: Thiết lập kết nối IKE (Internet Key Exchange): Khi các thông số kết nối đã được xác định, gateway VPN sẽ sử dụng giao thức IKE để thiết lập kết nối giữa các thiết bị. IKE sử dụng khóa công khai và khóa bí mật để xác thực và trao đổi thông tin giữa các thiết bị.

Bước 3: Thiết lập kết nối IPSec: Sau khi kết nối IKE đã được thiết lập, các gateway VPN sẽ sử dụng giao thức IPSec để thiết lập kết nối mã hóa giữa hai mạng. Các gói tin trong quá trình truyền tải sẽ được mã hóa và giải mã trên các cổng VPN.

Bước 4: Truyền tải dữ liệu: Sau khi kết nối IPSec đã được thiết lập, các thiết bị trong hai mạng sẽ có thể truyền tải dữ liệu qua VPN một cách an toàn và bảo mật.

Site-to-site IPSec VPN cho phép các doanh nghiệp kết nối các văn phòng với nhau và chia sẻ tài nguyên mạng, từ dữ liệu đến ứng dụng và máy chủ. Công nghệ này giúp giảm thiểu rủi ro bị đánh cắp thông tin và tăng cường tính bảo mật của các kết nối mạng.

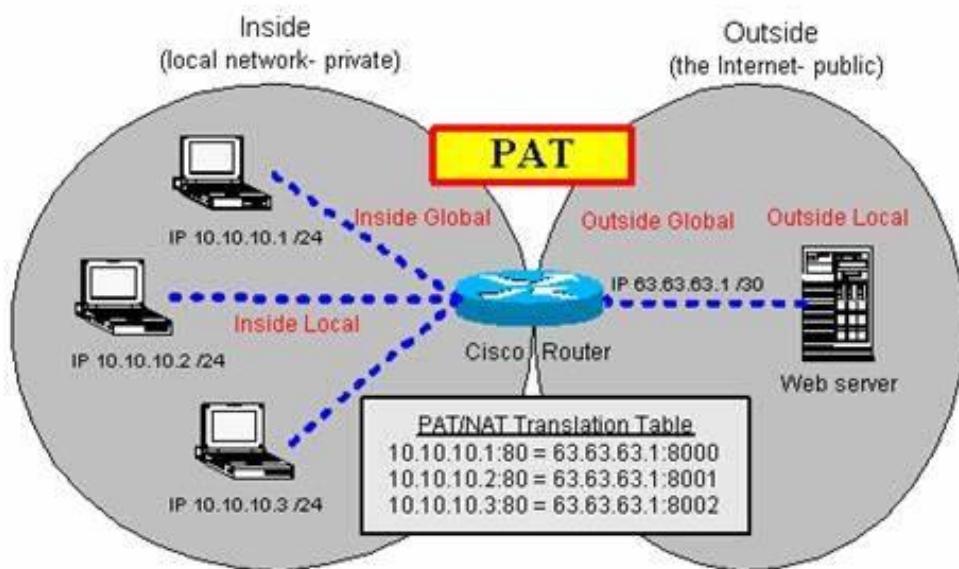
Tuy nhiên, việc triển khai Site-to-site IPSec VPN cần phải được thực hiện đúng cách và cẩn thận để đảm bảo tính bảo mật của hệ thống. Cần phải đảm bảo rằng các thiết bị được cấu hình đúng cách và được bảo vệ khỏi các cuộc tấn công từ bên ngoài.

Ngoài ra, việc triển khai Site-to-site IPSec VPN cũng có thể ảnh hưởng đến hiệu suất và tốc độ truyền tải của mạng. Tuy nhiên, điều này thường không ảnh hưởng đến hiệu suất của mạng cho đến khi mạng trở nên quá tải.

2.16 Port Address Translation (PAT - NAT Overload)

2.16.1 Giới thiệu về PAT

Port Address Translation (PAT) là một kỹ thuật định tuyến mạng, còn được gọi là NAT Overload (Network Address Translation Overload). Kỹ thuật này cho phép các thiết bị trong một mạng riêng truy cập vào internet thông qua một địa chỉ IP duy nhất. PAT sử dụng các cổng số để phân biệt các kết nối khác nhau và định tuyến chúng đến các thiết bị trong mạng.



Hình 2.16.1. 1 Mô hình hệ thống định tuyến PAT

Khi sử dụng PAT, các thiết bị trong mạng sẽ được gán một địa chỉ IP duy nhất, thường là địa chỉ IP của thiết bị đầu cuối, như router hoặc máy tính. Các kết nối đến các thiết bị trong mạng sẽ được xác định bằng cách sử dụng các cổng số riêng biệt.

Ví dụ, nếu một thiết bị trong mạng muốn truy cập internet, nó sẽ yêu cầu cho NAT (Network Address Translation) chuyển tiếp các yêu cầu này đi đến internet. NAT sẽ tiến hành gán một số cổng riêng biệt cho thiết bị này và lưu trữ thông tin về các kết nối này. Khi các gói tin trả về từ internet, NAT sẽ sử dụng thông tin này để định tuyến các gói tin đến thiết bị tương ứng trong mạng.

Như vậy, các thiết bị trong mạng có thể chia sẻ một địa chỉ IP duy nhất để truy cập internet, giúp tiết kiệm đáng kể các địa chỉ IP và ngăn chặn việc xung đột giữa các địa chỉ IP.

Tuy nhiên, PAT cũng có một số hạn chế. Trong quá trình định tuyến, PAT sử dụng các cổng số để phân biệt các kết nối khác nhau. Do đó, nếu có quá nhiều kết nối được tạo ra từ các thiết bị trong mạng, các cổng này sẽ bị sử dụng hết và không thể tạo ra các kết nối mới. Điều này có thể dẫn đến hiện tượng "chết cổng" (port exhaustion) và làm giảm hiệu suất của mạng.

Ngoài ra, PAT cũng có thể gây ra một số vấn đề liên quan đến bảo mật. Vì các thiết bị trong mạng chỉ có một địa chỉ IP duy nhất, việc theo dõi và quản lý các kết nối trở nên khó khăn hơn, và có thể cho phép các cuộc tấn công từ bên ngoài.

2.16.2 Các loại PAT

Có ba loại PAT chính:

Static PAT cho phép các kết nối từ một địa chỉ IP public được chuyển tiếp đến một địa chỉ IP private cụ thể trong mạng. Tức là, một địa chỉ IP public được ánh xạ một cách tĩnh với một địa chỉ IP private để kết nối tới một server hoặc một ứng dụng cụ thể. Ví dụ, khi một yêu cầu truy cập đến địa chỉ IP public của một website, PAT sẽ ánh xạ nó đến một địa chỉ IP private của các server web trong mạng.

Dynamic PAT cho phép các kết nối từ nhiều địa chỉ IP public được chuyển tiếp đến các địa chỉ IP private khác nhau trong mạng. Nghĩa là, các kết nối từ các địa

chỉ IP public sẽ được gán các cổng số riêng biệt và sau đó được chuyển tiếp đến các địa chỉ IP private tương ứng. Dynamic PAT cho phép nhiều thiết bị trong mạng truy cập internet thông qua một địa chỉ IP public duy nhất.

Overloading PAT, hay còn được gọi là Port Overloading, cho phép các kết nối từ nhiều địa chỉ IP private khác nhau trong mạng được chuyển tiếp đến một địa chỉ IP public duy nhất. Kỹ thuật này sử dụng các cổng số để phân biệt các kết nối khác nhau và định tuyến chúng đến các thiết bị trong mạng. Khi các gói tin trả về từ internet, Overloading PAT sẽ sử dụng thông tin này để định tuyến các gói tin đến thiết bị tương ứng trong mạng.

Mỗi loại PAT có ưu điểm và hạn chế riêng. Static PAT thích hợp cho các ứng dụng yêu cầu các địa chỉ IP cụ thể, như server web hoặc các ứng dụng truyền thông. Dynamic PAT cho phép nhiều thiết bị trong mạng truy cập internet thông qua một địa chỉ IP public duy nhất và giúp tiết kiệm đáng kể các địa chỉ IP. Overloading PAT cung cấp tính năng chia sẻ tài nguyên mạng cho các thiết bị trong mạng và giúp tiết kiệm đáng kể các địa chỉ IP.

2.16.3 Cách thức hoạt động

PAT hoạt động bằng cách ánh xạ các địa chỉ IP private và các cổng số tương ứng của chúng sang một địa chỉ IP public duy nhất. Điều này cho phép các kết nối từ các thiết bị trong mạng riêng có thể được gửi đến internet thông qua địa chỉ IP public duy nhất này. Trong quá trình này, PAT sử dụng các cổng số để phân biệt các kết nối khác nhau và định tuyến chúng đến các thiết bị trong mạng.

Khi một thiết bị trong mạng muốn truy cập internet, nó sẽ yêu cầu NAT (Network Address Translation) chuyển tiếp các yêu cầu này đi đến internet. NAT sẽ tiến hành gán một số cổng riêng biệt cho thiết bị này và lưu trữ thông tin về các kết nối này. Khi các gói tin trả về từ internet, NAT sẽ sử dụng thông tin này để định tuyến các gói tin đến thiết bị tương ứng trong mạng.

Ví dụ, khi một yêu cầu truy cập đến địa chỉ IP public của một website được gửi đến router của mạng, router sẽ sử dụng PAT để ánh xạ địa chỉ IP và cổng số của yêu cầu này sang một địa chỉ IP private tương ứng. Sau đó, yêu cầu này sẽ được chuyển tiếp đến thiết bị tương ứng trong mạng riêng.

Các loại PAT khác nhau có cách thức hoạt động khác nhau, nhưng đều sử dụng cơ chế ánh xạ địa chỉ IP và cổng số để phân biệt các kết nối khác nhau. Static PAT cho phép các kết nối từ một địa chỉ IP public được chuyển tiếp đến một địa chỉ IP private cụ thể trong mạng, Dynamic PAT cho phép các kết nối từ nhiều địa chỉ IP public được chuyển tiếp đến các địa chỉ IP private khác nhau trong mạng và Overloading PAT cho phép các kết nối từ nhiều địa chỉ IP private khác nhau trong mạng được chuyển tiếp đến một địa chỉ IP public duy nhất.

2.17 NTP và Syslog

Network Time Protocol (NTP) là một giao thức được sử dụng để đồng bộ hóa thời gian trên mạng. Nó cho phép các thiết bị trong mạng được đồng bộ hóa với cùng một chuẩn thời gian, giúp hệ thống hoạt động chính xác và hiệu quả hơn. Để đảm bảo tính chính xác của thời gian, các máy chủ NTP sử dụng một số nguồn thời gian chính xác như các đồng hồ lõi atom hoặc GPS.

NTP giao tiếp qua UDP trên cổng 123. Các thiết bị có thể yêu cầu thời gian từ một máy chủ NTP bằng cách gửi một gói tin yêu cầu tới máy chủ và sau đó đợi phản hồi. Các máy chủ NTP có thể được cấu hình để đồng bộ thời gian với một máy chủ NTP khác, tạo ra một chuỗi các máy chủ NTP kết nối lại với nhau để đồng bộ hóa thời gian.

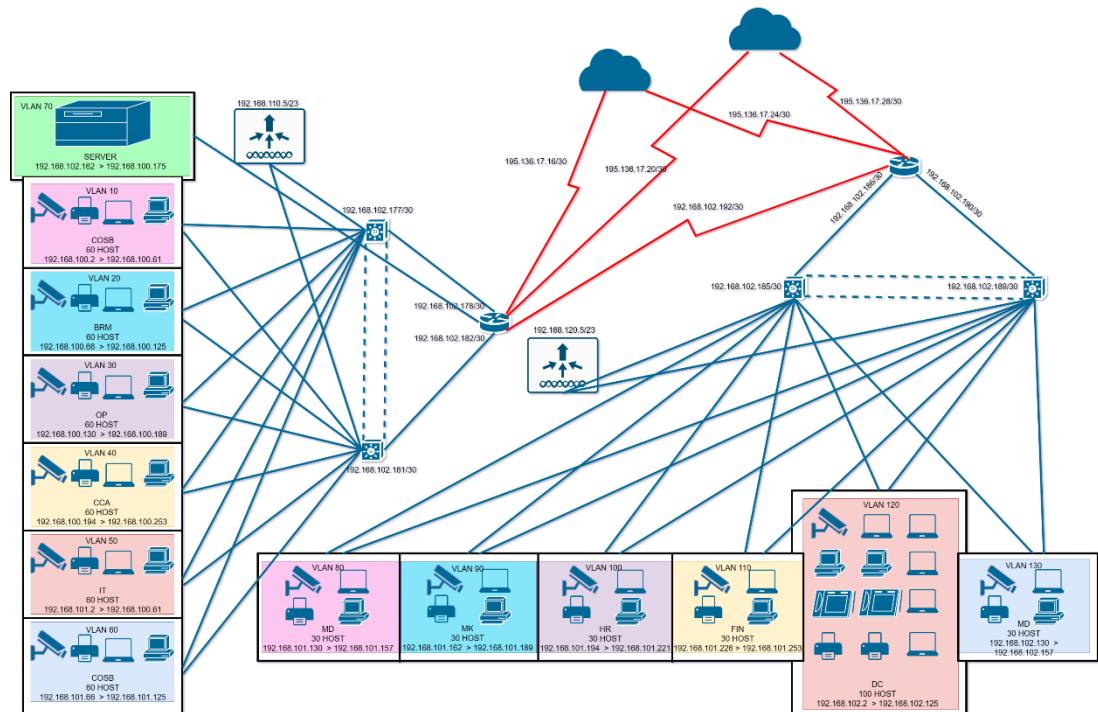
Syslog là một giao thức ghi nhật ký sự kiện trên hệ thống. Nó cho phép các ứng dụng, hệ thống hoặc thiết bị khác nhau trong mạng ghi lại các thông tin quan trọng để giám sát và phân tích sau này. Các thông tin này có thể bao gồm lỗi hệ thống, cảnh báo bảo mật hay các hoạt động của người dùng.

Một số ứng dụng của Syslog có thể kể đến như giám sát hệ thống, phân tích dữ liệu, cảnh báo an ninh và điều tra sự cố. Thông tin được ghi lại bởi Syslog có thể được lưu trữ trên máy chủ Syslog để phân tích hoặc đưa ra cảnh báo. Để giảm bớt mức độ ồn ào của các thông báo không quan trọng, Syslog có thể được cấu hình để chỉ ghi lại các sự kiện quan trọng.

Các bản ghi Syslog được gửi từ các thiết bị khác nhau trên mạng qua giao thức UDP trên cổng 514. Một số thiết bị có thể được cấu hình để gửi các bản ghi Syslog đến một máy chủ Syslog trung tâm để lưu trữ và phân tích.

PHẦN 3 THIẾT KẾ MẠNG LUẬN LÝ

3.1 Sơ đồ mạng logic



Hình 3.1. 1 Sơ đồ mạng logic

3.2 Phân chia địa chỉ IP cho các thiết bị

Trong hệ thống mạng, sử dụng dải địa chỉ 192.168.100.0 để đặt cho các thiết bị cụ thể:

Public IP: 195.136.17.16/30, 195.136.17.20/30,

195.136.17.24/30, 195.136.17.28/30

Router: 192.168.102.176 – 192.168.102.192

Server: 192.168.102.160 - 192.168.102.175

WLAN: 192.168.110.0 – 192.168.111.255, 192.168.120.0 – 192.168.121.255

Máy in: IP được gán tĩnh theo từng VLAN

Camera: IP được gán động theo từng VLAN

Laptop: IP được gán động theo từng VLAN khi kết nối tới LWAP

PC: được gán động theo từng VLAN

3.3 Thiết kế an ninh mạng

Xác định tài nguyên mạng:

- Thiết bị mạng (Router, Switch Layer 3, Switch Layer 2, ...)
- Các máy đầu cuối (Máy tính bàn, Laptop, Máy in, Camera, Tablet,...)

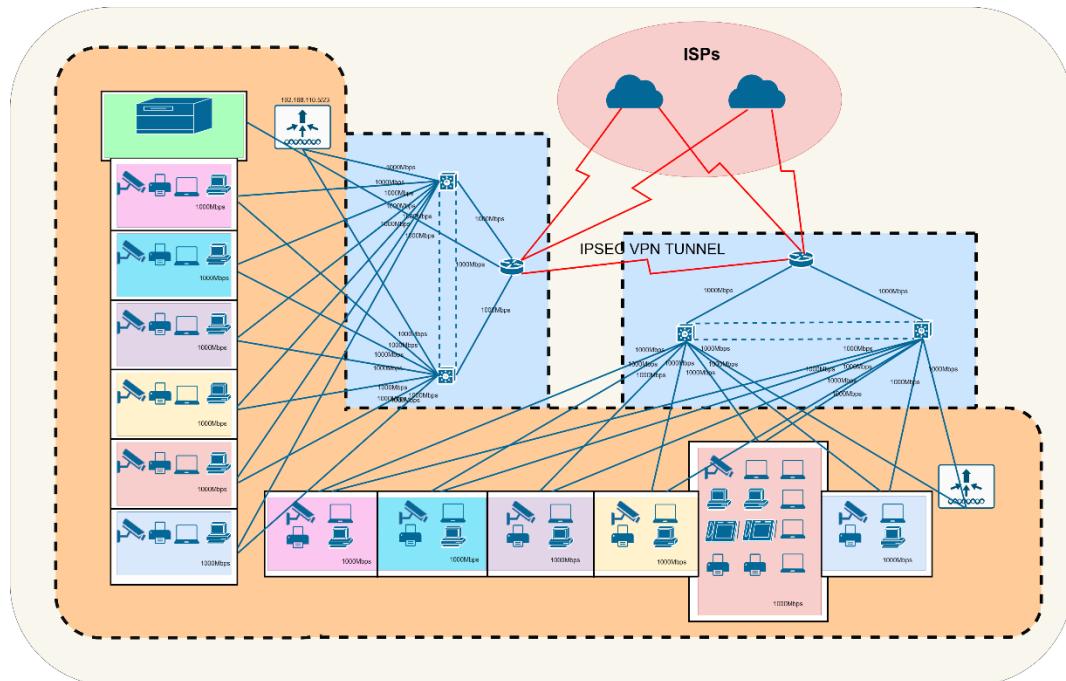
Xây dựng chính sách bảo mật:

- Các thiết bị mạng cần phải bảo mật để chỉ người quản trị có thể truy cập vào.
- Ngăn ngừa các truy cập trái phép vào trong mạng.
- Chặn truy cập từ các địa chỉ IP không hợp lệ hoặc địa chỉ IP bị nghi ngờ.
- Giới hạn truy cập vào các máy chủ chỉ cho phép những người dùng được ủy quyền hoặc xác thực.

- Chặn truy cập vào các giao diện hoặc cổng không được phép, bao gồm các cổng USB và cổng Ethernet.
- Chặn truy cập vào các trang web độc hại, phần mềm độc hại hoặc các trang web không an toàn.
- Kiểm soát quyền truy cập vào các tài khoản người dùng, giới hạn quyền truy cập theo vai trò hoặc cấp độ truy cập khác nhau.

PHẦN 4 THIẾT KẾ MẠNG VẬT LÝ

4.1 Sơ đồ mạng vật lý



Hình 4.1. 1 Sơ đồ mạng vật lý

4.2 Bảng thống kê hàng hóa

Thiết bị	Mô tả chi tiết	SL	Gía tiền	Tổng
HP EliteDesk 800 G6 SFF (PC)	Kích thước: Nhỏ gọn Tùy chọn CPU: Intel Gen10 i3/i5/i7/i9, Celeron, Pentium Chipset: Q470 GPU rời: GeForce GTX 1650 Low Profile	115	18,000,000 vnđ	2,070,000,000

	<p>RAM: DIMM DDR4-2933 với 4 khe cắm và tốc độ 2933 MT/s. RAM tối đa lên tới 128 GB.</p> <p>Cổng USB: USB-C 3.1, 4x USB-A 3.1, 4x USB-A 3.0 và 2x USB-A 2.0.</p> <p>Cổng video: 2 cổng DisplayPort.</p> <p>Các cổng khác: RJ45, Hdph, Headset, Line-Out.</p> <p>Các cổng tùy chọn: DP1.4/HDMI2.0a/VGA/USB-C(DP1.4)/2x USB-A 3.0/LAN/Thunderbolt3, Serial, đầu đọc thẻ SD.</p> <p>Số lượng cổng SATA: 3.</p> <p>Khe cắm PCI: PCIe 3.0 x16, 2x PCIe 3.0 x1 và PCIe 3.0 x16 (wired x4).</p> <p>Khe M.2: 2 khe M.2 2280/2230 M-key (PCIe x4) và 1 khe M.2 2230 (WiFi/BT).</p> <p>Khay ổ đĩa: 2 khay 2.5in, 2 khay 3.5in và 1 khay 5.25in (slim).</p> <p>Nguồn: 260/350 W.</p> <p>Trọng lượng: 6.13 kg (13.51 lb).</p> <p>Ngày ra mắt: 2020.</p>			
Hikvision DS- 2CD2346G2 -IU (Camera)	<p>Chất lượng hình ảnh cao với độ phân giải 4 MP.</p> <p>Hiệu suất chụp ảnh tốt trong điều kiện ánh sáng yếu nhờ công nghệ powered-by-DarkFighter.</p> <p>Hình ảnh rõ nét ngay cả trong điều kiện chiếu sáng mạnh nhờ công nghệ 120 dB WDR.</p>	32	6,500,000	201,500,000

	Công nghệ nén H.265+ hiệu quả giúp tối ưu hóa không gian lưu trữ. Tập trung vào phân loại đối tượng con người và xe cộ dựa trên học sâu. Microphone tích hợp sẵn giúp theo dõi âm thanh thời gian thực (trong model -U). Chống nước và bụi bẩn với khả năng chống nước IP67.			
HP LaserJet Enterprise M608dn (Máy in)	Tốc độ in: lên đến 61 trang/phút (trang A4). Độ phân giải: lên đến 1200 x 1200 dpi. Bộ nhớ chuẩn: 512 MB, có khả năng nâng cấp lên đến 2,5 GB. Khay giấy: khay đựng giấy tùy chọn đến 4 khay (bao gồm khay đa năng) với tổng dung lượng tối đa lên đến 3.600 tờ. Kích thước giấy hỗ trợ: từ A4 đến A6, bao gồm các kích thước giấy và tiêu chuẩn quốc tế khác. Cổng kết nối: USB 2.0, Ethernet, NFC. Hỗ trợ ngôn ngữ in: HP PCL 6, HP PCL 5c, HP postscript level 3 emulation, native PDF printing (v1.7), Apple AirPrint. Chu kỳ làm việc hàng tháng tối đa: lên đến 275.000 trang.	5	15,500,000	77,500,000
Canon Color imageCLASS MF644Cdw (Máy in)	Tốc độ in: lên đến 20 trang/phút (trang A4). Độ phân giải: lên đến 1200 x 1200 dpi. Bộ xử lý: Intel Atom Processor BayTrail 1,33GHz.	1		22,000,000

	Bộ nhớ chuẩn: 3 GB. Khay giấy đầu vào: khay đa năng dung lượng 100 tờ và khay cassette tiêu chuẩn dung lượng 550 tờ. Khay giấy đầu ra: dung lượng 250 tờ. Kích thước giấy hỗ trợ: từ A5 đến A3, bao gồm các kích thước giấy và tiêu chuẩn quốc tế khác. Cổng kết nối: USB 2.0, Ethernet, Wi-Fi. Hỗ trợ ngôn ngữ in: UFRII, PCL6, Adobe PostScript Level 3, PDF, XPS. Màn hình hiển thị: màn hình LCD cảm ứng màu rộng 10,1 inch.			
Laptop Dell Vostro 3590 (Laptop)	Bộ vi xử lý: Intel Core i5-10210U hoặc i7-10510U (thế hệ thứ 10) Card đồ họa: Intel UHD Graphics hoặc Nvidia GeForce MX230 RAM: 8GB hoặc 16GB DDR4-2666 SDRAM (có thể nâng cấp lên đến 32GB) Ổ đĩa cứng: 256GB hoặc 512GB SSD PCIe NVMe M.2 Màn hình: 15.6 inch Full HD IPS, độ phân giải 1920 x 1080 pixel Hệ điều hành: Windows 10 Home hoặc Pro 64-bit Cổng kết nối: 1 cổng USB Type-C, 2 cổng USB 3.1 Gen 1 Type-A, 1 cổng USB 2.0, 1 cổng HDMI, jack audio combo, khe cắm thẻ nhớ SD	200	14,000,000	2,800,000,000

	Kết nối mạng: Wi-Fi 802.11ac, Bluetooth 4.1 Pin: 4-cell, 42 Whr, tuổi thọ 6-7 giờ Trọng lượng: 1.91kg			
Cisco Aironet 1700 Series (LWAP)	Chuẩn Wi-Fi: IEEE 802.11a/b/g/n/ac Wave 2 Băng tần: Dual-band (2.4 GHz và 5 GHz) Tốc độ truyền dữ liệu tối đa: Lên đến 1.3 Gbps Anten: Internal omnidirectional anten với khả năng điều chỉnh góc phủ sóng Cổng kết nối: 1 cổng Ethernet Gigabit Hỗ trợ công suất truyền lên đến: 22 dBm (cho băng tần 2.4 GHz) và 23 dBm (cho băng tần 5 GHz) Hỗ trợ Power over Ethernet (PoE): 802.3af/at Hỗ trợ các tính năng bảo mật: WPA, WPA2, 802.11i, AES, TKIP, 802.1X Hệ điều hành: Cisco IOS-XE Kích thước: 21 x 21 x 4.7 cm Trọng lượng: 0.87 kg	26	10,000,000	260,000,000
Cisco ISR 4331/K9 (Router)	Chuẩn giao thức: IPv4, IPv6, IPSec, SSL, IEEE 802.11a/b/g/n/ac Tốc độ chuyển tiếp gói tin: 500 Mbps Số cổng LAN: 3 cổng Gigabit Ethernet Số cổng WAN: 2 cổng Gigabit Ethernet Tính năng bảo mật: VPN, Firewall, IPS, URL filtering, AES encryption, SHA-2 authentication, SSL VPN	2	58,000,000	116,000,000

	Hỗ trợ PoE (Power over Ethernet): Không Hỗ trợ VLAN: Có Hỗ trợ QoS (Quality of Service): Có Hỗ trợ NAT (Network Address Translation): Có Bộ nhớ flash: 4GB Bộ nhớ RAM: 4GB Kích thước: 438 x 438 x 44 mm Trọng lượng: 8 kg			
HPE ProLiant DL380 Gen10 (Server)	Bộ vi xử lý: Intel Xeon Scalable Processor, có hỗ trợ cho 2 bộ vi xử lý Số lượng core: Tối đa 56 cores Bộ nhớ RAM: Tối đa 3 TB với 24 khe cắm DIMM Số khe cắm ổ cứng: Tối đa 30 ổ cứng SAS/SATA/SSD 2.5 inch hoặc 20 ổ cứng SAS/SATA/SSD 3.5 inch Đồ họa: Hỗ trợ tính năng GPU Cổng kết nối: 4 cổng mạng Gigabit Ethernet Hỗ trợ RAID: Hỗ trợ RAID 0, 1, 5, 6, 10, 50, 60 Công nghệ bảo mật: TPM (Trusted Platform Module), Secure Boot, Secure Erase, Silicon Root of Trust Hỗ trợ virtualization: Hỗ trợ các nền tảng ảo hóa phổ biến như VMware, Microsoft Hyper-V và Citrix XenServer Kích thước: 17.54 x 72.14 x 63.52 cm (rộng x sâu x cao) Trọng lượng: Từ 16 đến 32 kg tùy thuộc vào cấu hình	1		135,000,000

Cisco Catalyst 9300 Series Switches (Switch)	Số lượng cổng: Tùy chọn từ 24 đến 48 cổng Chuẩn giao thức: IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.3ad, IEEE 802.3ae, IEEE 802.3az, IEEE 802.3z Băng thông chuyển tiếp: Lên đến 480 Gbps Tốc độ chuyển tiếp: Lên đến 720 Mbps Tính năng bảo mật: 802.1x, ACLs, DHCP snooping, Dynamic ARP Inspection, IPv6 First Hop Security, IP Source Guard, Private VLAN Edge, Secure Boot, TrustSec, MACsec, etc. Quản lý mạng: SNMP v1/v2/v3, RMON, syslog, NetFlow, SPAN, ERSPAN, etc. Hỗ trợ PoE (Power over Ethernet): Có Hỗ trợ stacking: Có Hỗ trợ Layer 3: Có Kích thước: 44 x 445 x 444 mm (rộng x sâu x cao) Trọng lượng: Từ 6 đến 8 kg tùy thuộc vào số lượng cổng	14	36,500,000	511,000,000
Fortinet FortiGate 100E (Firewall)	Số lượng cổng: 22 (16 x GE RJ45, 4 x GE SFP, 2 x GE RJ45 WAN) Tốc độ chuyển tiếp: Lên đến 3 Gbps Băng thông IPSec VPN: Lên đến 1.5 Gbps Khả năng xử lý: Lên đến 2.5 triệu sessions/ngày Tính năng bảo mật: Firewall, IPS, VPN, Web filtering, Anti-virus, Anti-spam,	2	40,000,000	80,000,000

	<p>Application control, URL filtering, etc.</p> <p>Quản lý mạng: Web-based GUI, CLI, SNMP v2/v3, FortiExplorer, FortiOS API</p> <p>Hỗ trợ Power over Ethernet (PoE): Không có</p> <p>Kích thước: 1.7 x 8.5 x 6.4 in. (rộng x sâu x cao)</p> <p>Trọng lượng: 3 lbs</p>			
Panduit PatchLink Horizontal Cable Manage	<p>Chiều cao: 1U (44.45mm)</p> <p>Chiều rộng: 483mm</p> <p>Số lượng thanh phân phối cáp mạng: Tùy chọn từ 5 đến 12 thanh</p> <p>Vật liệu: Thép có độ dày 1,5mm</p> <p>Màu sắc: Đen hoặc xám</p> <p>Phụ kiện đi kèm: Các ốc vít cần thiết để lắp đặt và các khung giá đỡ khi cần thiết</p>	20	3,000,000	60,000,000
Cat6a Ethernet Cable (Cáp)	<p>Tần số: có thể truyền tín hiệu lên đến 500 MHz.</p> <p>Tốc độ truyền dữ liệu: có thể đạt tốc độ truyền dữ liệu lên đến 10 Gbps.</p> <p>Điện trở: không quá 100 ohm.</p> <p>Chiều dài tối đa: khoảng 100 mét.</p> <p>Chất liệu: được làm từ đồng nguyên chất hoặc hợp kim đồng và bọc vỏ bằng nhựa PVC hoặc halogen-free.</p> <p>Thiết kế: có thiết kế xoắn đôi để giảm nhiễu và đảm bảo độ chính xác của tín hiệu truyền qua dây cáp.</p>	400 0	100,000	400,000,000
APC NetShelter SX 42U Rack		4	55,000,000	220,000,000

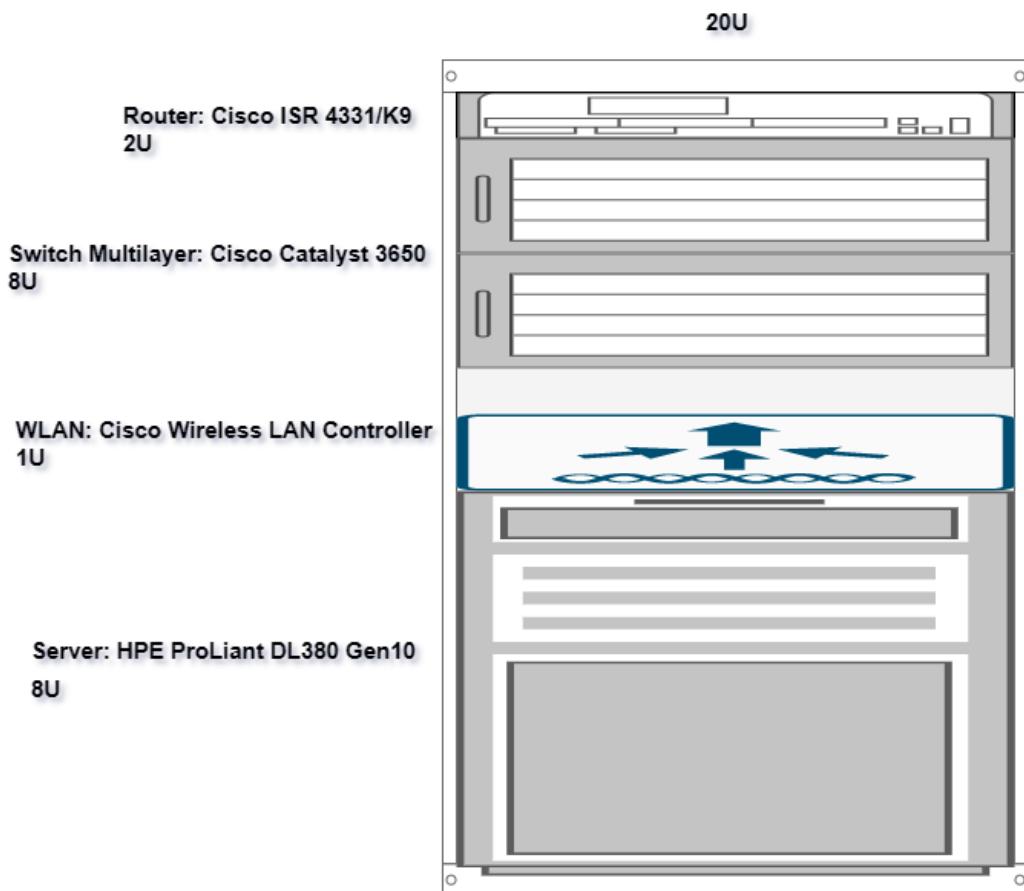
Enclosure (Rack)				
Cisco Catalyst 3650 (Switch Multi)	Số cổng Ethernet: Tùy chọn từ 24 đến 48 cổng RJ-45, hoặc 12 đến 24 cổng SFP Tốc độ truyền tải: Có khả năng hỗ trợ tốc độ truyền tải lên đến 10Gbps Hỗ trợ PoE/PoE+: Có khả năng hỗ trợ công nghệ Power over Ethernet và Power over Ethernet Plus Điện áp sử dụng: AC 120/230 V (50/60 Hz) Kích thước: Thông thường là 44.5 cm x 44.5 cm x 4.39 cm Trọng lượng: Thông thường từ 7kg đến 9kg	4	100,000,000	400,000,000
Cisco Wireless LAN Controller (WLAN)	Kiểu controller: Quản lý trung tâm cho mạng không dây Hỗ trợ APs: Có khả năng quản lý hàng ngàn APs Số lượng VLANs hỗ trợ: 4096 Tần số hoạt động: 2.4 GHz và/hoặc 5 GHz Hỗ trợ chuẩn Wi-Fi: IEEE 802.11a/b/g/n/ac Băng thông tối đa: Lên đến 40 Gbps Tính năng bảo mật: Bao gồm mã hóa, xác thực người dùng, giám sát và phân tích. Hỗ trợ tính năng định tuyến: Có khả năng hỗ trợ định tuyến động và định tuyến tĩnh Hỗ trợ tính năng QoS: Bao gồm WMM (Wi-Fi Multimedia), giới hạn băng thông và điều khiển luồng	2	80,000,000	160,000,000

	Giao diện kết nối: Ethernet, USB			
--	-------------------------------------	--	--	--

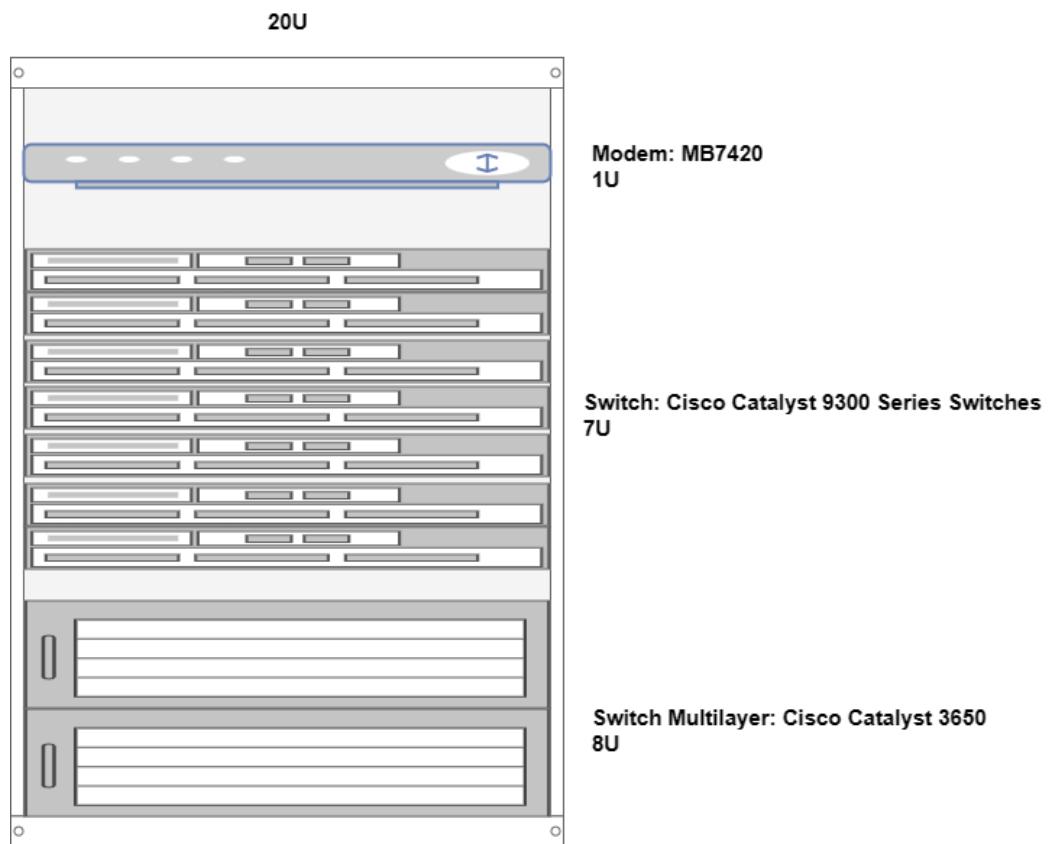
Bảng 4.2. 1 Bảng thống kê hàng hóa

Tổng ~ 7,253,260,000 vnđ

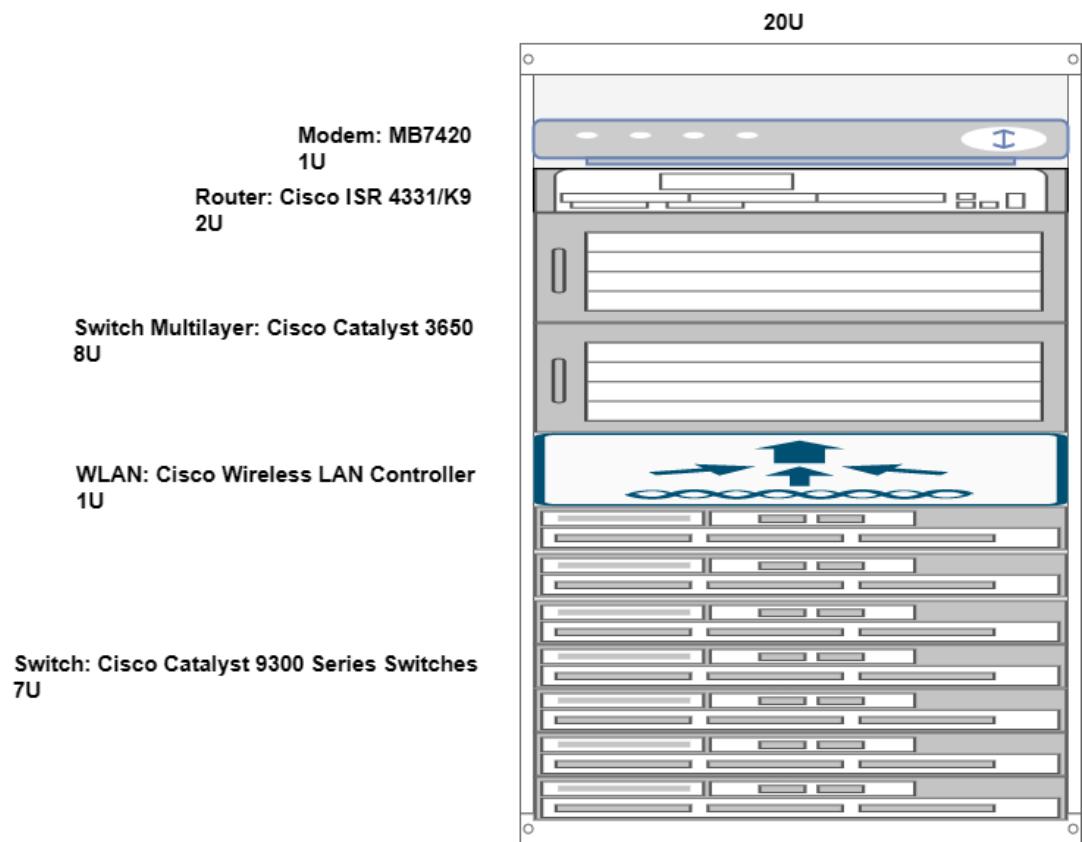
4.3 Sơ đồ Rack



Hình 4.3. 1 Sơ đồ RACK trong tòa nhà chính



Hình 4.3. 2 Sơ đồ RACK trong tòa nhà chính



Hình 4.3. 3 Sơ đồ RACK trong chi nhánh

4.4 Thông tin kết nối Port trong hệ thống mạng

Source to destination	Source Interface	Destination Interface	Trunking/Vlan
ISP1 to HQ-ROUTER	Se0/2/0	Se0/1/0	
ISP1 to BR-ROUTER	Se0/2/1	Se0/1/1	
ISP2 to HQ-ROUTER	Se0/3/0	Se0/2/1	
ISP2 to BR-ROUTER	Se0/3/1	Se0/2/0	
HQ-ROUTER to BR-ROUTER	Se0/2/0	Se0/1/0	
HQ-ROUTER to HQ-MUL-SW-1	Gig0/0	Gig1/0/1	
HQ-ROUTER to HQ-MUL-SW-2	Gig0/1	Gig1/0/1	
HQ-ROUTER to Server-SW	Gig0/2	Fa0/1	
HQ-MUL-SW-1 to HQ-MUL-SW-2	Gig1/0/10	Gig1/0/10	
	Gig1/0/9	Gig1/0/9	

Bảng 4.4. 1 Bảng thông tin kết nối port

Source to destination	Source Interface	Destination Interface	Trunking/Vlan
BR-ROUTER to BR-MUL-SW-3	Gig0/1	Gig1/0/1	
BR-ROUTER to BR-MUL-SW-4	Gig0/0	Gig1/0/1	
HQ-MUL-SW-3 to HQ-MUL-SW-4	Gig1/0/10	Gig1/0/10	
	Gig1/0/9	Gig1/0/9	
Server-SW to DNS-SER	Fa0/2	Fa0	
Server-SW to DHCP-SER	Fa0/3	Fa0	
Server-SW to Email-SER	Fa0/4	Fa0	
Server-SW to Web-SER	Fa0/5	Fa0	
HQ-MUL-SW-1 to COSB-SW	Gig1/0/2	Fa0/1	TRUNK
HQ-MUL-SW-1 to BRM-SW	Gig1/0/3	Fa0/1	TRUNK

Bảng 4.4. 2 Bảng thông tin kết nối port

Source to destination	Source Interface	Destination Interface	Trunking/Vlan
HQ-MUL-SW-1 to OP-SW	Gig1/0/4	Fa0/1	TRUNK
HQ-MUL-SW-1 to CCA-SW	Gig1/0/5	Fa0/1	TRUNK
HQ-MUL-SW-1 to IT-SW	Gig1/0/6	Fa0/1	TRUNK
HQ-MUL-SW-1 to CWA1-SW	Gig1/0/7	Fa0/1	TRUNK
HQ-MUL-SW-2 to COSB-SW	Gig1/0/2	Fa0/2	TRUNK
HQ-MUL-SW-2 to BRM-SW	Gig1/0/3	Fa0/2	TRUNK
HQ-MUL-SW-2 to OP-SW	Gig1/0/4	Fa0/2	TRUNK
HQ-MUL-SW-2 to CCA-SW	Gig1/0/5	Fa0/2	TRUNK
HQ-MUL-SW-2 to IT-SW	Gig1/0/6	Fa0/2	TRUNK

Bảng 4.4. 3 Bảng thông tin kết nối port

Source to destination	Source Inter-face	Destination Interface	Trunking/Vlan
HQ-MUL-SW-2 to CWA1-SW	Gig1/0/7	Fa0/2	TRUNK
BR-MUL-SW-3 to MD-SW	Gig1/0/2	Fa0/1	TRUNK
BR-MUL-SW-3 to MK-SW	Gig1/0/3	Fa0/1	TRUNK
BR-MUL-SW-3 to HR-SW	Gig1/0/4	Fa0/1	TRUNK
BR-MUL-SW-3 to FIN-SW	Gig1/0/5	Fa0/1	TRUNK
BR-MUL-SW-3 to DC-SW	Gig1/0/6	Fa0/1	TRUNK
BR-MUL-SW-3 to CWA2-SW	Gig1/0/7	Fa0/1	TRUNK
BR-MUL-SW-4 to MD-SW	Gig1/0/2	Fa0/2	TRUNK
BR-MUL-SW-4 to MK-SW	Gig1/0/3	Fa0/2	TRUNK
BR-MUL-SW-4 to HR-SW	Gig1/0/4	Fa0/2	TRUNK

Bảng 4.4. 4 Bảng thông tin kết nối port

Source to destination	Source Inter-face	Destination Interface	Trunking/Vlan
BR-MUL-SW-4 to FIN-SW	Gig1/0/5	Fa0/2	TRUNK
BR-MUL-SW-4 to DC-SW	Gig1/0/6	Fa0/2	TRUNK
BR-MUL-SW-4 to CWA2-SW	Gig1/0/7	Fa0/2	TRUNK
WLAN-SW1 to HQ-MUL-SW-1	Fa0/1	Gig1/0/8	TRUNK
WLAN-SW1 to HQ-MUL-SW-2	Fa0/2	Gig1/0/8	TRUNK
WLAN-SW2 to BR-MUL-SW-3	Fa0/1	Gig1/0/8	TRUNK
WLAN-SW2 to BR-MUL-SW-4	Fa0/2	Gig1/0/8	TRUNK
WLAN-SW1 to Wireless LAN Controller1	Fa0/4	Gig1	

Bảng 4.4. 5 Bảng thông tin kết nối port

Source to destination	Source Inter-face	Destination Interface	Trunking/Vlan
WLAN-SW1 to Laptop0	Fa0/5	Fa0	
WLAN-SW2 to Wireless LAN Controller0	Fa0/3	Gig1	
WLAN-SW2 to Laptop7	Fa0/4	Fa0	
WLAN-SW1 to LWAP2	Fa0/10	Gig0	TRUNK
WLAN-SW1 to LWAP3	Fa0/11	Gig0	TRUNK
WLAN-SW1 to LWAP4	Fa0/12	Gig0	TRUNK
WLAN-SW1 to LWAP5	Fa0/13	Gig0	TRUNK
WLAN-SW1 to LWAP6	Fa0/14	Gig0	TRUNK
WLAN-SW1 to LWAP7	Fa0/15	Gig0	TRUNK
WLAN-SW2 to LWAP1	Fa0/5	Gig0	TRUNK

Bảng 4.4. 6 Bảng thông tin kết nối port

Source to destination	Source Inter-face	Destination Interface	Trunking/Vlan
WLAN-SW2 to LWAP8	Fa0/6	Gig0	TRUNK
WLAN-SW2 to LWAP9	Fa0/7	Gig0	TRUNK
WLAN-SW2 to LWAP10	Fa0/8	Gig0	TRUNK
WLAN-SW2 to LWAP11	Fa0/9	Gig0	TRUNK
WLAN-SW2 to LWAP12	Fa0/10	Gig0	TRUNK

Bảng 4.4. 7 Bảng thông tin kết nối port

4.5 Thông tin VLAN, Inter-VLAN, IP trong hệ thống mạng

Department	VLAN	Network Address	Subnet Mask	Host Address Range	Broadcast Address
HQ					
COSB	10	192.168.100.0	255.255.255.192/26	.1 to .62	192.168.100.63
BRM	20	192.168.100.64	255.255.255.192/26	.65 to .126	192.168.100.127
OP	30	192.168.100.128	255.255.255.192/26	.129 to .190	192.168.100.191
CCA	40	192.168.100.192	255.255.255.192/26	.193 to .254	192.168.100.255
IT	50	192.168.101.0	255.255.255.192/26	.1 to .62	192.168.101.63
CWA1	60	192.168.101.64	255.255.255.192/26	.65 to .126	192.168.101.127
BR					

MD	80	192.168.101.128	255.255.255.224/27	.129 to .158	192.168.101.159			
MK	90	192.168.101.160	255.255.255.224/27	.161 to .190	192.168.101.191			
HR	100	192.168.101.192	255.255.255.224/27	.193 to .222	192.168.101.223			
FIN	110	192.168.101.224	255.255.255.224/27	.225 to .254	192.168.101.255			
DC	120	192.168.102.0	255.255.255.128/25	.1 to .126	192.168.102.127			
CWA2	130	192.168.102.128	255.255.255.224/27	.129 to .158	192.168.102.159			
Server								
SSS	70	192.168.102.160	255.255.255.240/28	.161 to .176	192.168.102.175			
			Wireless LAN					
Wlan1	140	192.168.110.0	255.255.254.0/23					
Wlan2	150	192.168.120.0	255.255.254.0/23					
Between the Routers and Layer-3 Switches								
HQ-R <> HQ-MLSW1			192.168.102.176/30					
HQ-R <> HQ-MLSW2			192.168.102.180/30					
BR-R <> BR-MLSW1			192.168.102.184/30					
BR-R <> BR-MLSW2			192.168.102.188/30					
HQ-R <> BR-R			192.168.102.192/30					
Between the Routers and ISPs								
Public IP : 195.136.17.16/30, 195.136.17.20/30, 195.136.17.24/30, 195.136.17.28/30								

Bảng 4.5. 1 Bảng thông tin VLAN, Inter-VLAN, IP trong hệ thống mạng

4.6 Thông tin chi tiết quy hoạch địa chỉ IP trong hệ thống mạng

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
ISP1	Se0/2/0		195.136.17.18	/30	

	Se0/2/1		195.136.17.25	/30	
--	---------	--	---------------	-----	--

Bảng 4.6. 1 Bảng thông tin chi tiết quy hoạch địa chỉ IP

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
ISP2	Se0/3/0		195.136.17.22	/30	
	Se0/3/1		195.136.17.29	/30	
HQ-ROUTER	Gig0/0		192.168.102.178	/30	
	Gig0/1		192.168.102.182	/30	
	Gig0/2.70		192.168.102.161	/28	
	Se0/1/0		195.136.17.17	/30	
	Se0/2/0		192.168.102.193	/30	
	Se0/2/1		195.136.17.21	/30	
BR-ROUTER	Gig0/0		192.168.102.190	/30	
	Gig0/1		192.168.102.186	/30	

	Se0/1/0		192.168.102.194	/30	
--	---------	--	-----------------	-----	--

Bảng 4.6. 2 Bảng thông tin chi tiết quy hoạch địa chỉ IP

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
BR-ROUTER	Se0/1/1		195.136.17.26	/30	
	Se0/2/0		195.136.17.30	/30	
HQ-MUL-SW-1	Gig1/0/1		192.168.102.177	/30	
	Gig1/0/2	10	192.168.100.1	/26	
	Gig1/0/3	20	192.168.100.65	/26	
	Gig1/0/4	30	192.168.100.129	/26	
	Gig1/0/5	40	192.168.100/193	/26	
	Gig1/0/6	50	192.168.101.1	/26	
	Gig1/0/7	60	192.168.101.65	/26	
	Gig1/0/8	140	192.168.110.1	/23	

Bảng 4.6. 3 Bảng thông tin chi tiết quy hoạch địa chỉ IP

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
HQ-MUL-SW-2	Gig1/0/1		192.168.102.181	/30	
	Gig1/0/2	10	192.168.100.1	/26	
	Gig1/0/3	20	192.168.100.65	/26	
	Gig1/0/4	30	192.168.100.129	/26	
	Gig1/0/5	40	192.168.100.193	/26	
	Gig1/0/6	50	192.168.101.1	/26	
	Gig1/0/7	60	192.168.101.65	/26	
	Gig1/0/8	140	192.168.110.1	/23	
Server-SW	Fa0/2	70	192.168.102.162	/28	192.168.102.161
	Fa0/3	70	192.168.102.163	/28	192.168.102.161

Bảng 4.6. 4 Bảng thông tin chi tiết quy hoạch địa chỉ IP

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
Server-SW	Fa0/4	70	192.168.102.164	/28	192.168.102.161
	Fa0/5	70	192.168.102.165	/28	192.168.102.161
COSB-SW	Fa0/3	10	DHCP	/26	192.168.100.1
	Fa0/4	10	DHCP	/26	192.168.100.1
	Fa0/5	10	DHCP	/26	192.168.100.1
	Fa0/6	10	DHCP	/26	192.168.100.1
BRM-SW	Fa0/3	20	DHCP	/26	192.168.100.65
	Fa0/4	20	DHCP	/26	192.168.100.65
	Fa0/5	20	DHCP	/26	192.168.100.65
	Fa0/6	20	DHCP	/26	192.168.100.65

Bảng 4.6. 5 Bảng thông tin chi tiết quy hoạch địa chỉ IP

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
OP-SW	Fa0/3	30	DHCP	/26	192.168.100.129
	Fa0/4	30	DHCP	/26	192.168.100.129
	Fa0/5	30	DHCP	/26	192.168.100.129
	Fa0/6	30	DHCP	/26	192.168.100.129
CCA-SW	Fa0/3	40	DHCP	/26	192.168.100.193
	Fa0/4	40	DHCP	/26	192.168.100.193
	Fa0/5	40	DHCP	/26	192.168.100.193
	Fa0/6	40	DHCP	/26	192.168.100.193
IT-SW	Fa0/3	50	DHCP	/26	192.168.101.1
	Fa0/4	50	DHCP	/26	192.168.101.1

Bảng 4.6. 6 Bảng thông tin chi tiết quy hoạch địa chỉ IP

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
IT-SW	Fa0/5	50	DHCP	/26	192.168.101.1
	Fa0/6	50	DHCP	/26	192.168.101.1
CWA1-SW	Fa0/3	60	DHCP	/26	192.168.101.65
	Fa0/4	60	DHCP	/26	192.168.101.65
	Fa0/5	60	DHCP	/26	192.168.101.65
	Fa0/6	60	DHCP	/26	192.168.101.65
MD-SW	Fa0/3	80	DHCP	/27	192.168.101.129
	Fa0/4	80	DHCP	/27	192.168.101.129
	Fa0/5	80	DHCP	/27	192.168.101.129
	Fa0/6	80	DHCP	/27	192.168.101.129

Bảng 4.6. 7 Bảng thông tin chi tiết quy hoạch địa chỉ IP

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
MK-SW	Fa0/3	90	DHCP	/27	192.168.101.161
	Fa0/4	90	DHCP	/27	192.168.101.161
	Fa0/5	90	DHCP	/27	192.168.101.161
	Fa0/6	90	DHCP	/27	192.168.101.161
HR-SW	Fa0/3	100	DHCP	/27	192.168.101.193
	Fa0/4	100	DHCP	/27	192.168.101.193
	Fa0/5	100	DHCP	/27	192.168.101.193
	Fa0/6	100	DHCP	/27	192.168.101.193
FIN-SW	Fa0/3	110	DHCP	/27	192.168.101.225
	Fa0/4	110	DHCP	/27	192.168.101.225

Bảng 4.6. 8 Bảng thông tin chi tiết quy hoạch địa chỉ IP

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
FIN-SW	Fa0/5	110	DHCP	/27	192.168.101.225
	Fa0/6	110	DHCP	/27	192.168.101.225
DC-SW	Fa0/3	120	DHCP	/25	192.168.102.1
	Fa0/4	120	DHCP	/25	192.168.102.1
	Fa0/5	120	DHCP	/25	192.168.102.1
	Fa0/6	120	DHCP	/25	192.168.102.1
CWA2-SW	Fa0/3	130	DHCP	/27	192.168.102.129
	Fa0/4	130	DHCP	/27	192.168.102.129
	Fa0/5	130	DHCP	/27	192.168.102.129
	Fa0/6	130	DHCP	/27	192.168.102.129

Bảng 4.6. 9 Bảng thông tin chi tiết quy hoạch địa chỉ IP

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
WLAN-SW1	Fa0/4	140	192.168.110.5	/23	192.168.110.1
	Fa0/5	140	DHCP	/23	192.168.110.1
	Fa0/10	140	DHCP	/23	192.168.110.1
	Fa0/11	140	DHCP	/23	192.168.110.1
	Fa0/12	140	DHCP	/23	192.168.110.1
	Fa0/13	140	DHCP	/23	192.168.110.1
	Fa0/14	140	DHCP	/23	192.168.110.1
	Fa0/15	140	DHCP	/23	192.168.110.1
WLAN-SW1	Fa0/3	150	192.168.120.5	/23	192.168.120.1
	Fa0/4	150	DHCP	/23	192.168.120.1

Bảng 4.6. 10 Bảng thông tin chi tiết quy hoạch địa chỉ IP

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
WLAN-SW2	Fa0/5	150	DHCP	/23	192.168.120.1
	Fa0/6	150	DHCP	/23	192.168.120.1
	Fa0/7	150	DHCP	/23	192.168.120.1
	Fa0/8	150	DHCP	/23	192.168.120.1
	Fa0/9	150	DHCP	/23	192.168.120.1
	Fa0/10	150	DHCP	/23	192.168.120.1
Laptop		10	DHCP	/26	192.168.100.1
		20	DHCP	/26	192.168.100.65
		30	DHCP	/26	192.168.100.129
		40	DHCP	/26	192.168.100.193

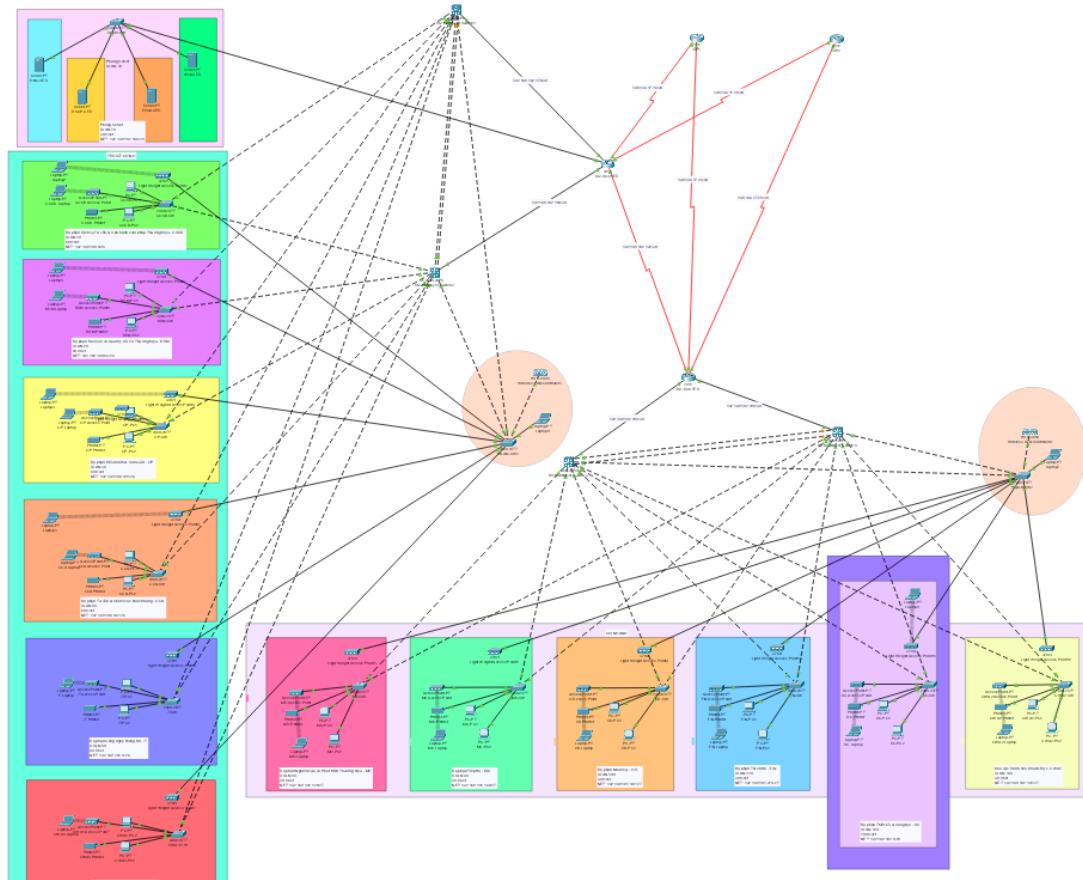
Bảng 4.6. 11 Bảng thông tin chi tiết quy hoạch địa chỉ IP

Server	Interface	Vlan	IP Address	Subnet Mask	Gate Way
Laptop		50	DHCP	/26	192.168.101.1
		60	DHCP	/26	192.168.101.65
		80	DHCP	/27	192.168.101.129
		90	DHCP	/27	192.168.101.161
		100	DHCP	/27	192.168.101.192
		110	DHCP	/27	192.168.101.225
		120	DHCP	/25	192.168.102.1
		130	DHCP	/27	192.168.102.129

Bảng 4.6. 12 Bảng thông tin chi tiết quy hoạch địa chỉ IP

PHẦN 5 THỰC NGHIỆM

5.1 Sơ đồ hệ thống mạng trên Cisco Packet Tracer



Hình 5.1. 1 Sơ đồ hệ thống mạng trong Cisco Packet Tracer

5.2 Cấu hình bảo mật cơ bản trên thiết bị

13 Switches

enable

conf t

hostname

enable password cisco

banner motd #Unauthorized system access warning !!!#

no ip domain lookup

```
line console 0  
password cisco  
login  
exit  
service password-encryption
```

4 Multilayer Switches, HQ-ROUTER and BR-ROUTER

```
enable  
conf t  
hostname .....  
enable password cisco  
banner motd #Unauthorized system access warning !!!#  
no ip domain lookup
```

```
line console 0  
password cisco  
login  
exit  
service password-encryption  
ip domain name cisco.net  
username duongthanhquy password cisco
```

```
crypto key generate rsa
```

```
1024
```

```
line vty 0 15
```

```
login local
```

```
transport input ssh
```

```
exit
```

```
do wr
```

5.3 Cấu hình VLANs và Trunking trên các thiết bị

5.3.1 Tạo các VLANs

13 Switches

```
vlan 130
```

```
name CWA2
```

```
exit
```

```
int range fa0/1-2
```

```
switchport mode trunk
```

```
exit
```

```
int range fa0/3-24
```

```
switchport mode access
```

```
switchport access vlan 130
```

exit

2 HQ Multilayer Switches

vlan 10

vlan 20

vlan 30

vlan 40

vlan 50

vlan 60

int range gigabitEthernet 1/0/2-7

switchport mode trunk

exit

2 BR Multilayer Switches

vlan 80

vlan 90

vlan 100

vlan 110

vlan 120

vlan 130

int range gigabitEthernet 1/0/2-7

switchport mode trunk

exit

5.3.2 Cấu hình Port-Security cho Server

Server Switch

interface range fastEthernet 0/3-24

switchport port-security maximum 1

switchport port-security mac-address sticky

switchport port-security violation shutdown

exit

do wr

5.3.3 Cấu hình Inter-VLANs

HQ-ROUTER

HQ-ROUTER(config)#interface gigabitEthernet 0/2

HQ-ROUTER(config-if)#no ip ad

HQ-ROUTER(config-if)#no ip address

HQ-ROUTER(config-if)#exit

HQ-ROUTER(config)#interface gigabitEthernet 0/2.70

HQ-ROUTER(config-subif)#encapsulation dot1Q 70

HQ-ROUTER(config-subif)#ip address 192.168.102.161 255.255.255.240

HQ-ROUTER(config-subif)#no shutdown

HQ-ROUTER(config-subif)#exit

HQ-ROUTER(config)#do wr

HQ-M-SW1

HQ-Mul-SW-1(config)#interface vlan 10

HQ-Mul-SW-1(config-if)#ip address 192.168.100.1 255.255.255.192

HQ-Mul-SW-1(config-if)#ip helper-address 192.168.102.163

HQ-Mul-SW-1(config-if)#exit

HQ-Mul-SW-1(config)#interface vlan 20

HQ-Mul-SW-1(config-if)#ip address 192.168.100.65 255.255.255.192

HQ-Mul-SW-1(config-if)#ip helper-address 192.168.102.163

HQ-Mul-SW-1(config-if)#exit

HQ-Mul-SW-1(config)#interface vlan 30

HQ-Mul-SW-1(config-if)#ip address 192.168.100.129 255.255.255.192

HQ-Mul-SW-1(config-if)#ip helper-address 192.168.102.163

HQ-Mul-SW-1(config-if)#exit

HQ-Mul-SW-1(config)#interface vlan 40

HQ-Mul-SW-1(config-if)#ip address 192.168.100.193 255.255.255.192

HQ-Mul-SW-1(config-if)#ip helper-address 192.168.102.163

HQ-Mul-SW-1(config-if)#exit

HQ-Mul-SW-1(config)#interface vlan 50

HQ-Mul-SW-1(config-if)#ip address 192.168.101.1 255.255.255.192

HQ-Mul-SW-1(config-if)#ip helper-address 192.168.102.163

HQ-Mul-SW-1(config-if)#exit

HQ-Mul-SW-1(config)#interface vlan 60

HQ-Mul-SW-1(config-if)#ip address 192.168.101.65 255.255.255.192

HQ-Mul-SW-1(config-if)#ip helper-address 192.168.102.163

HQ-Mul-SW-1(config-if)#exit

HQ-Mul-SW-1(config)#do wr

HQ-M-SW2

HQ-Mul-SW-2(config)#interface vlan 10

HQ-Mul-SW-2(config-if)#ip address 192.168.100.1 255.255.255.192

HQ-Mul-SW-2(config-if)#ip helper-address 192.168.102.163

HQ-Mul-SW-2(config-if)#exit

HQ-Mul-SW-2(config)#interface vlan 20

HQ-Mul-SW-2(config-if)#ip address 192.168.100.65 255.255.255.192

HQ-Mul-SW-2(config-if)#ip helper-address 192.168.102.163

HQ-Mul-SW-2(config-if)#exit

```
HQ-Mul-SW-2(config)#interface vlan 30
HQ-Mul-SW-2(config-if)#ip address 192.168.100.129 255.255.255.192
HQ-Mul-SW-2(config-if)#ip helper-address 192.168.102.163
HQ-Mul-SW-2(config-if)#exit
HQ-Mul-SW-2(config)#interface vlan 40
HQ-Mul-SW-2(config-if)#ip address 192.168.100.193 255.255.255.192
HQ-Mul-SW-2(config-if)#ip helper-address 192.168.102.163
HQ-Mul-SW-2(config-if)#exit
HQ-Mul-SW-2(config)#interface vlan 50
HQ-Mul-SW-2(config-if)#ip address 192.168.101.1 255.255.255.192
HQ-Mul-SW-2(config-if)#ip helper-address 192.168.102.163
HQ-Mul-SW-2(config-if)#exit
HQ-Mul-SW-2(config)#interface vlan 60
HQ-Mul-SW-2(config-if)#ip address 192.168.101.65 255.255.255.192
HQ-Mul-SW-2(config-if)#ip helper-address 192.168.102.163
HQ-Mul-SW-2(config-if)#exit
HQ-Mul-SW-2(config)#do wr
```

BR-M-SW1

```
BR-Mul-SW-3(config)#interface vlan 80
```

```
BR-Mul-SW-3(config-if)#ip address 192.168.101.129 255.255.255.224
BR-Mul-SW-3(config-if)#ip helper-address 192.168.102.163
BR-Mul-SW-3(config-if)#exit
BR-Mul-SW-3(config)#interface vlan 90
BR-Mul-SW-3(config-if)#ip address 192.168.101.161 255.255.255.224
BR-Mul-SW-3(config-if)#ip helper-address 192.168.102.163
BR-Mul-SW-3(config-if)#exit
BR-Mul-SW-3(config)#interface vlan 100
BR-Mul-SW-3(config-if)#ip address 192.168.101.193 255.255.255.224
BR-Mul-SW-3(config-if)#ip helper-address 192.168.102.163
BR-Mul-SW-3(config-if)#exit
BR-Mul-SW-3(config)#interface vlan 110
BR-Mul-SW-3(config-if)#ip address 192.168.101.225 255.255.255.224
BR-Mul-SW-3(config-if)#ip helper-address 192.168.102.163
BR-Mul-SW-3(config-if)#exit
BR-Mul-SW-3(config)#interface vlan 120
BR-Mul-SW-3(config-if)#ip address 192.168.102.1 255.255.255.128
BR-Mul-SW-3(config-if)#ip helper-address 192.168.102.163
BR-Mul-SW-3(config-if)#exit
```

BR-Mul-SW-3(config)#interface vlan 130

BR-Mul-SW-3(config-if)#ip address 192.168.102.129 255.255.255.224

BR-Mul-SW-3(config-if)#ip helper-address 192.168.102.163

BR-Mul-SW-3(config-if)#exit

BR-Mul-SW-3(config)#do wr

BR-M-SW2

BR-Mul-SW-4(config)#interface vlan 80

BR-Mul-SW-4(config-if)#ip address 192.168.101.129 255.255.255.224

BR-Mul-SW-4(config-if)#ip helper-address 192.168.102.163

BR-Mul-SW-4(config-if)#exit

BR-Mul-SW-4(config)#interface vlan 90

BR-Mul-SW-4(config-if)#ip address 192.168.101.161 255.255.255.224

BR-Mul-SW-4(config-if)#ip helper-address 192.168.102.163

BR-Mul-SW-4(config-if)#exit

BR-Mul-SW-4(config)#interface vlan 100

BR-Mul-SW-4(config-if)#ip address 192.168.101.193 255.255.255.224

BR-Mul-SW-4(config-if)#ip helper-address 192.168.102.163

BR-Mul-SW-4(config-if)#exit

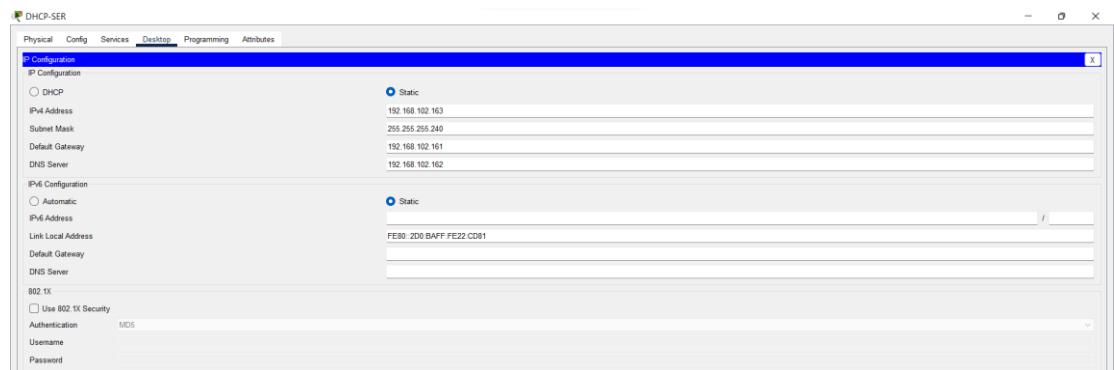
BR-Mul-SW-4(config)#interface vlan 110

```
BR-Mul-SW-4(config-if)#ip address 192.168.101.225 255.255.255.224  
BR-Mul-SW-4(config-if)#ip helper-address 192.168.102.163  
BR-Mul-SW-4(config-if)#exit  
BR-Mul-SW-4(config)#interface vlan 120  
BR-Mul-SW-4(config-if)#ip address 192.168.102.1 255.255.255.128  
BR-Mul-SW-4(config-if)#ip helper-address 192.168.102.163  
BR-Mul-SW-4(config-if)#exit  
BR-Mul-SW-4(config)#interface vlan 130  
BR-Mul-SW-4(config-if)#ip address 192.168.102.129 255.255.255.224  
BR-Mul-SW-4(config-if)#ip helper-address 192.168.102.163  
BR-Mul-SW-4(config-if)#exit  
BR-Mul-SW-4(config)#do wr
```

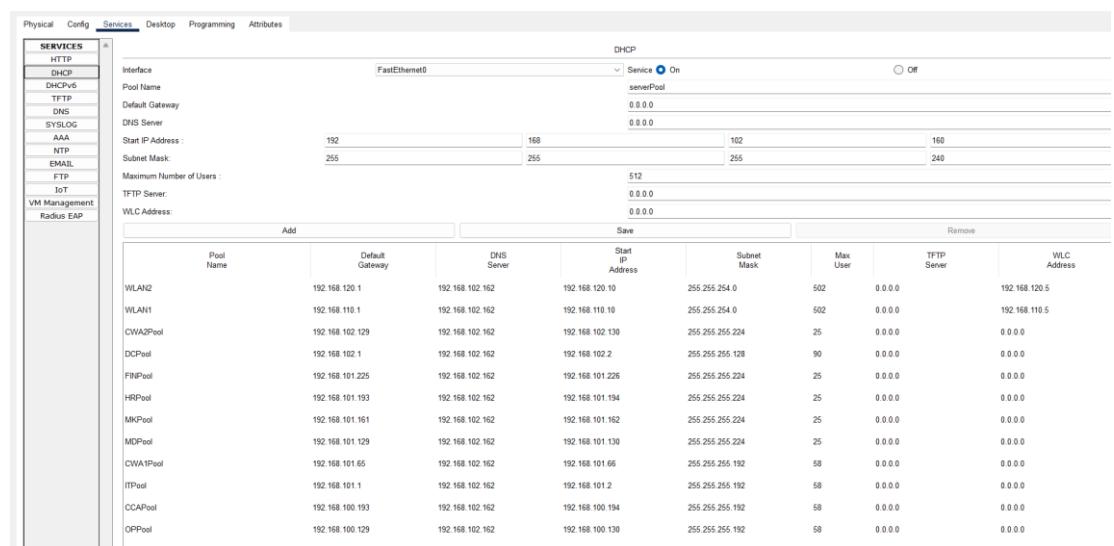
5.4 Cấu hình dịch vụ tại Server

5.4.1 Tạo DHCP Server

Tạo các Pool DHCP



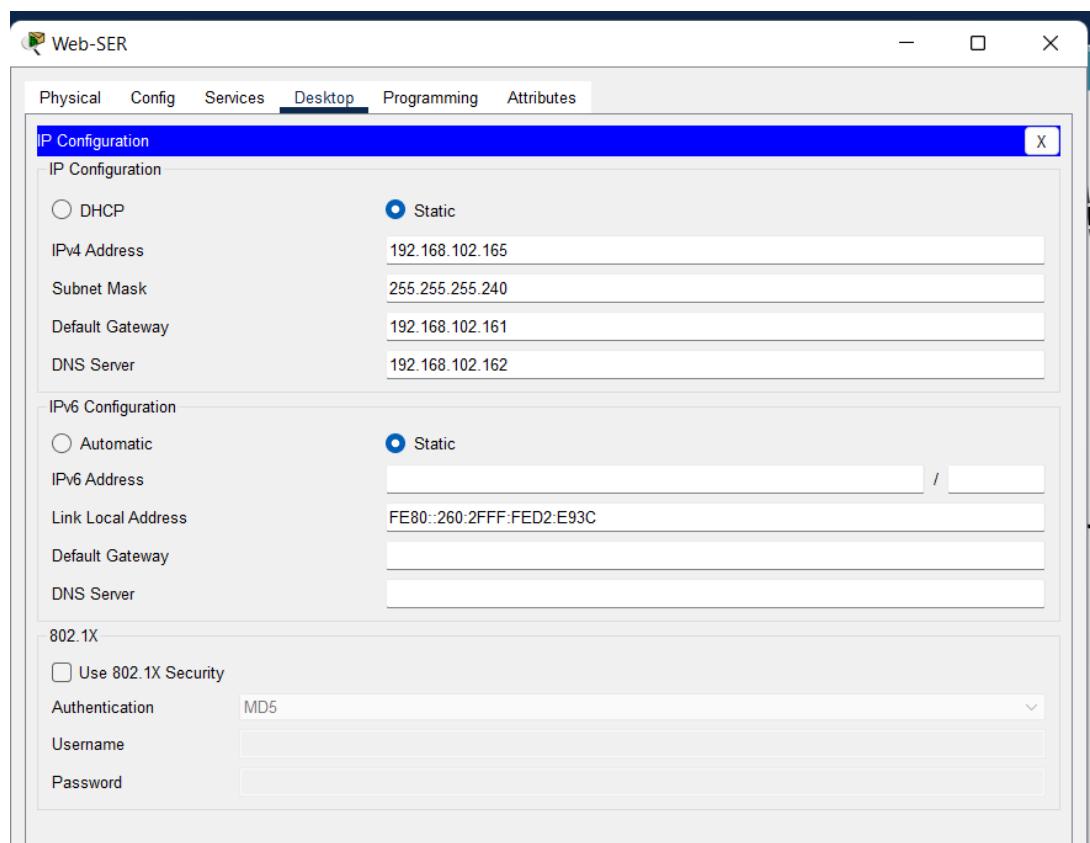
Hình 5.4.1. 1 Tạo các Pool DHCP



Hình 5.4.1. 2 Cập nhật danh sách các Pool DHCP

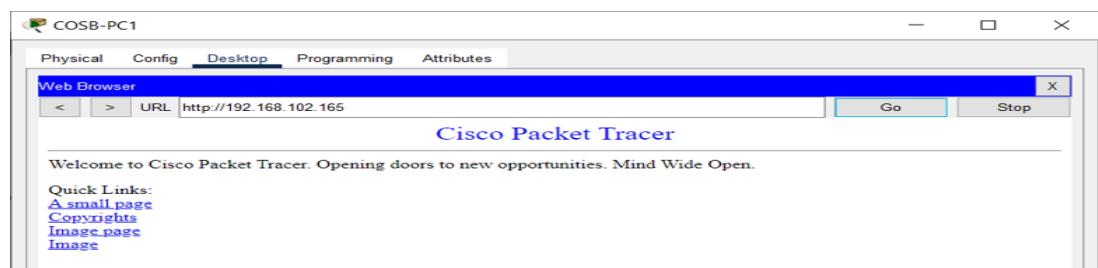
BRMPool	192.168.100.65	192.168.102.162	192.168.100.66	255.255.255.192	58	0.0.0.0	0.0.0.0
COSBPool	192.168.100.1	192.168.102.162	192.168.100.2	255.255.255.192	58	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.102.160	255.255.255.240	512	0.0.0.0	0.0.0.0

5.4.2 Tạo WEB Server



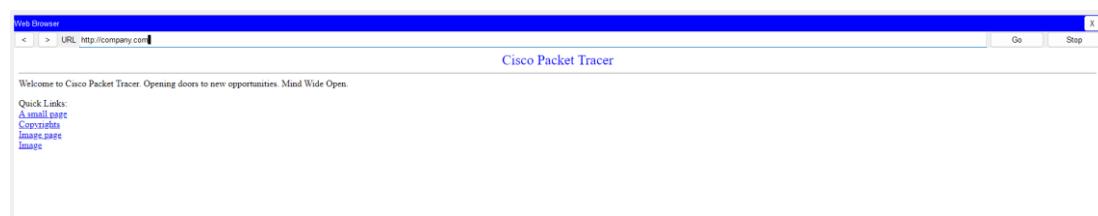
Hình 5.4.2. 1 Đặt IP tĩnh cho Web Server

Truy cập dịch vụ web bằng địa chỉ IP



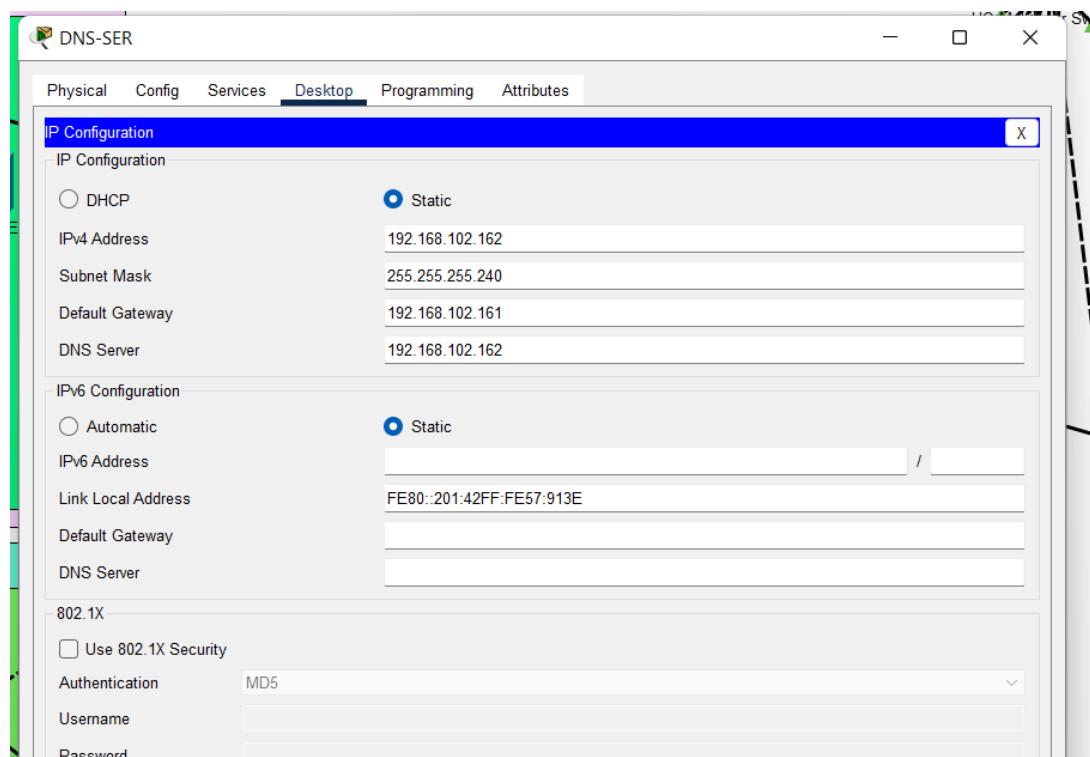
Hình 5.4.2. 2 Truy cập dịch vụ bằng IP

Truy cập dịch vụ web bằng tên miền

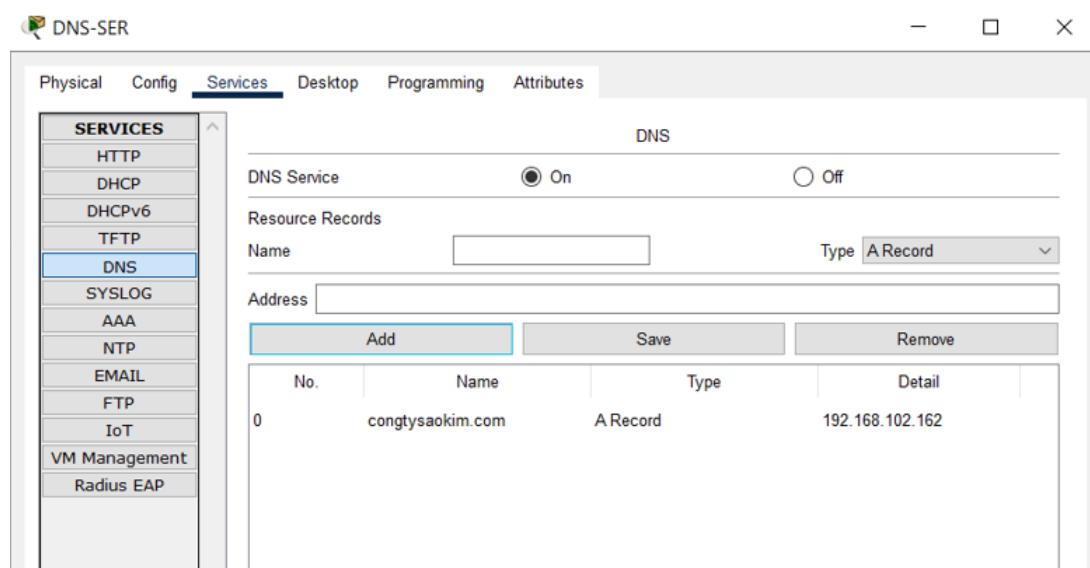


Hình 5.4.2. 3 Truy cập dịch vụ bằng tên miền

5.4.3 Tao DNS Server

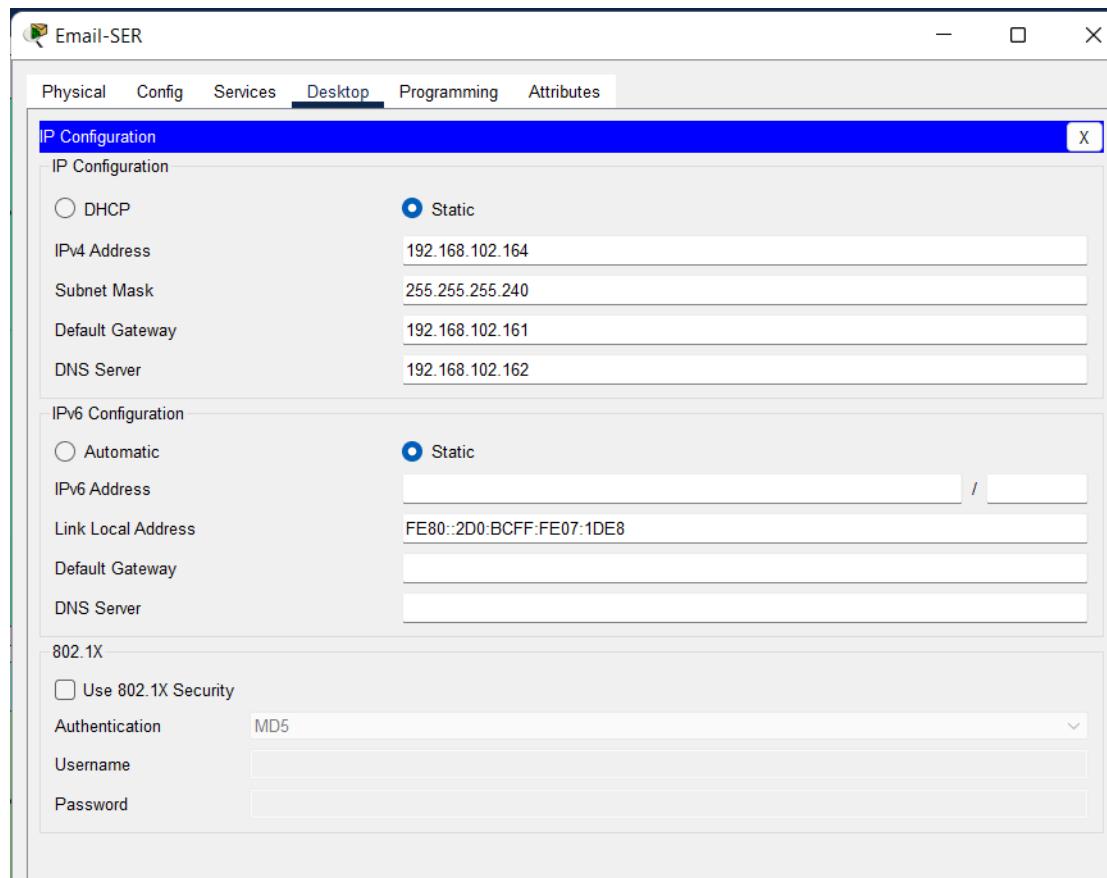


Hình 5.4.3. 1 Đặt IP tĩnh cho DNS Server



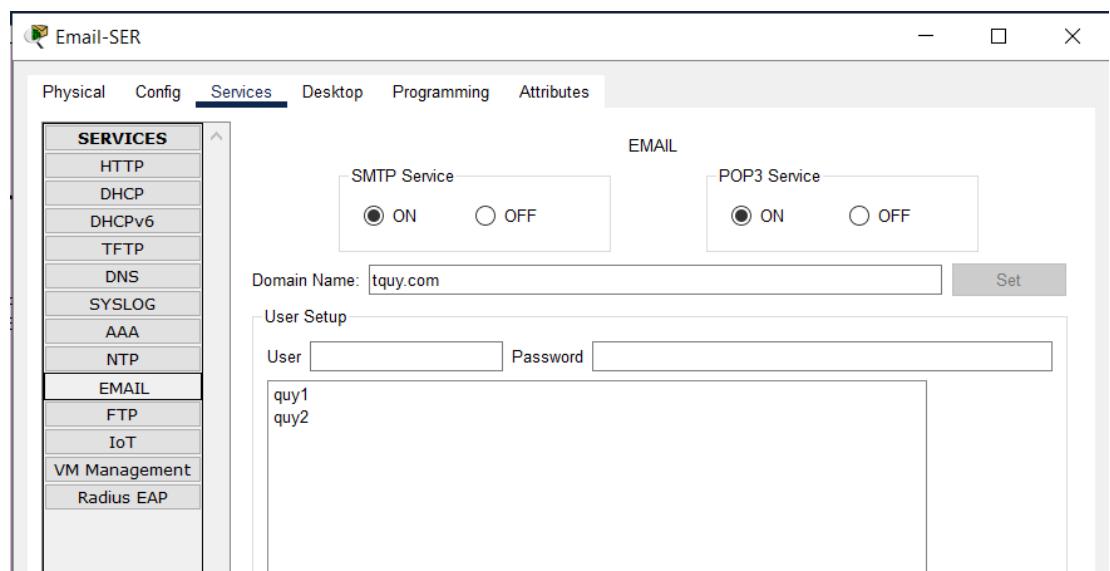
Hình 5.4.3. 2 Đăng ký dịch vụ DNS

5.4.4 Tao Email Server



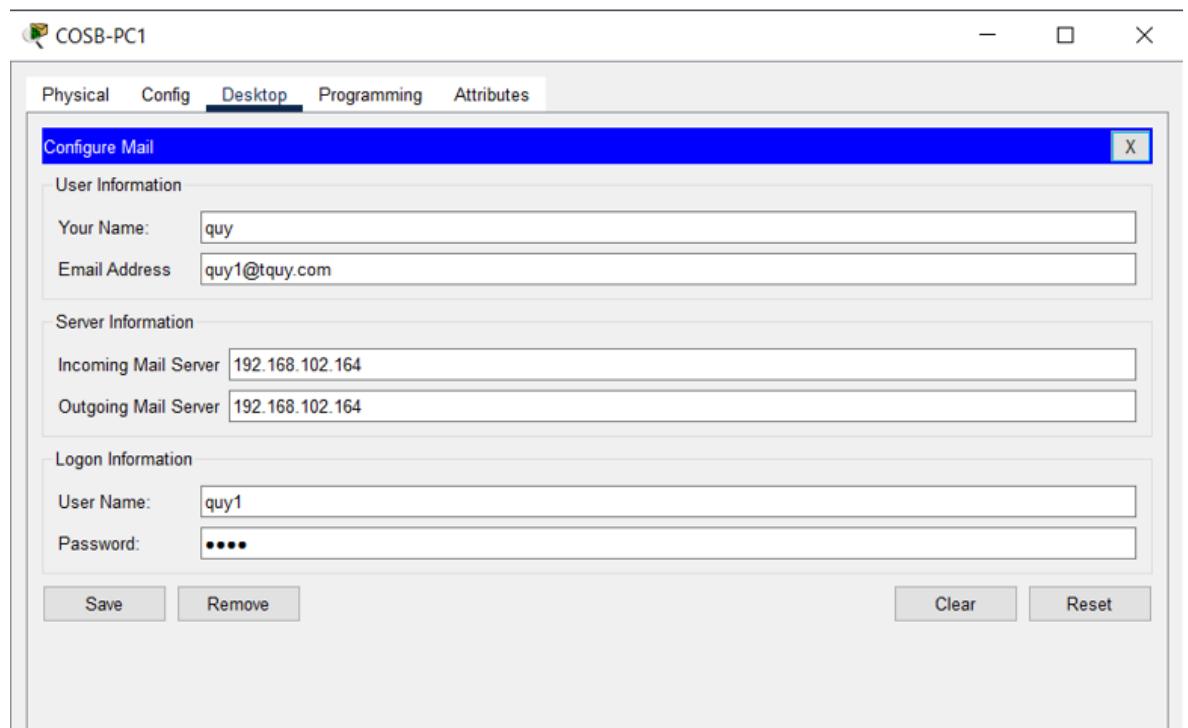
Hình 5.4.4. 1 Đặt IP tĩnh cho Email Server

Trên Email Server tạo quy1/quy1 quy2/quy2

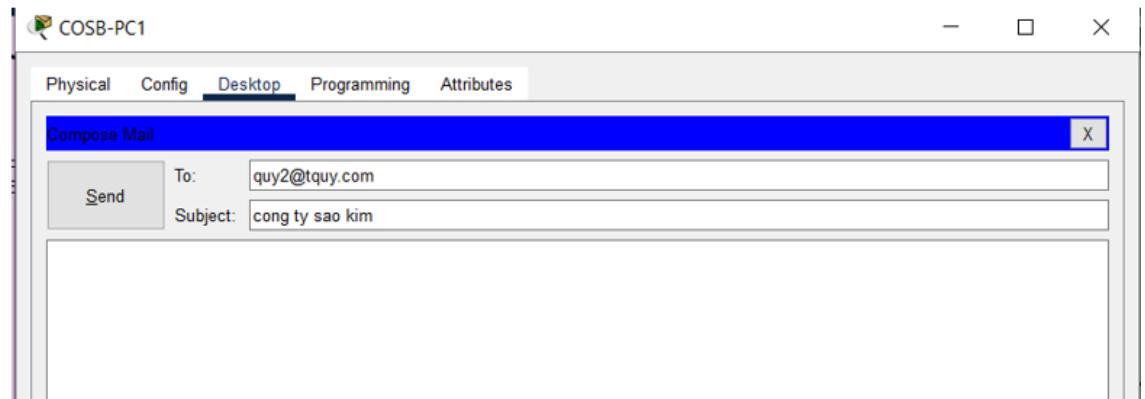


Hình 5.4.4. 2 Tạo các tài khoản trên Email Server

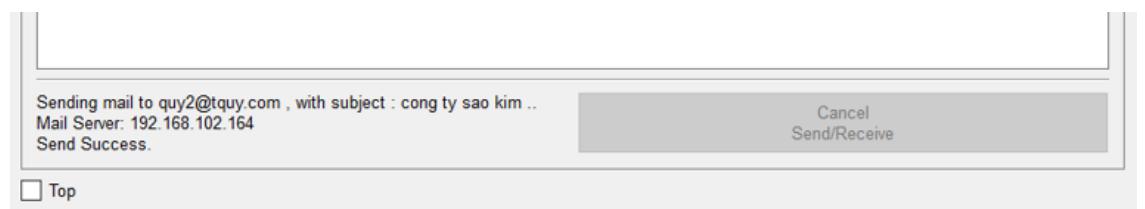
Tiến hành sử dụng dịch vụ Email trên các thiết bị



Hình 5.4.4. 3 Đăng ký tài khoản tại PC, Laptop

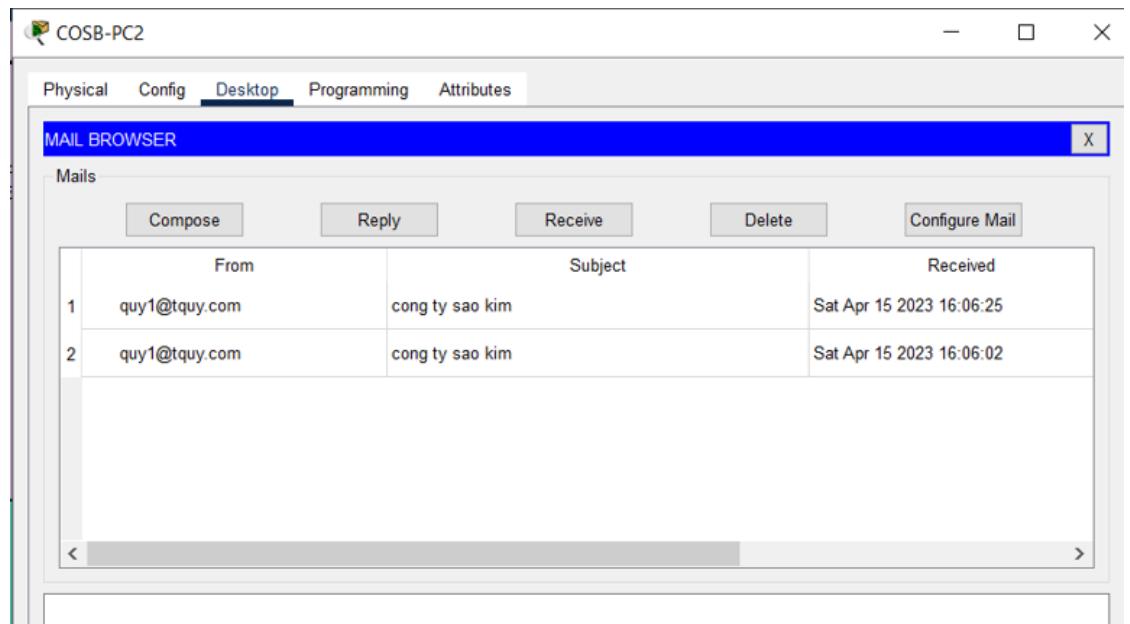


Hình 5.4.4. 4 Gửi Email đến một tài khoản khác



Hình 5.4.4. 5 Thông báo gửi Email thành công

User2 reply User1



Hình 5.4.4. 6 Phản hồi lại thành công

5.4.5 Dịch vụ FTP

Trên Server tạo user1 và user2

```
C:\>ftp 192.168.102.164
Trying to connect...192.168.102.164
Connected to 192.168.102.164
220- Welcome to PT Ftp server
Username:user1
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Hình 5.4.5. 1 Tạo các user trên Server

Tạo 1 file có tên Test.txt trên thiết bị COSB-PC2 và đẩy lên server

```
C:\>ftp 192.168.102.164
Trying to connect...192.168.102.164
Connected to 192.168.102.164
220- Welcome to PT Ftp server
Username:user1
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put test.txt

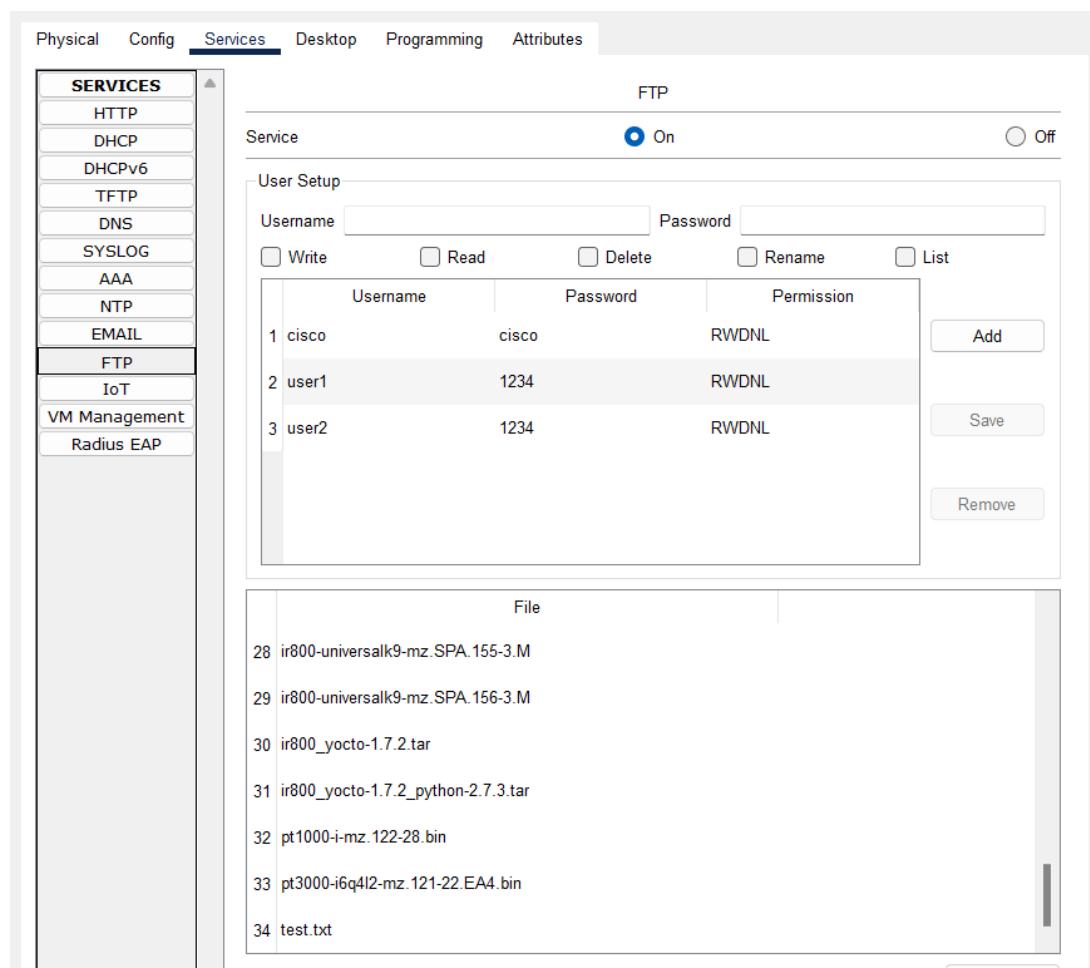
Writing file test.txt to 192.168.102.164:
File transfer in progress...

[Transfer complete - 6 bytes]

6 bytes copied in 0.051 secs (117 bytes/sec)
ftp>
```

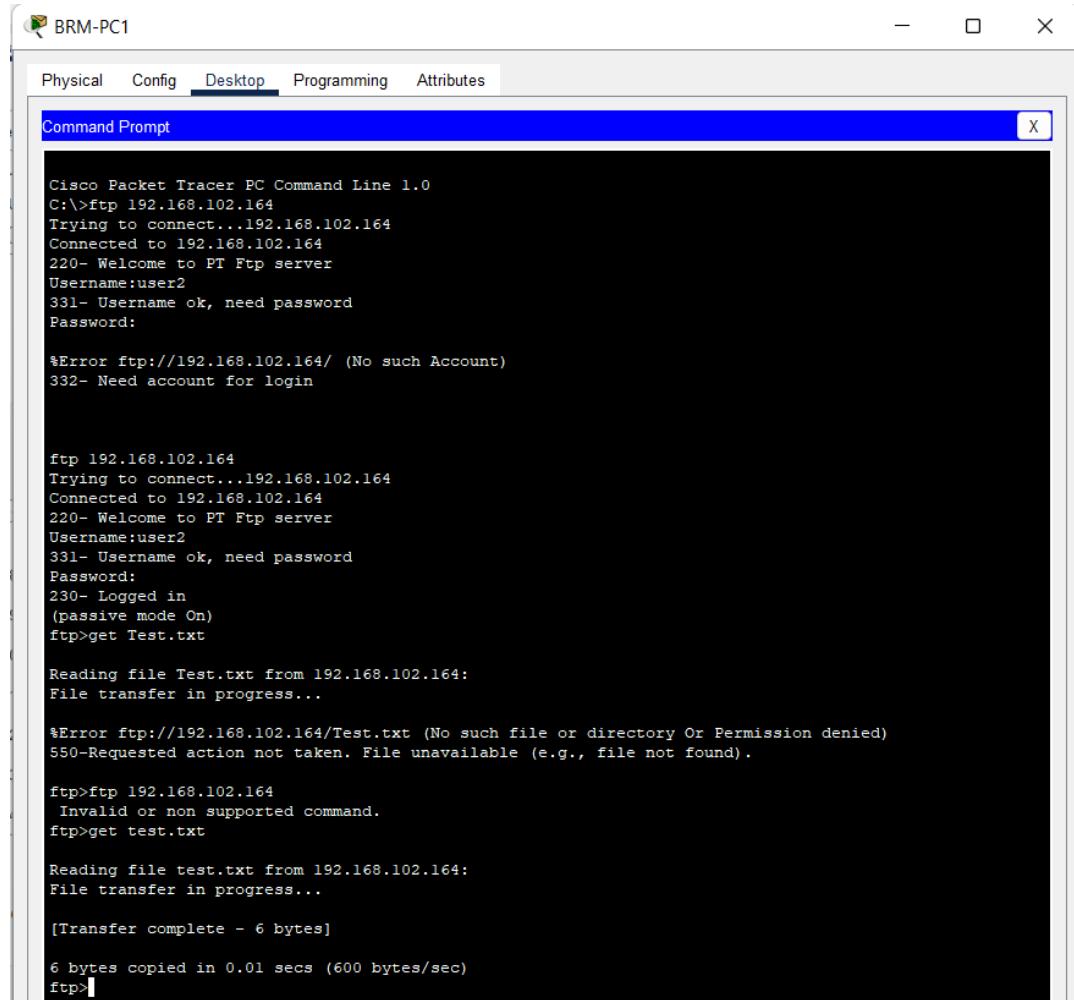
Hình 5.4.5. 2 Tạo file .txt và đẩy lên Server

Trên Server ta sẽ thấy file Test đã được đưa lên



Hình 5.4.5. 3 Cập nhật file thành công trên Server

Tiến hành lấy file đó về trên các thiết bị khác



The screenshot shows a Cisco Packet Tracer window titled "BRM-PC1". The "Desktop" tab is selected in the menu bar. A "Command Prompt" window is open, displaying the following text:

```

Cisco Packet Tracer PC Command Line 1.0
C:>ftp 192.168.102.164
Trying to connect...192.168.102.164
Connected to 192.168.102.164
220- Welcome to PT Ftp server
Username:user2
331- Username ok, need password
Password:

*Error ftp://192.168.102.164/ (No such Account)
332- Need account for login


ftp 192.168.102.164
Trying to connect...192.168.102.164
Connected to 192.168.102.164
220- Welcome to PT Ftp server
Username:user2
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get Test.txt

Reading file Test.txt from 192.168.102.164:
File transfer in progress...

*Error ftp://192.168.102.164/Test.txt (No such file or directory Or Permission denied)
550-Requested action not taken. File unavailable (e.g., file not found).

ftp>ftp 192.168.102.164
  Invalid or non supported command.
ftp>get test.txt

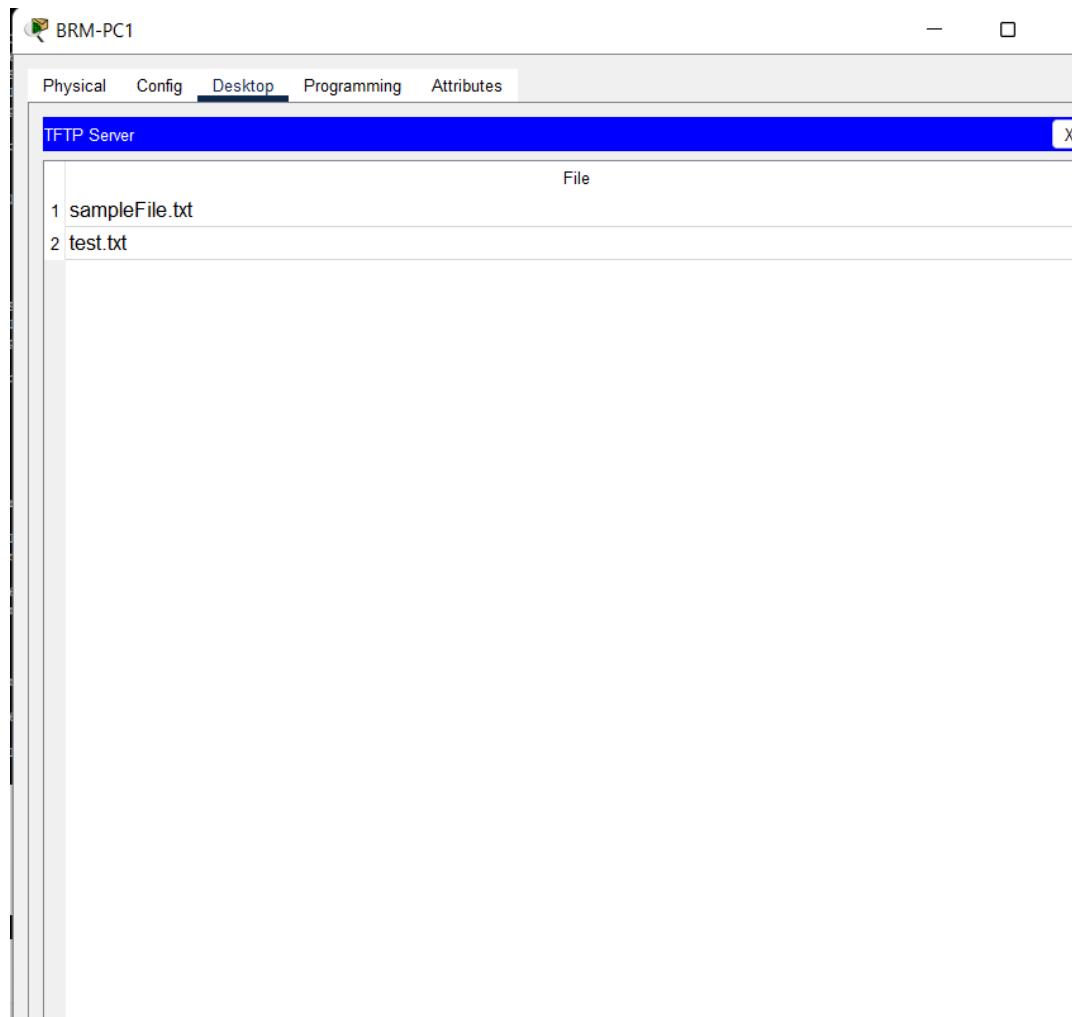
Reading file test.txt from 192.168.102.164:
File transfer in progress...

[Transfer complete - 6 bytes]
6 bytes copied in 0.01 secs (600 bytes/sec)
ftp>

```

Hình 5.4.5. 4 Truyền file đến các thiết bị khác

File đã có trên thiết bị



Hình 5.4.5. 5 Truyền file thành công

5.5 Subnetting và gán địa chỉ IP

HQ-MLSW1

```
HQ-Mul-SW-1(config-if)#interface gigabitEthernet 1/0/1
```

```
HQ-Mul-SW-1(config-if)#no switchport
```

```
HQ-Mul-SW-1(config-if)#ip address 192.168.102.177 255.255.255.252
```

```
HQ-Mul-SW-1(config-if)#no shutdown
```

```
HQ-Mul-SW-1(config-if)#exit
```

```
HQ-Mul-SW-1(config)#do wr//
```

HQ-MLSW2

```
HQ-Mul-SW-2(config)#interface gigabitEthernet 1/0/1
```

```
HQ-Mul-SW-2(config-if)#no switchport
```

```
HQ-Mul-SW-2(config-if)#ip address 192.168.102.181 255.255.255.252
```

```
HQ-Mul-SW-2(config-if)#no shutdown
```

```
HQ-Mul-SW-2(config-if)#exit
```

```
HQ-Mul-SW-2(config)#do wr
```

BR-MLSW1

```
BR-Mul-SW-3(config)#interface gigabitEthernet 1/0/1
```

```
BR-Mul-SW-3(config-if)#no switchport
```

```
BR-Mul-SW-3(config-if)#ip address 192.168.102.185 255.255.255.252
```

```
BR-Mul-SW-3(config-if)#no shutdown
```

```
BR-Mul-SW-3(config-if)#exit
```

```
BR-Mul-SW-3(config)#do wr//
```

```
BR-MLSW2//
```

```
BR-Mul-SW-4(config)#interface gigabitEthernet 1/0/1
```

```
BR-Mul-SW-4(config-if)#no switchport
```

```
BR-Mul-SW-4(config-if)#ip address 192.168.102.189 255.255.255.252
```

BR-Mul-SW-4(config-if)#no shutdown

BR-Mul-SW-4(config)#do wr//

5 Port HQ-ROUTER

HQ-ROUTER(config)#interface gigabitEthernet 0/0

HQ-ROUTER(config-if)#ip address 192.168.102.178 255.255.255.252

HQ-ROUTER(config-if)#no shutdown

HQ-ROUTER(config-if)#exit

HQ-ROUTER(config)#interface gigabitEthernet 0/1

HQ-ROUTER(config-if)#ip address 192.168.102.182 255.255.255.252

HQ-ROUTER(config-if)#no shutdown

HQ-ROUTER(config-if)#exit

HQ-ROUTER(config)#interface serial 0/2/0

HQ-ROUTER(config-if)#ip address 192.168.102.193 255.255.255.252

HQ-ROUTER(config-if)#no shutdown

HQ-ROUTER(config-if)#exit

HQ-ROUTER(config)#interface serial 0/1/0

HQ-ROUTER(config-if)#ip address 195.136.17.17 255.255.255.252

HQ-ROUTER(config-if)#no shutdown

HQ-ROUTER(config-if)#exit

```
HQ-ROUTER(config)#interface serial 0/2/1
```

```
HQ-ROUTER(config-if)#ip address 195.136.17.21 255.255.255.252
```

```
HQ-ROUTER(config-if)#no shutdown
```

```
HQ-ROUTER(config-if)#exit
```

```
HQ-ROUTER(config)#do wr
```

5 Port BR-ROUTER

```
BR-ROUTER(config)#interface gigabitEthernet 0/1
```

```
BR-ROUTER(config-if)#ip address 192.168.102.186 255.255.255.252
```

```
BR-ROUTER(config-if)#no shutdown
```

```
BR-ROUTER(config-if)#exit
```

```
BR-ROUTER(config)#interface gigabitEthernet 0/0
```

```
BR-ROUTER(config-if)#ip address 192.168.102.190 255.255.255.252
```

```
BR-ROUTER(config-if)#no shutdown
```

```
BR-ROUTER(config-if)#exit
```

```
BR-ROUTER(config)#interface serial 0/1/0
```

```
BR-ROUTER(config-if)#ip address 192.168.102.194 255.255.255.252
```

```
BR-ROUTER(config-if)#no shutdown
```

```
BR-ROUTER(config-if)#exit
```

```
BR-ROUTER(config)#interface serial 0/1/1
```

```
BR-ROUTER(config-if)#ip address 195.136.17.26 255.255.255.252
```

```
BR-ROUTER(config-if)#no shutdown
```

```
BR-ROUTER(config-if)#exit
```

```
BR-ROUTER(config)#interface serial 0/2/0
```

```
BR-ROUTER(config-if)#ip address 195.136.17.30 255.255.255.252
```

```
BR-ROUTER(config-if)#no shutdown
```

```
BR-ROUTER(config-if)#exit
```

```
BR-ROUTER(config)#do wr
```

ISP1

```
Router(config)#interface serial 0/2/0
```

```
Router(config-if)#ip address 195.136.17.18 255.255.255.252
```

```
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
```

```
Router(config)#do wr
```

```
Router(config)#interface serial 0/2/1
```

```
Router(config-if)#ip address 195.136.17.25 255.255.255.252
```

```
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
```

```
Router(config)#do wr
```

ISP2

Router(config)#interface serial 0/3/0

Router(config-if)#ip address 195.136.17.22 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#do wr

Router(config)#interface serial 0/3/1

Router(config-if)#ip address 195.136.17.29 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#do wr

Kích hoạt định tuyến trên cách SWL3: ip routing

5.6 Cấu hình OSPF**HQ-M-SW1**

HQ-Mul-SW-1(config)#router ospf 10

HQ-Mul-SW-1(config-router)#network 192.168.100.0 0.0.0.63 area 0

HQ-Mul-SW-1(config-router)#network 192.168.100.64 0.0.0.63 area 0

HQ-Mul-SW-1(config-router)#network 192.168.100.128 0.0.0.63 area 0

HQ-Mul-SW-1(config-router)#network 192.168.100.192 0.0.0.63 area 0

HQ-Mul-SW-1(config-router)#network 192.168.101.0 0.0.0.63 area 0

HQ-Mul-SW-1(config-router)#network 192.168.101.64 0.0.0.63 area 0

HQ-Mul-SW-1(config-router)#network 192.168.102.176 0.0.0.3 area 0

HQ-M-SW2

HQ-Mul-SW-2(config)#router ospf 10

HQ-Mul-SW-2(config-router)#network 192.168.100.0 0.0.0.63 area 0

HQ-Mul-SW-2(config-router)#network 192.168.100.64 0.0.0.63 area 0

HQ-Mul-SW-2(config-router)#network 192.168.100.128 0.0.0.63 area 0

HQ-Mul-SW-2(config-router)#network 192.168.100.192 0.0.0.63 area 0

HQ-Mul-SW-2(config-router)#network 192.168.101.0 0.0.0.63 area 0

HQ-Mul-SW-2(config-router)#network 192.168.101.64 0.0.0.63 area 0

HQ-Mul-SW-2(config-router)#network 192.168.102.180 0.0.0.3 area 0

BR-M-SW1

BR-Mul-SW-3(config)#router ospf 10

BR-Mul-SW-3(config-router)#network 192.168.101.128 0.0.0.31 area 0

BR-Mul-SW-3(config-router)#network 192.168.101.160 0.0.0.31 area 0

BR-Mul-SW-3(config-router)#network 192.168.101.192 0.0.0.31 area 0

BR-Mul-SW-3(config-router)#network 192.168.101.224 0.0.0.31 area 0

BR-Mul-SW-3(config-router)#network 192.168.102.0 0.0.0.127 area 0

BR-Mul-SW-3(config-router)#network 192.168.102.128 0.0.0.31 area 0

BR-Mul-SW-3(config-router)#network 192.168.102.184 0.0.0.3 area 0

BR-M-SW2

BR-Mul-SW-4(config)#router ospf 10

BR-Mul-SW-4(config-router)#network 192.168.101.128 0.0.0.31 area 0

BR-Mul-SW-4(config-router)#network 192.168.101.160 0.0.0.31 area 0

BR-Mul-SW-4(config-router)#network 192.168.101.192 0.0.0.31 area 0

BR-Mul-SW-4(config-router)#network 192.168.101.224 0.0.0.31 area 0

BR-Mul-SW-4(config-router)#network 192.168.102.0 0.0.0.127 area 0

BR-Mul-SW-4(config-router)#network 192.168.102.128 0.0.0.31 area 0

BR-Mul-SW-4(config-router)#network 192.168.102.188 0.0.0.3 area 0

HQ-ROUTER

HQ-ROUTER(config)#router ospf 10

HQ-ROUTER(config-router)#network 192.168.102.176 0.0.0.3 area 0

HQ-ROUTER(config-router)#network 192.168.102.180 0.0.0.3 area 0

HQ-ROUTER(config-router)#network 192.168.102.192 0.0.0.3 area 0

HQ-ROUTER(config-router)#network 195.136.17.16 0.0.0.3 area 0

HQ-ROUTER(config-router)#network 195.136.17.20 0.0.0.3 area 0

HQ-ROUTER(config-router)#network 192.168.102.160 0.0.0.15 area 0

BR-ROUTER

```
BR-ROUTER(config)#router ospf 10  
BR-ROUTER(config-router)#network 192.168.102.184 0.0.0.3 area 0  
BR-ROUTER(config-router)#network 192.168.102.188 0.0.0.3 area 0  
BR-ROUTER(config-router)#network 192.168.102.192 0.0.0.3 area 0  
BR-ROUTER(config-router)#network 195.136.17.24 0.0.0.3 area 0  
BR-ROUTER(config-router)#network 195.136.17.28 0.0.0.3 area 0
```

ISP1

```
Router(config)#router ospf 10  
Router(config-router)#network 195.136.17.16 0.0.0.3 area 0  
Router(config-router)#network 195.136.17.24 0.0.0.3 area 0
```

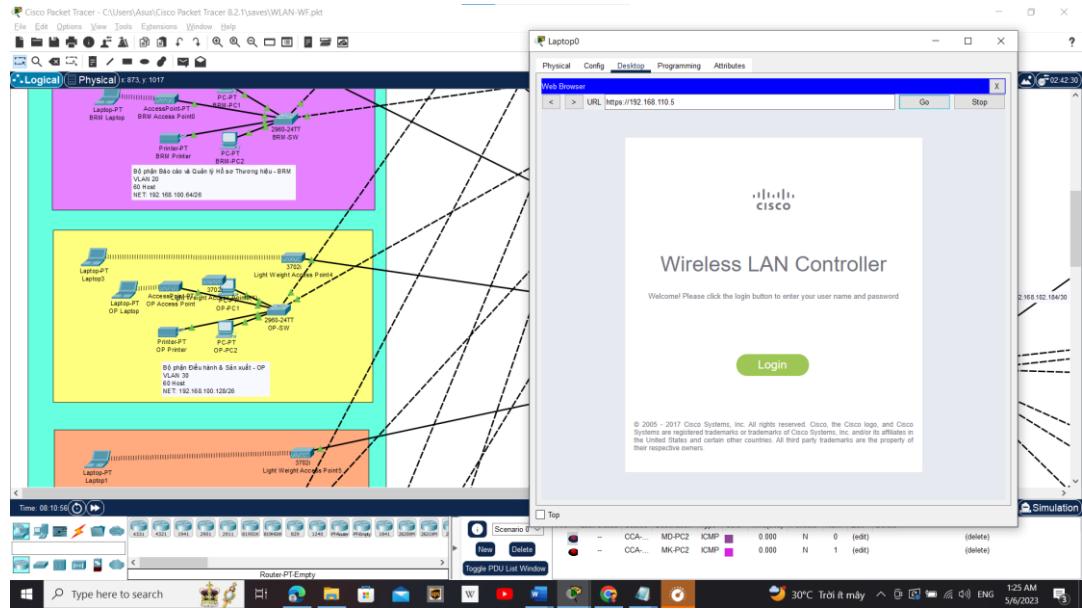
ISP2

```
Router(config)#router ospf 10  
Router(config-router)#network 195.136.17.20 0.0.0.3 area 0  
Router(config-router)#network 195.136.17.28 0.0.0.3 area 0
```

5.7 Cấu hình Wireless Network

Laptop0

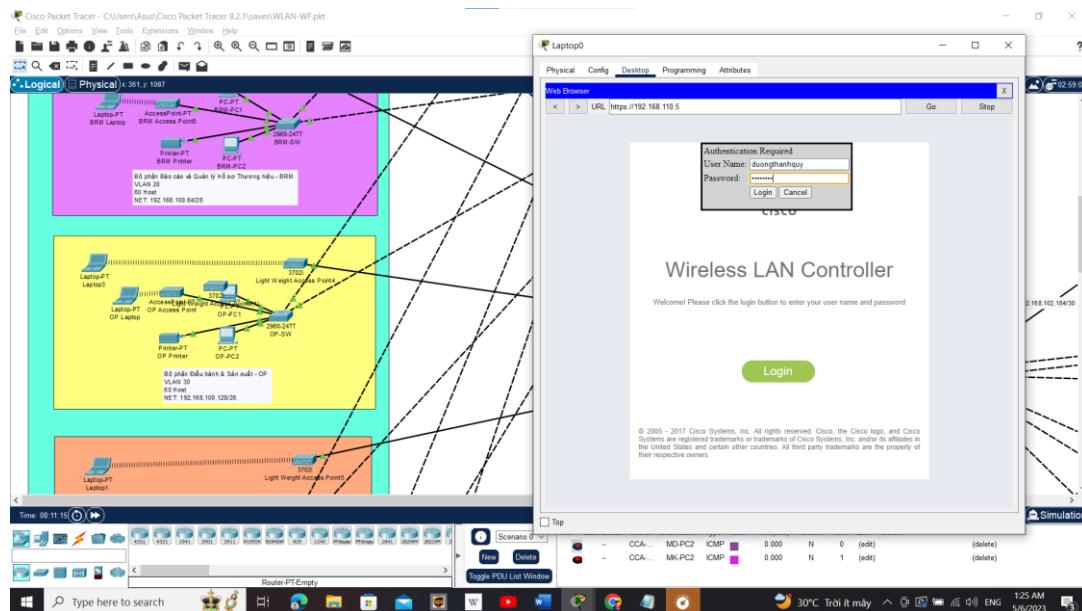
Đăng nhập vào địa chỉ của Wireless LAN



Hình 5.7. 1 Đăng nhập vào dịch vụ WLAN

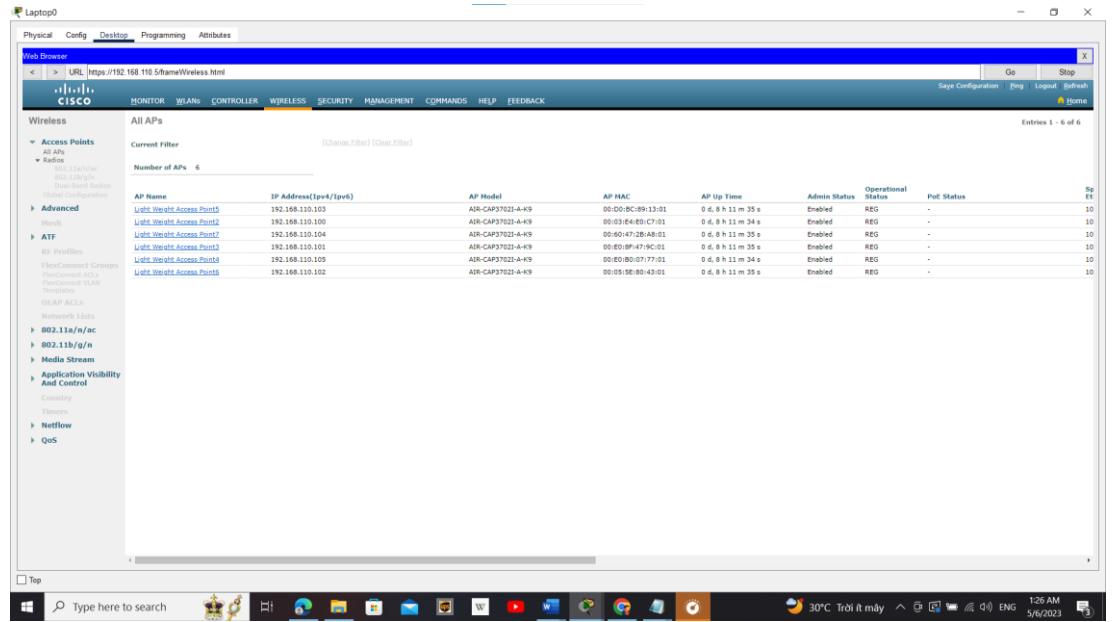
Username: duongthanhquy

Password: Cisco123



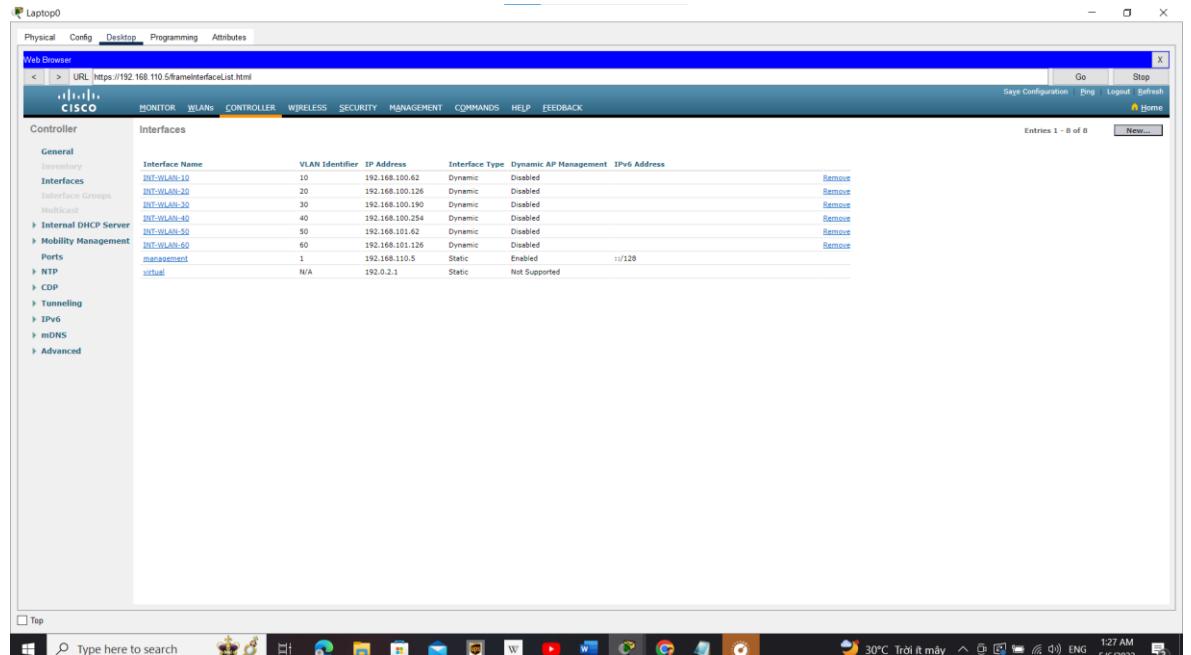
Hình 5.7. 2 Nhập Username và Passwork

Kiểm tra các kết nối của Aps



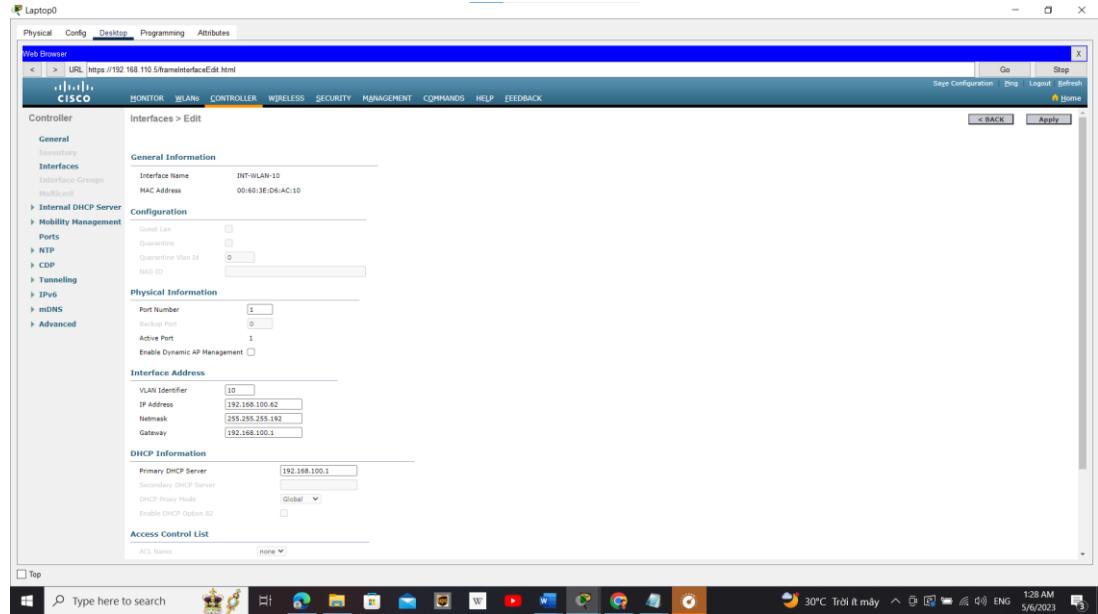
Hình 5.7. 3 Kiểm tra các kết nối đến Light Weight Access Point

Vào mục Controller để tạo các Interface

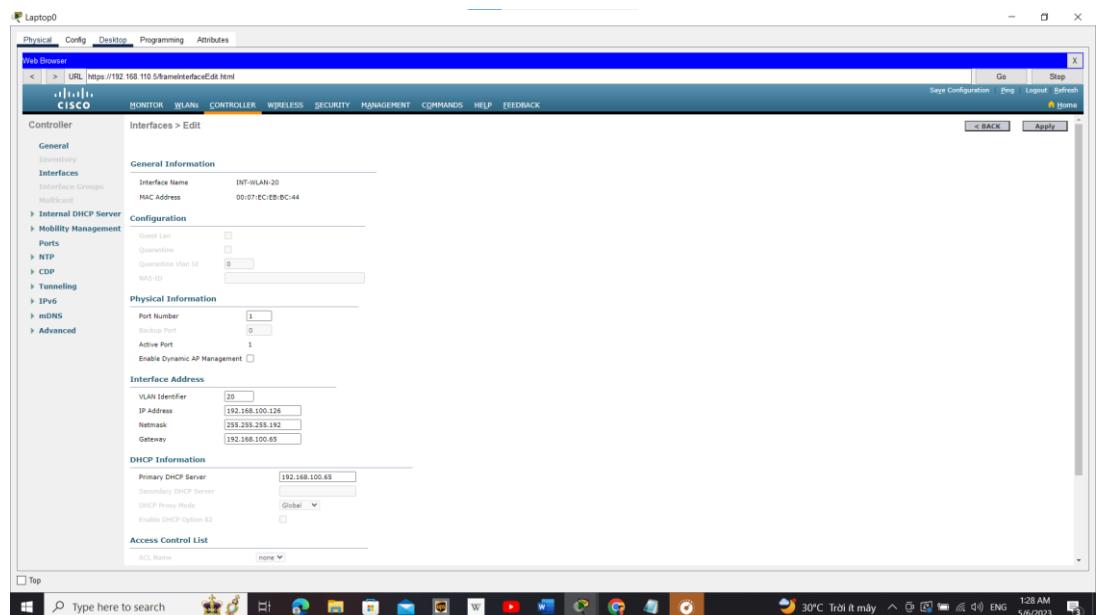


Hình 5.7. 4 Danh sách các Interface đã tạo trên Controller

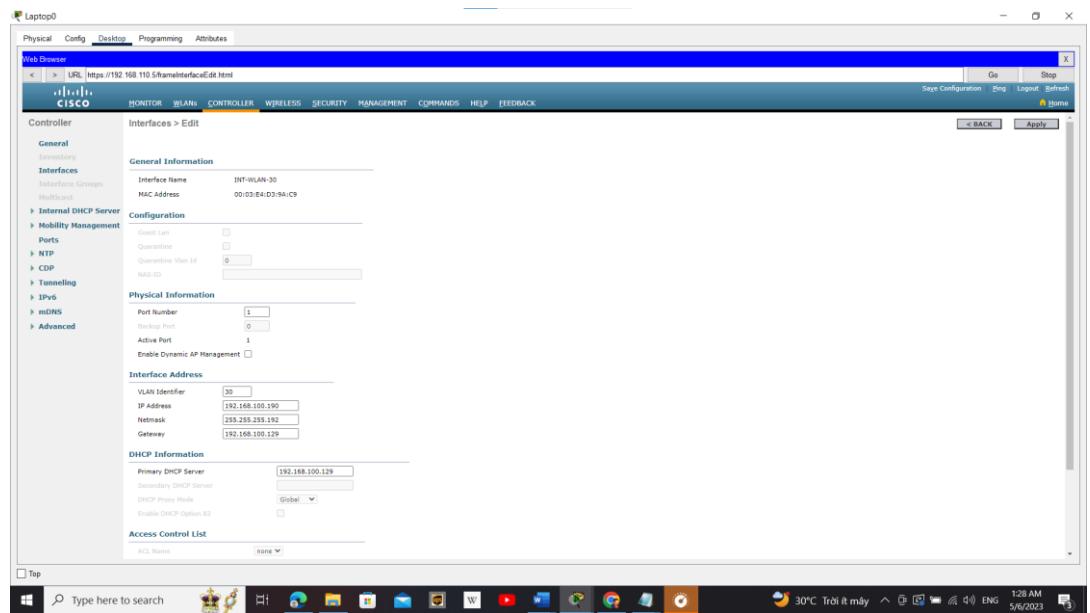
Cấu hình chuẩn WPA



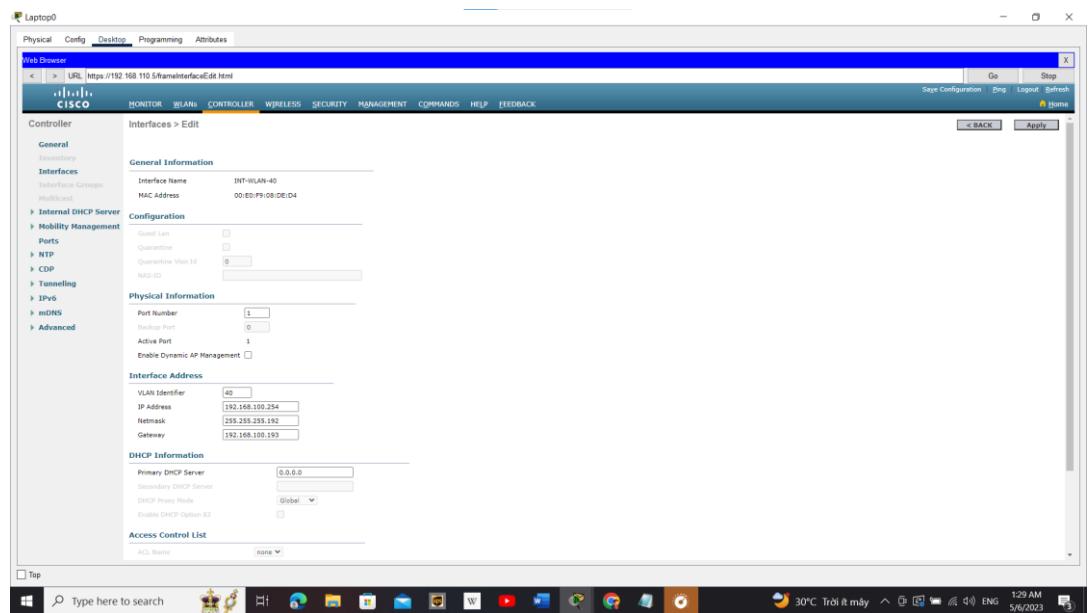
Hình 5.7. 5 Chi tiết Interface VLAN 10



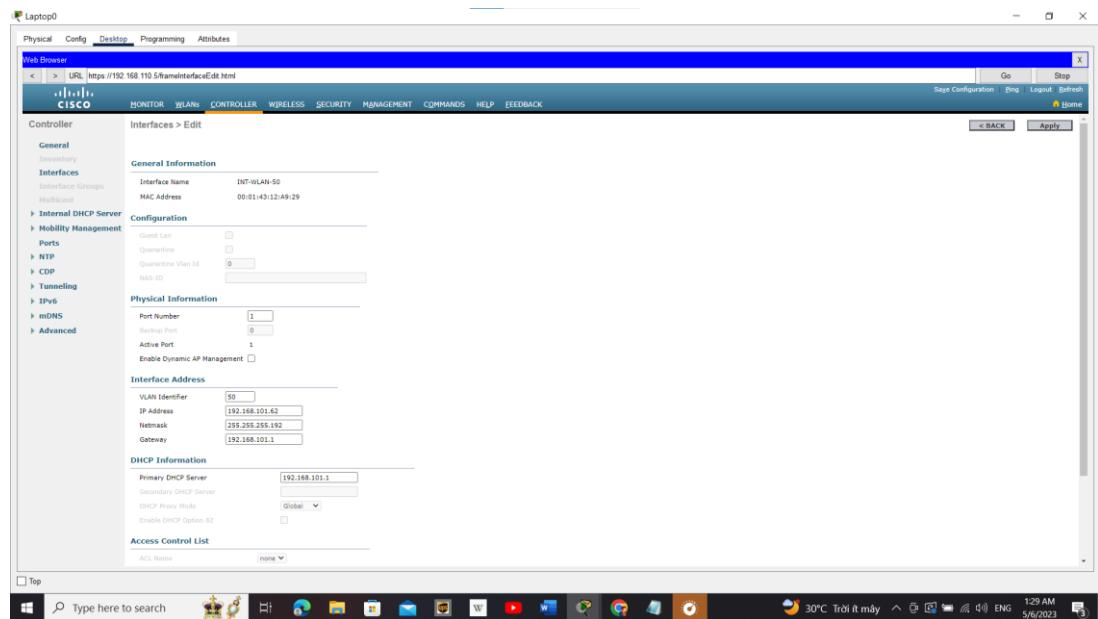
Hình 5.7. 6 Chi tiết Interface VLAN 20



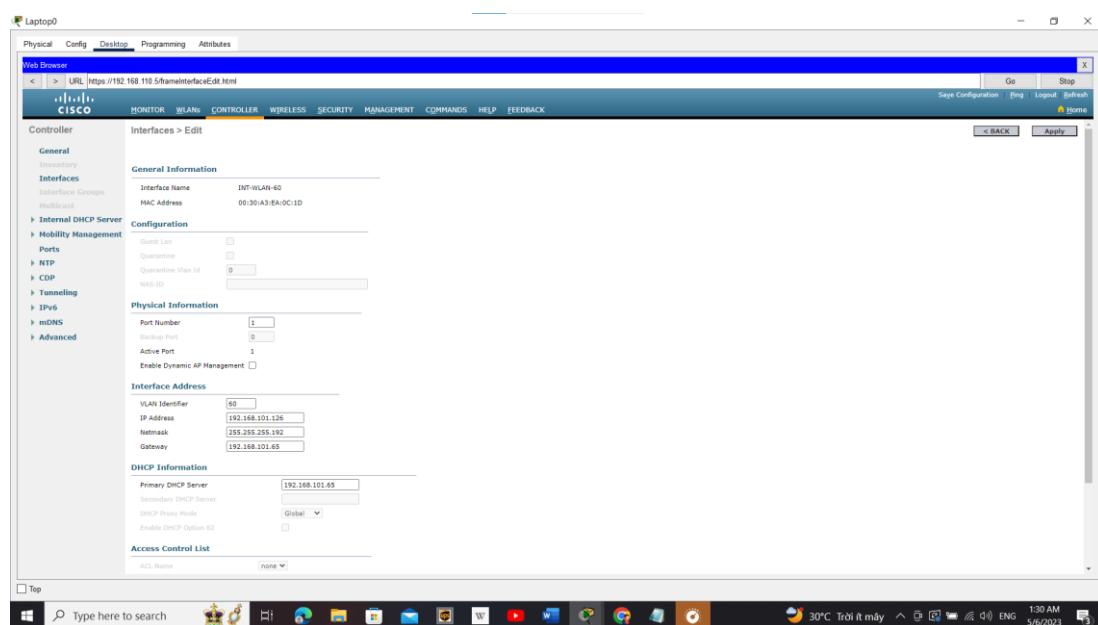
Hình 5.7. 7 Chi tiết Interface VLAN 30



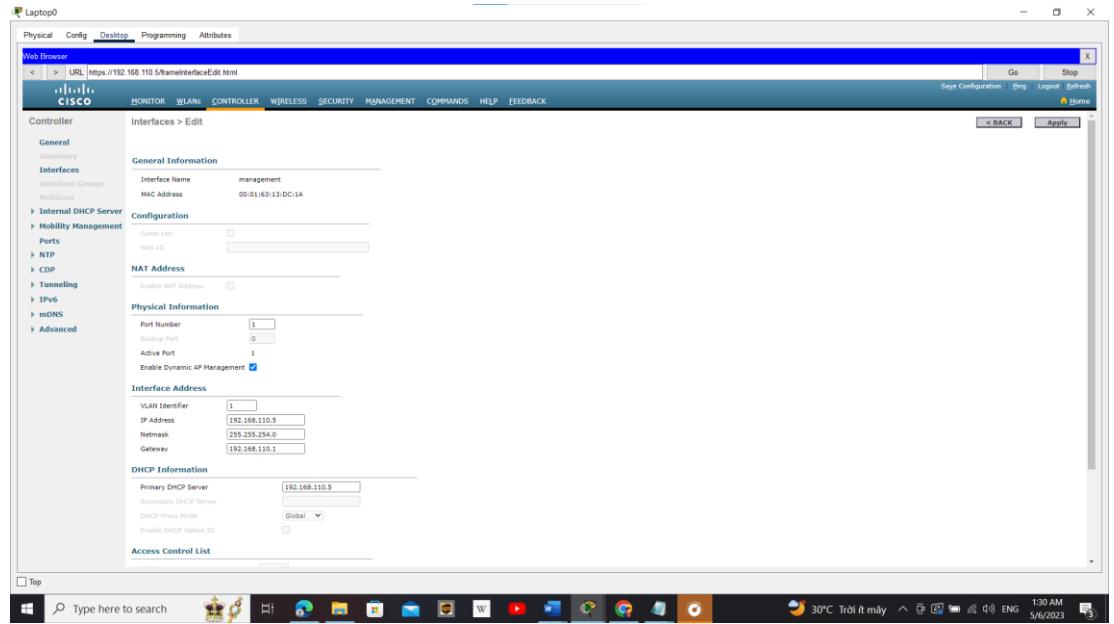
Hình 5.7. 8 Chi tiết Interface VLAN 40



Hình 5.7. 9 Chi tiết Interface VLAN 50



Hình 5.7. 10 Chi tiết Interface VLAN 60



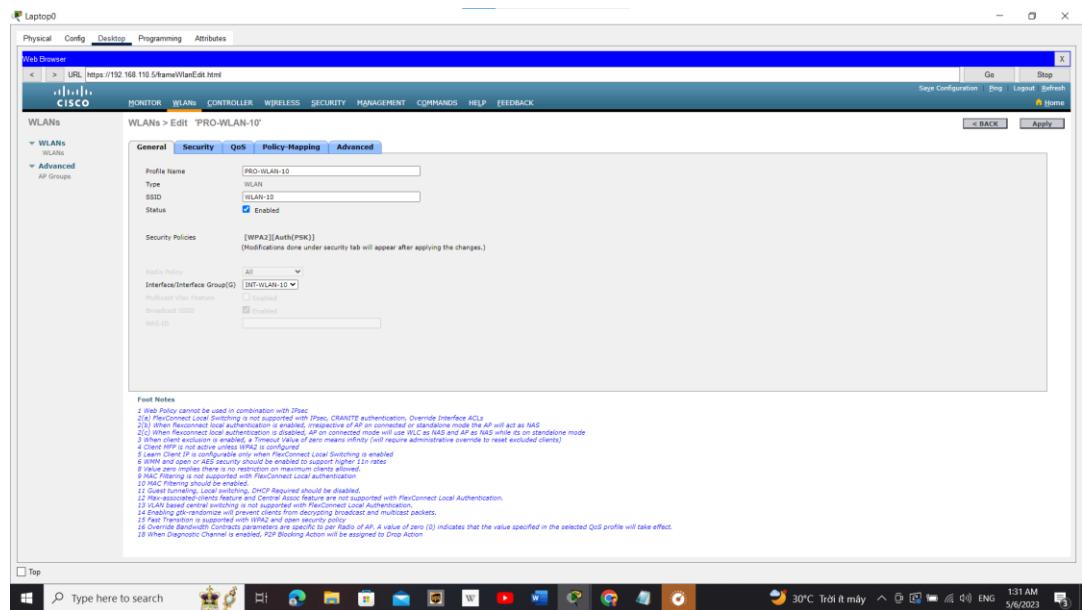
Hình 5.7. 11 Chi tiết Interface management

Vào WLAN để cấu hình

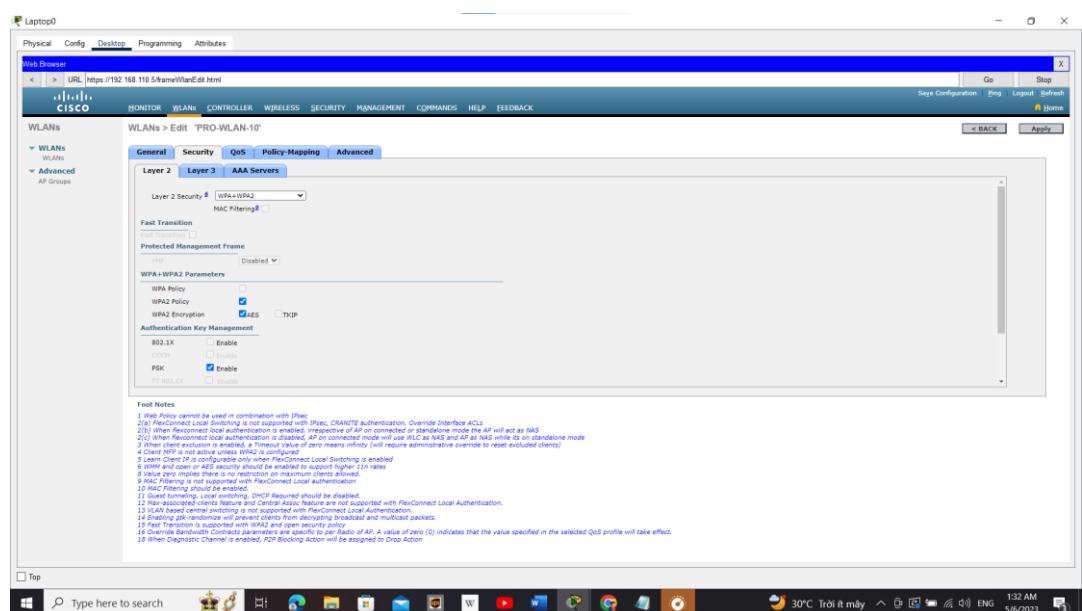
WLANs

Current Filter: [Change Filter] [Clear Filter]						
	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/>	1	WLAN	PRO-WLAN-10	WLAN-10	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/>	2	WLAN	PRO-WLAN-20	WLAN-20	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	3	WLAN	PRO-WLAN-30	WLAN-30	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	4	WLAN	PRO-WLAN-40	WLAN-40	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	5	WLAN	PRO-WLAN-50	WLAN-50	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	6	WLAN	PRO-WLAN-60	WLAN-60	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	7	WLAN	PRO-WLAN-140	WLAN-140	Enabled	[WPA2][Auth(PSK)]

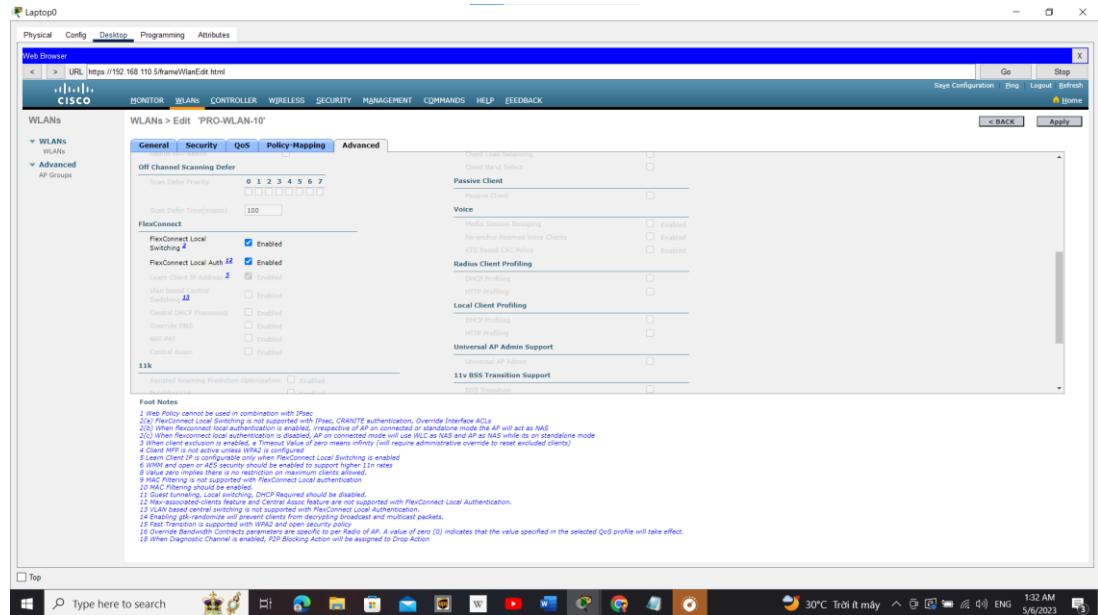
Hình 5.7. 12 Danh sách các WLANs đã đăng ký



Hình 5.7. 13 Chi tiết đăng ký WLAN và VLAN 10



Hình 5.7. 14 Chi tiết đăng ký WLAN và VLAN 10



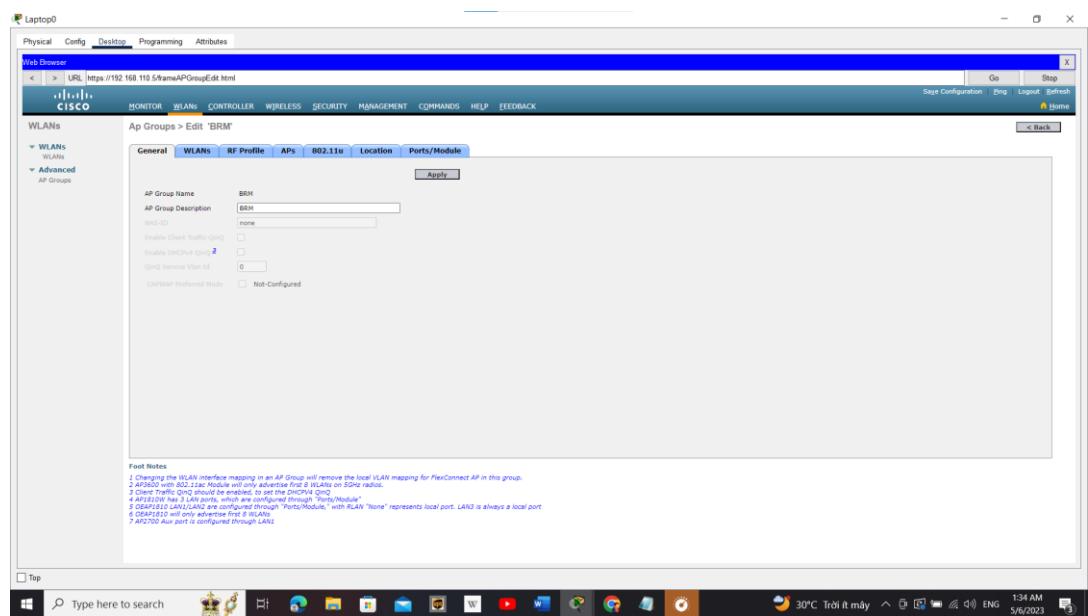
Hình 5.7. 15 Chi tiết đăng ký WLAN và VLAN 10

Các WLAN 20, 30, 40, 50, 60 làm tương tự như WLAN 10

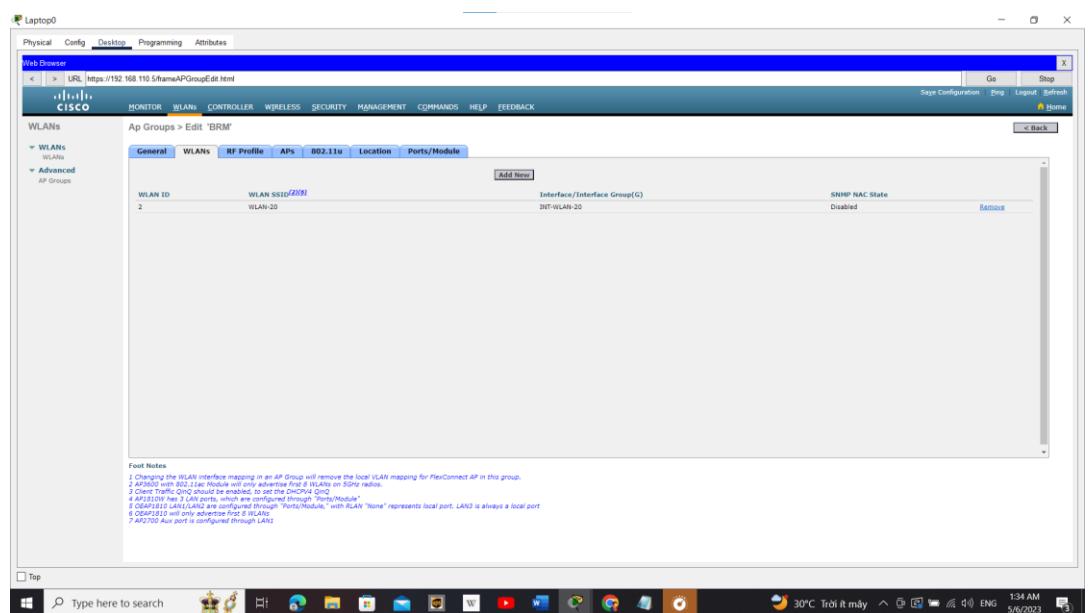
Tạo Group cho các WLAN để các LAP ở VLAN nào thì kết nối được với các thiết bị ở VLAN đó

AP Group Name	AP Group Description	Action
BRM	BRM	Remove
CCA	CCA	Remove
COSB	COSB	Remove
CWA1	CWA1	Remove
IT	IT	Remove
QP	QP	Remove
default-group		

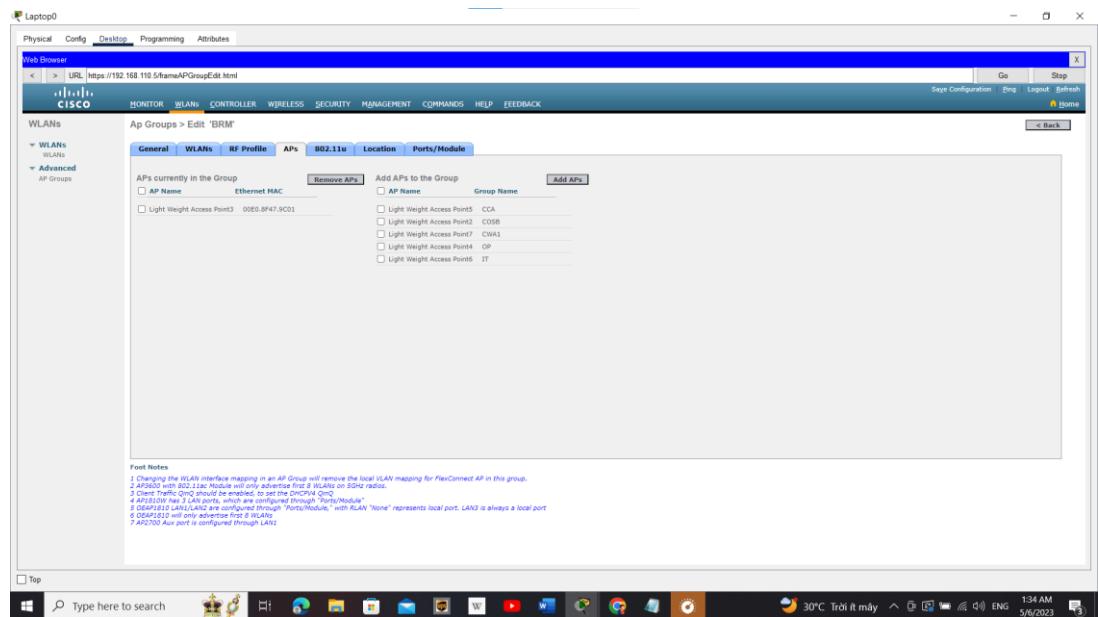
Hình 5.7. 16 Danh sách Groups đã tạo theo từng VLAN cho WLAN



Hình 5.7. 17 Chi tiết tạo Group cho WLAN BRM



Hình 5.7. 18 Chi tiết tạo Group cho WLAN BRM



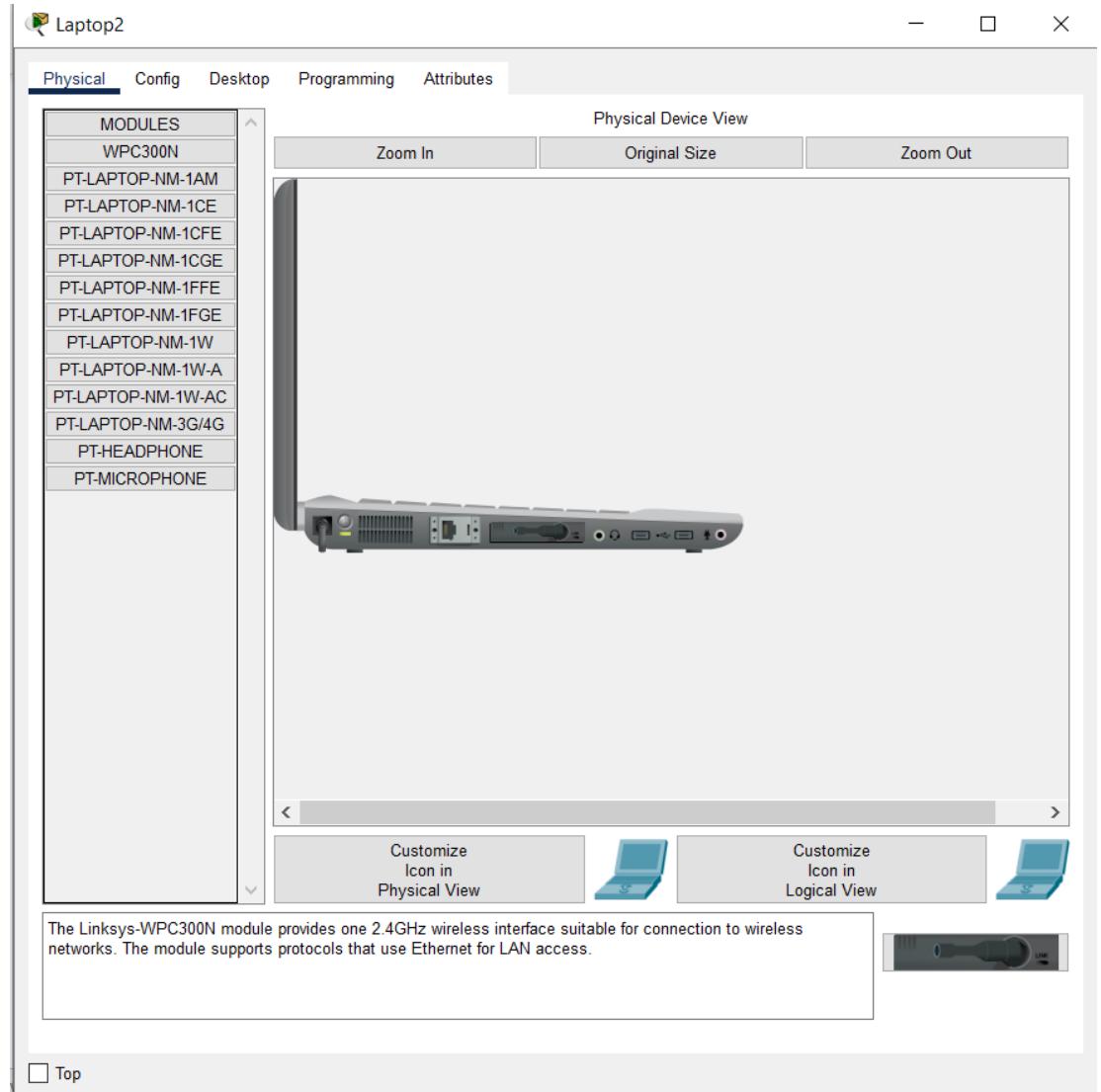
Hình 5.7. 19 Chi tiết tạo Group cho WLAN BRM

Các Group CCA, COSB, SWA1, IT, OP làm tương tự như Group BRM

* Wireless LAN ở Chi nhánh cũng thực hiện tương tự các bước trên

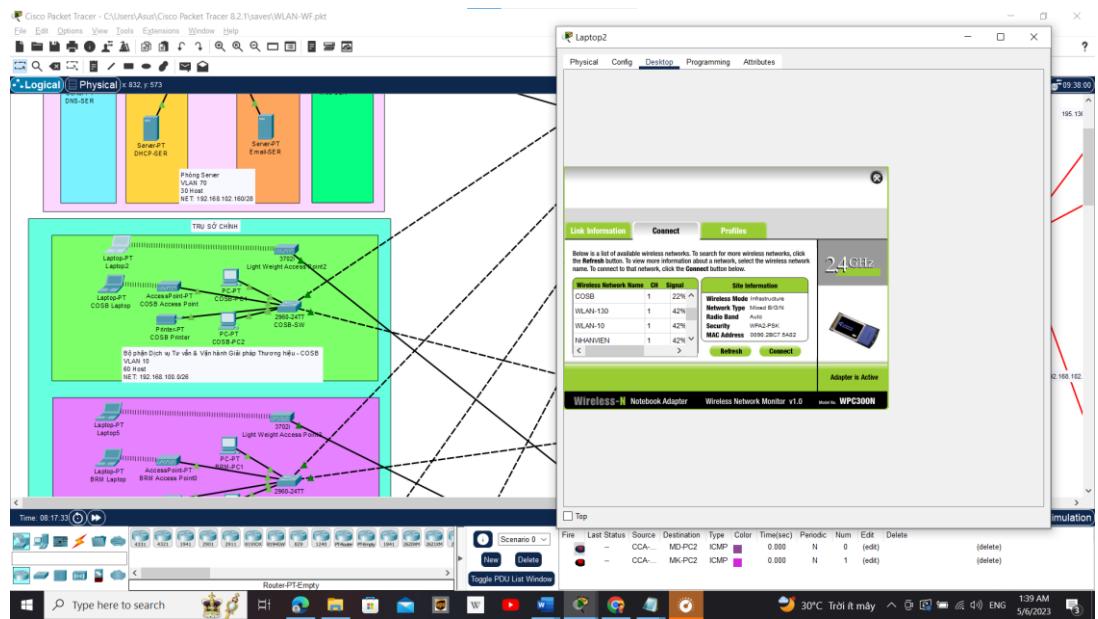
Kết nối thiết bị đến Light Weight Access Point

Chọn 1 Laptop, gắn Card mạng WPC300N cho Laptop



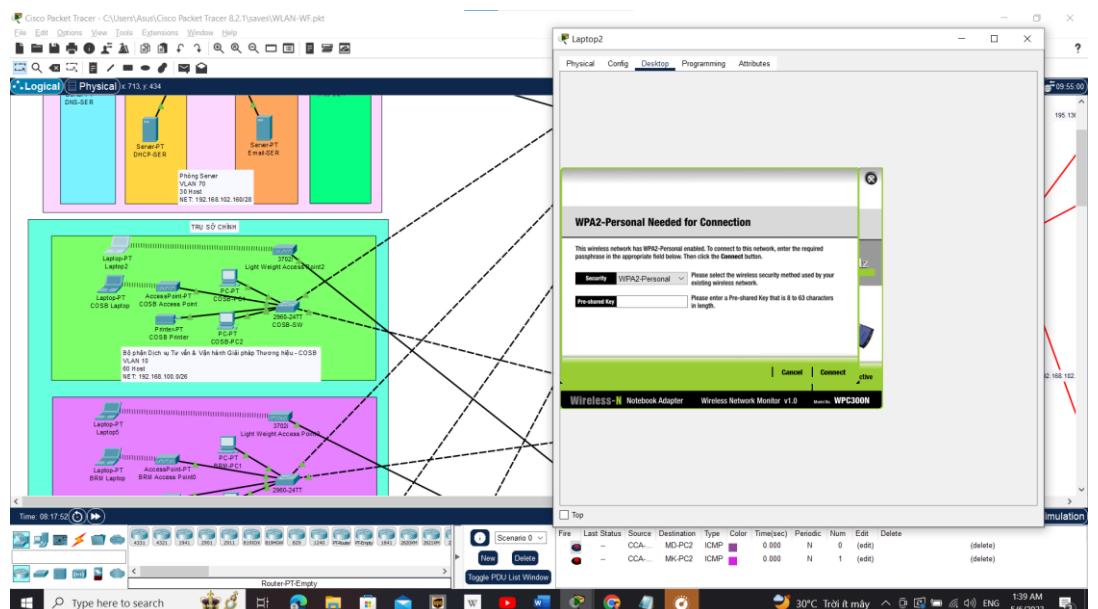
Hình 5.7. 20 Gắn Card mạng cho LAPTOP

Vào Connect, nhấn chọn Refresh



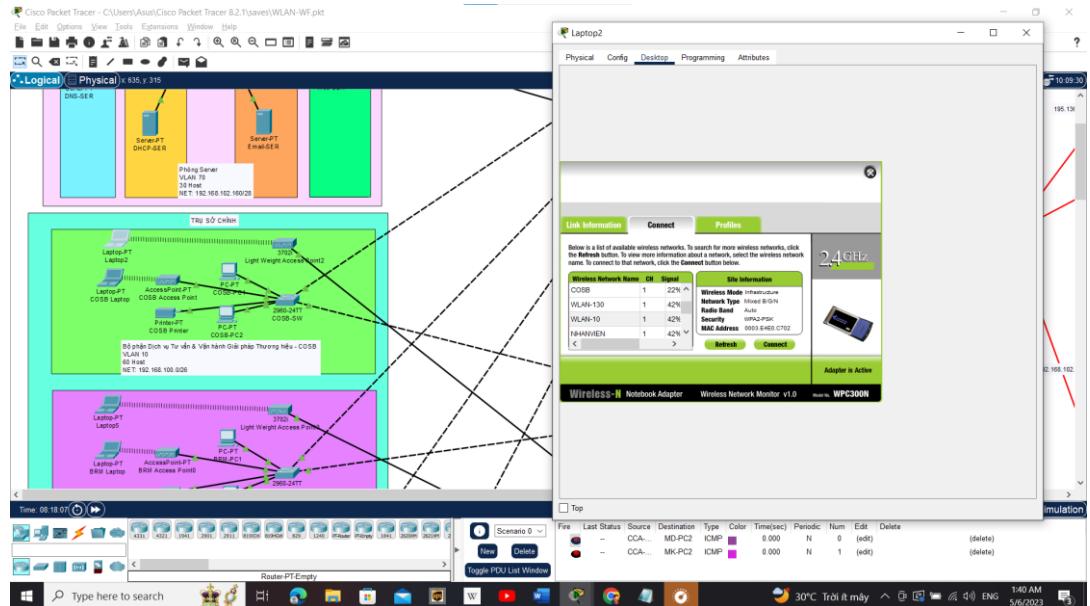
Hình 5.7. 21 Refresh để tìm kiếm WLAN tương ứng theo từng VLAN

Nhấn chọn WLAN-10, rồi chọn Conect



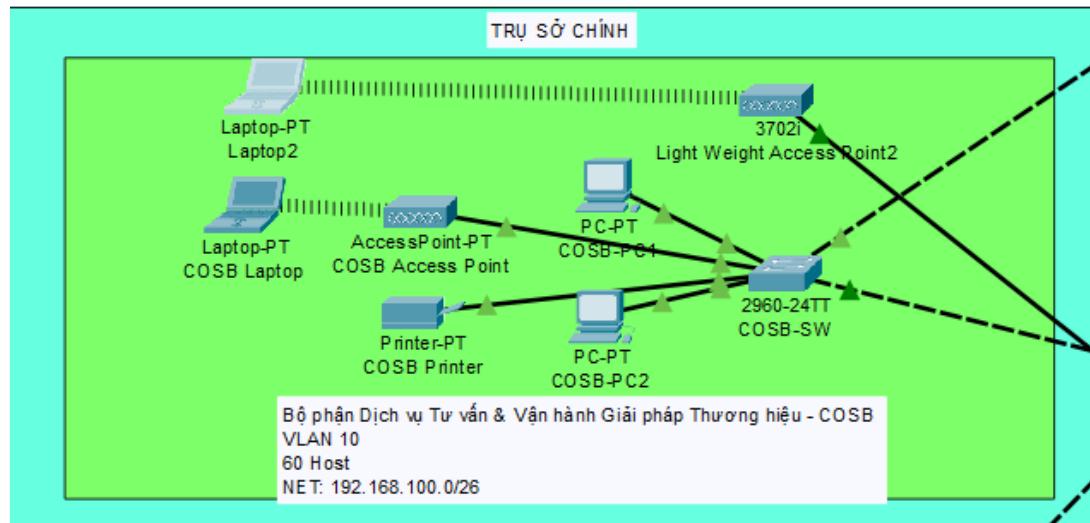
Hình 5.7. 22 Chọn WLAN phù hợp theo từng VLAN

Nhập mật khẩu là Cisco123 để kết nối



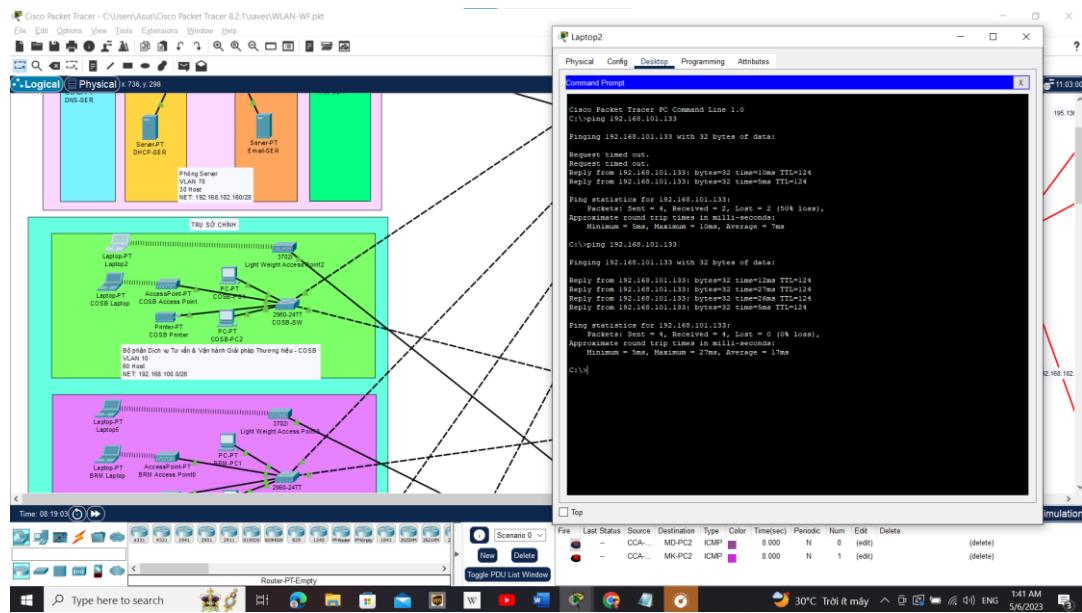
Hình 5.7. 23 Kết nối đến WLAN

Kết nối thành công.



Hình 5.7. 24 Kết nối thành công

Ping từ PC2 đến địa chỉ thuộc VLAN bất kỳ để kiểm tra

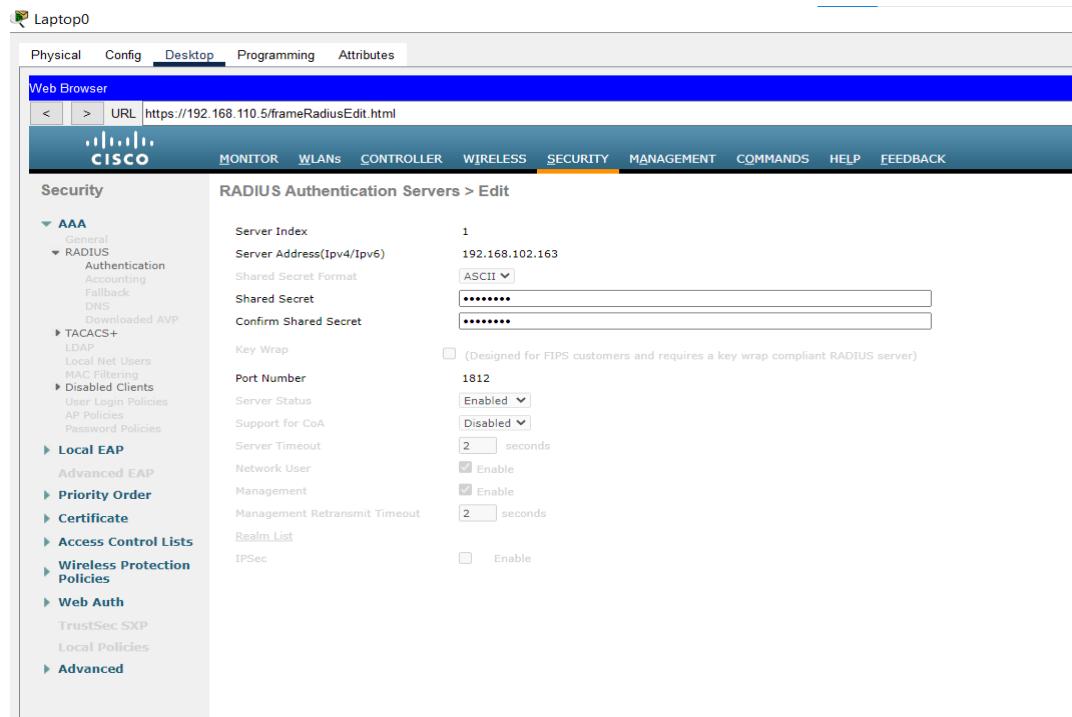


Hình 5.7. 25 Ping thành công thiết bị kết nối WLAN đến các thiết bị khác

Ping thành công

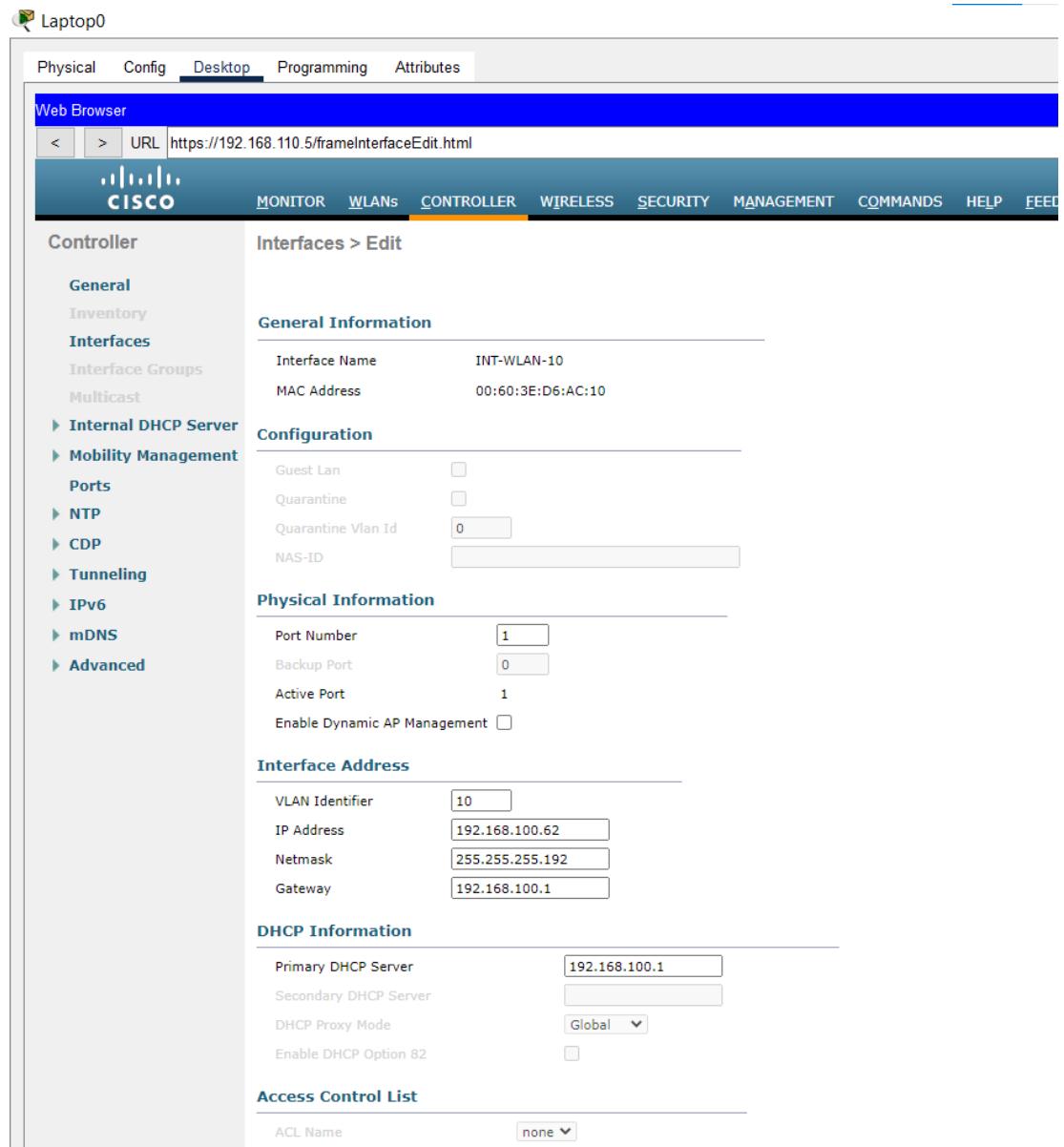
CẤU HÌNH CHUẨN 802.1X

Tại SECURITY đặt các giá trị như sau:



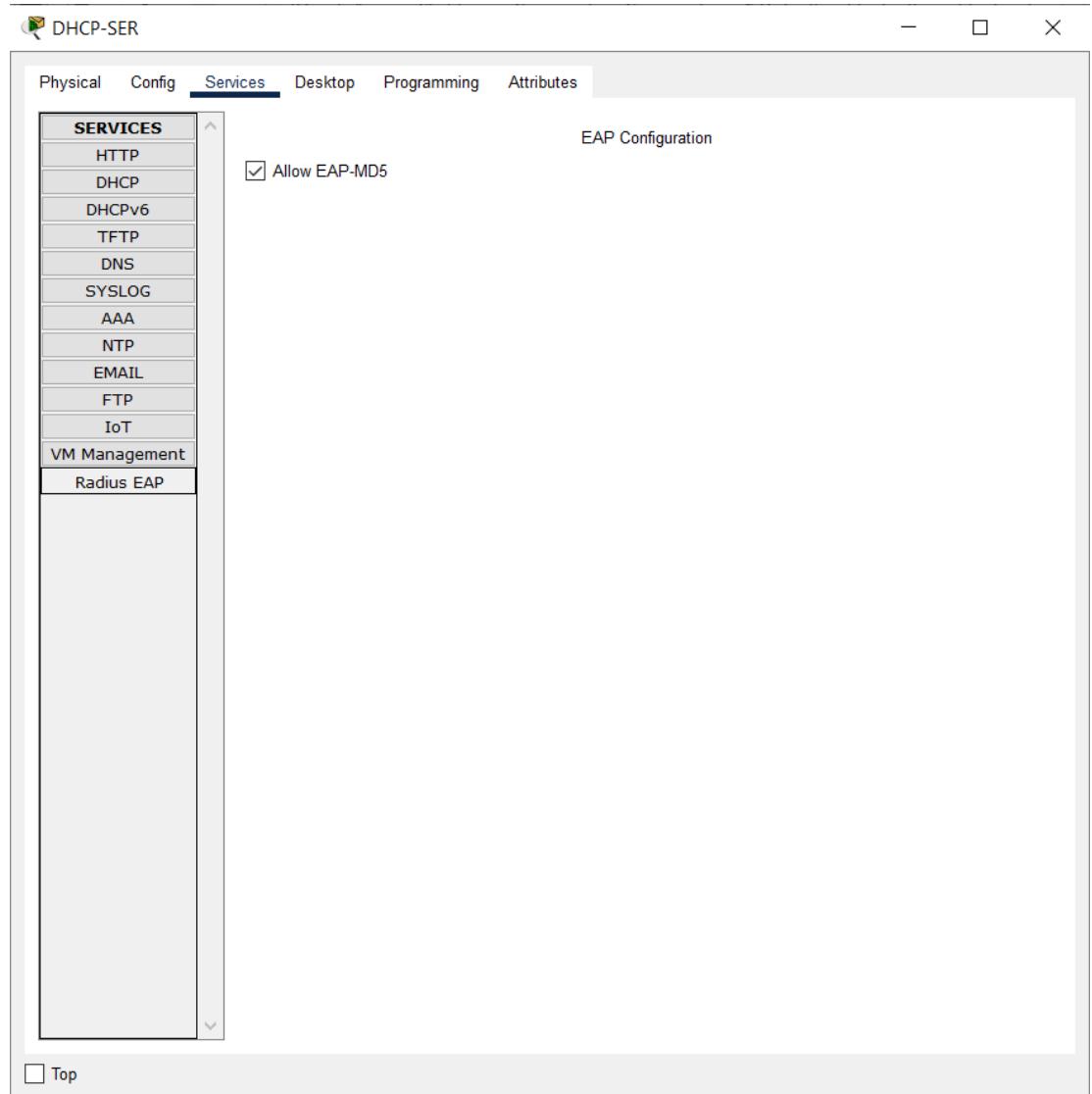
Hình 5.7. 26 Cấu hình tại SECURITY

Tại CONTROLLER > Interfaces, tạo một INT-WLAN-10



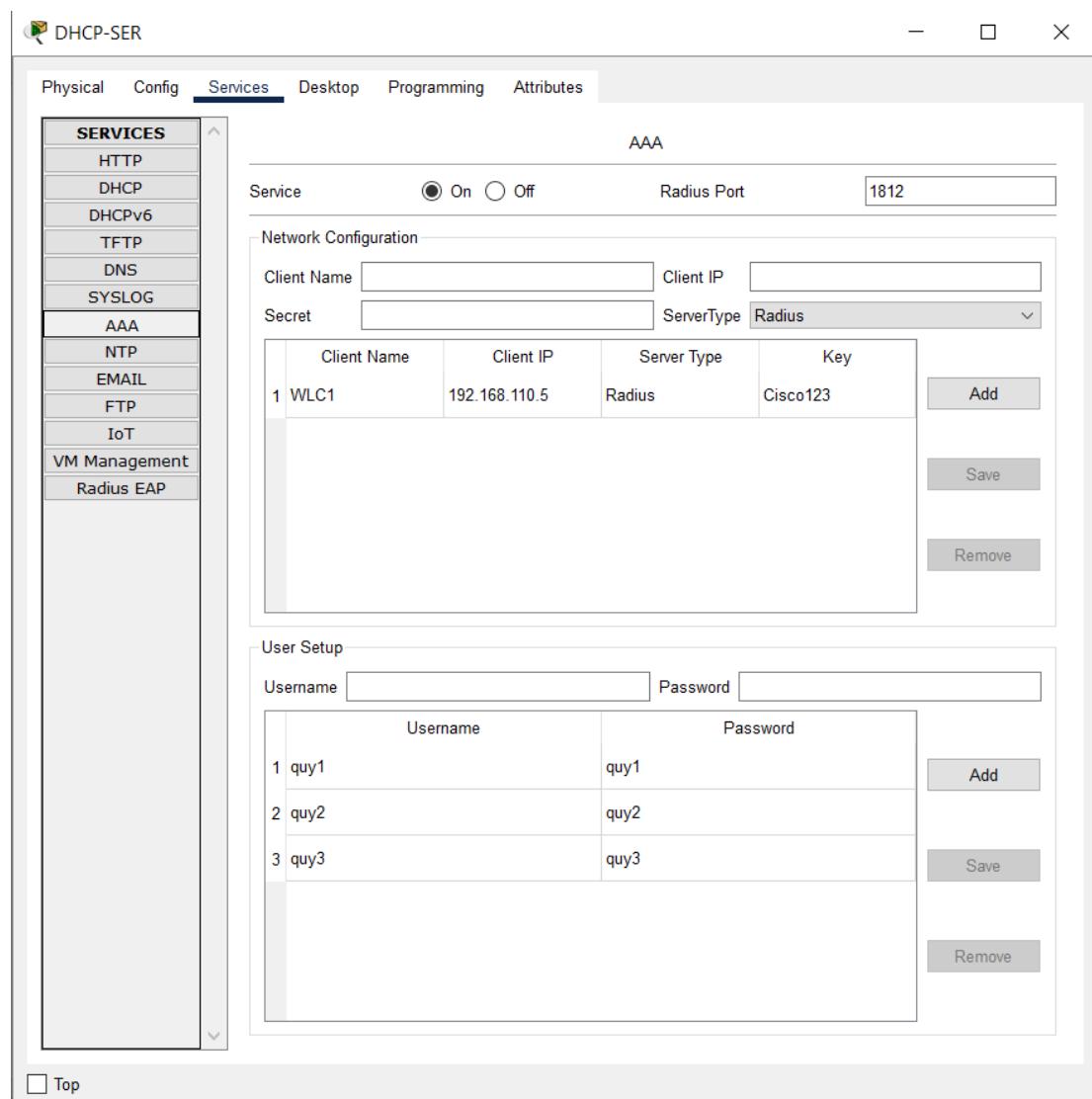
Hình 5.7. 27 Cấu hình tại CONTROLLER > interfaces

Tại Server > Service , bật Radius EAP



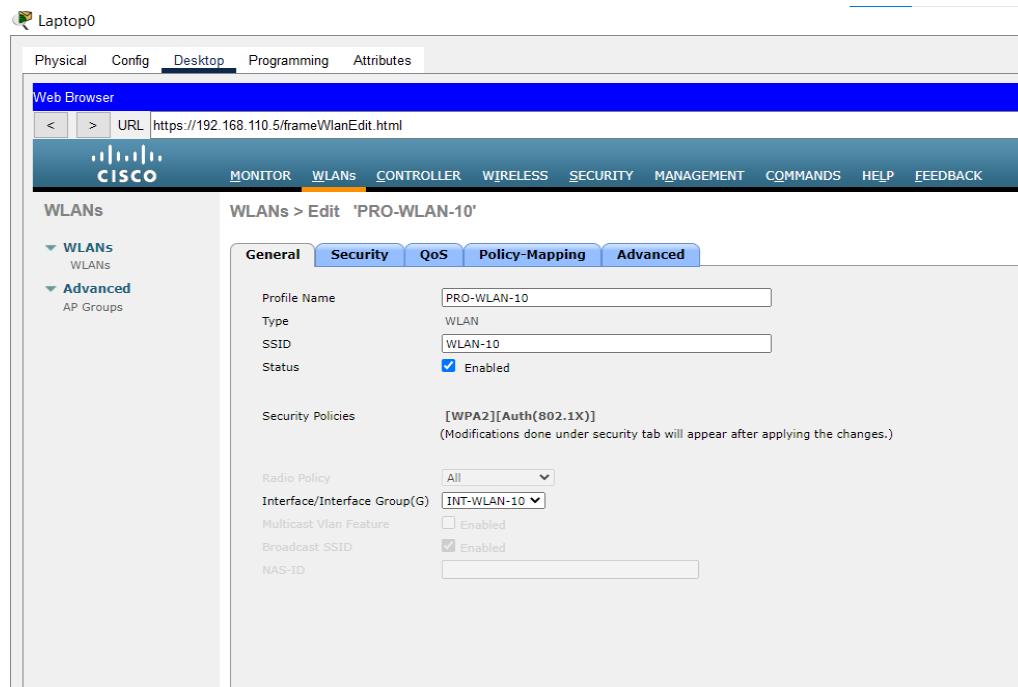
Hình 5.7. 28 Bật EAP-MD5

Tiếp tục, tại Server > Service > AAA cấu hình như dưới:

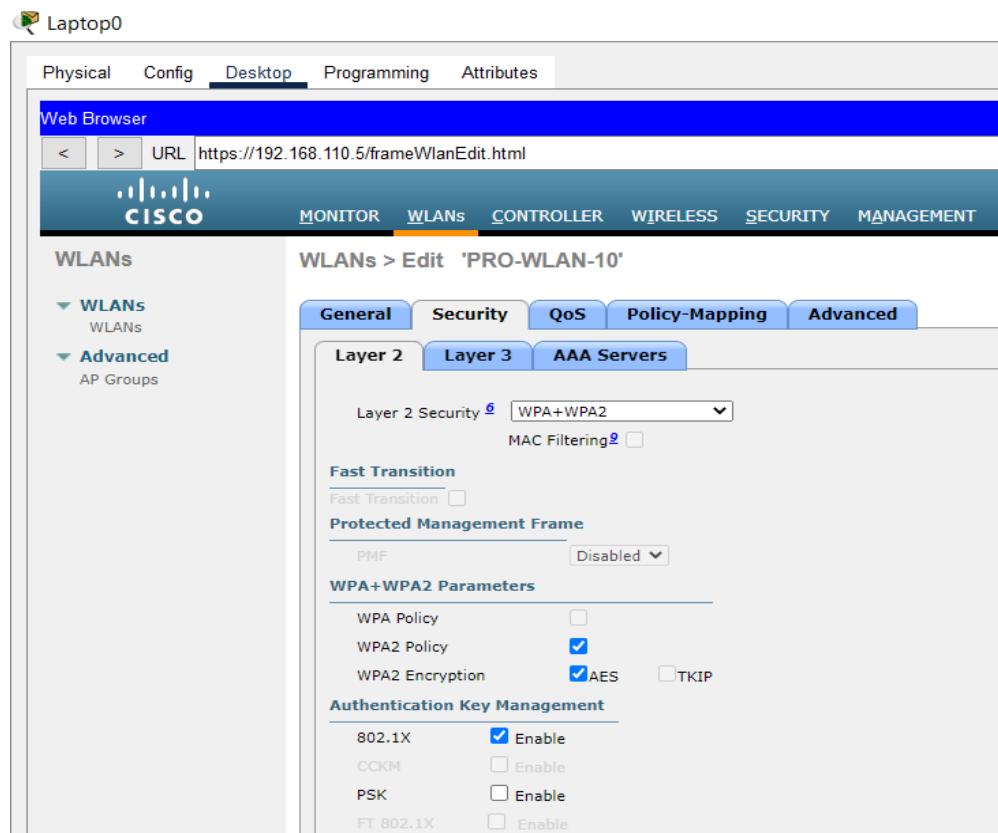


Hình 5.7. 29 Cấu hình AAA tại Server

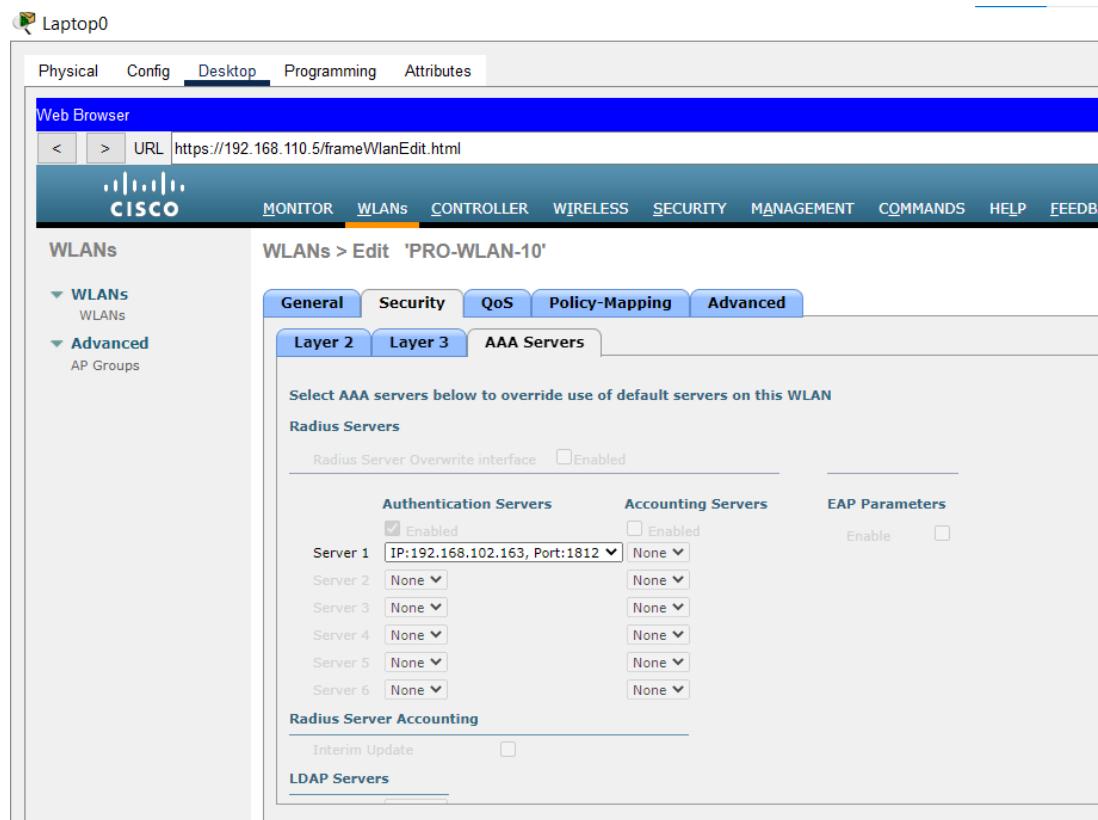
Tại WLANs, tạo PRO-WLAN-10 theo các thông số bên dưới:



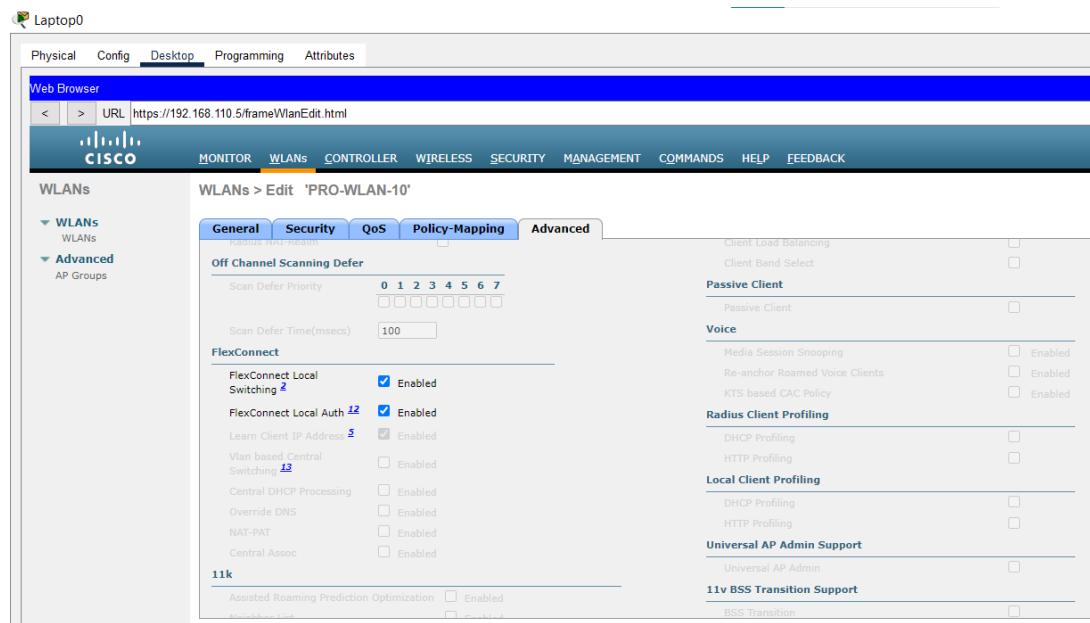
Hình 5.7. 30 Cấu hình WLAN-10 mục General



Hình 5.7. 31 Cấu hình WLAN-10 mục Security > Layer 2



Hình 5.7. 32 Cấu hình WLAN-10 mục Security > AAA Servers

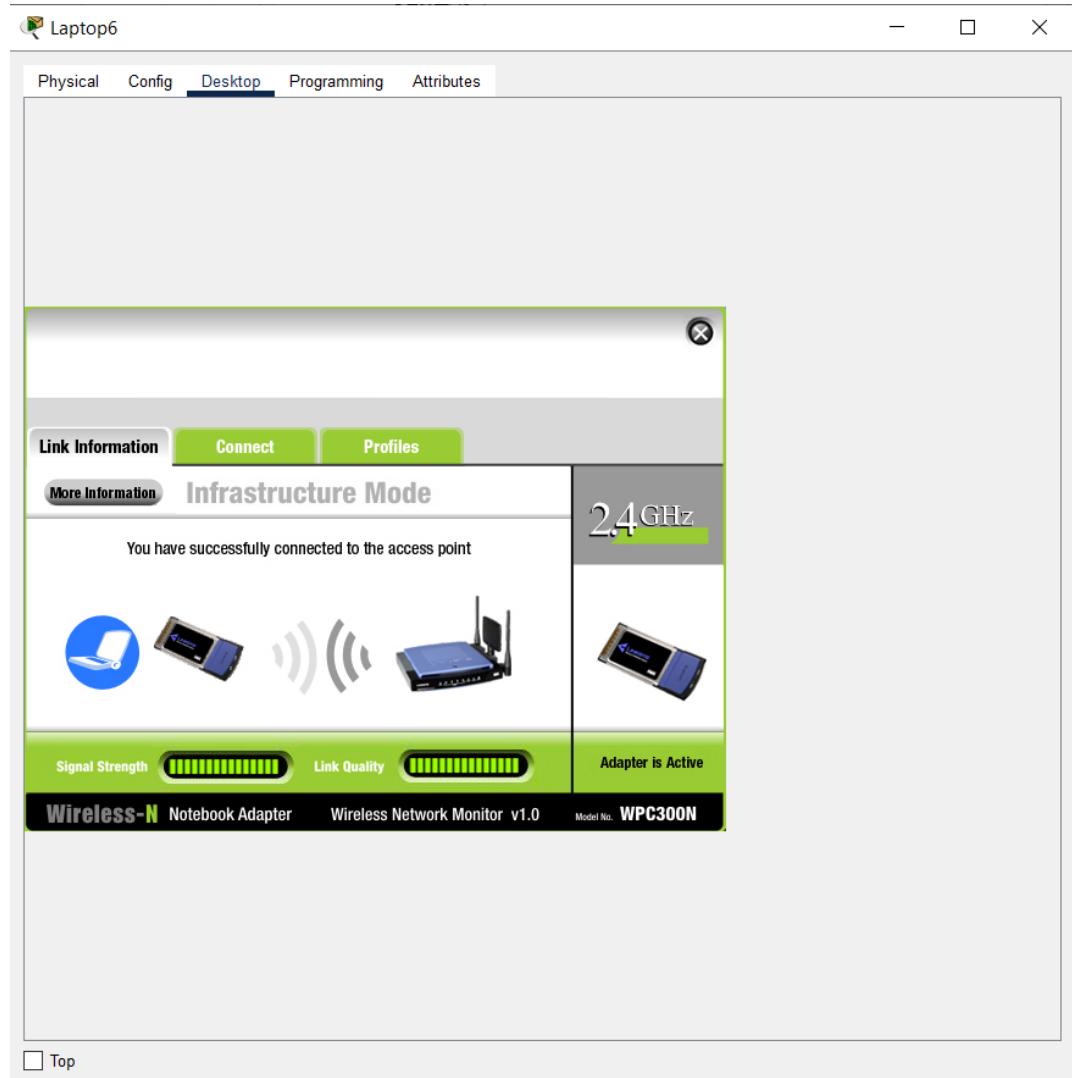


Hình 5.7. 33 Cấu hình WLAN-10 mục Advanced

Kiểm tra thử kết nối

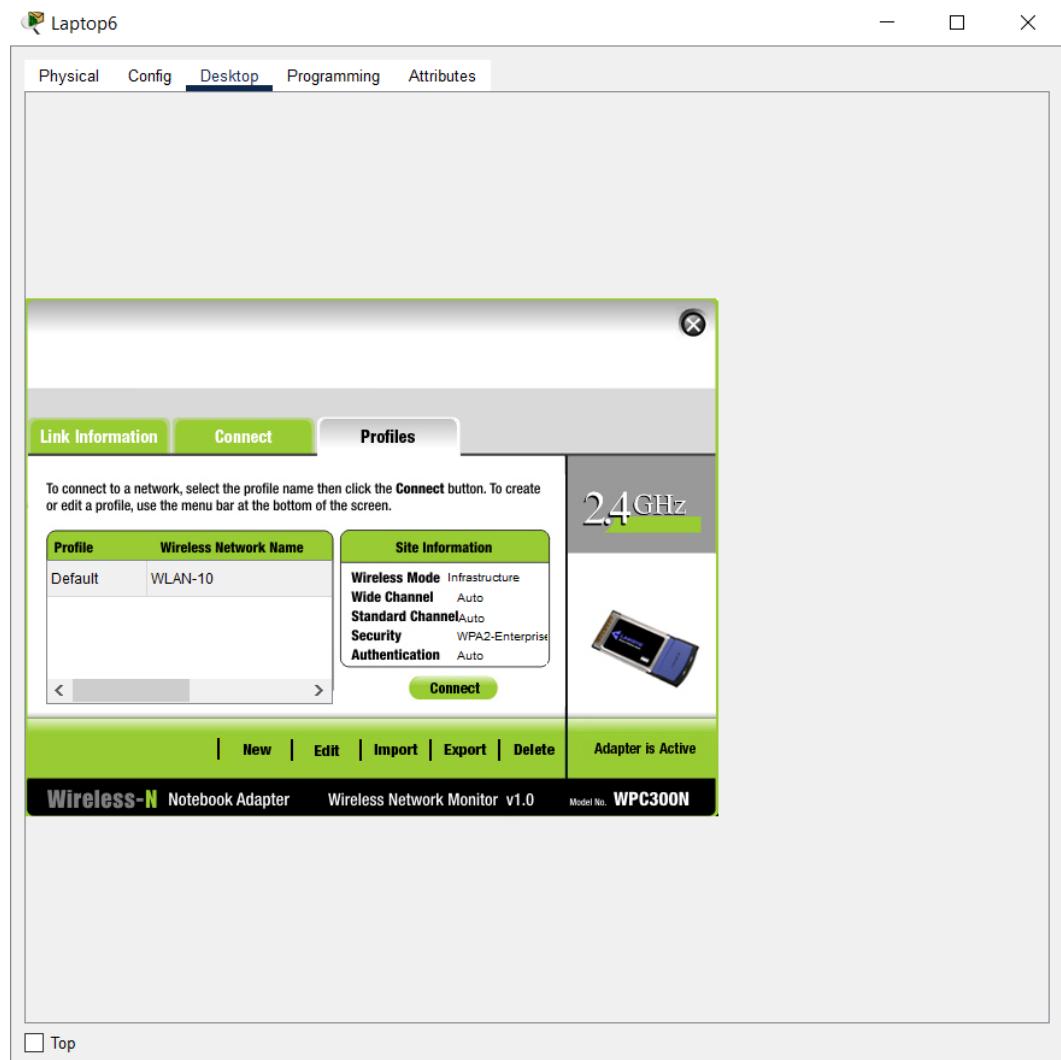
Chọn một Laptop bất kỳ đã gắn WPC300N

Vào Desktop > PC Wireless



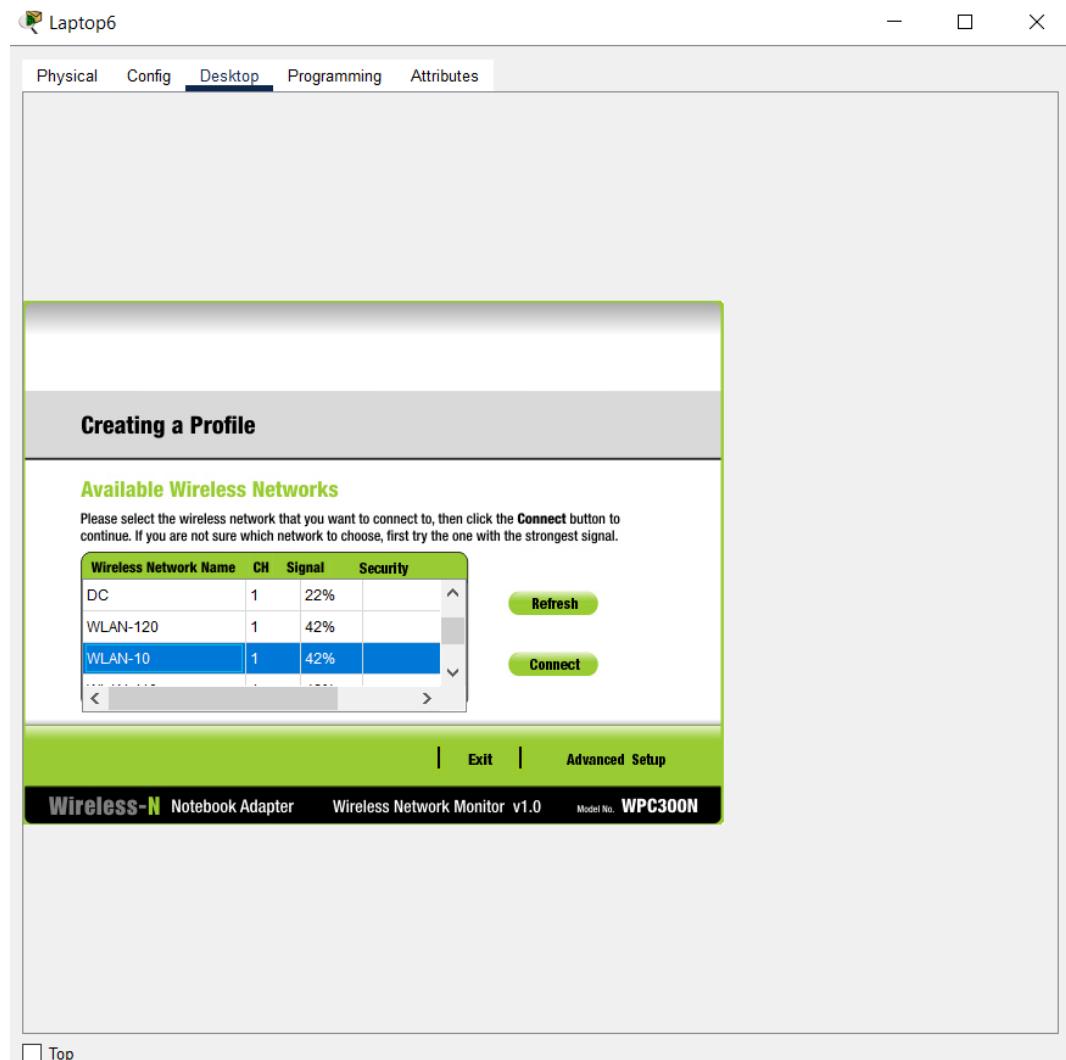
Hình 5.7. 34 Giao diện PC Wireless

Chọn Profiles > chọn WLAN-10 > Edit



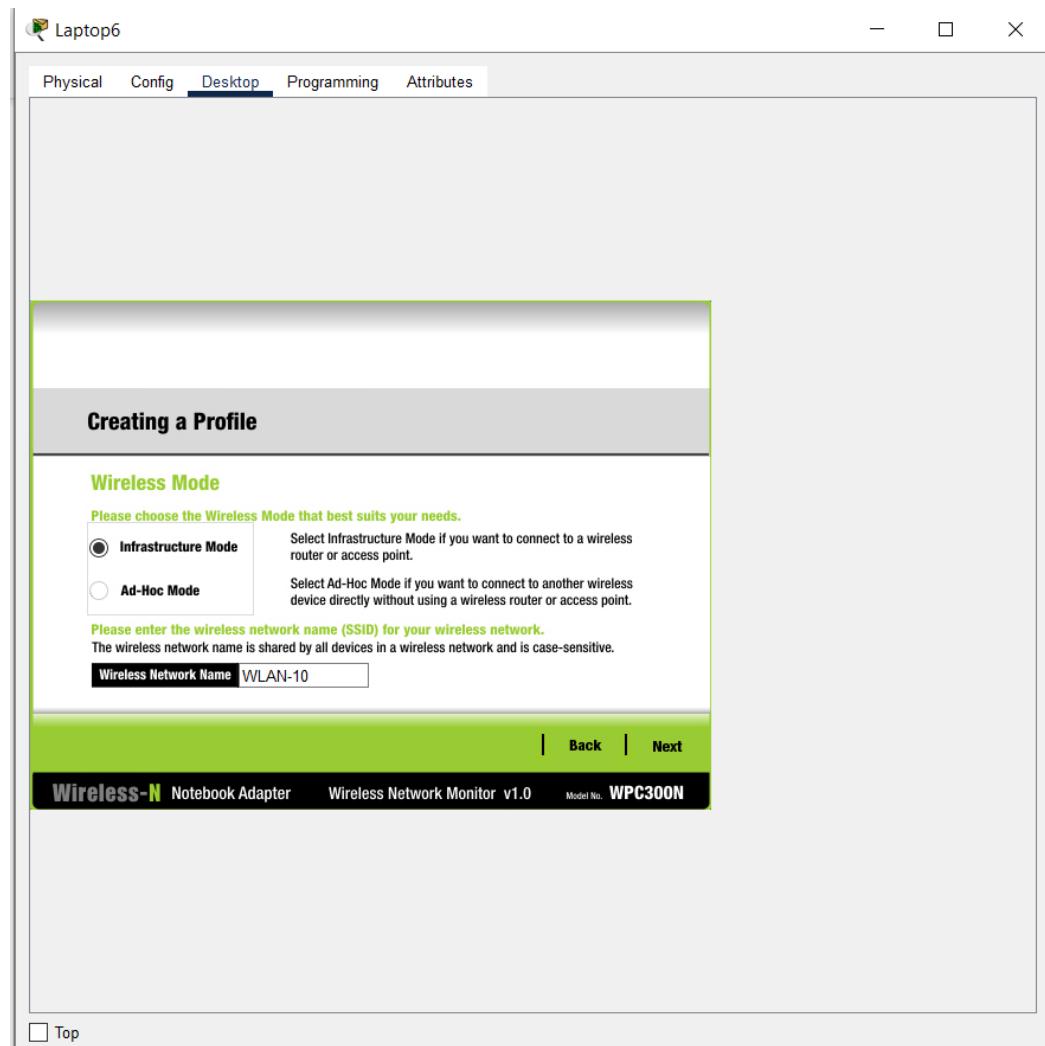
Hình 5.7. 35 Giao diện Profiles

Tại Edit, chọn WLAN-10 > Advanced Setup



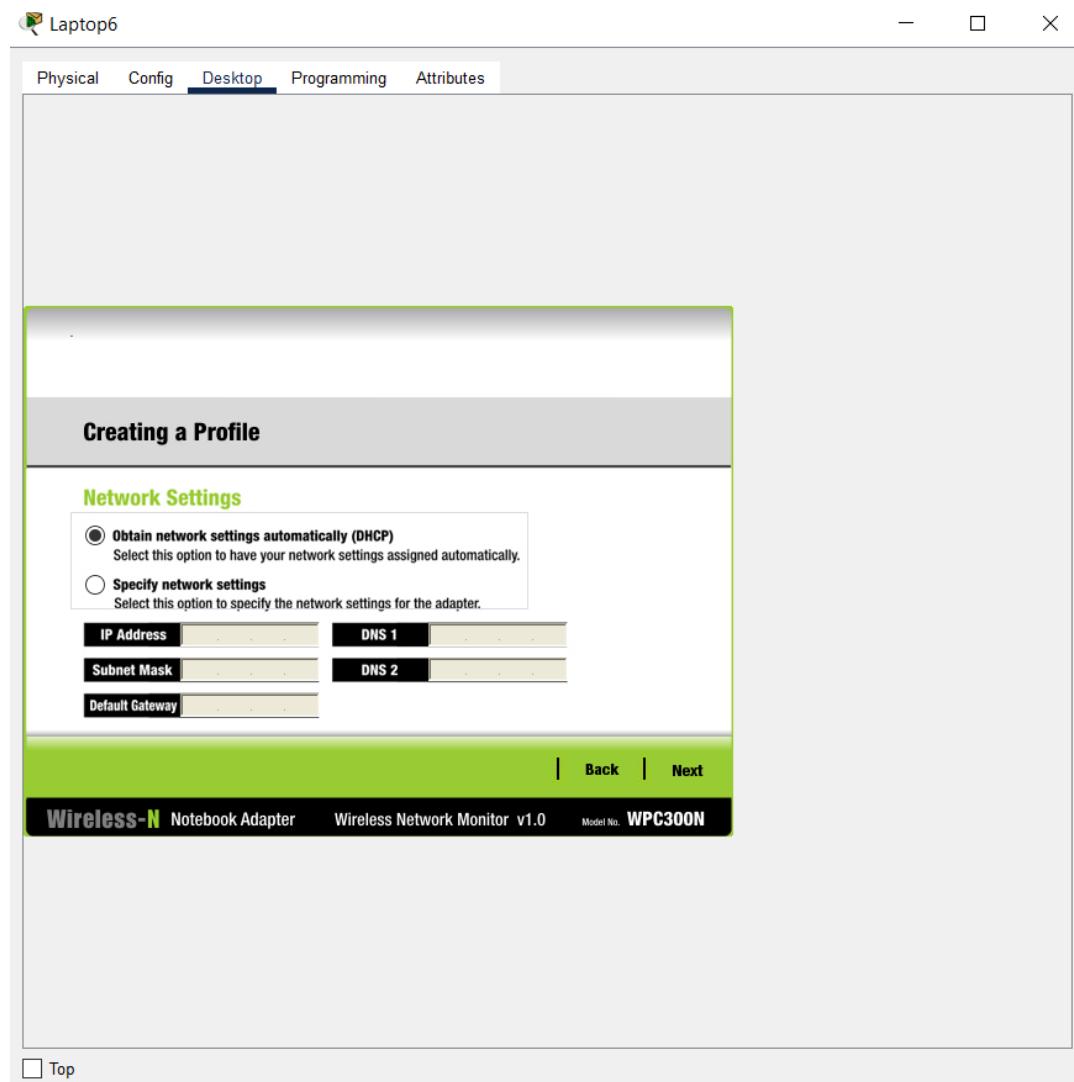
Hình 5.7. 36 Tạo một Profile là WLAN-10

Wireless Network Name sẽ tự động cập nhật là WLAN-10, nhấn Next để tiếp tục



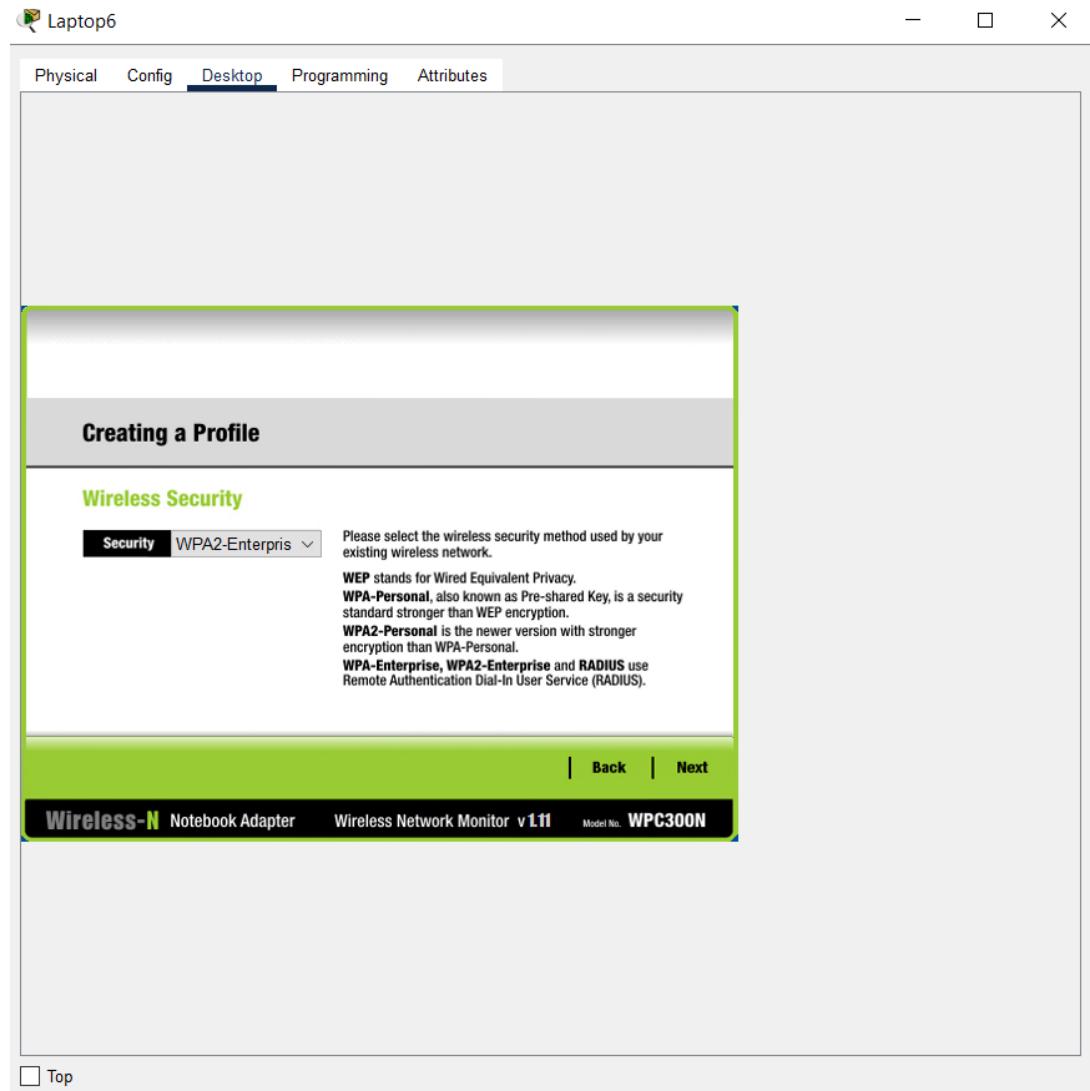
Hình 5.7. 37 Cập nhật tự động Wireless Network Name

Tiếp tục nhấn Next



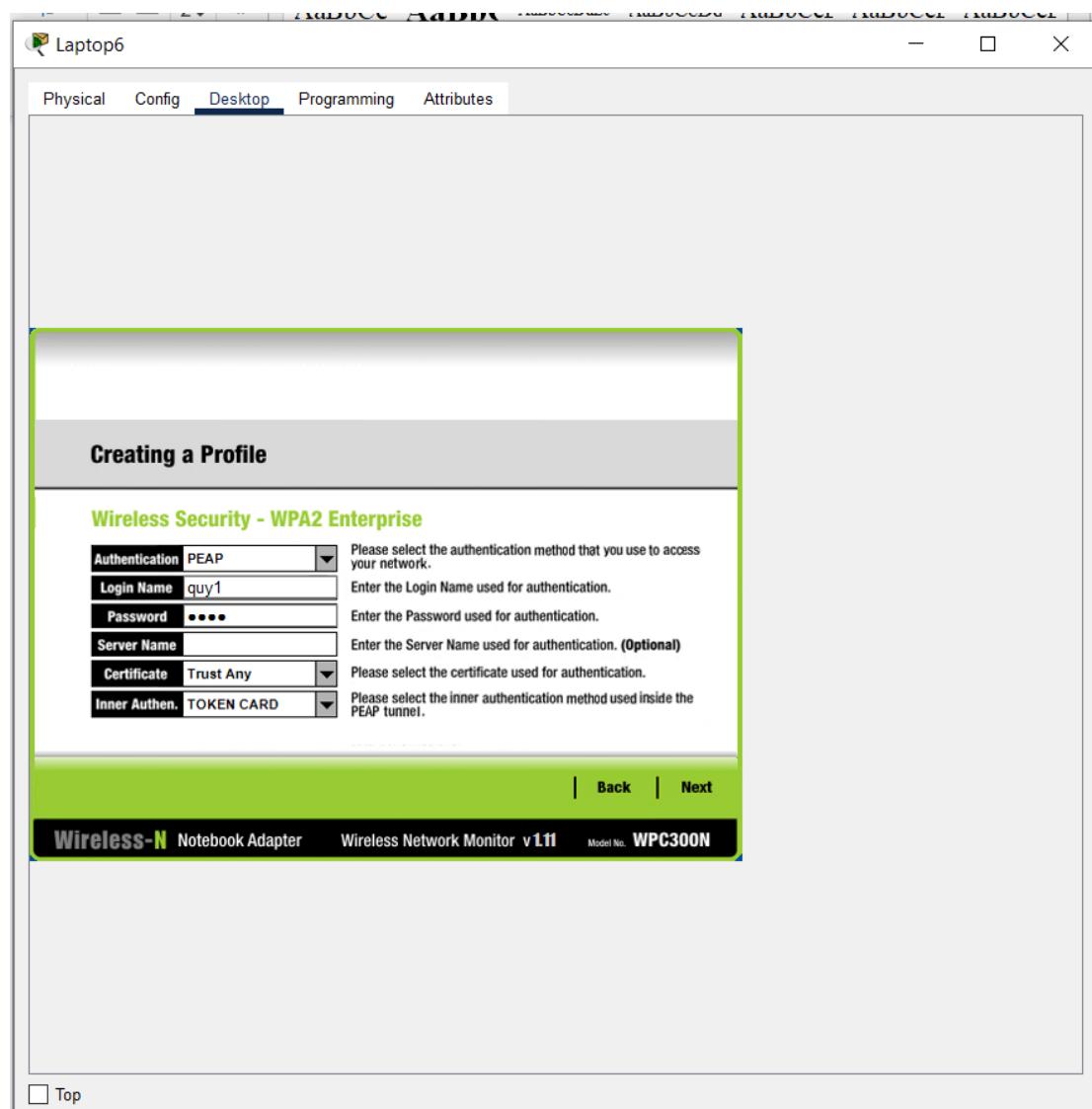
Hình 5.7. 38 Nhận cài đặt IP tự động theo DHCP

Tại mục Security chọn chuẩn WPA2-Enterpris, rồi tiếp tục Next



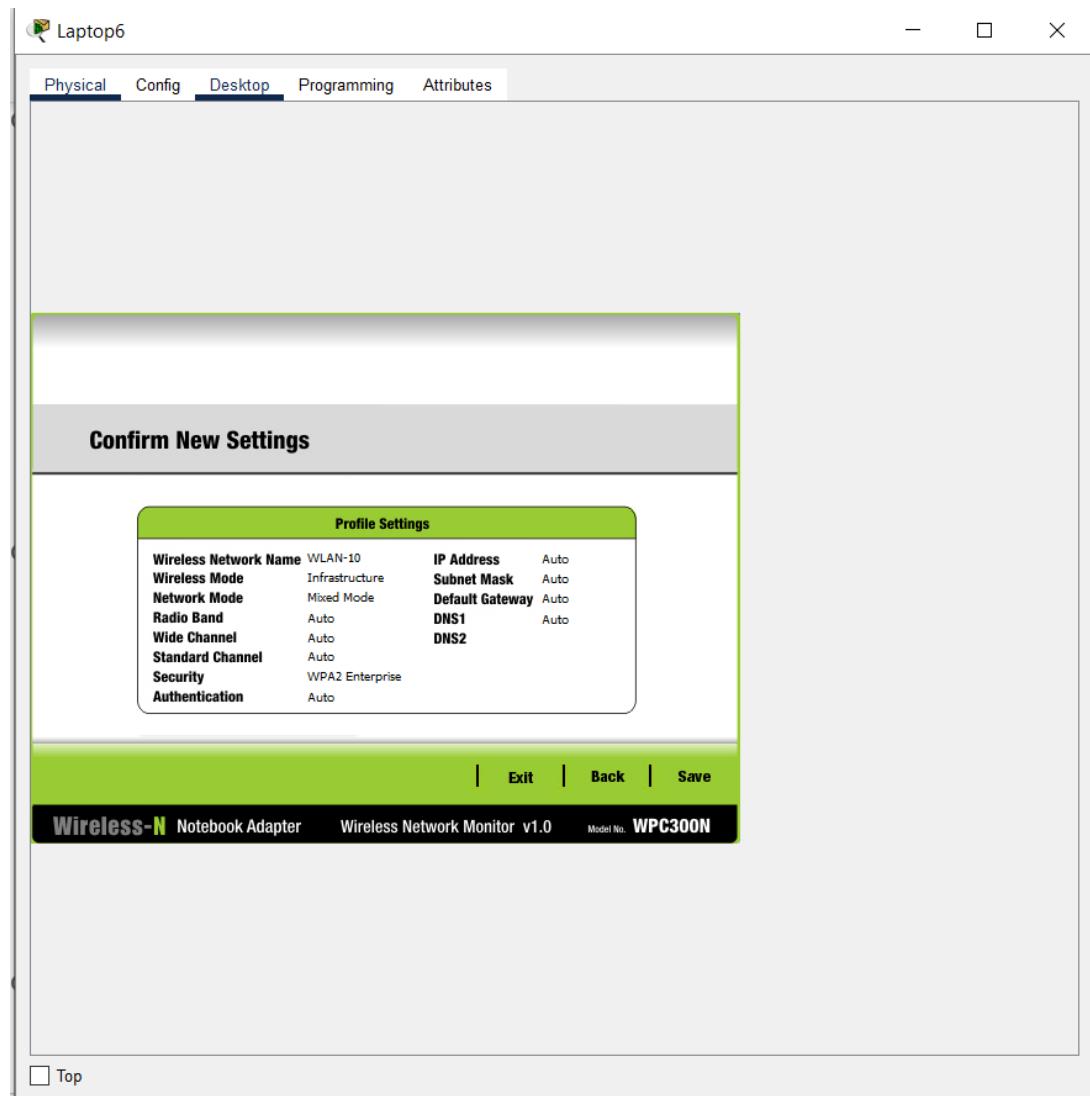
Hình 5.7. 39 Chọn chuẩn bảo mật là WPA2-Enterprise

Tại đây, nhập Login Name là quy1 và Password là quy1, sau đó nhấn Next

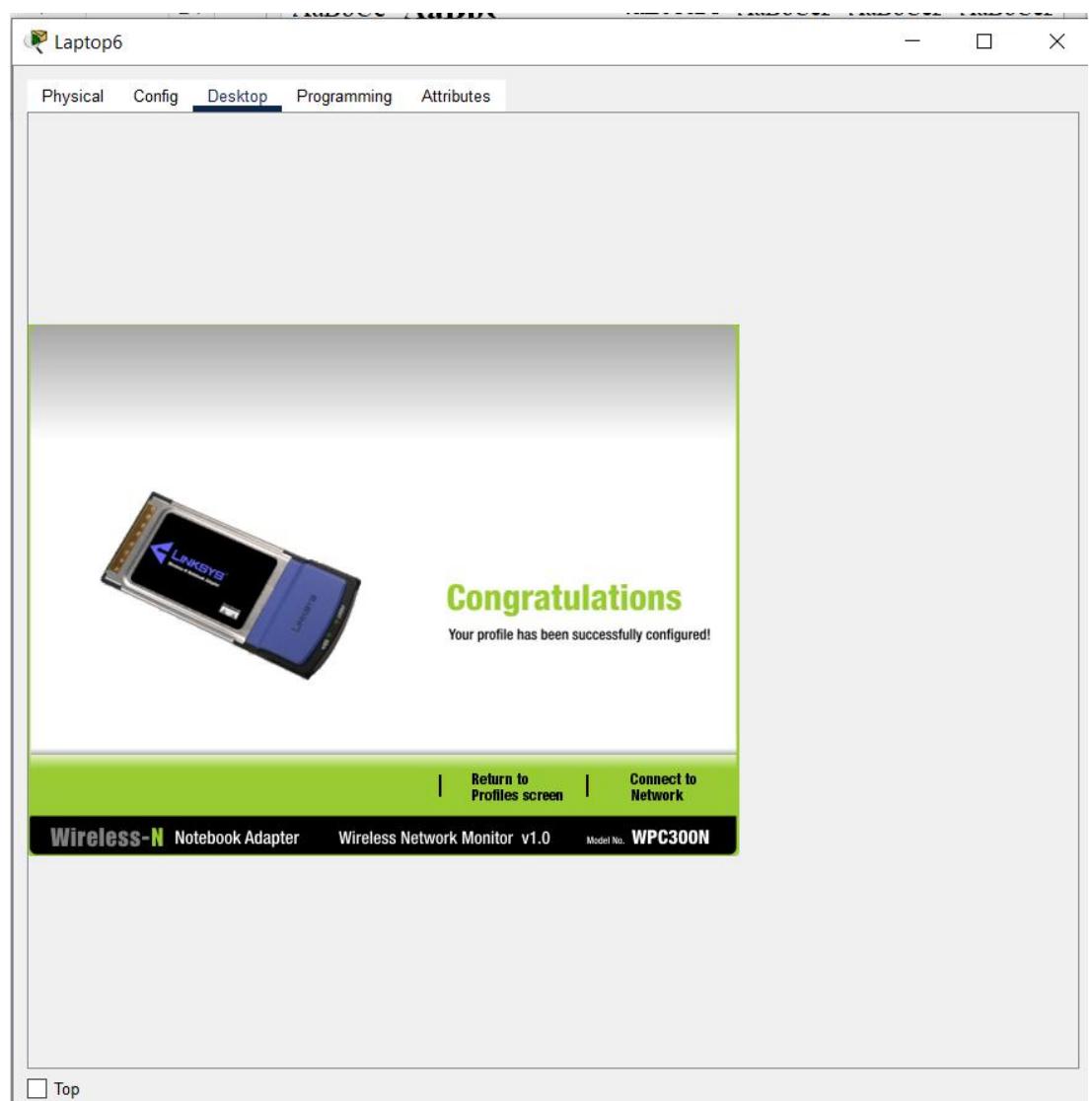


Hình 5.7. 40 Nhập Login Name và Password

Nhấn Save

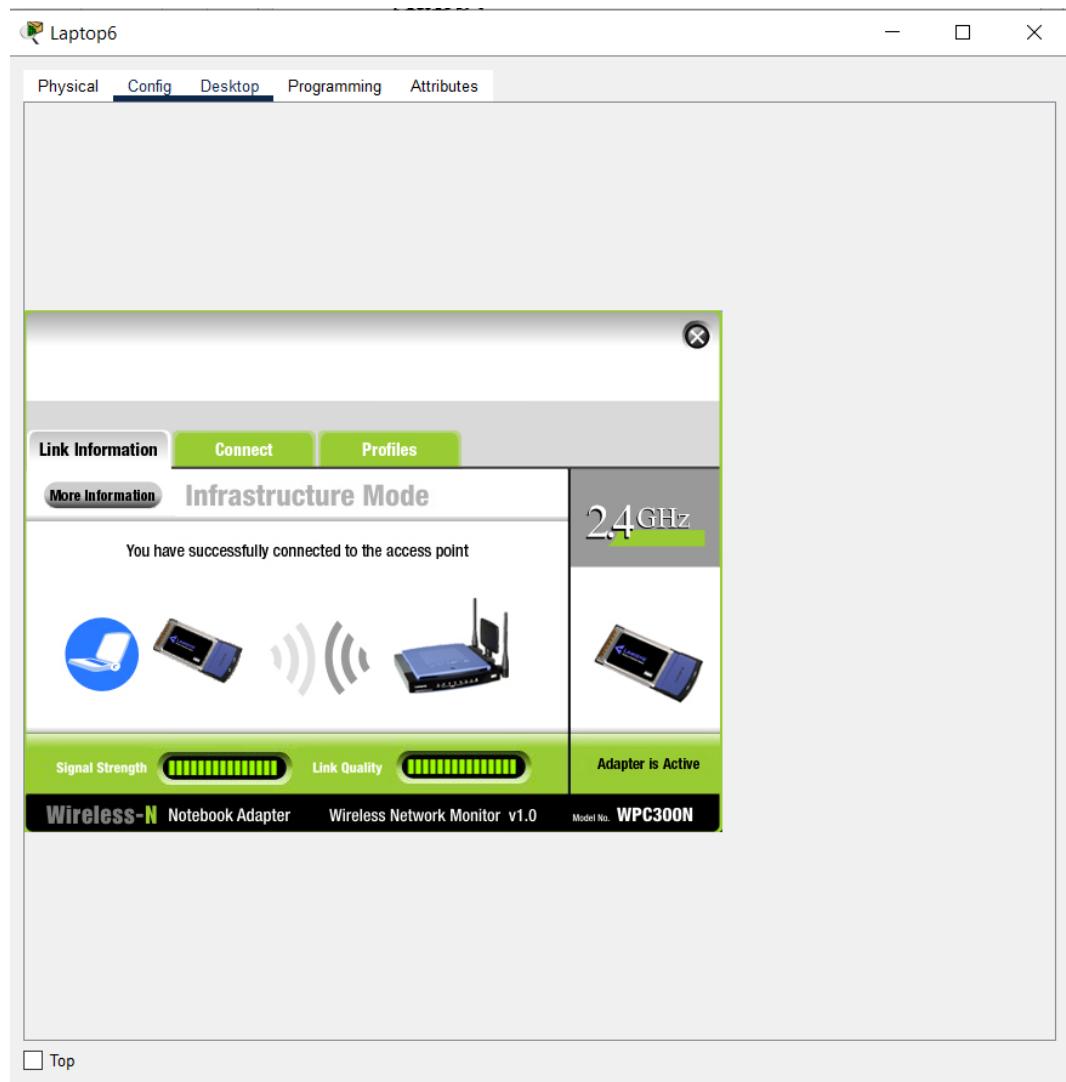


Hình 5.7. 41 Bảng thông tin Cài đặt
Nhân Connect to Network



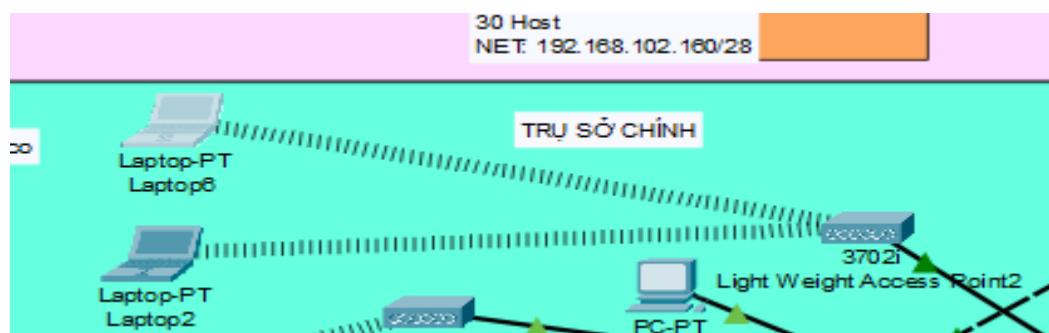
Hình 5.7. 42 Tạo thành công một card mạng

Kết nối thành công



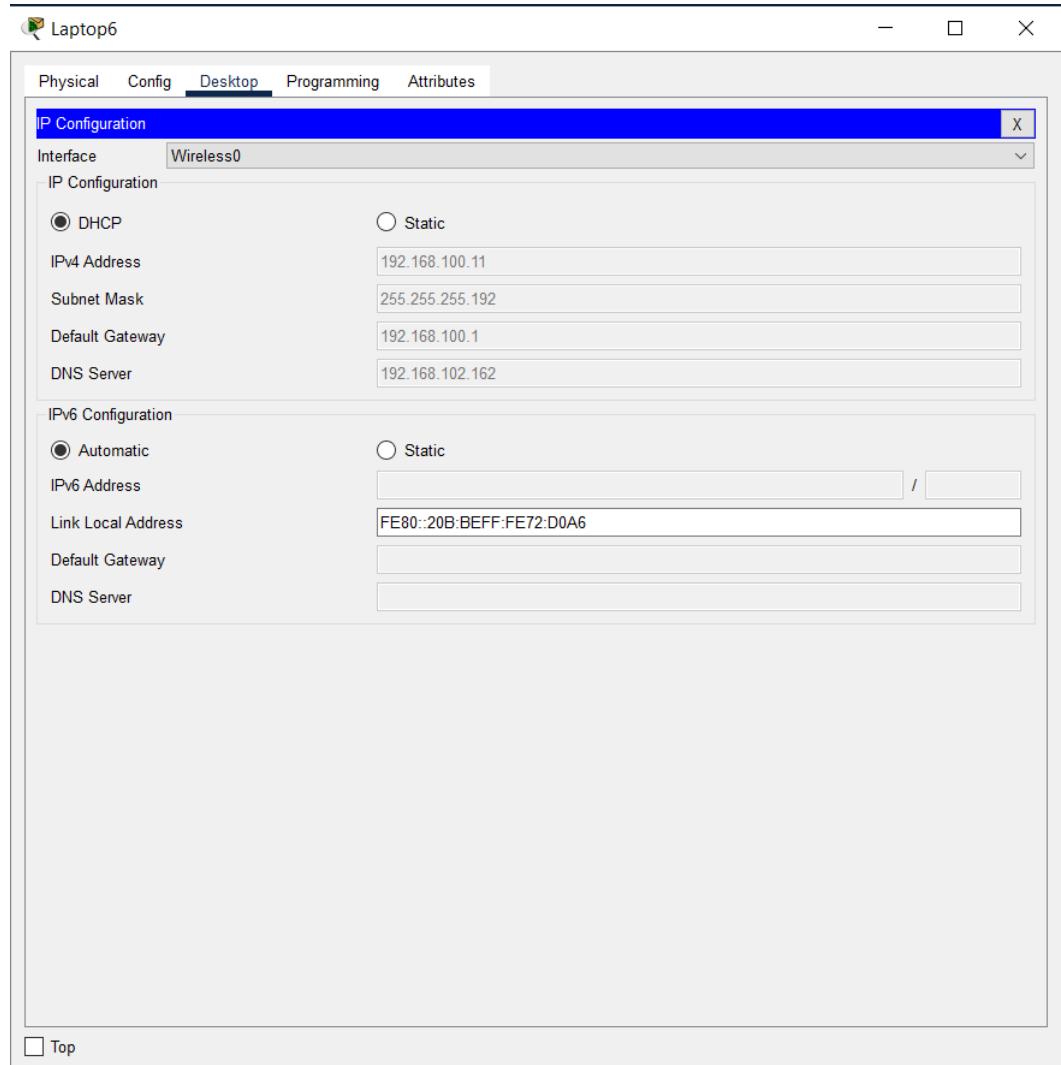
Hình 5.7. 43 Kết nối thành công đến các thiết bị khác

PC6 đã kết nối đến Light Weight Access Point



Hình 5.7. 44 Laptop6 kết nối đến Light Weight Access Point2

Địa chỉ IP được cập nhật đúng với VLAN 10



Hình 5.7. 45 Cập nhật IP động cho Laptop 6 thành công

5.8 Cấu hình PAT

HQ-ROUTER

```
HQ-ROUTER(config)#interface Serial0/2/0
```

```
HQ-ROUTER(config-if)#clock rate 64000
```

```
HQ-ROUTER(config-if)#exit
```

```
HQ-ROUTER(config)#interface Serial0/2/1
```

```
HQ-ROUTER(config-if)#clock rate 64000
```

```
HQ-ROUTER(config-if)#exit

HQ-ROUTER(config)#interface Serial0/1/0

HQ-ROUTER(config-if)#clock rate 64000

HQ-ROUTER(config-if)#exit

HQ-ROUTER(config)#do wr

HQ-ROUTER(config)#interface serial 0/1/0

HQ-ROUTER(config-if)#ip nat out

HQ-ROUTER(config-if)#ip nat outside

HQ-ROUTER(config-if)#exit

HQ-ROUTER(config)#int

HQ-ROUTER(config)#interface se

HQ-ROUTER(config)#interface serial 0/2/1

HQ-ROUTER(config-if)#ip nat outside

HQ-ROUTER(config-if)#exit

HQ-ROUTER(config)#do wr

HQ-ROUTER(config)#interface range gigabitEthernet 0/0-2

HQ-ROUTER(config-if-range)#ip nat inside

HQ-ROUTER(config-if-range)#exit

HQ-ROUTER(config)#do wr
```

```
HQ-ROUTER(config)#ip nat inside source list 1 interface serial 0/1/0  
overload
```

```
HQ-ROUTER(config)#ip nat inside source list 1 interface serial 0/2/1  
overload
```

```
HQ-ROUTER(config)#do wr
```

```
HQ-ROUTER(config)#access-list 1 permit 192.168.100.0 0.0.0.63
```

```
HQ-ROUTER(config)#access-list 1 permit 192.168.100.64 0.0.0.63
```

```
HQ-ROUTER(config)#access-list 1 permit 192.168.100.128 0.0.0.63
```

```
HQ-ROUTER(config)#access-list 1 permit 192.168.100.192 0.0.0.63
```

```
HQ-ROUTER(config)#access-list 1 permit 192.168.101.0 0.0.0.63
```

```
HQ-ROUTER(config)#access-list 1 permit 192.168.101.64 0.0.0.63
```

```
HQ-ROUTER(config)#do wr
```

BR-ROUTER

```
BR-ROUTER(config)#interface Serial0/2/0
```

```
BR-ROUTER(config-if)#clock rate 64000
```

```
BR-ROUTER(config-if)#exit
```

```
BR-ROUTER(config)#interface Serial0/1/1
```

```
BR-ROUTER(config-if)#clock rate 64000
```

```
BR-ROUTER(config-if)#exit
```

```
BR-ROUTER(config)#do wr
```

```
BR-ROUTER(config)#interface serial 0/2/0  
  
BR-ROUTER(config-if)#ip nat outside  
  
BR-ROUTER(config-if)#exit  
  
BR-ROUTER(config)#interface serial 0/1/1  
  
BR-ROUTER(config-if)#ip nat outside  
  
BR-ROUTER(config-if)#exit  
  
BR-ROUTER(config)#do wr  
  
BR-ROUTER(config)#interface range gigabitEthernet 0/0-1  
  
BR-ROUTER(config-if-range)#ip nat inside  
  
BR-ROUTER(config-if-range)#exit  
  
BR-ROUTER(config)#do wr  
  
BR-ROUTER(config)#ip nat inside source list 1 interface serial 0/2/0 overload  
  
BR-ROUTER(config)#ip nat inside source list 1 interface serial 0/1/1 overload  
  
BR-ROUTER(config)#do wr  
  
BR-ROUTER(config)#access-list 1 permit 192.168.101.128 0.0.0.31  
  
BR-ROUTER(config)#access-list 1 permit 192.168.101.160 0.0.0.31  
  
BR-ROUTER(config)#access-list 1 permit 192.168.101.192 0.0.0.31  
  
BR-ROUTER(config)#access-list 1 permit 192.168.101.224 0.0.0.31  
  
BR-ROUTER(config)#access-list 1 permit 192.168.102.0 0.0.0.127
```

BR-ROUTER(config)#access-list 1 permit 192.168.102.128 0.0.0.31

BR-ROUTER(config)#do wr

5.9 Cấu hình Access Control List

HQ-ROUTER

HQ-ROUTER(config)#access-list 110 permit ip 192.168.100.0 0.0.0.255
192.168.101.128 0.0.0.127

HQ-ROUTER(config)#access-list 110 permit ip 192.168.100.0 0.0.0.255
192.168.102.0 0.0.0.255

HQ-ROUTER(config)#access-list 110 permit ip 192.168.101.0 0.0.0.127
192.168.101.128 0.0.0.127

HQ-ROUTER(config)#access-list 110 permit ip 192.168.101.0 0.0.0.127
192.168.102.0 0.0.0.255

HQ-ROUTER(config)#do wr

BR-ROUTER

BR-ROUTER(config)#access-list 110 permit ip 192.168.101.128 0.0.0.127
192.168.100.0 0.0.0.255

BR-ROUTER(config)#access-list 110 permit ip 192.168.101.128 0.0.0.127
192.168.101.0 0.0.0.127

BR-ROUTER(config)#access-list 110 permit ip 192.168.102.0 0.0.0.255
192.168.100.0 0.0.0.255

BR-ROUTER(config)#access-list 110 permit ip 192.168.102.0 0.0.0.255
192.168.101.0 0.0.0.127

```
BR-ROUTER(config)#do wr
```

5.10 Cấu hình bảo mật Site-to-site IPSec VPN

HQ-ROUTER

```
HQ-ROUTER(config)#license boot module c2900 technology-package securityk9
```

```
HQ-ROUTER(config)#do reload
```

```
HQ-ROUTER(config)#crypto isakmp policy 10
```

```
HQ-ROUTER(config-isakmp)#encryption aes 256
```

```
HQ-ROUTER(config-isakmp)#authentication pre-share
```

```
HQ-ROUTER(config-isakmp)#group 5
```

```
HQ-ROUTER(config-isakmp)#ex
```

```
HQ-ROUTER(config)#crypto isakmp key dtq address 192.168.102.194
```

```
HQ-ROUTER(config)#do wr
```

```
HQ-ROUTER(config)#crypto ipsec transform-set VPN-SK esp-aes esp-sha-hmac
```

```
HQ-ROUTER(config)#crypto map VPN-SK-MAP 10 ipsec-isakmp
```

```
HQ-ROUTER(config-crypto-map)#description VPN Sao Kim connects to Branch SaoKim Network.
```

```
HQ-ROUTER(config-crypto-map)#set peer 192.168.102.194
```

HQ-ROUTER(config-crypto-map)#set transform-set VPN-SK

HQ-ROUTER(config-crypto-map)#match address 110

HQ-ROUTER(config-crypto-map)#exit

HQ-ROUTER(config)#interface serial 0/2/0

HQ-ROUTER(config-if)#crypto map VPN-SK-MAP

HQ-ROUTER(config-if)#exit

HQ-ROUTER(config)#do wr

BR-ROUTER

BR-ROUTER(config)#license boot module c2900 technology-package securityk9

BR-ROUTER(config)#do reload

BR-ROUTER(config)#crypto isakmp policy 10

BR-ROUTER(config-isakmp)#encryption aes 256

BR-ROUTER(config-isakmp)#authentication pre-share

BR-ROUTER(config-isakmp)#group 5

BR-ROUTER(config-isakmp)#exit

BR-ROUTER(config)#crypto isakmp key dtq address 192.168.102.193

BR-ROUTER(config)#do wr

```
BR-ROUTER(config)#crypto ipsec transform-set VPN-SK esp-aes esp-sha-hmac
```

```
BR-ROUTER(config)#crypto map VPN-SK-MAP 10 ipsec-isakmp
```

```
BR-ROUTER(config-crypto-map)#description VPN connection to Sao Kim Headquarters.
```

```
BR-ROUTER(config-crypto-map)#set peer 192.168.102.193
```

```
BR-ROUTER(config-crypto-map)#set transform-set VPN-SK
```

```
BR-ROUTER(config-crypto-map)#match address 110
```

```
BR-ROUTER(config-crypto-map)#exit
```

```
BR-ROUTER(config)#interface serial 0/1/0
```

```
BR-ROUTER(config-if)#crypto map VPN-SK-MAP
```

```
BR-ROUTER(config-if)#exit
```

```
BR-ROUTER(config)#do wr
```

5.11 Cấu hình Default/Static Route

HQ-M-SW1

```
HQ-Mul-SW-1(config)#ip route 0.0.0.0 0.0.0.0 192.168.102.178
```

HQ-M-SW2

```
HQ-Mul-SW-2(config)#ip route 0.0.0.0 0.0.0.0 192.168.102.182
```

BR-M-SW1

```
BR-Mul-SW-3(config)#ip route 0.0.0.0 0.0.0.0 192.168.102.186
```

BR-M-SW2

```
BR-Mul-SW-4(config)#ip route 0.0.0.0 0.0.0.0 192.168.102.190
```

HQ-R

```
HQ-ROUTER(config)#ip route 0.0.0.0 0.0.0.0 195.136.17.18
```

```
HQ-ROUTER(config)#ip route 0.0.0.0 0.0.0.0 195.136.17.22 70
```

BR-R

```
HQ-ROUTER(config)#ip route 0.0.0.0 0.0.0.0 195.136.17.29
```

```
HQ-ROUTER(config)#ip route 0.0.0.0 0.0.0.0 195.136.17.25 70
```

5.12 Cấu hình Spanning Tree (STP)**HQ-Multilayer-SW-1**

```
spanning-tree mode rapid
```

```
spanning-tree vlan 10 root primary
```

```
spanning-tree vlan 20 root primary
```

```
spanning-tree vlan 30 root primary
```

```
spanning-tree vlan 40 root secondary
```

```
spanning-tree vlan 50 root secondary
```

```
spanning-tree vlan 60 root secondary
```

```
spanning-tree vlan 140 root primary
```

```
end
```

write

HQ-Multilayer-SW-2

spanning-tree mode rapid

spanning-tree vlan 40 root primary

spanning-tree vlan 50 root primary

spanning-tree vlan 60 root primary

spanning-tree vlan 10 root secondary

spanning-tree vlan 20 root secondary

spanning-tree vlan 30 root secondary

spanning-tree vlan 140 root secondary

end

write

BR-Multilayer-SW-1

spanning-tree mode rapid

spanning-tree vlan 80 root primary

spanning-tree vlan 90 root primary

spanning-tree vlan 100 root primary

spanning-tree vlan 110 root secondary

spanning-tree vlan 120 root secondary

spanning-tree vlan 130 root secondary

spanning-tree vlan 150 root primary

end

write

BR-Multilayer-SW-2

spanning-tree mode rapid

spanning-tree vlan 110 root primary

spanning-tree vlan 120 root primary

spanning-tree vlan 130 root primary

spanning-tree vlan 80 root secondary

spanning-tree vlan 90 root secondary

spanning-tree vlan 100 root secondary

spanning-tree vlan 150 root secondary

end

write

TÀI LIỆU THAM KHẢO

- [1]. Slide
- [2]. CCNA_200-301_Official_Cert_Guide.pdf
- [3]. ITN_Module_11-IPv4 Addressing.pdf
- [4]. ITN_Module_7-Ethernet Switching
- [5]. ITN_Module_10-Basic Router Configuration
- [6]. ITN_Module_16-Network Security Fundamentals
- [7]. vdocuments.net_ccna-book
- [8]. CCNA_Wireless_Official_Certification_Guide
- [9]. Data Link Layer - Ethernet LAN - ARP - Physical.pdf
- [10]. VLAN, TRUNK, VTP.pdf
- [11]. STP - RSTP - Portfast.pdf
- [12]. Port Security, VLAN Hopping, SPAN, BPDU Guard
- [13]. NAT.pdf
- [14]. VPN.pdf
- [15]. Wireless Fundamental + Architecture