

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



**MÔN AN TOÀN MẠNG KHÔNG DÂY  
VÀ DI ĐỘNG**

**Xây dựng hệ thống mạng  
cho doanh nghiệp**

**Người hướng dẫn: TS. BÙI QUY ANH  
Họ và tên: Võ Mạnh Cường - 52200319  
Lớp: 22050401**

**HỒ CHÍ MINH – 2025**

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



**MÔN AN TOÀN MẠNG KHÔNG DÂY  
VÀ DI ĐỘNG**

**Xây dựng hệ thống mạng  
cho doanh nghiệp**

**Người hướng dẫn: TS. BÙI QUY ANH  
Họ và tên: Võ Mạnh Cường - 52200319  
Lớp: 22050401**

**HỒ CHÍ MINH – 2025**

## LỜI CẢM ƠN

Chúng em xin chân thành gửi lời cảm ơn sâu sắc đến TS. Bùi Quy Anh đã tận tình giảng dạy, hỗ trợ và truyền đạt kiến thức trong suốt quá trình học tập. Nhờ sự hướng dẫn của thầy, em đã xây dựng được nền tảng lý thuyết vững chắc để hoàn thành bài báo cáo cuối kì.

Tuy nhiên chúng em còn hạn chế nhiều về môn *An toàn mạng không dây và di động* nên không thể tránh khỏi những thiếu sót trong quá trình hoàn thành bài báo cáo cuối kỳ này. Mong thầy xem và góp ý để bài báo cáo của em được cải thiện hơn.

Em xin chân thành cảm ơn thầy vì đã hỗ trợ em trong quá trình thực hiện bài báo cáo này!

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

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

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

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

*TP.Hồ Chí Minh, ngày 21 tháng 5 năm 2025*

*Tác giả*

*(ký và ghi rõ họ tên)*

*Võ Mạnh Cường*

## TÓM TẮT

Báo cáo này trình bày quá trình thiết kế và triển khai hệ thống mạng doanh nghiệp cho công ty Chooky, tích hợp đồng thời giao thức IPv4 và IPv6, đáp ứng các yêu cầu về kết nối, định tuyến, chuyển mạch, phân phối địa chỉ và bảo mật. Đối với IPv4, hệ thống được cấu hình với các kết nối điểm-điểm (PPP), GRE tunnel, định tuyến nội bộ (OSPF, EIGRP), chuyển mạch VLAN, NAT, DHCP và kiểm soát truy cập qua ACL. Đối với IPv6, các cấu hình bao gồm gán địa chỉ, định tuyến động (EIGRPv6) và tĩnh, cùng phân phối địa chỉ tự động thông qua DHCPv6.

Hệ thống mạng đã được kiểm tra kỹ lưỡng, vận hành ổn định, đảm bảo kết nối thông suốt giữa các khu vực (trụ sở, chi nhánh, và từ xa), cung cấp dịch vụ mạng đáng tin cậy và bảo vệ dữ liệu nhạy cảm thông qua các biện pháp bảo mật như WPA2/WPA3, 802.1X, và VPN. Báo cáo đề xuất các giải pháp mở rộng, bao gồm tích hợp IPsec cho GRE tunnel và NAT64 để tăng cường tương thích IPv4/IPv6, tạo nền tảng cho các hệ thống mạng hiện đại, dễ mở rộng trong tương lai.

# Mục lục

<b>CHƯƠNG 1</b>	<b>Giới thiệu chung</b>	<b>1</b>
	Mục tiêu báo cáo	1
	Khảo sát quy mô và yêu cầu của doanh nghiệp	2
	Dữ liệu cần bảo vệ	3
<b>CHƯƠNG 2</b>	<b>Cơ sở lý thuyết</b>	<b>5</b>
2.1	Tổng quan về hệ thống mạng doanh nghiệp	5
2.2	Lý thuyết mạng có dây	6
2.2.1	Sơ đồ địa chỉ và phân bổ IP (IPv4)	6
2.2.2	Kết nối PPP (Point-to-Point Protocol)	7
2.2.3	Tunneling GRE (Generic Routing Encapsulation)	9
2.2.4	Định tuyến	9
2.2.5	Chuyển mạch	11
2.2.6	NAT và DHCP	13
2.2.7	ACL (Access Control List)	14
2.3	Lý thuyết IPv6	15
2.3.1	Sơ đồ địa chỉ IPv6	15
2.3.2	Định tuyến IPv6	16
2.3.3	DHCPv6	17
2.4	Lý thuyết mạng không dây	18
2.4.1	Tổng quan mạng không dây (WLAN)	18
2.4.2	Chuẩn WiFi (IEEE 802.11)	20
2.4.3	Kiến trúc mạng WiFi	22
2.4.4	Mô hình Mesh WiFi và Range Extender	23

2.4.5 Bảo mật mạng WiFi . . . . .	25
2.5 VPN (Virtual Private Network) . . . . .	27
2.6 Mô hình OSI và TCP/IP . . . . .	30
2.6.1 Mô hình OSI . . . . .	30
2.6.2 Mô hình TCP/IP . . . . .	33
<b>CHƯƠNG 3 Sơ đồ mạng tổng thể . . . . .</b>	<b>35</b>
3.1 Sơ đồ mạng (Network Diagram) . . . . .	35
3.2 Mô hình thiết kế hệ thống mạng khu vực HQ . . . . .	39
3.2.1 Kiến trúc tổng thể . . . . .	39
3.2.2 Phân tích thiết kế . . . . .	40
3.2.3 Loại thiết bị . . . . .	41
3.2.4 Bố trí không gian . . . . .	44
3.2.5 Tính toán suy hao mạng không dây . . . . .	45
3.2.6 Phân tích độ phủ sóng (Heatmap) . . . . .	48
3.2.7 Yêu cầu kỹ thuật . . . . .	49
3.3 Kế hoạch địa chỉ IPv4 . . . . .	49
3.4 Kế hoạch địa chỉ IPv6 . . . . .	51
3.5 Giải pháp bảo mật . . . . .	52
3.5.1 Tổng quan giải pháp bảo mật . . . . .	53
3.5.2 An ninh vật lý . . . . .	54
3.5.3 Phân vùng mạng và kiểm soát truy cập . . . . .	55
3.5.4 Bảo mật mạng không dây . . . . .	56
3.5.5 Bảo mật VPN . . . . .	57
3.5.6 Quản lý truy cập từ xa . . . . .	58
3.5.7 Phát hiện và ngăn chặn tấn công . . . . .	59
3.5.8 Quản lý người dùng . . . . .	60
3.5.9 Giám sát và phản ứng sự cố . . . . .	61
3.5.10 Ứng dụng trong kịch bản Chooky . . . . .	62
<b>CHƯƠNG 4 Mô tả cấu hình hệ thống - IPv4 . . . . .</b>	<b>64</b>

4.1 Cấu hình địa chỉ IPv4 . . . . .	64
4.2 Cấu hình xác thực PPP . . . . .	67
4.3 Cấu hình Tunneling GRE . . . . .	68
4.4 Cấu hình định tuyến . . . . .	69
4.5 Cấu hình chuyển mạch . . . . .	75
4.6 Cấu hình NAT và DHCP . . . . .	79
4.7 Cấu hình ACL và yêu cầu khác . . . . .	81
<b>CHƯƠNG 5 Mô tả cấu hình mạng không dây . . . . .</b>	<b>85</b>
5.1 Cấu hình chuẩn bị . . . . .	85
5.2 Cấu hình mạng không dây . . . . .	86
5.2.1 Cấu hình Radius Server - Xác thực AAA . . . . .	87
5.2.2 Cấu hình Interface WLANs . . . . .	89
5.2.3 Cấu hình Interface WLANs . . . . .	90
5.2.4 Cấu hình bảo mật SSID . . . . .	93
5.2.5 Cấu hình mạng không dây khu vực REMOTE . . . . .	97
5.3 Cấu hình VPN . . . . .	97
<b>CHƯƠNG 6 Mô tả cấu hình hệ thống - IPv6 . . . . .</b>	<b>101</b>
6.1 Cấu hình địa chỉ IPv6 . . . . .	101
6.2 Định tuyến IPv6 . . . . .	104
6.3 Cấu hình DHCPv6 . . . . .	109
<b>CHƯƠNG 7 Kết quả đạt được mạng có dây . . . . .</b>	<b>111</b>
7.1 Cấu hình xác thực kết nối PPP . . . . .	111
7.2 Kết quả cấu hình GRE tunnel . . . . .	112
7.3 Kết quả cấu hình định tuyến IPv4 . . . . .	113
7.4 Kết quả cấu hình chuyển mạch . . . . .	115
7.5 Kết quả cấu hình NAT và DHCP . . . . .	117
7.6 Kết quả cấu hình ACL . . . . .	119
7.7 Kết quả cấu hình IPv6 và DHCPv6 . . . . .	121



<b>CHƯƠNG 8</b>	<b>Kết quả đạt được mạng không dây . . . .</b>	<b>.123</b>
8.1	Kết quả mạng không dây khu vực HQ . . . . .	123
8.2	Kết quả đạt được VPN . . . . .	130
<b>KẾT LUẬN</b>	<b>. . . . .</b>	<b>.132</b>
<b>TÀI LIỆU THAM KHẢO</b>	<b>. . . . .</b>	<b>.134</b>

# Danh sách hình vẽ

Hình 3.1.	Sơ đồ tổng quan hệ thống mạng . . . . .	35
Hình 3.2.	Sơ đồ tầng 1 . . . . .	44
Hình 3.3.	Sơ đồ tầng 2 . . . . .	45
Hình 3.4.	Sơ đồ phủ sóng tầng 1 . . . . .	46
Hình 3.5.	Sơ đồ phủ sóng tầng 2 . . . . .	47
Hình 5.1.	Minh họa cấu hình port trunk. . . . .	85
Hình 5.2.	Cấu hình IP cho WLC và LAP. . . . .	86
Hình 5.3.	Đăng nhập vào WLC. . . . .	86
Hình 5.4.	Đăng nhập vào được WLC. . . . .	87
Hình 5.5.	Kiểm tra kết nối các LAP. . . . .	87
Hình 5.6.	Cấu hình thông tin Radius AAA trên WLC. . . . .	88
Hình 5.7.	Hoàn tất cấu hình Radius trên WLC. . . . .	88
Hình 5.8.	Cấu hình xác thực AAA trên Server. . . . .	89
Hình 5.9.	Cấu hình tài khoản truy cập. . . . .	89
Hình 5.10.	Truy cập menu WLANs. . . . .	89
Hình 5.11.	Tạo WLANs. . . . .	90
Hình 5.12.	Tạo thành công 4 WLANs. . . . .	90
Hình 5.13.	Truy cập Interfaces trong Controller. . . . .	90
Hình 5.14.	Tạo interface WLANs. . . . .	91
Hình 5.15.	Cấu hình thông tin Interface WLAN. . . . .	92
Hình 5.16.	Cấu hình hoàn tất các Interface WLAN. . . . .	93
Hình 5.17.	Truy cập menu WLANs. . . . .	93
Hình 5.18.	Cấu hình bảo mật cho Marketing. . . . .	93
Hình 5.19.	Cấu hình bảo mật cho Marketing. . . . .	94

Hình 5.20. Cấu hình bảo mật cho Marketing. . . . .	94
Hình 5.21. Cấu hình bảo mật cho Marketing. . . . .	95
Hình 5.22. Cấu hình bảo mật cho IoT. . . . .	96
Hình 5.23. Không bảo mật cho wifi GUEST. . . . .	96
Hình 5.24. Hoàn thành cấu hình bảo mật WLANs. . . . .	96
Hình 5.25. Mô phỏng mạng không dây khu vực REMOTE. . . . .	97
Hình 7.1. Kết quả cấu hình PPP PAP trên R7 và R6. . . . .	111
Hình 7.2. Kết quả cấu hình PPP CHAP trên R7 và R8. . . . .	111
Hình 7.3. Thông mạng R7 đến R6 và R8. . . . .	112
Hình 7.4. Kết quả trạng thái GRE tunnel trên R6 và R8. . . . .	112
Hình 7.5. Thông mạng R6 và R8 trên GRE Tunnel. . . . .	112
Hình 7.6. Miền OSPF trên R1, R2, R3 và R5. . . . .	113
Hình 7.7. Bảng định tuyến trên Router R5. . . . .	113
Hình 7.8. Kết quả thông mạng khu vực chi nhánh ra Internet . . . .	114
Hình 7.9. Bảng định tuyến trên Router R4. . . . .	114
Hình 7.10. Bảng định tuyến trên Router R7. . . . .	115
Hình 7.11. Thông mạng từ R6 và R8 ra Internet. . . . .	115
Hình 7.12. Kết quả cấu hình EtherChannel. . . . .	116
Hình 7.13. Kết quả cấu hình Spanning-tree. . . . .	116
Hình 7.14. Kết quả cấu hình VTP Client-Server. . . . .	116
Hình 7.15. Kết quả cấu hình SSH. . . . .	116
Hình 7.16. Kết quả cấu hình NAT. . . . .	117
Hình 7.17. Kết quả cấu hình DHCPv4, host nhận IP động. . . . .	117
Hình 7.18. PC từ ngoài Internet truy cập web thành công. . . . .	117
Hình 7.19. PC từ ngoài Internet truy cập web không thành công. . .	118
Hình 7.20. Kết quả cấu hình DHCPv6, host nhận IP động. . . . .	121
Hình 7.21. Thiết lập quan hệ láng giềng trong miền EIGRP . . . . .	122
Hình 8.1. Kiểm tra các LAP đều phát sóng Wifi. . . . .	123
Hình 8.2. Kiểm tra kết nối wifi Business. . . . .	124

Hình 8.3.	Kiểm tra kết nối wifi Business. . . . .	124
Hình 8.4.	Kiểm tra kết nối wifi Marketing. . . . .	125
Hình 8.5.	Kiểm tra kết nối wifi Marketing. . . . .	125
Hình 8.6.	Kiểm tra kết nối wifi IoT. . . . .	126
Hình 8.7.	Kiểm tra kết nối wifi IoT. . . . .	126
Hình 8.8.	Kiểm tra kết nối wifi GUEST. . . . .	127
Hình 8.9.	Kiểm tra kết nối wifi GUEST. . . . .	127
Hình 8.10.	Marketing to Branch . . . . .	128
Hình 8.11.	Marketing to Server . . . . .	128
Hình 8.12.	Marketing to REMOTE . . . . .	128
Hình 8.13.	Marketing to Intenet . . . . .	129
Hình 8.14.	Marketing to Local Network . . . . .	129
Hình 8.15.	Marketing to Internet . . . . .	130
Hình 8.16.	Guest truy cập Web bằng tên miền . . . . .	130
Hình 8.17.	Kiểm tra cấu hình VPN . . . . .	131
Hình 8.18.	Kiểm tra cấu hình mã hóa IPsec VPN . . . . .	131
Hình 8.19.	Kiểm tra thông mạng REMOTE . . . . .	131

# Danh sách bảng

3.1 Cấp phát địa chỉ cho VLAN tại trụ sở chính . . . . .	50
3.2 Cấp phát địa chỉ Loopback tại chi nhánh . . . . .	50
3.3 IP và Subnet cho các liên kết trong mô hình mạng . . . . .	50
3.4 Địa chỉ IPv6 cho kết nối giữa các router . . . . .	51
3.5 Địa chỉ IPv6 cho các mạng LAN . . . . .	52
3.6 Địa chỉ IPv6 cấp phát cho các VLAN . . . . .	52
3.7 Địa chỉ IPv6 Link-local cấu hình trên các thiết bị . . . . .	52

# Danh mục các từ viết tắt

AAA	Authentication, Authorization, Accounting – Xác thực, Ủy quyền, Kế toán
ACL	Access Control List – Danh sách kiểm soát truy cập
AP	Access Point – Điểm truy cập
CHAP	Challenge Handshake Authentication Protocol – Giao thức xác thực bắt tay thử thách
DHCP	Dynamic Host Configuration Protocol – Giao thức cấp phát địa chỉ động
DNS	Domain Name System – Hệ thống phân giải tên miền
EIGRP	Enhanced Interior Gateway Routing Protocol – Giao thức định tuyến cổng nội bộ nâng cao
GRE	Generic Routing Encapsulation – Đóng gói định tuyến chung
HTTP	HyperText Transfer Protocol – Giao thức truyền siêu văn bản
HTTPS	HyperText Transfer Protocol Secure – Giao thức truyền siêu văn bản bảo mật
IDS/IPS	Intrusion Detection System/Intrusion Prevention System – Hệ thống phát hiện/Phòng ngừa xâm nhập
IoT	Internet of Things – Internet vạn vật
IP	Internet Protocol – Giao thức Internet
IPv4	Internet Protocol version 4 – Giao thức Internet phiên bản 4
IPv6	Internet Protocol version 6 – Giao thức Internet phiên bản 6
LAN	Local Area Network – Mạng cục bộ

NAT	Network Address Translation – Chuyển đổi địa chỉ mạng
OSPF	Open Shortest Path First – Giao thức định tuyến đường ngắn nhất mở
PAP	Password Authentication Protocol – Giao thức xác thực mật khẩu
PPP	Point-to-Point Protocol – Giao thức điểm-điểm
PVST	Per-VLAN Spanning Tree – Cây bao trùm theo VLAN
RADIUS	Remote Authentication Dial-In User Service – Dịch vụ xác thực quay số từ xa
SSH	Secure Shell – Vỏ bảo mật
STP	Spanning Tree Protocol – Giao thức cây bao trùm
TCP	Transmission Control Protocol – Giao thức điều khiển truyền tải
UDP	User Datagram Protocol – Giao thức dữ liệu người dùng
VLAN	Virtual LAN – Mạng LAN ảo
VTP	VLAN Trunking Protocol – Giao thức trunking VLAN
VPN	Virtual Private Network – Mạng riêng ảo
WLAN	Wireless Local Area Network – Mạng cục bộ không dây
WPA2	Wi-Fi Protected Access 2 – Truy cập được bảo vệ Wi-Fi phiên bản 2
WPA3	Wi-Fi Protected Access 3 – Truy cập được bảo vệ Wi-Fi phiên bản 3

# Chương 1

## Giới thiệu chung

### Mục tiêu báo cáo

Báo cáo này được xây dựng nhằm thiết kế và triển khai một hệ thống mạng tích hợp cho doanh nghiệp Chooky, một công ty khởi nghiệp trong lĩnh vực công nghệ, đồng thời đáp ứng các yêu cầu về bảo mật và khả năng mở rộng. Các mục tiêu chính bao gồm:

- Xây dựng một hệ thống mạng hiệu quả, bao gồm:
  - + Hệ thống mạng có dây (LAN) sử dụng giao thức IPv4 và IPv6, hỗ trợ kết nối ổn định cho các thiết bị cố định.
  - + Hệ thống mạng không dây (WiFi) đảm bảo phủ sóng toàn diện trên diện tích 500m<sup>2</sup>, đáp ứng nhu cầu truy cập của nhân viên, khách hàng và thiết bị IoT.
- Đề xuất các giải pháp bảo mật tiên tiến nhằm:
  - + Bảo vệ dữ liệu nhạy cảm như cơ sở dữ liệu, tài liệu nội bộ, hệ thống tài chính và email doanh nghiệp.
  - + Sử dụng các giao thức mã hóa hiện đại (WPA3 hoặc WPA2), xác thực an toàn (802.1X với RADIUS), và phân vùng mạng (VLAN) để tách biệt các nhóm người dùng.
- Đảm bảo khả năng mở rộng và quản lý từ xa:
  - + Tích hợp VPN để hỗ trợ nhân viên làm việc từ xa và kết nối với chi nhánh, tận dụng hạ tầng GRE tunnel đã triển khai.



- + Sử dụng các giao thức định tuyến (OSPF, EIGRP) để đảm bảo hệ thống có thể mở rộng trong tương lai.
- Thực hiện thử nghiệm và trình diễn hệ thống:
  - + Kiểm tra hiệu quả của hệ thống mạng, bao gồm kết nối có dây, không dây, và từ xa.
  - + Đánh giá các giải pháp bảo mật qua các kịch bản thực tế, đảm bảo tính an toàn và dự phòng.

## **Khảo sát quy mô và yêu cầu của doanh nghiệp**

Doanh nghiệp Chooky là một startup công nghệ đang phát triển nhanh, với các đặc điểm và yêu cầu cụ thể như sau:

- Quy mô doanh nghiệp:
  - + Văn phòng 2 tầng với tổng diện tích 500m<sup>2</sup>, đặt tại một khu công nghiệp công nghệ.
  - + Gồm 3 phòng ban chính: Marketing (20 nhân viên), Kinh doanh (15 nhân viên), và Quản lý (10 nhân viên), tổng cộng 45 nhân viên.
- Nhu cầu sử dụng mạng:
  - + Truy cập internet tốc độ cao để phục vụ công việc hàng ngày như họp trực tuyến, nghiên cứu thị trường, và giao dịch với khách hàng.
  - + Chia sẻ tài liệu nội bộ thông qua server (địa chỉ 12.0.4.194) và quản lý dữ liệu tài chính.
  - + Giám sát an ninh qua 10 camera IP phân bố trên 2 tầng.
  - + Hỗ trợ kết nối cho các thiết bị IoT (cảm biến, khóa thông minh) tại tầng 2.
- Số lượng và loại thiết bị truy cập mạng:
  - + PC và laptop: 50 thiết bị, chủ yếu phục vụ nhân viên và quản lý.
  - + Máy in: 3 máy in mạng, đặt tại mỗi phòng ban (Marketing, Kinh doanh, Quản lý).

- + Camera IP: 10 thiết bị, đảm bảo giám sát toàn bộ khu vực văn phòng.
- + Server nội bộ: 1 server tại địa chỉ 12.0.4.194, lưu trữ dữ liệu và đóng vai trò RADIUS Server cho xác thực.
- + Thiết bị IoT: 15 thiết bị (cảm biến nhiệt độ, khóa thông minh), chủ yếu tại tầng 2.
- + Thiết bị khách: Dự kiến 20-30 thiết bị (smartphone, laptop) của khách hàng, kết nối qua mạng WiFi khách.
- Loại hình truy cập:
  - + Mạng có dây: Sử dụng cho server, máy in, và một số PC cố định, tận dụng hạ tầng LAN đã triển khai với IPv4 và IPv6.
  - + Mạng không dây: Triển khai WiFi thông qua Access Point (AP) để phục vụ nhân viên, khách hàng, và thiết bị IoT.
  - + Truy cập từ xa: Sử dụng VPN để hỗ trợ nhân viên làm việc từ xa và kết nối với chi nhánh, tích hợp với GRE tunnel đã thiết lập giữa các router.

## **Dữ liệu cần bảo vệ**

Doanh nghiệp Chooky sở hữu nhiều loại dữ liệu quan trọng cần được bảo vệ nghiêm ngặt, bao gồm:

- Các loại dữ liệu cần bảo vệ:
  - + Cơ sở dữ liệu: Lưu trữ thông tin khách hàng, chiến lược marketing, và dữ liệu tài chính nhạy cảm, được quản lý trên server tại địa chỉ 12.0.4.194.
  - + Tài liệu nội bộ: Bao gồm hợp đồng với đối tác, báo cáo kinh doanh hàng quý, và kế hoạch phát triển sản phẩm mới.
  - + Hệ thống tài chính: Dữ liệu giao dịch, quản lý ngân sách, và các báo cáo tài chính của công ty.
  - + Email doanh nghiệp: Các giao tiếp nội bộ giữa nhân viên và với đối

tác, chứa thông tin quan trọng về chiến lược và hợp tác.

– Yêu cầu bảo mật:

- + Áp dụng các giao thức mã hóa mạnh như WPA2/WPA3 cho mạng WiFi và 802.1X với RADIUS để xác thực người dùng.
- + Phân vùng mạng bằng VLAN để tách biệt các nhóm người dùng (nhân viên, khách, IoT), giảm nguy cơ truy cập trái phép.
- + Sử dụng VPN để bảo vệ dữ liệu khi truy cập từ xa, tận dụng hạ tầng GRE tunnel đã triển khai.
- + Đảm bảo giám sát và phản ứng nhanh với các sự cố bảo mật thông qua hệ thống IDS/IPS và nhật ký hoạt động.

## Chương 2

# Cơ sở lý thuyết

### 2.1 Tổng quan về hệ thống mạng doanh nghiệp

Hệ thống mạng doanh nghiệp Chooky được thiết kế tích hợp cả mạng có dây (LAN), không dây (WiFi), và VPN, nhằm đáp ứng nhu cầu kết nối đa dạng của nhân viên, khách hàng, thiết bị IoT, và các chi nhánh. Phần lý thuyết này bao gồm các kiến thức nền tảng về các thành phần mạng.

– Mạng có dây (LAN):

- + Là nền tảng kết nối ổn định cho các thiết bị cố định như server, máy in, và PC.
- + Sử dụng giao thức IPv4 và IPv6 để cấp phát địa chỉ và định tuyến.
- + Tích hợp các giao thức như PPP, GRE tunnel, và định tuyến động (OSPF, EIGRP) để đảm bảo kết nối hiệu quả.

– Mạng không dây (WiFi):

- + Cung cấp khả năng truy cập linh hoạt cho nhân viên, khách hàng, và thiết bị IoT.
- + Được triển khai với các Access Point (AP) hỗ trợ chuẩn WiFi hiện đại (802.11ax).
- + Đảm bảo bảo mật thông qua các giao thức mã hóa (WPA3) và xác thực (802.1X).

– VPN (Virtual Private Network):

- + Tạo kết nối an toàn giữa các khu vực (HQ và chi nhánh) qua Internet.
- + Sử dụng IPsec để mã hóa dữ liệu, đảm bảo an toàn cho các thông tin nhạy cảm.
- + Hỗ trợ nhân viên làm việc từ xa và kết nối giữa các router (R6, R7, R8).

## 2.2 Lý thuyết mạng có dây

### 2.2.1 Sơ đồ địa chỉ và phân bổ IP (IPv4)

#### *Lý thuyết*

- **Địa chỉ IPv4:** Địa chỉ 32-bit, biểu diễn dưới dạng 4 octet (ví dụ: **192.168.1.1**). Được chia thành phần mạng và phần host dựa trên subnet mask (ví dụ: **/24** tương ứng với **255.255.255.0**).
- **Subnetting:** Chia một dải địa chỉ IP thành các mạng con nhỏ hơn để đáp ứng nhu cầu số lượng host và tổ chức mạng.
  - + Công thức tính số host:  $2^{(32-\text{prefix})} - 2$  (trừ 2 địa chỉ cho network và broadcast).
  - + Ví dụ: Để hỗ trợ 200 host, cần **/24** ( $256 - 2 = 254$  host); cho 300 host, cần **/23** ( $512 - 2 = 510$  host).
- **VLAN (Virtual Local Area Network):** Phân tách lưu lượng mạng logic trên cùng một switch. Mỗi VLAN được gán một subnet riêng để quản lý địa chỉ IP.
- **Point-to-Point Network:** Sử dụng subnet nhỏ (thường **/30**) để kết nối hai router, cung cấp 2 địa chỉ host (một cho mỗi router).

#### *Ứng dụng tại Chooky*

- **HQ VLANs** (Bảng 2):
  - + VLAN 10 (Marketing, 200 host): Cần subnet **/24** (254 host).  
Ví dụ: **X.X.1.0/24**.

- + VLAN 20 (Business, 300 host): Cần subnet /23 (510 host).  
Ví dụ: **X.X.2.0/23**.
- + VLAN 30 (IoT, 100 host): Cần subnet /25 (126 host).  
Ví dụ: **X.X.4.0/25**.
- + VLAN 40 (GUEST, 50 host): Cần subnet /26 (62 host).  
Ví dụ: **X.X.4.128/26**.
- + VLAN 50 (SERVERS, 10 host): Cần subnet /28 (14 host).  
Ví dụ: **X.X.4.192/28**.
- + VLAN 60 (Management, 20 host): Cần subnet /27 (30 host).  
Ví dụ: **X.X.4.224/27**.
- **Chi nhánh Loopback** (Bảng 3):
  - + R1 Lo0 (500 host): Cần subnet /23. Ví dụ: **Y.Y.1.0/23**.
  - + R1 Lo1 (300 host): Cần subnet /23. Ví dụ: **Y.Y.3.0/23**.
  - + R2 Lo0 (100 host): Cần subnet /25. Ví dụ: **Y.Y.5.0/25**.
  - + R3 Lo0 (200 host): Cần subnet /24. Ví dụ: **Y.Y.6.0/24**.
  - + R3 Lo1 (100 host): Cần subnet /25. Ví dụ: **Y.Y.7.0/25**.
- **Point-to-Point** (Bảng 1):
  - + R7 ↔ R6: **200.0.100.0/30** (host: **200.0.100.1**, **200.0.100.2**).
  - + R7 ↔ R8: **200.0.100.4/30** (host: **200.0.100.5**, **200.0.100.6**).
  - + R5 ↔ ACCESS:  
**200.0.100.8/30** (host: **200.0.100.9**, **200.0.100.10**).

## 2.2.2 Kết nối PPP (Point-to-Point Protocol)

### *Lý thuyết*

- **PPP**: Giao thức tầng liên kết dữ liệu, cung cấp kết nối trực tiếp giữa hai node. Hỗ trợ xác thực, nén dữ liệu, và phát hiện lỗi.
- + **PAP (Password Authentication Protocol)**: Gửi tên người dùng

và mật khẩu dưới dạng plaintext. Dễ cấu hình nhưng kém an toàn.

+ **CHAP (Challenge Handshake Authentication Protocol):**

Sử dụng cơ chế challenge-response, router gửi một chuỗi ngẫu nhiên (challenge), đối phương trả lời bằng giá trị băm (response) dựa trên mật khẩu. An toàn hơn PAP.

– **Cấu hình PPP:**

1. Bật PPP encapsulation: `encapsulation ppp`.
2. Cấu hình xác thực:
  - + PAP: `ppp pap sent-username <username> password <password>`.
  - + CHAP: `ppp chap hostname <hostname>`, `ppp chap password <password>`.
3. Gán tên người dùng/mật khẩu trong cơ sở dữ liệu: `username <name> password <password>`.

*Ứng dụng tại Chooky*

- Cấu hình PPP giữa R7 và R6 với xác thực PAP:
  1. Bật PPP encapsulation: `encapsulation ppp`.
  2. Cấu hình xác thực trên R7: `ppp pap sent-username R6 password cisco123`.
  3. Cấu hình xác thực trên R6: `username R7 password cisco123`.
- Cấu hình PPP giữa R7 và R8 với xác thực CHAP:
  1. Bật PPP encapsulation: `encapsulation ppp`.
  2. Cấu hình trên R7: `ppp chap hostname R7`, `ppp chap password cisco456`.
  3. Cấu hình trên R8: `ppp chap hostname R8`, `ppp chap password cisco456`, `username R7 password cisco456`.
- Đảm bảo các interface serial được cấu hình với `encapsulation ppp` và địa chỉ IP từ `200.0.100.0/30` và `200.0.100.4/30`.

## 2.2.3 Tunneling GRE (Generic Routing Encapsulation)

### *Lý thuyết*

- **GRE:** Giao thức đường hầm tầng 3, đóng gói các gói tin của nhiều giao thức (IPv4, IPv6, MPLS) để truyền qua mạng IP.
  - + Cấu trúc: GRE thêm header vào gói tin gốc, sau đó đóng gói trong gói IP mới.
  - + Ưu điểm: Linh hoạt, hỗ trợ nhiều giao thức.
  - + Nhược điểm: Không mã hóa, cần kết hợp với IPsec nếu yêu cầu bảo mật.
- **Cấu hình GRE:**
  1. Tạo interface tunnel: `interface tunnel <number>`.
  2. Gán địa chỉ IP cho tunnel.
  3. Chỉ định nguồn (source) và đích (destination) của tunnel.
  4. Cấu hình định tuyến để lưu lượng đi qua tunnel.

### *Ứng dụng tại Chooky*

- **GRE giữa R6 và R8:**
  - + Tạo tunnel với địa chỉ mạng `X.X.X.X/A` (hỗ trợ 2 host, ví dụ: `/30`).
  - + Source: Interface vật lý của R6 (ví dụ: `200.0.100.2`).
  - + Destination: Interface vật lý của R8 (ví dụ: `200.0.100.5`).
  - + Cấu hình tuyến tĩnh: `ip route 0.0.0.0 0.0.0.0 tunnel <number>` hoặc động (EIGRP).

## 2.2.4 Định tuyến

### *Lý thuyết*

- **EIGRP (Enhanced Interior Gateway Routing Protocol):**
  - + Giao thức định tuyến lai, sử dụng thuật toán DUAL (Diffusing Update Algorithm).



- + Metric: Dựa trên băng thông, độ trễ, độ tin cậy, tải, và MTU.
- + Cấu hình: Kích hoạt EIGRP với AS number, thêm mạng bằng lệnh `network`.
- + Passive interface: Ngăn gửi bản cập nhật EIGRP trên interface: `passive-interface <interface>`.
- + Redistribution: Chuyển tuyến từ giao thức khác vào EIGRP bằng lệnh `redistribute`.
- **OSPF (Open Shortest Path First):**
  - + Giao thức trạng thái liên kết, sử dụng thuật toán Dijkstra để tính đường đi ngắn nhất.
  - + Chia mạng thành các area để giảm lưu lượng cập nhật.
  - + Cấu hình: Kích hoạt OSPF với process ID, thêm mạng bằng lệnh `network <network> <wildcard> area <area>`.
  - + Passive interface: Tương tự EIGRP.
- **Default Route:** Tuyến mặc định (`0.0.0.0/0`) được cấu hình để gửi lưu lượng không khớp đến một điểm cụ thể.
- **Redistribution:** Cho phép chia sẻ tuyến giữa các giao thức định tuyến khác nhau, cần đảm bảo metric tương thích.

### *Ứng dụng tại Chooky*

- **EIGRP tại HQ:**
  - + Kích hoạt EIGRP với AS number chung: `router eigrp 100`.
  - + Thêm các mạng của HQ (ví dụ: VLAN subnets, `200.0.100.0/30`).
  - + Đặt interface không cần gửi bản cập nhật (ví dụ: interface kết nối host) thành passive: `passive-interface <interface>`.
- **OSPF đa khu vực tại chi nhánh:**
  - + Kích hoạt OSPF với process ID: `router ospf 1`.

- + Gán các mạng chi nhánh (Loopback, WAN links) vào các area khác nhau.
- + Cấu hình passive interface cho các interface không cần gửi bản cập nhật: `passive-interface <interface>`.
- **Default Route trên R5:**
  - + Cấu hình: `ip route 0.0.0.0 0.0.0.0 <ACCESS-IP>`.
  - + Phân phối vào EIGRP: `redistribute static`.
  - + Phân phối vào OSPF: `default-information originate`.
- **Redistribution:**
  - + Trên router biên: Redistribute EIGRP vào OSPF và ngược lại, đảm bảo metric phù hợp: `redistribute eigrp 100 metric 10`.

## 2.2.5 Chuyển mạch

### *Lý thuyết*

- **VTP (VLAN Trunking Protocol):**
  - + Quản lý tập trung VLAN trên nhiều switch.
  - + VTP Server: Tạo, sửa, xóa VLAN và đồng bộ với client.
  - + VTP Client: Nhận VLAN từ server, không thể chỉnh sửa.
- **Rapid PVST+ (Per-VLAN Spanning Tree):**
  - + Phiên bản cải tiến của STP, hội tụ nhanh hơn (vài giây so với 30-50 giây của STP).
  - + Mỗi VLAN có một cây spanning tree riêng.
  - + Root Bridge: Switch có Bridge ID thấp nhất (Priority + MAC address).
- **EtherChannel:**
  - + Kết hợp nhiều liên kết vật lý thành một liên kết logic.
  - + LACP (Link Aggregation Control Protocol): Giao thức chuẩn IEEE,

tự động thương lượng.

– **Router-on-a-Stick:**

- + Sử dụng một interface router với nhiều sub-interface, mỗi sub-interface gán một VLAN và địa chỉ IP.
- + Yêu cầu trunk link giữa router và switch.

– **SSH:**

- + Giao thức quản lý từ xa an toàn.
- + Cấu hình: Tạo domain name, khóa RSA, tài khoản người dùng, và bật SSH trên VTY lines.

*Ứng dụng tại Chooky*

– **VTP:**

- + S1 là VTP Server, các switch khác là Client.
- + Cấu hình domain name và password cho VTP: `vtp domain <domain>`, `vtp password <password>`.

– **Rapid PVST+:**

- + Bật chế độ: `spanning-tree mode rapid-per-vlan`.
- + Đặt S1 làm root bridge cho VLAN 10, 20, 30: `spanning-tree vlan 10,20,30 root primary`.
- + Đặt S2 làm root bridge cho VLAN 40, 50, 60: `spanning-tree vlan 40,50,60 root primary`.

– **EtherChannel:**

- + Cấu hình LACP trên các interface kết nối giữa switch: `channel-group <number> mode active`.

– **Router-on-a-Stick trên R4:**

- + Tạo sub-interface cho mỗi VLAN (10, 20, 30, 40, 50, 60).
- + Gán địa chỉ IP gateway (ví dụ: `X.X.1.1/24` cho VLAN 10).

- + Bật encapsulation: `encapsulation dot1q <vlan-id>`.
- **SSH:**
  - + Cấu hình trên tất cả switch: `ip domain-name <domain>`, `crypto key generate rsa`, `line vty 0 15`, `transport input ssh`.

## 2.2.6 NAT và DHCP

### *Lý thuyết*

- **NAT Overload (PAT):**
  - + Ánh xạ nhiều địa chỉ IP riêng sang một địa chỉ IP công cộng, sử dụng các cổng khác nhau.
  - + Cấu hình: Tạo ACL để xác định địa chỉ nguồn, gán NAT trên interface inside/outside.
- **DHCP:**
  - + Server cấp phát địa chỉ IP, subnet mask, gateway, và DNS cho client.
  - + Cấu hình: Tạo DHCP pool cho mỗi VLAN, chỉ định dải địa chỉ và các tham số.
- **Port Forwarding:**
  - + Chuyển tiếp lưu lượng từ cổng cụ thể trên địa chỉ công cộng đến máy chủ nội bộ.
  - + Cấu hình: Sử dụng NAT tĩnh với cổng (ví dụ: TCP 80, 443).

### *Ứng dụng tại Chooky*

- **NAT Overload trên Access:**
  - + Tạo ACL cho các mạng nội bộ (HQ và chi nhánh): `access-list 1 permit <HQ-subnet>`, `access-list 1 permit <Branch-subnet>`.
  - + Cấu hình: `ip nat inside source list 1 interface <outside> overload`.
  - + Gán interface: `ip nat inside` cho HQ/chi nhánh, `ip nat outside`

cho Internet.

– **DHCP trên R4:**

- + Tạo pool cho VLAN 10, 20, 30, 40.
- + Ví dụ: `ip dhcp pool VLAN10, network X.X.1.0 255.255.255.0, default-router X.X.1.1, dns-server <IP>`.

– **Port Forwarding:**

- + Cấu hình NAT tĩnh: `ip nat inside source static tcp <server-IP> 80 <public-IP> 80`, tương tự cho HTTPS (`ip nat inside source static tcp <server-IP> 443 <public-IP> 443`).

## 2.2.7 ACL (Access Control List)

### *Lý thuyết*

– **ACL:**

- + Standard ACL: Lọc dựa trên địa chỉ nguồn, áp dụng gần đích.
- + Extended ACL: Lọc dựa trên nguồn, đích, giao thức, cổng, áp dụng gần nguồn.
- + Cấu hình: `access-list <number> permit/deny <criteria>`, áp dụng bằng `ip access-group`.

– **Ứng dụng ACL:**

- + Hạn chế truy cập vào mạng nội bộ.
- + Cho phép truy cập dịch vụ cụ thể (như SSH).

### *Ứng dụng tại Chooky*

– **ACL cho VLAN GUEST:**

- + Tạo extended ACL:  
`access-list 101 deny ip <GUEST-subnet> <HQ-subnets>`,  
`access-list 101 permit ip <GUEST-subnet> any`.
- + Áp dụng trên interface VLAN 40: `ip access-group 101 in`.

– **ACL cho VLAN SERVERS:**

+ Tạo extended ACL:

```
access-list 102 permit tcp <SERVERS-subnet> any eq 22,  
access-list 102 deny ip <SERVERS-subnet> any.
```

+ Áp dụng trên VTY lines của switch: `access-class 102 in`.

## 2.3 Lý thuyết IPv6

### 2.3.1 Sơ đồ địa chỉ IPv6

#### *Lý thuyết*

– **Địa chỉ IPv6:** 128-bit, biểu diễn dưới dạng 8 nhóm 16-bit (ví dụ: `2019:ABBA:CDDC:0001::1`). Các loại địa chỉ:

+ **Link-local:** `FE80::/10`, tự động gán cho mọi interface, dùng trong cùng liên kết.

+ **Global unicast:** Dùng cho giao tiếp toàn cầu.  
Ví dụ: `2019:ABBA:CDDC::/48`.

– **Subnetting IPv6:**

+ Thường sử dụng `/64` cho mạng LAN (cung cấp  $2^{64}$  địa chỉ).

+ Chia mạng lớn (ví dụ: `/48`) thành các subnet `/64` bằng cách thay đổi 16 bit tiếp theo.

– **SLAAC (Stateless Address Autoconfiguration):**

+ Host tự động tạo địa chỉ IPv6 dựa trên prefix từ router và ID interface (thường là địa chỉ MAC).

#### *Ứng dụng tại Chooky*

– **Link-local address:**

+ Gán tĩnh cho mọi interface: Ví dụ, `FE80::1/10` cho R7, `FE80::2/10` cho R6.

– **VLAN subnets:**

- + Chia `2019:ABBA:CDDC:/48` thành 5 subnet `/64`:
  - VLAN 10: `2019:ABBA:CDDC:1::/64`,  
gateway: `2019:ABBA:CDDC:1::1`.
  - VLAN 20: `2019:ABBA:CDDC:2::/64`,  
gateway: `2019:ABBA:CDDC:2::1`.
  - VLAN 30: `2019:ABBA:CDDC:3::/64`,  
gateway: `2019:ABBA:CDDC:3::1`.
  - VLAN 40: `2019:ABBA:CDDC:4::/64`,  
gateway: `2019:ABBA:CDDC:4::1`.
  - VLAN 50: `2019:ABBA:CDDC:5::/64`,  
gateway: `2019:ABBA:CDDC:5::1`.
- **Router connections** (Bảng 4):
  - + Access ↔ R5: `2019:ABBA:AAAA:1::/64`.
  - + R4, R5, R7: `2019:ABBA:BBBB:1::/64`.
  - + R7 ↔ R6: `2019:ABBA:CCCC:1::/64`.
  - + R7 ↔ R8: `2019:ABBA:DDDD:1::/64`.
  - + LAN R6: `2019:ABBA:EEEE:1::/64`.
  - + LAN R8: `2019:ABBA:FFFF:1::/64`.

### 2.3.2 Định tuyến IPv6

#### *Lý thuyết*

- **EIGRP cho IPv6:**
  - + Tương tự EIGRP IPv4, nhưng yêu cầu bật IPv6 unicast routing: `ipv6 unicast-routing`.
  - + Kích hoạt trên interface: `ipv6 eigrp <AS>`.
  - + Không sử dụng lệnh `network`, thay vào đó bật trực tiếp trên interface.
- **Default Route:**

- + Cấu hình: `ipv6 route ::/0 <next-hop>`.
- + Phân phối: `redistribute static` trong EIGRP.
- **Inter-VLAN Routing:**
  - + Tương tự IPv4, sử dụng sub-interface với encapsulation dot1q, nhưng gán địa chỉ IPv6.

### *Ứng dụng tại Chooky*

- **EIGRP IPv6 tại HQ:**
  - + Bật: `ipv6 unicast-routing`.
  - + Kích hoạt EIGRP trên các interface VLAN và WAN: `ipv6 eigrp <AS>`.
- **Default Route trên R5:**
  - + Cấu hình: `ipv6 route ::/0 <ACCESS-IPv6>`.
  - + Phân phối: `redistribute static` trong EIGRP.
- **Inter-VLAN Routing trên R4:**
  - + Tạo sub-interface cho VLAN 10, 20, 30, 40, 50.
  - + Gán địa chỉ gateway (ví dụ: `2019:ABBA:CDDC:1::1/64` cho VLAN 10).
  - + Bật encapsulation: `encapsulation dot1q <vlan-id>`.

## **2.3.3 DHCPv6**

### *Lý thuyết*

- **Stateful DHCPv6:**
  - + Server DHCPv6 duy trì trạng thái địa chỉ, cấp phát địa chỉ IPv6 duy nhất và thông tin bổ sung (DNS, domain) từ pool được định nghĩa.
  - + Cấu hình: Tạo DHCPv6 pool, chỉ định prefix địa chỉ và DNS server, sau đó áp dụng pool lên interface.



## *Ứng dụng tại Chooky*

### – **Stateful DHCPv6 trên R4:**

+ Tạo pool cho các VLAN:

- `ipv6 dhcp pool VLAN10`  
với `address prefix 2019:ABBA:CDDC:1000::/64`.
- `ipv6 dhcp pool VLAN20`  
với `address prefix 2019:ABBA:CDDC:2000::/64`.
- `ipv6 dhcp pool VLAN30`  
với `address prefix 2019:ABBA:CDDC:3000::/64`.
- `ipv6 dhcp pool VLAN40`  
với `address prefix 2019:ABBA:CDDC:4000::/64`.

+ Cấu hình DNS: `dns-server 2001:4860:4860::8888` cho tất cả pool.

+ Áp dụng pool lên các interface:

- `interface GigabitEthernet0/0/0.10:`  
`ipv6 dhcp server VLAN10.`
- `interface GigabitEthernet0/0/0.20:`  
`ipv6 dhcp server VLAN20.`
- `interface GigabitEthernet0/0/0.30:`  
`ipv6 dhcp server VLAN30.`
- `interface GigabitEthernet0/0/0.40:`  
`ipv6 dhcp server VLAN40.`

+ Bật thông báo sử dụng DHCPv6: `ipv6 nd other-config-flag` trên các interface VLAN.

## **2.4 Lý thuyết mạng không dây**

### **2.4.1 Tổng quan mạng không dây (WLAN)**

#### – **Khái niệm WLAN (Wireless Local Area Network):**

+ Là một mạng cục bộ không dây, sử dụng sóng vô tuyến (radio frequency

- RF) để kết nối các thiết bị mà không cần cáp vật lý.
- + Dựa trên tiêu chuẩn IEEE 802.11, thường được gọi là WiFi (Wireless Fidelity).
- + Ứng dụng trong các môi trường như doanh nghiệp, trường học, gia đình, và không gian công cộng.
- + Tại Chooky: WLAN được triển khai để cung cấp kết nối không dây cho 45 nhân viên, 20-30 thiết bị khách, và 15 thiết bị IoT.
- **So sánh mạng có dây và không dây:**
  - + Về chi phí:
    - Mạng không dây giảm chi phí lắp đặt cáp và cơ sở hạ tầng vật lý, nhưng yêu cầu đầu tư vào các thiết bị như Access Point (AP) và hệ thống bảo mật.
    - Mạng có dây có chi phí ban đầu cao hơn do cần cáp và switch, nhưng chi phí bảo trì thường thấp hơn.
  - + Về tính linh hoạt:
    - Mạng không dây cho phép người dùng di chuyển tự do trong vùng phủ sóng, phù hợp với laptop, smartphone, và thiết bị IoT.
    - Mạng có dây yêu cầu thiết bị cố định tại một vị trí, hạn chế tính cơ động.
  - + Về bảo mật:
    - Mạng không dây dễ bị tấn công hơn do tín hiệu phát qua không khí (như nghe lén, giả mạo AP), cần mã hóa mạnh (WPA3) và xác thực (802.1X).
    - Mạng có dây an toàn hơn do yêu cầu truy cập vật lý, nhưng vẫn cần bảo vệ trước các mối đe dọa nội bộ.
  - + Về hiệu suất:
    - Mạng không dây có tốc độ và độ ổn định thấp hơn, dễ bị ảnh hưởng bởi nhiễu và vật cản.

- Mạng có dây cung cấp tốc độ cao và ổn định, phù hợp cho server và thiết bị cố định.
- **Ưu điểm của WLAN trong doanh nghiệp:**
  - + Tăng tính linh hoạt: Nhân viên có thể làm việc từ bất kỳ vị trí nào trong văn phòng mà không cần cáp.
  - + Hỗ trợ khách hàng: Cung cấp WiFi khách để đối tác và khách truy cập Internet.
  - + Dễ mở rộng: Thêm Access Point hoặc triển khai Mesh WiFi để mở rộng vùng phủ sóng khi doanh nghiệp phát triển.
  - + Hỗ trợ IoT: Kết nối các thiết bị thông minh như camera IP, cảm biến, và khóa thông minh.
- **Nhược điểm của WLAN:**
  - + Phụ thuộc vào môi trường: Sóng WiFi bị ảnh hưởng bởi vật cản (tường, kính), nhiễu từ thiết bị điện tử, và thời tiết.
  - + Hiệu suất giảm khi mật độ thiết bị cao: Quá nhiều thiết bị kết nối cùng lúc có thể gây nghẽn.
  - + Rủi ro bảo mật: Dễ bị tấn công nếu không cấu hình bảo mật đúng cách (như sử dụng WEP hoặc mật khẩu yếu).

## 2.4.2 Chuẩn WiFi (IEEE 802.11)

- **Tổng quan:**
  - + IEEE 802.11 là tập hợp các tiêu chuẩn cho mạng không dây, được phát triển từ năm 1997.
  - + Các chuẩn định nghĩa tần số, tốc độ, phạm vi, và công nghệ hỗ trợ (như MIMO, MU-MIMO).
- **Các chuẩn phổ biến:**
  - + 802.11a (1999):
    - Tần số: 5GHz.

- Tốc độ tối đa: 54Mbps.
  - Phạm vi: Khoảng 35m trong nhà, ít nhiều hơn 2.4GHz nhưng tín hiệu yếu hơn qua vật cản.
- + 802.11b (1999):
- Tần số: 2.4GHz.
  - Tốc độ tối đa: 11Mbps.
  - Phạm vi: Khoảng 50m trong nhà, dễ bị nhiễu từ thiết bị khác (lò vi sóng, điện thoại không dây).
- + 802.11g (2003):
- Tần số: 2.4GHz.
  - Tốc độ tối đa: 54Mbps.
  - Phạm vi: Tương tự 802.11b, tương thích ngược với 802.11b.
- + 802.11n (2009):
- Tần số: Hỗ trợ cả 2.4GHz và 5GHz.
  - Tốc độ tối đa: 600Mbps (với 4 luồng MIMO).
  - Phạm vi: Lên đến 70m trong nhà, sử dụng MIMO (Multiple Input Multiple Output) để tăng hiệu suất.
- + 802.11ac (WiFi 5, 2013):
- Tần số: 5GHz.
  - Tốc độ tối đa: 1.3Gbps (kênh 80MHz, 3 luồng).
  - Phạm vi: Tương tự 802.11n, hỗ trợ MU-MIMO (Multi-User MIMO) để phục vụ nhiều thiết bị cùng lúc.
- + 802.11ax (WiFi 6, 2019):
- Tần số: Hỗ trợ cả 2.4GHz, 5GHz, và 6GHz (với WiFi 6E).
  - Tốc độ tối đa: 9.6Gbps (kênh 160MHz, 8 luồng).
  - Phạm vi: Tương tự 802.11ac, nhưng hiệu quả hơn nhờ OFDMA (Orthogonal Frequency Division Multiple Access).

- Ưu điểm: Tối ưu cho mật độ thiết bị cao, giảm độ trễ, tiết kiệm năng lượng với TWT (Target Wake Time).
- **Ứng dụng tại Chooky:**
  - + Sử dụng chuẩn **802.11ax** (WiFi 6) để đảm bảo tốc độ và độ ổn định cho hơn 80 thiết bị (50 thiết bị nhân viên, 20-30 thiết bị khách, 15 thiết bị IoT).
  - + Tần số 5GHz được ưu tiên để giảm nhiễu trong môi trường văn phòng.

### 2.4.3 Kiến trúc mạng WiFi

- **Mô hình Infrastructure Mode:**
  - + Là mô hình phổ biến trong doanh nghiệp, sử dụng Access Point (AP) làm trung tâm kết nối.
  - + Các thiết bị (client) kết nối với AP, sau đó AP chuyển tiếp dữ liệu đến mạng LAN.
  - + Ưu điểm:
    - Quản lý tập trung, dễ dàng cấu hình bảo mật và giám sát.
    - Hỗ trợ nhiều thiết bị cùng lúc, phù hợp với Chooky (80+ thiết bị).
  - + Nhược điểm:
    - Phụ thuộc vào AP, nếu AP hỏng sẽ mất kết nối.
- **Mô hình Ad-Hoc Mode:**
  - + Các thiết bị kết nối trực tiếp với nhau mà không cần AP, tạo thành mạng ngang hàng.
  - + Ưu điểm:
    - Không cần hạ tầng, phù hợp cho các mạng tạm thời (như hội thảo).
  - + Nhược điểm:
    - Khó quản lý, không hỗ trợ bảo mật mạnh, không phù hợp cho doanh nghiệp.
  - + Tại Chooky: Không áp dụng do yêu cầu quản lý tập trung và bảo mật

cao.

– **Thành phần mạng:**

+ Router WiFi:

- Đóng vai trò gateway, kết nối mạng nội bộ với Internet.
- Tại Chooky: Router ACCESS (203.0.113.1) đảm nhận chức năng này.

+ Access Point (AP):

- Thiết bị phát sóng WiFi, kết nối với switch (S1-S4) để tích hợp vào mạng LAN.
- Tại Chooky: Sử dụng AP hỗ trợ 802.11ax, đặt trên 2 tầng để phủ sóng 500m<sup>2</sup>.

+ Repeater (Bộ mở rộng sóng):

- Nhận tín hiệu từ AP và phát lại để mở rộng vùng phủ sóng.
- Tại Chooky: Không áp dụng do diện tích 500m<sup>2</sup> có thể được phủ bằng AP độc lập.

+ Mesh WiFi:

- Hệ thống nhiều AP hoạt động như một mạng lưới, tự động chuyển giao tín hiệu.
- Tại Chooky: Có thể xem xét trong tương lai nếu mở rộng quy mô.

+ Wireless Controller:

- Quản lý tập trung nhiều AP, tối ưu cho doanh nghiệp lớn.
- Tại Chooky: Chưa áp dụng do quy mô nhỏ, nhưng có thể triển khai nếu cần.

## 2.4.4 Mô hình Mesh WiFi và Range Extender

– **Mesh WiFi:**

- + Là hệ thống gồm nhiều node (AP) hoạt động như một mạng lưới, tự động kết nối với nhau.

- + Cách hoạt động:
  - Một node chính kết nối với router, các node khác tạo thành mạng lưới liên kết.
  - Client tự động chuyển giao (roaming) giữa các node mà không mất kết nối.
- + Ưu điểm:
  - Phủ sóng liên mạch trên diện tích lớn, không có điểm chết.
  - Hỗ trợ mật độ thiết bị cao, phù hợp cho doanh nghiệp mở rộng.
  - Dễ quản lý qua ứng dụng hoặc controller.
- + Nhược điểm:
  - Chi phí cao hơn do cần nhiều node (mỗi node tương đương một AP).
  - Cấu hình phức tạp hơn, cần đảm bảo các node tương thích với nhau.
- **Range Extender (Bộ mở rộng sóng):**
  - + Là thiết bị nhận tín hiệu từ AP chính và phát lại để mở rộng vùng phủ sóng.
  - + Cách hoạt động:
    - Kết nối không dây hoặc có dây với AP, sau đó tạo một SSID mới hoặc dùng cùng SSID.
    - Client cần chuyển đổi thủ công giữa AP và extender nếu SSID khác nhau.
  - + Ưu điểm:
    - Chi phí thấp, dễ triển khai trong các không gian nhỏ.
    - Phù hợp để mở rộng vùng phủ sóng tạm thời.
  - + Nhược điểm:
    - Giảm tốc độ do lặp tín hiệu (thường giảm 50% băng thông).
    - Không hiệu quả khi mật độ thiết bị cao, dễ gây nghẽn.
    - Chuyển giao tín hiệu không mượt mà, có thể gây gián đoạn.

– **Ứng dụng tại Chooky:**

- + Hiện tại: Sử dụng 2-3 AP độc lập hỗ trợ **802.11ax**, đủ phủ sóng diện tích 500m<sup>2</sup> với mật độ 80+ thiết bị.
- + Trong tương lai: Có thể triển khai Mesh WiFi nếu doanh nghiệp mở rộng diện tích hoặc tăng số lượng thiết bị.

## **2.4.5 Bảo mật mạng WiFi**

– **Giao thức mã hóa:**

- + WEP (Wired Equivalent Privacy):
  - Giao thức mã hóa đầu tiên cho WiFi, sử dụng khóa RC4 64-bit hoặc 128-bit.
  - Yếu điểm: Dễ bị tấn công (như công cụ Aircrack-ng), không còn được sử dụng từ năm 2004.
- + WPA (WiFi Protected Access):
  - Ra đời năm 2003 để thay thế WEP, sử dụng TKIP (Temporal Key Integrity Protocol) để tăng bảo mật.
  - Yếu điểm: TKIP vẫn có lỗ hổng, không đủ mạnh so với các tấn công hiện đại.
- + WPA2:
  - Ra đời năm 2004, sử dụng mã hóa AES (Advanced Encryption Standard), an toàn hơn WPA.
  - Có hai chế độ: WPA2-PSK (dùng mật khẩu chung) và WPA2 - Enterprise (dùng 802.1X).
  - Yếu điểm: Lỗ hổng KRACK (2017) cho phép tấn công giải mã dữ liệu.
- + WPA3:
  - Ra đời năm 2018, cải tiến từ WPA2, sử dụng mã hóa AES-256 và giao thức Dragonfly Key Exchange.



- Ưu điểm:
    - Bảo vệ chống tấn công brute-force (tăng độ khó khi đoán mật khẩu).
    - Forward secrecy: Dữ liệu vẫn an toàn ngay cả khi mật khẩu bị lộ sau phiên kết nối.
    - Dễ cấu hình cho thiết bị IoT với chế độ WPA3-SAE (Simultaneous Authentication of Equals).
  - Ứng dụng tại Chooky: Sử dụng **WPA3 - Enterprise** cho SSID nhân viên và IoT, **WPA3 - PSK** cho SSID khách. Do giới hạn trên Cisco Packet Tracer bản miễn phí nên chỉ cấu hình **WPA2 - Enterprise** và **WPA2 - PSK**.
- **Cơ chế xác thực:**
- + PSK (Pre-Shared Key):
    - Sử dụng một mật khẩu chung cho tất cả thiết bị, dễ cấu hình nhưng kém an toàn.
    - Yếu điểm: Nếu mật khẩu bị lộ, toàn bộ mạng sẽ bị xâm phạm.
    - Ứng dụng tại Chooky: Dùng cho SSID khách (GUEST) với mật khẩu đơn giản nhưng thay đổi định kỳ.
  - + 802.1X với RADIUS:
    - Sử dụng server RADIUS để xác thực người dùng qua thông tin đăng nhập (username/password).
    - Ưu điểm:
      - Mỗi người dùng có tài khoản riêng, dễ quản lý và thu hồi quyền truy cập.
      - Tích hợp với giao thức EAP (Extensible Authentication Protocol), an toàn hơn PSK.
    - Ứng dụng tại Chooky: Sử dụng **802.1X** với RADIUS Server (12.0.4.194) cho SSID nhân viên và IoT.

– **Các biện pháp bảo mật bổ sung:**

+ Cập nhật firmware:

- Định kỳ cập nhật firmware cho AP và router để vá các lỗ hổng bảo mật.
- Tại Chooky: Kiểm tra firmware hàng tháng để đảm bảo an toàn.

+ Ẩn SSID broadcast:

- Tắt phát sóng SSID trên SSID nhân viên và IoT để giảm nguy cơ bị phát hiện bởi hacker.
- Người dùng cần nhập SSID thủ công để kết nối.

+ Giám sát và phát hiện xâm nhập:

- Sử dụng hệ thống IDS/IPS (Intrusion Detection/Prevention System) để phát hiện các kết nối bất thường.
- Tại Chooky: Tích hợp IDS/IPS trên router ACCESS để giám sát lưu lượng WiFi.

+ Kiểm soát truy cập:

- Sử dụng MAC filtering để chỉ cho phép các thiết bị được phê duyệt kết nối vào SSID nhân viên.
- Tại Chooky: Danh sách MAC của thiết bị nhân viên được lưu trên AP.

+ Phân vùng mạng:

- Tích hợp VLAN (đã triển khai) để tách biệt lưu lượng giữa SSID nhân viên, khách, và IoT.
- Ví dụ: SSID nhân viên trên VLAN 10-40, SSID khách trên VLAN 40, SSID IoT trên VLAN 50.

## **2.5 VPN (Virtual Private Network)**

– **Khái niệm VPN:**

- + VPN là một mạng riêng ảo, tạo ra một kết nối an toàn qua mạng công

cộng (như Internet) bằng cách mã hóa dữ liệu.

- + Mục đích: Bảo vệ dữ liệu, cho phép truy cập từ xa, và kết nối các chi nhánh của doanh nghiệp.
- + Tại Chooky: VPN được triển khai để hỗ trợ nhân viên làm việc từ xa và kết nối giữa các khu vực (HQ và chi nhánh).

#### – Các loại VPN:

##### + Site-to-Site VPN:

- Kết nối giữa hai mạng nội bộ (LAN) qua Internet, thường dùng để liên kết các chi nhánh.
- Tại Chooky: VPN giữa R6-R7 và R7-R8 là Site-to-Site VPN, kết nối các mạng 128.1.7.0/24, 12.0.0.0/16, và 12.0.6.0/24.

##### + Remote Access VPN:

- Cho phép người dùng từ xa truy cập vào mạng nội bộ, thường dùng cho nhân viên làm việc tại nhà.
- Tại Chooky: Có thể triển khai trong tương lai để hỗ trợ nhân viên truy cập từ xa.

#### – Giao thức VPN:

##### + IPsec (Internet Protocol Security):

- Là bộ giao thức bảo mật phổ biến cho VPN, hoạt động ở tầng mạng (Layer 3).
- Bao gồm:
  - AH (Authentication Header): Xác thực tính toàn vẹn và nguồn gốc dữ liệu.
  - ESP (Encapsulating Security Payload): Mã hóa và xác thực dữ liệu.
- Tại Chooky: Sử dụng **ESP** với **esp-aes 256 esp-sha-hmac** cho VPN giữa R6-R7 và R7-R8.

##### + ISAKMP/IKE (Internet Security Association and Key Management

Protocol / Internet Key Exchange):

- ISAKMP: Định nghĩa khung quản lý kết nối bảo mật (Security Association - SA).
- IKE: Giao thức trao đổi khóa, hoạt động trong 2 giai đoạn:
  - Phase 1: Thiết lập kênh an toàn (SA chính), sử dụng **Diffie-Hellman Group 2**.
  - Phase 2: Thiết lập SA cho IPsec, mã hóa dữ liệu.
- Tại Chooky: Sử dụng **crypto isakmp policy 67** (R6 - R7) và **policy 78** (R7 - R8) với **aes 256**, **sha**, và **pre-share**.

#### – Cơ chế hoạt động của VPN:

+ Thiết lập chính sách bảo mật:

- Định nghĩa các tham số mã hóa (**encryption aes 256**), băm (**hash sha**), và xác thực (**pre-share**).
- Tại Chooky: Chính sách 67 (R6-R7) và 78 (R7-R8) sử dụng **group 2** (Diffie-Hellman 1024-bit).

+ Trao đổi khóa:

- Sử dụng khóa được chia sẻ trước (**VPNKeyR6R7!** và **VPNKeyR7R8!**) để xác thực giữa các router.

+ Mã hóa và truyền dữ liệu:

- Transform-set (**SET67**, **SET78**) định nghĩa phương thức mã hóa **esp-aes 256** và xác thực **esp-sha-hmac**.
- Dữ liệu được mã hóa trước khi truyền qua Internet.

+ Kiểm soát lưu lượng:

- ACL (Access Control List) xác định lưu lượng cần mã hóa:
  - R6-R7: ACL 110 cho phép lưu lượng giữa **128.1.7.0/24**, **12.0.0.0/16**, **128.1.0.0/24**, và **200.0.100.0/30**.
  - R7-R8: ACL 120 cho phép lưu lượng giữa **12.0.6.0/24**, **12.0.0.0/16**, **128.1.0.0/24**, và **200.0.100.0/30**.

- + Áp dụng VPN:
  - Crypto map ([VPN-MAP](#), [VPN-MAP2](#)) ánh xạ ACL và transform-set, áp dụng trên interface [S0/1/0](#) và [S0/1/1](#).
- **Ưu điểm của VPN:**
  - + Bảo mật cao: Dữ liệu được mã hóa, ngăn chặn nghe lén và giả mạo.
  - + Kết nối an toàn từ xa: Hỗ trợ nhân viên làm việc từ xa hoặc kết nối chi nhánh.
  - + Tích hợp với hạ tầng hiện có: Tại Chooky, VPN tận dụng GRE tunnel (200.0.100.0/30) để định tuyến.
- **Nhược điểm:**
  - + Độ trễ tăng: Quá trình mã hóa/giải mã làm giảm tốc độ truyền dữ liệu.
  - + Cấu hình phức tạp: Yêu cầu đồng bộ chính sách giữa các router (R6, R7, R8).
  - + Tại Chooky: Cần giám sát kết nối VPN để đảm bảo không bị gián đoạn.
- **Ứng dụng tại Chooky:**
  - + VPN giữa R6 và R7: Kết nối mạng HQ (128.1.7.0/24) với chi nhánh (12.0.0.0/16) qua địa chỉ [200.0.100.1](#) và [200.0.100.2](#).
  - + VPN giữa R7 và R8: Kết nối mạng chi nhánh (12.0.6.0/24) với HQ qua địa chỉ [200.0.100.5](#) và [200.0.100.6](#).
  - + Mục đích: Bảo vệ dữ liệu tài chính và tài liệu nội bộ khi truyền giữa các khu vực.

## 2.6 Mô hình OSI và TCP/IP

### 2.6.1 Mô hình OSI

- **Khái niệm mô hình OSI (Open Systems Interconnection):**

- + Là một mô hình tham chiếu mạng do Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) phát triển vào năm 1977.
  - + Mục đích: Chuẩn hóa các giao thức mạng, đảm bảo khả năng tương thích giữa các hệ thống khác nhau.
  - + Gồm 7 tầng (layers), mỗi tầng đảm nhiệm một chức năng cụ thể trong quá trình truyền thông mạng.
- **Các tầng của mô hình OSI:**
- + Tầng 1 - Tầng vật lý (Physical Layer):
    - Chịu trách nhiệm truyền tín hiệu vật lý qua phương tiện truyền thông (cáp, sóng vô tuyến).
    - Định nghĩa các đặc điểm phần cứng: đầu nối, điện áp, tần số, băng thông.
    - Ví dụ: Chuẩn Ethernet (IEEE 802.3), cáp UTP, chuẩn WiFi (IEEE 802.11).
  - + Tầng 2 - Tầng liên kết dữ liệu (Data Link Layer):
    - Đảm bảo truyền dữ liệu không lỗi giữa hai node trên cùng một mạng.
    - Xử lý định dạng khung (frame), kiểm soát lỗi (CRC), và kiểm soát truy cập (MAC).
    - Giao thức: Ethernet, PPP, chuẩn WiFi (802.11).
  - + Tầng 3 - Tầng mạng (Network Layer):
    - Quản lý định tuyến và chuyển tiếp gói tin giữa các mạng khác nhau.
    - Xử lý địa chỉ logic (như [IPv4](#), [IPv6](#)) và giao thức định tuyến (như [OSPF](#), [EIGRP](#)).
    - Giao thức: IP, ICMP.
  - + Tầng 4 - Tầng giao vận (Transport Layer):
    - Đảm bảo truyền dữ liệu đáng tin cậy giữa hai thiết bị.
    - Quản lý kiểm soát lỗi, kiểm soát luồng, và phân đoạn dữ liệu.

- Giao thức: **TCP** (đảm bảo độ tin cậy), **UDP** (nhANH, không đảm bảo).
- + Tầng 5 - Tầng phiên (Session Layer):
  - Quản lý và duy trì các phiên kết nối giữa hai thiết bị.
  - Hỗ trợ thiết lập, duy trì, và kết thúc phiên giao tiếp.
  - Ví dụ: Các giao thức như NetBIOS, RPC.
- + Tầng 6 - Tầng trình diễn (Presentation Layer):
  - Xử lý định dạng và mã hóa dữ liệu để các ứng dụng có thể hiểu được.
  - Chuyển đổi dữ liệu (như mã hóa SSL/TLS), nén dữ liệu, và chuẩn hóa định dạng.
  - Ví dụ: **SSL/TLS**, JPEG, MPEG.
- + Tầng 7 - Tầng ứng dụng (Application Layer):
  - Cung cấp giao diện cho người dùng và ứng dụng để truy cập dịch vụ mạng.
  - Giao thức: **HTTP**, **FTP**, **DNS**, **SMTP**.
- **Ứng dụng tại Chooky:**
  - + Tầng vật lý: Sử dụng cáp UTP (Cat6) cho mạng LAN, chuẩn **802.11ax** cho mạng WiFi.
  - + Tầng liên kết dữ liệu: Áp dụng **PPP** giữa R6-R7, **EtherChannel** giữa các switch (S1-S4).
  - + Tầng mạng: Sử dụng **IPv4** (12.0.0.0/16, 128.1.7.0/24), **IPv6** (2019:ABBA:CDDC::/48), và các giao thức định tuyến **EIGRP**, **OSPF**.
  - + Tầng giao vận: Sử dụng **TCP** cho các dịch vụ như SSH (truy cập switch), **UDP** cho DHCP.
  - + Tầng phiên: Quản lý phiên VPN giữa R6-R7 và R7-R8 bằng **ISAKMP/IKE**.

- + Tầng trình diễn: Áp dụng **SSL/TLS** cho truy cập web server (12.0.4.194) qua port **443**.
- + Tầng ứng dụng: Sử dụng **HTTP/HTTPS** cho web server, **DNS** (8.8.8.8) cho phân giải tên miền.

## 2.6.2 Mô hình TCP/IP

### – Khái niệm mô hình TCP/IP:

- + Là một mô hình tham chiếu mạng thực tế, được phát triển bởi Bộ Quốc phòng Hoa Kỳ (DoD) vào những năm 1970.
- + Là nền tảng của Internet, tập trung vào tính thực tiễn và khả năng triển khai.
- + Gồm 4 tầng, ánh xạ tương ứng với mô hình OSI.

### – Các tầng của mô hình TCP/IP:

- + Tầng liên kết (Link Layer):
  - Tương ứng với tầng vật lý và tầng liên kết dữ liệu của OSI.
  - Quản lý phần cứng và truyền dữ liệu trong cùng một mạng.
  - Giao thức: Ethernet, **PPP**, **802.11**.
- + Tầng Internet (Internet Layer):
  - Tương ứng với tầng mạng của OSI.
  - Chịu trách nhiệm định tuyến và truyền gói tin giữa các mạng.
  - Giao thức: **IP** (IPv4, IPv6), **ICMP**.
- + Tầng giao vận (Transport Layer):
  - Tương ứng với tầng giao vận của OSI.
  - Quản lý truyền dữ liệu giữa các thiết bị, kiểm soát lỗi và luồng.
  - Giao thức: **TCP**, **UDP**.
- + Tầng ứng dụng (Application Layer):
  - Tương ứng với tầng phiên, tầng trình diễn, và tầng ứng dụng của OSI.



- Cung cấp các dịch vụ mạng cho ứng dụng người dùng.
- Giao thức: [HTTP](#), [DNS](#), [FTP](#), [SMTP](#), [SSH](#).

#### – So sánh OSI và TCP/IP:

##### + Về tính lý thuyết và thực tiễn:

- OSI là mô hình lý thuyết, chuẩn hóa các giao thức trước khi triển khai.
- TCP-doupletử TCP/IP là mô hình thực tiễn, được phát triển dựa trên các giao thức đã hoạt động (như IP, TCP).

##### + Về số tầng:

- OSI có 7 tầng, phân chia chi tiết.
- TCP/IP có 4 tầng, gộp các chức năng để đơn giản hơn.

##### + Về tính ứng dụng:

- OSI được dùng để giảng dạy và tham chiếu lý thuyết.
- TCP/IP là nền tảng thực tế của Internet và hầu hết các mạng hiện đại.

#### – Ứng dụng tại Chooky:

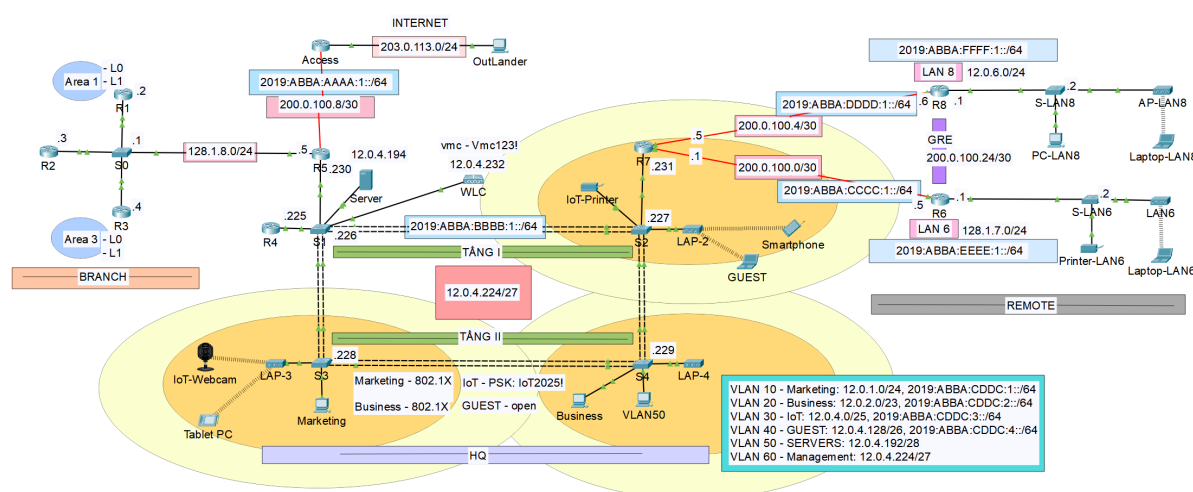
- + Tầng liên kết: Sử dụng [Ethernet](#) cho mạng LAN, [PPP](#) giữa R6-R7 và R7-R8, [802.11ax](#) cho mạng WiFi.
- + Tầng Internet: Áp dụng [IPv4](#) (12.0.0.0/16, 128.1.7.0/24), [IPv6](#) (2019:ABBA:CDDC::/48), và [ICMP](#) để kiểm tra kết nối (ping).
- + Tầng giao vận: Sử dụng [TCP](#) cho các dịch vụ đáng tin cậy (SSH, HTTPS), [UDP](#) cho các dịch vụ nhanh (DHCP, DNS).
- + Tầng ứng dụng: Triển khai [HTTP/HTTPS](#) cho web server (12.0.4.194), [DNS](#) (8.8.8.8, 2001:4860:4860::8888), [SSH](#) để quản lý switch (S1-S4).

## Chương 3

# Sơ đồ mạng tổng thể

### 3.1 Sơ đồ mạng (Network Diagram)

Sơ đồ mạng của doanh nghiệp Chooky thể hiện một hệ thống mạng phức hợp, tích hợp các công nghệ định tuyến, chuyển mạch, mạng không dây, VPN, và quản lý bảo mật. Mạng được thiết kế để kết nối Trụ sở chính (HQ) với các chi nhánh, hỗ trợ cả IPv4 và IPv6, và đáp ứng nhu cầu của hơn 80 thiết bị bao gồm nhân viên, khách, và thiết bị IoT. Dưới đây là mô tả chi tiết từ tổng quan đến các thành phần cụ thể.



Hình 3.1: Sơ đồ tổng quan hệ thống mạng

#### – Tổng quan hệ thống mạng:

- + Hệ thống bao gồm hai khu vực chính: Trụ sở chính (HQ) và các chi nhánh, kết nối qua các liên kết **PPP**, **GRE Tunnel**, và **VPN IPsec**.

- + HQ được tổ chức với các VLAN (10, 20, 30, 40, 50, 60) được đổi tên thành Marketing, Business, IoT, GUEST, SERVERS, và Management, phục vụ các phòng ban và thiết bị khác nhau.
  - + Mạng không dây được triển khai tại HQ với Wireless LAN Controller (WLC) và Lightweight Access Points (LAP), cùng với mạng không dây mở rộng tại LAN6 và LAN8.
  - + Kết nối Internet được thực hiện qua router Access, hỗ trợ NAT và DHCP, trong khi VPN đảm bảo an toàn cho lưu lượng giữa các khu vực.
  - + Bảo mật được tăng cường với ACL, RADIUS Server, và giao thức mã hóa **WPA2**.
- **Cấu trúc khu vực HQ (Headquarters):**
- + Router:
    - R4 thực hiện định tuyến liên VLAN (router-on-a-stick), kết nối với switch S1 qua trunk link để định tuyến giữa các VLAN (10, 20, 30, 40, 50).
    - R5 là trung tâm kết nối với router Access, cấu hình tuyến mặc định (**0.0.0.0/0, ::/0**) và redistribution giữa **EIGRP** và **OSPF**.
    - R6 kết nối với R7 qua **PPP** (xác thực PAP) và thiết lập **GRE Tunnel** với R8, hỗ trợ VPN IPsec.
    - R7 là router biên trung tâm, kết nối với R6, R8 qua **PPP** và VPN, sử dụng **EIGRP** cho định tuyến.
    - R8 kết nối với R7 qua **PPP** (xác thực CHAP) và tham gia **GRE Tunnel** với R6, hỗ trợ VPN IPsec.
  - + Switches:
    - S1 là **VTP Server**, quản lý các VLAN và đồng bộ với S2, S3, S4 (**VTP Clients**).
    - S2, S3, S4 gắn các LAP trong VLAN 60 (Management), hỗ trợ mạng

không dây với WLC.

- Tất cả switch sử dụng **Rapid PVST+** (S1 là root bridge cho VLAN 10, 20, 30; S2 cho VLAN 40, 50, 60) và **EtherChannel** với **LACP** giữa các switch.
- Cấu hình **SSH** chỉ cho phép từ VLAN 50 (SERVERS).

+ Mạng không dây:

- WLC quản lý các LAP gắn tại S2, S3, S4 trong VLAN 60, hỗ trợ mạng WiFi cho VLAN 10 (Marketing), 20 (Business), 30 (IoT), 40 (GUEST).
- SSID được bảo mật với **WPA2-Enterprise** (VLAN 10, 20) và **WPA2-PSK** (VLAN 30), tích hợp RADIUS Server tại **12.0.4.194**. SSID cho VLAN 40 để ở chế độ **Open**.

+ Server:

- Server tại VLAN 50 (**12.0.4.194/28**) đóng vai trò Web Server (hỗ trợ **HTTP/HTTPS**) và RADIUS Server cho xác thực **802.1X**.

+ Dịch vụ mạng:

- **NAT Overload** tại router Access ánh xạ nội bộ (**12.0.0.0/16**, **128.1.0.0/24**) ra **203.0.113.1**.
- **DHCP Server** trên R4 cấp IP động cho VLAN 10, 20, 30, 40.
- Port Forwarding chuyển tiếp **HTTP/HTTPS** (port **80**, **443**) đến server.

– **Cấu trúc khu vực Chi nhánh (Branch):**

+ Router:

- R1, R2, R3 sử dụng **OSPF đa khu vực**, với các Loopback (R1: **128.1.1.0/23**, **128.1.3.0/23**; R2: **128.1.5.0/25**; R3: **128.1.6.0/24**, **128.1.7.0/25**).

– **Mở rộng mạng không dây tại LAN6 và LAN8:**

- + LAN6 (chi nhánh R6) và LAN8 (chi nhánh R8) được mở rộng với switch và AP, hỗ trợ mạng không dây.

- + LAN6: Kết nối qua R6 với mạng `128.1.7.0/24` (IPv4) và `2019:ABBA:EEEE:1::/64` (IPv6).
- + LAN8: Kết nối qua R8 với mạng `12.0.6.0/24` (IPv4) và `2019:ABBA:FFFF:1::/64` (IPv6).
- + AP tại LAN6 và LAN8 sử dụng SSID riêng, bảo mật với **WPA2-PSK**.
- **Khu vực REMOTE:**
  - + PPP:
    - R7 ↔ R6: Sử dụng xác thực **PAP**, địa chỉ `200.0.100.0/30`.
    - R7 ↔ R8: Sử dụng xác thực **CHAP**, địa chỉ `200.0.100.4/30`.
  - + GRE Tunnel:
    - Thiết lập giữa R6 và R8 với mạng `200.0.100.24/30`, yêu cầu ít nhất 2 máy chủ kiểm tra kết nối.
  - + VPN IPsec:
    - Triển khai giữa R6-R7 và R7-R8, sử dụng **ESP** với `esp-aes 256 esp-sha-hmac`, khóa chia sẻ (**VPNKeyR6R7!**, **VPNKeyR7R8!**).
- **Cấu hình bảo mật và ACL:**
  - + ACL:
    - Chặn VLAN 30 (IoT) và VLAN 40 (GUEST) truy cập mạng nội bộ, chỉ cho phép ra Internet qua router Access.
    - Ví dụ:

```
access-list 101 deny ip 12.0.4.0 0.0.0.127 12.0.0.0 0.0.255.255,
```

```
access-list 101 permit ip 12.0.4.0 0.0.0.127 any
```

cho VLAN 30.
    - Chỉ VLAN 50 (SERVERS) được phép **SSH** vào switch.
  - + IPv6:
    - Phân bổ địa chỉ từ `2019:ABBA:CDDC::/48` cho 5 VLAN (10, 20, 30, 40, 50).

- Gán **link-local** tĩnh (**FE80::/10**) cho các interface.
- Sử dụng **EIGRP for IPv6** tại HQ, tuyến mặc định từ R5 truyền vào **EIGRP**.
- Inter-VLAN routing sử dụng sub-interface tương tự IPv4.

Sơ đồ mạng được tối ưu hóa để đảm bảo hiệu suất, bảo mật, và khả năng mở rộng, hỗ trợ các yêu cầu thực tế của doanh nghiệp Chooky.

## 3.2 Mô hình thiết kế hệ thống mạng khu vực HQ

Phần này trình bày mô hình thiết kế hệ thống mạng không dây cho trụ sở chính công ty Chooky, bao gồm hai tầng (Tầng 1 và Tầng 2) với tổng diện tích 500m<sup>2</sup> (250m<sup>2</sup>/tầng). Mục tiêu là thiết kế một hệ thống mạng ổn định, hiệu quả, đảm bảo độ phủ sóng WiFi mạnh mẽ và liên tục, đồng thời hỗ trợ các hoạt động kinh doanh, quản lý, và vận hành nội bộ. Thiết kế dựa trên các nguyên tắc kỹ thuật hiện đại, tận dụng các thiết bị mạng tiên tiến và phân tích tính hiệu thực tế.

### 3.2.1 Kiến trúc tổng thể

Hệ thống được thiết kế theo mô hình phân cấp (hierarchical design) với ba lớp chính:

- **Lớp truy cập (Access Layer)**: Bao gồm các Access Point (LAP) và Switch để kết nối các thiết bị cuối.
- **Lớp phân phối (Distribution Layer)**: Bao gồm Router và Wireless LAN Controller (WLC) để quản lý lưu lượng và định tuyến dữ liệu giữa các tầng.
- **Lớp lõi (Core Layer)**: Bao gồm Server trung tâm để lưu trữ dữ liệu và quản lý toàn bộ hệ thống.

Kiến trúc này đảm bảo khả năng mở rộng, quản lý tập trung, và giảm thiểu điểm nghẽn trong mạng.

### 3.2.2 Phân tích thiết kế

Thiết kế hệ thống được thực hiện dựa trên các yếu tố sau:

#### *Nhu cầu sử dụng*

- **Phòng máy (Tầng 1):** Cần kết nối ổn định cho Server, Router, Switch, và WLC, đồng thời hỗ trợ các thiết bị IoT (camera, cảm biến, điều hòa).
- **Phòng Quản lý (Tầng 1):** Phục vụ công việc quản lý, yêu cầu tín hiệu WiFi mạnh mẽ và liên tục.
- **Phòng Kinh doanh và Marketing (Tầng 2):** Yêu cầu băng thông cao, hỗ trợ họp trực tuyến và trao đổi dữ liệu.
- **Phòng nghỉ trưa (Tầng 2):** Cần phủ sóng WiFi nhẹ để nhân viên sử dụng, và điều hòa để đảm bảo tiện nghi.

#### *Phân tích môi trường*

- **Diện tích:** Mỗi tầng 250m<sup>2</sup> (25m x 10m), với tường bê tông dày 0.5m, cửa sổ kính, và các góc tường gây nhiễu xạ.
- **Vật cản:**
  - + Tường bê tông: Suy giảm tín hiệu 3 dBm mỗi bức.
  - + Cửa sổ kính: Suy giảm 2 dBm do khúc xạ.
  - + Góc tường: Suy giảm 2 dBm do nhiễu xạ.

#### *Mật độ thiết bị*

Tổng cộng khoảng 80-100 thiết bị cùng lúc, bao gồm:

- PC, laptop, điện thoại: Dành cho 40-50 nhân viên (mỗi người 1 laptop và 1 điện thoại).
- Thiết bị IoT (camera, cảm biến, đèn, máy in): Phân bổ đều cho các phòng.

#### **Phân bổ:**

- Tầng 1: 40 thiết bị (Phòng máy: 10, Phòng Quản lý: 30).

- Tầng 2: 60 thiết bị (Phòng Kinh doanh: 25, Phòng Marketing: 25, Phòng nghỉ trưa: 10).

### *Phạm vi phủ sóng*

- Mỗi LAP (Cisco Aironet 1852I) có phạm vi lý tưởng 20m (bán kính), nhưng bị ảnh hưởng bởi vật cản.
- Tầng 1: 1 LAP (S2) tại trung tâm Phòng Quản lý (12,5), đảm bảo phủ sóng toàn tầng.
- Tầng 2: 2 LAP (S3 tại 6,5, S4 tại 16,5) để phủ sóng đồng đều, giảm thiểu vùng chết.

### *Tối ưu hóa*

- Đặt LAP tại trung tâm các phòng lớn để tối đa hóa vùng phủ sóng.
- Sử dụng WLC để quản lý tập trung, tối ưu hóa hiệu suất và giảm nhiễu.
- Đảm bảo vùng chồng lấn tín hiệu giữa các LAP ở Tầng 2 để tránh gián đoạn.

## **3.2.3 Loại thiết bị**

Hệ thống sử dụng các thiết bị mạng và thiết bị cuối hiện đại, được lựa chọn dựa trên tính năng, hiệu suất, và độ tương thích. Danh sách thiết bị bao gồm:

### *Access Point (LAP)*

- **Model:** Cisco Aironet 1852I.
- **Thông số kỹ thuật:**
  - + Chuẩn WiFi: 802.11ac Wave 2, hỗ trợ 2.4 GHz và 5 GHz.
  - + Tốc độ tối đa: 1.7 Gbps.
  - + Phạm vi phủ sóng: 20m (bán kính) trong điều kiện lý tưởng.
  - + Công suất phát: Có thể điều chỉnh, tối đa -20 dBm.



- + Số lượng kết nối đồng thời: Hỗ trợ tối đa 50 thiết bị.
- **Số lượng:** 3 (S2 tại Tầng 1, S3 và S4 tại Tầng 2).

### *Router*

- **Model:** Cisco ISR 1000 Series (R4, R5, R7).
- **Thông số kỹ thuật:**
  - + Tốc độ định tuyến: Lên đến 1 Gbps.
  - + Cổng: 4 cổng Gigabit Ethernet.
  - + Hỗ trợ: VPN, QoS, và bảo mật nâng cao.
- **Số lượng:** 3, đặt tại Phòng máy (Tầng 1).

### *Switch*

- **Model:** Cisco Catalyst 9200 Series (S1, S2, S3, S4).
- **Thông số kỹ thuật:**
  - + Cổng: 24 cổng Gigabit Ethernet.
  - + Tốc độ chuyển mạch: 128 Gbps.
  - + Hỗ trợ: PoE+ (Power over Ethernet) để cấp nguồn cho LAP và camera.
- **Số lượng:** 4 (S1 và S2 tại Tầng 1, S3 và S4 tại Tầng 2).

### *Wireless LAN Controller (WLC)*

- **Model:** Cisco Catalyst 9800-L.
- **Thông số kỹ thuật:**
  - + Quản lý: Tối đa 250 LAP và 5,000 thiết bị.
  - + Hỗ trợ: WPA3, xác thực RADIUS, tối ưu hóa kênh tự động.
- **Vị trí:** Phòng máy (Tầng 1).

### *Server*

- **Model:** Dell PowerEdge R240.

- **Thông số kỹ thuật:**
  - + CPU: Intel Xeon E-2224.
  - + RAM: 16GB.
  - + Lưu trữ: 2TB HDD (RAID 1).
  - + Hệ điều hành: Windows Server 2019.
  - + Địa chỉ IP: 12.0.4.194.
- **Vị trí:** Phòng máy (Tầng 1).

### *Thiết bị cuối*

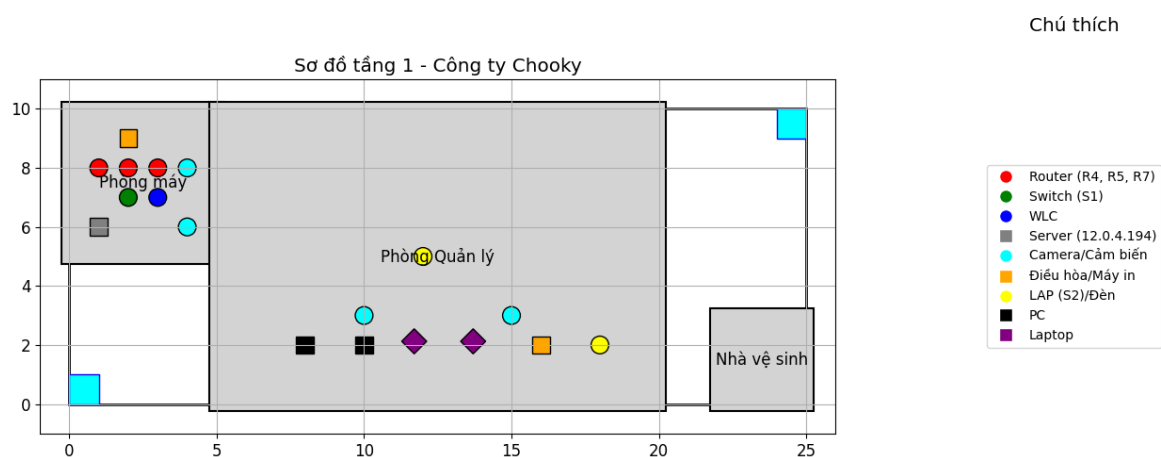
- **Tầng 1:**
  - + Phòng máy: 5 camera, 5 cảm biến, 1 điều hòa.
  - + Phòng Quản lý: 10 laptop, 5 điện thoại, 5 camera, 5 cảm biến, 2 máy in, 3 đèn, 1 điều hòa.
- **Tầng 2:**
  - + Phòng Kinh doanh: 10 laptop, 10 điện thoại, 5 camera, 5 cảm biến, 2 máy in, 3 đèn, 1 điều hòa.
  - + Phòng Marketing: 10 laptop, 10 điện thoại, 5 camera, 5 cảm biến, 2 máy in, 3 đèn, 1 điều hòa.
  - + Phòng nghỉ trưa: 5 điện thoại, 2 camera, 2 cảm biến, 1 đèn, 1 điều hòa.
- **Tổng cộng:**
  - + Laptop: 30.
  - + Điện thoại: 30.
  - + Camera: 17.
  - + Cảm biến: 17.
  - + Máy in: 6.
  - + Đèn: 10.

- + Điều hòa: 5 (mỗi phòng 1 chiếc).

### 3.2.4 Bố trí không gian

#### – Tầng 1 (25m x 10m):

- + **Phòng máy:** Góc trái (0,5) đến (5,10), chứa Server, Router (R4, R5, R7), Switch S1, WLC, 5 camera, 5 cảm biến, 1 điều hòa.
- + **Phòng Quản lý:** (5,0) đến (20,10), chứa LAP (S2) tại (12,5), 10 laptop, 5 điện thoại, 5 camera, 5 cảm biến, 2 máy in, 3 đèn, 1 điều hòa.
- + **Nhà vệ sinh:** Góc phải (22,0) đến (25,3).
- + **Cửa ra vào:** Góc dưới bên trái (0,0).
- + **Cửa sổ:** Góc trên bên phải (24,9).

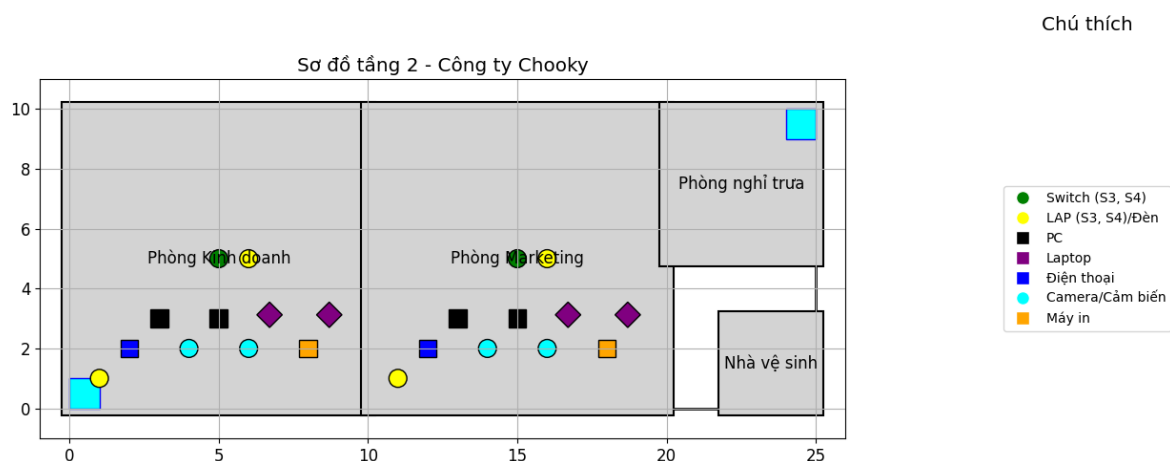


Hình 3.2: Sơ đồ tầng 1

#### – Tầng 2 (25m x 10m):

- + **Phòng Kinh doanh:** (0,0) đến (10,10), chứa Switch S3, LAP (S3) tại (6,5), 10 laptop, 10 điện thoại, 5 camera, 5 cảm biến, 2 máy in, 3 đèn, 1 điều hòa.
- + **Phòng Marketing:** (10,0) đến (20,10), chứa Switch S4, LAP (S4) tại (16,5), 10 laptop, 10 điện thoại, 5 camera, 5 cảm biến, 2 máy in, 3 đèn, 1 điều hòa.

- + **Phòng nghỉ trưa:** Góc trên phải (20,5) đến (25,10), chứa 5 điện thoại, 2 camera, 2 cảm biến, 1 đèn, 1 điều hòa.
- + **Nhà vệ sinh:** Góc dưới phải (22,0) đến (25,3).
- + **Cửa ra vào:** Góc dưới bên trái (0,0).
- + **Cửa sổ:** Góc trên bên phải (24,9).



Hình 3.3: Sơ đồ tầng 2

Bố trí được tối ưu hóa để LAP đặt tại trung tâm các phòng lớn, đảm bảo phủ sóng đều và giảm thiểu tín hiệu bị suy yếu bởi tường hoặc góc cạnh.

### 3.2.5 Tính toán suy hao mạng không dây

Suy hao tín hiệu được tính toán dựa trên mô hình **Log-Distance Path Loss** và ảnh hưởng của vật cản trong môi trường văn phòng. Các tham số chính bao gồm:

*Công thức Path Loss*

$$PL = PL_0 + 10 \cdot n \cdot \log_{10}(d/d_0)$$

- $PL_0$ : Path Loss tại khoảng cách tham chiếu  $d_0 = 1m$ , giả định  $PL_0 = 40$  dB (tần số 2.4 GHz).
- $n$ : Hệ số suy giảm, chọn  $n = 2.0$  (môi trường văn phòng thoáng).

- $d$ : Khoảng cách từ LAP đến điểm nhận tín hiệu.
- $d_0$ : Khoảng cách tham chiếu, 1m.

### Công suất phát

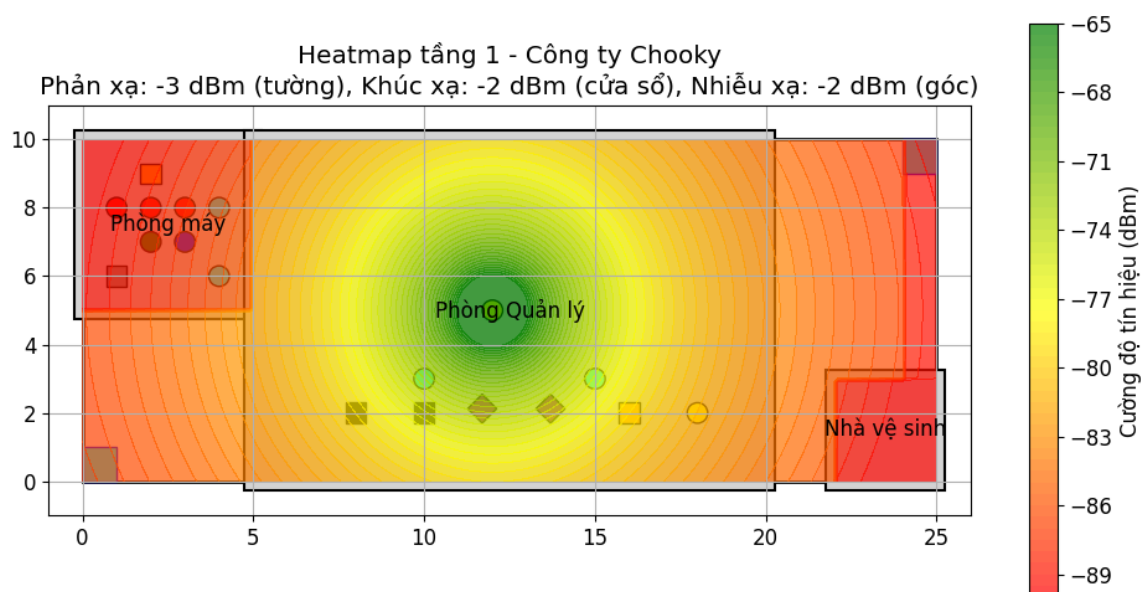
- LAP Cisco Aironet 1852I: -20 dBm (mức trung bình).

### Suy giảm do vật cản

- Tường bê tông: -3 dBm mỗi bức.
- Cửa sổ kính (khúc xạ): -2 dBm.
- Nhiều xạ (góc tường): -2 dBm.

### Tính toán tại các điểm cụ thể

- **Tầng 1 - LAP (S2) tại (12,5):**



Hình 3.4: Sơ đồ phủ sóng tầng 1

- + **Điểm A (12,8) - Cách LAP 3m, không vật cản:**

$$PL = 40 + 10 \cdot 2 \cdot \log_{10}(3/1) = 40 + 20 \cdot 0.477 = 40 + 9.54 = 49.54 \text{ dB}$$

$$\text{RSSI} = -20 - 49.54 = -69.54 \text{ dBm (vùng vàng, tín hiệu trung bình).}$$

- + **Điểm B (2,5) - Cách LAP 10m, qua tường phòng máy (x=5):**

$$PL = 40 + 10 \cdot 2 \cdot \log_{10}(10/1) = 40 + 20 \cdot 1 = 60 \text{ dB}$$

Suy giảm vật cản: -3 dBm (tường) + -2 dBm (nhiều xạ) = -5 dBm.

RSSI = -20 - 60 - 5 = -85 dBm (vùng đỏ, tín hiệu yếu).

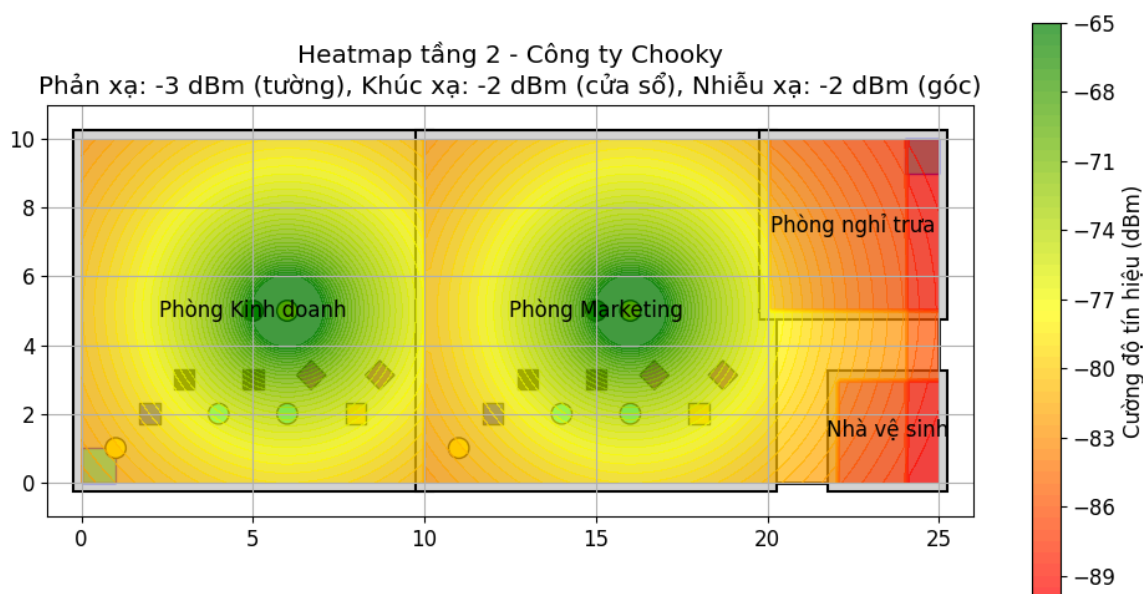
- + **Điểm C (24,9) - Cách LAP 13m, qua cửa sổ (x=24):**

$$PL = 40 + 10 \cdot 2 \cdot \log_{10}(13/1) = 40 + 20 \cdot 1.114 = 40 + 22.28 = 62.28 \text{ dB}$$

Suy giảm vật cản: -2 dBm (cửa sổ) + -2 dBm (nhiều xạ) = -4 dBm.

RSSI = -20 - 62.28 - 4 = -86.28 dBm (vùng đỏ, tín hiệu yếu).

- **Tầng 2 - LAP (S3) tại (6,5):**



Hình 3.5: Sơ đồ phủ sóng tầng 2

- + **Điểm D (6,8) - Cách LAP 3m, không vật cản:**

$$PL = 40 + 10 \cdot 2 \cdot \log_{10}(3/1) = 49.54 \text{ dB}$$

RSSI = -20 - 49.54 = -69.54 dBm (vùng vàng).

- + **Điểm E (15,5) - Cách LAP 9m, qua tường giữa phòng (x=10):**

$$PL = 40 + 10 \cdot 2 \cdot \log_{10}(9/1) = 40 + 20 \cdot 0.954 = 40 + 19.08 = 59.08 \text{ dB}$$

Suy giảm vật cản:  $-3 \text{ dBm (tường)} + -2 \text{ dBm (nhiều xạ)} = -5 \text{ dBm}$ .

$\text{RSSI} = -20 - 59.08 - 5 = -84.08 \text{ dBm (vùng đỏ)}$ .

### *Kết luận suy hao*

- Tín hiệu mạnh nhất ( $-20 \text{ dBm}$ ) tại vị trí LAP, giảm dần theo khoảng cách.
- Vùng xanh ( $-20 \text{ dBm}$  đến  $-50 \text{ dBm}$ ) kéo dài 3-4m, vùng vàng ( $-50 \text{ dBm}$  đến  $-70 \text{ dBm}$ ) kéo dài 8-10m.
- Vật cản (tường, cửa sổ, góc) làm tín hiệu suy giảm đáng kể, nhưng hệ thống vẫn đảm bảo phủ sóng toàn bộ hai tầng.

### **3.2.6 Phân tích độ phủ sóng (Heatmap)**

Heatmap được xây dựng dựa trên mô hình Log-Distance Path Loss với các tham số:

- **Công suất phát:**  $-20 \text{ dBm}$ .
- **Hệ số suy giảm:**  $n = 2.0$ .
- **Suy giảm vật cản:**
  - + Tường bê tông:  $-3 \text{ dBm}$ .
  - + Cửa sổ kính:  $-2 \text{ dBm}$ .
  - + Nhiều xạ:  $-2 \text{ dBm}$ .
- **Phạm vi tín hiệu:**
  - + Vùng xanh ( $-20 \text{ dBm}$  đến  $-50 \text{ dBm}$ ): Tín hiệu mạnh, kéo dài 3-4m từ LAP.
  - + Vùng vàng ( $-50 \text{ dBm}$  đến  $-70 \text{ dBm}$ ): Tín hiệu trung bình, kéo dài 8-10m.
  - + Vùng đỏ ( $-70 \text{ dBm}$  đến  $-90 \text{ dBm}$ ): Tín hiệu yếu, còn lại trong phạm vi.
- **Kết quả:**
  - + **Tầng 1:** LAP (S2) tại (12,5) phủ sóng toàn bộ Phòng Quản lý, giảm

nhẹ qua tường phòng máy và nhà vệ sinh.

- + **Tầng 2:** LAP (S3) và (S4) tại (6,5) và (16,5) đảm bảo phủ sóng toàn tầng, với vùng chồng lấn giữa hai LAP ở giữa phòng.

### 3.2.7 Yêu cầu kỹ thuật

- **Băng thông:** Đảm bảo tốc độ tối thiểu 50 Mbps cho mỗi người dùng, phù hợp với nhu cầu kinh doanh và quản lý.
- **Bảo mật:** Sử dụng mã hóa WPA2/WPA3, xác thực RADIUS qua WLC.
- **Khả năng mở rộng:** Hệ thống hỗ trợ thêm LAP hoặc thiết bị khi công ty mở rộng.
- **Quản lý:** Sử dụng phần mềm Cisco DNA Center để giám sát và tối ưu hóa mạng.

## Kết luận phần mô hình

Mô hình thiết kế hệ thống mạng không dây cho công ty Chooky được xây dựng với sự cân nhắc kỹ lưỡng về phân tích nhu cầu, lựa chọn thiết bị, bố trí không gian, và tính toán suy hao tín hiệu. Bố trí hai tầng với tổng cộng 3 LAP, kết hợp WLC và Server trung tâm, đảm bảo đáp ứng nhu cầu sử dụng thực tế, đồng thời cung cấp nền tảng cho việc nâng cấp trong tương lai.

## 3.3 Kế hoạch địa chỉ (Address Planning - IPv4)

### Trụ sở chính (HQ) - Class A: 12.0.0.0/8

- Mạng trụ sở HQ sử dụng địa chỉ lớp A 12.0.0.0/8, cung cấp khoảng 16.7 triệu địa chỉ.
- Các VLAN tại trụ sở chính được cấp phát địa chỉ như sau:



Bảng 3.1: Cấp phát địa chỉ cho VLAN tại trụ sở chính

VLAN	Tên VLAN	Số Host	Subnet	Host khả dụng	Gateway
10	Marketing	200	12.0.1.0/24	254	12.0.1.1
20	Business	300	12.0.2.0/23	510	12.0.2.1
30	IoT	100	12.0.4.0/25	126	12.0.4.1
40	GUEST	50	12.0.4.128/26	62	12.0.4.129
50	SERVERS	10	12.0.4.192/28	14	12.0.4.193
60	Management	20	12.0.4.224/27	30	12.0.4.225

## Chi nhánh (Branch) - Class B: 128.1.0.0/16

- Chi nhánh sử dụng địa chỉ lớp B 128.1.0.0/16, cung cấp khoảng 65 nghìn địa chỉ.
- Các Loopback được cấu hình như sau (từ Bảng 3):

Bảng 3.2: Cấp phát địa chỉ Loopback tại chi nhánh

Thiết bị	Interface	Số Host	Subnet	Host khả dụng	Gateway
R1	Lo0	500	128.1.0.0/23	510	128.1.0.1
R1	Lo1	300	128.1.2.0/23	510	128.1.2.1
R2	Lo0	100	128.1.4.0/25	126	128.1.4.1
R3	Lo0	200	128.1.5.0/24	254	128.1.5.1
R3	Lo1	100	128.1.6.0/25	126	128.1.6.1

## Các liên kết trong mô hình mạng

Bảng 3.3: IP và Subnet cho các liên kết trong mô hình mạng

Liên kết	Mạng / Subnet	Thiết bị - Địa chỉ IP
R7 ↔ R6	200.0.100.0/30	R7: 200.0.100.1, R6: 200.0.100.2
R7 ↔ R8	200.0.100.4/30	R7: 200.0.100.5, R8: 200.0.100.6
R5 ↔ ACCESS	200.0.100.8/30	R5: 200.0.100.9, ACCESS: 200.0.100.10
R1 ↔ S0	128.1.8.0/24	R1: 128.1.8.2, S0: 128.1.8.1 (VLAN 1)
R2 ↔ S0	128.1.8.0/24	R2: 128.1.8.3, S0: 128.1.8.1 (VLAN 1)
R3 ↔ S0	128.1.8.0/24	R3: 128.1.8.4, S0: 128.1.8.1 (VLAN 1)
R5 ↔ S1	128.1.8.0/24	R5: 128.1.8.5, S0: 128.1.8.1 (VLAN 1)
S1, S2, S3, S4 ↔ R4, R5, R7	12.0.4.224/27	S1: 12.0.4.226, S2: 12.0.4.227, S3: 12.0.4.228, S4: 12.0.4.229 R4: 12.0.4.225, R5: 12.0.4.230, R7: 12.0.4.231 (VLAN 60)

- Tại khu vực Branch, switch S0 được cấu hình với VLAN 1 (128.1.8.0/24) để kết nối các router R1, R2, R3.
- Địa chỉ IP của S0 là 128.1.8.1/24, trong khi R1, R2, R3 được gán địa chỉ trong cùng subnet (128.1.8.2, 128.1.8.3, 128.1.8.4) trên giao diện kết nối với S0.

## Kết nối GRE Tunnel

- GRE Tunnel giữa R6 và R8 sử dụng địa chỉ 200.0.100.24/30:
  - + R6: 200.0.100.25
  - + R8: 200.0.100.26

## LAN cục bộ

- LAN 6 (kết nối với R6): 128.1.7.0/24
- LAN 8 (kết nối với R8): 12.0.6.0/24

## 3.4 Kế hoạch địa chỉ IPv6

- Hệ thống mạng sử dụng địa chỉ IPv6 theo chuẩn /64 cho mỗi mạng con.
- Các dải địa chỉ được cấp phát theo chức năng như sau:

### 3.4.1 Kết nối các liên kết mạng

Bảng 3.4: Địa chỉ IPv6 cho kết nối giữa các router

Kết nối	Dải địa chỉ IPv6	Thiết bị
ACCESS ↔ R5	2019:ABBA:AAAA:1::/64	ACCESS: ::1, R5: ::2
R4, R5, R7 (liên kết ba chiều)	2019:ABBA:BBBB:1::/64	R4: ::1, R5: ::2, R7: ::3
R7 ↔ R6	2019:ABBA:CCCC:1::/64	R7: ::1, R6: ::2
R7 ↔ R8	2019:ABBA:DDDD:1::/64	R7: ::1, R8: ::2

### 3.4.2 LAN nội bộ

Bảng 3.5: Địa chỉ IPv6 cho các mạng LAN

Thiết bị	Dải địa chỉ IPv6	Ghi chú
LAN R6	2019:ABBA:EEEE:1::/64	Mạng LAN cục bộ tại R6
LAN R8	2019:ABBA:FFFF:1::/64	Mạng LAN cục bộ tại R8

### 3.4.3 VLAN tại Trụ sở chính (HQ)

Bảng 3.6: Địa chỉ IPv6 cấp phát cho các VLAN

VLAN	Tên	Địa chỉ IPv6
10	Marketing	2019:ABBA:CDDC:1::/64
20	Business	2019:ABBA:CDDC:2::/64
30	IoT	2019:ABBA:CDDC:3::/64
40	GUEST	2019:ABBA:CDDC:4::/64

### 3.4.4 Link-local Address ( $FE80::/10$ )

- Tất cả thiết bị mạng cần cấu hình địa chỉ link-local thuộc dải  $FE80::/10$ .

Bảng 3.7: Địa chỉ IPv6 Link-local cấu hình trên các thiết bị

Interface	R4	R5	R6	R7	R8	ACCESS
Gig0/0/0.10	FE80::4:10					
Gig0/0/0.20	FE80::4:20					
Gig0/0/0.30	FE80::4:30					
Gig0/0/0.40	FE80::4:40					
Gig0/0/0.60	FE80::4					
S0/1/0		FE80::5:1		FE80::7:2	FE80::8	FE80::A
Gig0/0/1		FE80::5				
Gig0/0/0			FE80::6:1	FE80::7	FE80::8:1	
S0/1/0			FE80::6			
S0/1/1				FE80::7:1		

## 3.5 Giải pháp bảo mật

Phần này trình bày các giải pháp bảo mật toàn diện được triển khai trong hệ thống mạng của doanh nghiệp Chooky, nhằm đảm bảo an toàn cho

dữ liệu, thiết bị, và lưu lượng mạng trên cả mạng có dây, mạng không dây, kết nối VPN, và quản lý truy cập. Các biện pháp bảo mật được thiết kế để bảo vệ lưu lượng giữa trụ sở chính (HQ) và chi nhánh, ngăn chặn truy cập trái phép, đảm bảo tính toàn vẹn dữ liệu, và đáp ứng yêu cầu bảo vệ trước các mối đe dọa từ bên trong lẫn bên ngoài. Phạm vi áp dụng bao gồm toàn bộ hệ thống mạng với hơn 80 thiết bị (nhân viên, khách, IoT) tại HQ, chi nhánh, và khu vực REMOTE.

### 3.5.1 Tổng quan giải pháp bảo mật

– **Mục tiêu:**

- + Bảo vệ lưu lượng giữa HQ và chi nhánh, đảm bảo dữ liệu của hơn 45 nhân viên và 15 thiết bị IoT được an toàn.
- + Ngăn chặn truy cập trái phép từ các nguồn không được phép (như VLAN GUEST, IoT).
- + Đảm bảo tính toàn vẹn dữ liệu, đặc biệt trên các kết nối từ xa và mạng không dây.

– **Các biện pháp chính:**

- + Phân vùng mạng bằng VLAN và Access Control List (ACL) để kiểm soát truy cập.
- + Mã hóa lưu lượng qua VPN IPsec và bảo mật WiFi với [WPA3](#).
- + Xác thực người dùng qua RADIUS Server và quản lý truy cập từ xa qua [SSH](#).
- + Triển khai firewall và IDS/IPS để phát hiện và ngăn chặn tấn công.

– **Phạm vi áp dụng:**

- + Toàn bộ hệ thống mạng tại công ty Chooky, bao gồm:
  - **HQ (Tầng 1 và Tầng 2):** 80-100 thiết bị (30 laptop, 30 điện thoại, 17 camera, 17 cảm biến, 6 máy in, 10 đèn, 5 điều hòa).
  - **Chi nhánh và khu vực REMOTE:** Kết nối qua VPN IPsec

giữa các router (R6-R7, R7-R8).

- Các tài nguyên nội bộ như Server tại địa chỉ 12.0.4.194.

### 3.5.2 An ninh vật lý

An ninh vật lý tập trung vào việc bảo vệ các thiết bị mạng và cơ sở hạ tầng vật lý của công ty Chooky, ngăn chặn truy cập trái phép và đảm bảo an toàn cho các tài sản quan trọng.

#### *Bảo vệ thiết bị mạng*

- **Vị trí thiết bị:** Các thiết bị quan trọng như Server (Dell PowerEdge R240), Router (Cisco ISR 1000 Series: R4, R5, R7), Switch (Cisco Catalyst 9200 Series: S1, S3, S4), và Wireless LAN Controller (WLC - Cisco Catalyst 9800-L) được đặt trong Phòng máy tại Tầng 1. Phòng máy được thiết kế với cửa thép chống trộm và khóa mã số, đảm bảo chỉ có nhân viên được ủy quyền mới có thể truy cập.
- **Tủ rack khóa:** Các thiết bị mạng được đặt trong tủ rack có khóa vật lý, với các biện pháp chống rung và chống cháy (hệ thống báo cháy tự động được lắp đặt trong phòng).
- **Hệ thống làm mát:** Phòng máy được trang bị điều hòa (Daikin Inverter 1.5HP) để duy trì nhiệt độ ổn định (22-24°C), tránh tình trạng quá nhiệt gây hỏng thiết bị.

#### *Kiểm soát truy cập phòng máy*

- **Hệ thống kiểm soát truy cập:** Sử dụng thẻ từ RFID để kiểm soát ra vào Phòng máy. Mỗi nhân viên được cấp thẻ từ riêng, và hệ thống ghi lại nhật ký ra vào (giờ, mã nhân viên) để theo dõi.
- **Camera giám sát:** Lắp đặt 5 camera trong Phòng máy để giám sát 24/7, với góc quay bao phủ toàn bộ khu vực đặt thiết bị. Hình ảnh được lưu trữ trên Server trong 30 ngày để phục vụ điều tra nếu cần.

- **Nhân sự trực ban:** Bố trí nhân viên IT trực ban tại Phòng máy trong giờ làm việc (8:00-17:00) để xử lý sự cố ngay lập tức. Ngoài giờ, hệ thống báo động được kích hoạt và kết nối với điện thoại của quản lý IT.

### 3.5.3 Phân vùng mạng và kiểm soát truy cập

Phân vùng mạng và kiểm soát truy cập giúp tách biệt lưu lượng giữa các nhóm người dùng và thiết bị, giảm nguy cơ lây lan mã độc và truy cập trái phép.

*Sử dụng VLAN để tách biệt lưu lượng*

#### – Cấu hình VLAN:

- + VLAN 10 (Marketing): Dành cho nhân viên Phòng Marketing (Tầng 2), bao gồm 10 laptop và 10 điện thoại.
- + VLAN 20 (Business): Dành cho nhân viên Phòng Kinh doanh (Tầng 2) và Phòng Quản lý (Tầng 1), bao gồm 20 laptop và 20 điện thoại.
- + VLAN 30 (IoT): Dành cho thiết bị IoT tại cả hai tầng (17 camera, 17 cảm biến, 10 đèn, 5 điều hòa).
- + VLAN 40 (GUEST): Dành cho khách, bao gồm kết nối WiFi tạm thời (5 điện thoại tại Phòng nghỉ trưa Tầng 2).
- + VLAN 50 (SERVERS): Dành cho Server tại địa chỉ 12.0.4.194 (Phòng máy, Tầng 1).
- + VLAN 60 (Management): Dành cho quản lý, bao gồm WLC, Router, Switch, và các thiết bị quản trị (12.0.4.224/27).

#### – Cô lập VLAN:

- + VLAN 30 (IoT) và VLAN 40 (GUEST) bị cô lập khỏi VLAN nội bộ (10, 20, 50) để ngăn chặn truy cập trái phép.
- + Thiết bị IoT chỉ được phép giao tiếp với Server tại 12.0.4.194 (ví dụ: gửi dữ liệu từ camera, cảm biến).

## Áp dụng Access Control List (ACL)

### – Chặn truy cập trái phép:

#### + VLAN 30 (IoT):

- `access-list 101 deny ip 12.0.4.0 0.0.0.127 12.0.0.0 0.0.255.255`: Chặn VLAN 30 truy cập mạng nội bộ.
- `access-list 101 permit ip 12.0.4.0 0.0.0.127 any`  
Cho phép ra Internet.

#### + VLAN 40 (GUEST):

- `access-list 102 deny ip 12.0.4.128 0.0.0.63 12.0.0.0 0.0.255.255`: Chặn VLAN 40 truy cập mạng nội bộ.
- `access-list 102 permit ip 12.0.4.128 0.0.0.63 any`  
Cho phép ra Internet.

### – Quản lý truy cập quản trị:

#### + Chỉ VLAN 50 (SERVERS) được phép SSH vào Switch:

- `access-list 103 permit tcp 12.0.4.192 0.0.0.15 any eq 22`: Cho phép Server tại 12.0.4.194 truy cập SSH.

#### + Quản lý từ xa chỉ cho phép từ VLAN 60 (Management):

- `access-list 104 permit tcp 12.0.4.224 0.0.0.31 any eq 22`: Cho phép từ 12.0.4.224/27.
- `access-list 104 deny tcp any any eq 22`: Chặn các kết nối SSH khác.

## 3.5.4 Bảo mật mạng không dây

Bảo mật mạng không dây đảm bảo an toàn cho các kết nối WiFi tại HQ, chi nhánh, và khu vực REMOTE, đồng thời hỗ trợ roaming liên mạch và quản lý tập trung.

*Triển khai WPA3 cho các SSID*

### – SSID tại HQ, LAN6, và LAN8:

- + SSID cho VLAN 10 (Marketing), VLAN 20 (Business), và VLAN 30 (IoT):
  - Sử dụng **WPA3-Enterprise** với xác thực **802.1X**, tích hợp RADIUS Server tại **12.0.4.194**.
  - RADIUS Server xác thực người dùng và thiết bị IoT dựa trên chứng chỉ số (certificate-based authentication).
- + SSID cho VLAN 40 (GUEST):
  - Sử dụng **WPA3-PSK** với mật khẩu thay đổi định kỳ (hàng tuần) để giảm nguy cơ bị xâm nhập.
  - Mật khẩu được quản lý bởi đội ngũ IT và chỉ cung cấp cho khách khi cần thiết.

### *Quản lý tập trung qua WLC*

- WLC (Cisco Catalyst 9800-L) trong VLAN 60 (Management) quản lý 3 LAP (S2, S3, S4) tại HQ, đảm bảo:
  - + Roaming liên mạch giữa các LAP (nhân viên di chuyển giữa các phòng không bị mất kết nối).
  - + Áp dụng chính sách bảo mật đồng bộ (ví dụ: **WPA3**, ACL) trên tất cả LAP.

### *Cô lập thiết bị IoT*

- Thiết bị IoT trong VLAN 30 (17 camera, 17 cảm biến, 10 đèn, 5 điều hòa) bị giới hạn truy cập:
  - + Chỉ được phép giao tiếp với Server tại **12.0.4.194** để gửi/nhận dữ liệu (ví dụ: dữ liệu nhiệt độ từ cảm biến, video từ camera).
  - + ACL trên Switch (S1, S3, S4) chặn các kết nối khác từ VLAN 30.

## **3.5.5 Bảo mật VPN**

Bảo mật VPN đảm bảo an toàn cho các kết nối từ xa giữa HQ, chi nhánh, và khu vực REMOTE, đặc biệt là lưu lượng giữa các router R6-R7



và R7-R8.

### *VPN IPsec trong khu vực REMOTE*

#### – Cấu hình VPN IPsec:

- + Sử dụng **ESP** (Encapsulating Security Payload) với:
  - **esp-aes 256 esp-sha-hmac**: Mã hóa bằng AES-256 và xác thực bằng SHA-HMAC.
- + Khóa chia sẻ:
  - R6-R7: **VPNKeyR6R7!**.
  - R7-R8: **VPNKeyR7R8!**.
- + ACL xác định lưu lượng cần mã hóa:
  - R6-R7: **access-list 110 permit ip 128.1.7.0 0.0.0.255 12.0.0.0 0.0.255.255** (và ngược lại).
  - R7-R8: **access-list 120 permit ip 12.0.6.0 0.0.0.255 128.1.7.0 0.0.255.255** (và ngược lại).

#### – Chính sách ISAKMP:

- + Sử dụng **AES 256**, **SHA**, và nhóm Diffie-Hellman 2 để thiết lập kênh bảo mật (phase 1).
- + Phase 2 sử dụng **ESP** để mã hóa lưu lượng thực tế.

### *VPN cho nhân viên từ xa*

- Sử dụng Cisco AnyConnect VPN trên Router Cisco ISR 1000 Series để hỗ trợ nhân viên làm việc từ xa:
  - + Mã hóa lưu lượng bằng IPsec (AES-256).
  - + Xác thực qua MFA (mật khẩu + OTP, xem phần Quản lý người dùng).

## 3.5.6 Quản lý truy cập từ xa

Quản lý truy cập từ xa đảm bảo chỉ các quản trị viên được ủy quyền mới có thể truy cập hệ thống mạng từ xa.

### *Sử dụng SSH để quản lý thiết bị*

- **Thiết bị áp dụng:** Router (R1-R8) và Switch (S1-S4).
- **Kiểm soát truy cập:**
  - + Chỉ cho phép truy cập từ VLAN 60 (Management) hoặc địa chỉ cụ thể (12.0.4.224/27).
  - + ACL:
    - `access-list 104 permit tcp 12.0.4.224 0.0.0.31 any eq 22`: Cho phép SSH từ 12.0.4.224/27.
    - `access-list 104 deny tcp any any eq 22`: Chặn các kết nối SSH khác.

### *Quản lý mật khẩu*

- Mật khẩu quản trị được mã hóa bằng lệnh `service password-encryption` trên các thiết bị Cisco.
- Yêu cầu mật khẩu phức tạp: ít nhất 12 ký tự, bao gồm chữ hoa, chữ thường, số, và ký tự đặc biệt.

## **3.5.7 Phát hiện và ngăn chặn tấn công**

Phát hiện và ngăn chặn tấn công giúp bảo vệ hệ thống mạng trước các mối đe dọa từ bên ngoài và bên trong.

### *Firewall tại Router Access*

- **Thiết bị:** Cisco Secure Firewall (dòng Firepower 1000 Series) được triển khai trên Router R4, R5, R7.
- **Chính sách:**
  - + Chặn các cổng không cần thiết:
    - `access-list 105 deny tcp any any eq 23`: Chặn Telnet.
  - + Chỉ cho phép lưu lượng HTTP/HTTPS đến Web Server (12.0.4.194):
    - `access-list 105 permit tcp any host 12.0.4.194 eq`

80 443: Cho phép HTTP/HTTPS.

### *IDS/IPS trên R5*

- **Giải pháp:** Tích hợp IDS/IPS trên Cisco Secure Firewall (R5), sử dụng cơ sở dữ liệu chữ ký của Cisco Talos.
- **Chức năng:**
  - + Phát hiện các hành vi bất thường như quét cổng, DDoS.
  - + Ví dụ: Phát hiện lưu lượng bất thường từ VLAN 40 (GUEST) và tự động chặn nguồn IP.
- **Phản ứng:** Gửi cảnh báo qua email/SMS đến quản trị viên khi phát hiện mối đe dọa.

### *Giám sát lưu lượng*

- Sử dụng **Network Analyzer** (tích hợp trong Cisco DNA Center) để:
  - + Theo dõi hiệu suất mạng (băng thông, độ trễ).
  - + Phát hiện các mối đe dọa tiềm ẩn (ví dụ: lưu lượng tăng đột biến từ một thiết bị).

## 3.5.8 Quản lý người dùng

Quản lý người dùng tập trung vào việc kiểm soát quyền truy cập và bảo vệ danh tính người dùng.

### *Chính sách phân quyền truy cập*

- **Phân quyền theo vai trò (RBAC):**
  - + **Quản trị viên (Admin):** Quyền truy cập toàn bộ hệ thống (Server, WLC, Firewall), chỉ dành cho đội ngũ IT (2-3 người).
  - + **Nhân viên (Employee):** Quyền truy cập VLAN 10 và 20, không truy cập được Server trừ khi được cấp quyền.
  - + **Khách (Guest):** Quyền truy cập VLAN 40, chỉ sử dụng WiFi cơ bản, không truy cập tài nguyên nội bộ.

- **Triển khai:** Sử dụng Cisco Identity Services Engine (ISE) để quản lý chính sách phân quyền, tích hợp với WLC và RADIUS Server tại [12.0.4.194](#).

### *Xác thực đa yếu tố (MFA)*

- **Giải pháp:** Áp dụng MFA cho tất cả tài khoản quản trị viên và nhân viên truy cập từ xa qua VPN.
- **Cơ chế:**
  - + Yếu tố 1: Mật khẩu cá nhân (ít nhất 12 ký tự, bao gồm chữ hoa, chữ thường, số, và ký tự đặc biệt).
  - + Yếu tố 2: Mã OTP gửi qua ứng dụng Google Authenticator hoặc SMS.
- **Lợi ích:**
  - + Giảm nguy cơ truy cập trái phép nếu mật khẩu bị đánh cắp.
  - + Đảm bảo an toàn cho các kết nối từ xa.

### **3.5.9 Giám sát và phản ứng sự cố**

Giám sát và phản ứng sự cố nhằm phát hiện kịp thời các mối đe dọa và xử lý hiệu quả để giảm thiểu thiệt hại.

#### *Hệ thống giám sát*

- **Công cụ:** Sử dụng Cisco DNA Center để giám sát toàn bộ hệ thống mạng:
  - + Theo dõi trạng thái của LAP, Switch, Router, và WLC (uptime, tải CPU, băng thông sử dụng).
  - + Phát hiện bất thường (ví dụ: lưu lượng tăng đột biến, thiết bị ngoại lai kết nối vào mạng).
- **Camera và cảm biến:** Tích hợp dữ liệu từ 17 camera và 17 cảm biến để giám sát vật lý và môi trường (nhiệt độ, độ ẩm trong Phòng máy).
- **Lịch sử truy cập:** Nhật ký từ hệ thống kiểm soát truy cập (thể từ

RFID) và Cisco ISE được lưu trữ trên Server trong 90 ngày.

### *Kế hoạch ứng phó sự cố*

#### – **Phát hiện:**

- + Cisco Secure Firewall (IDS/IPS) và Cisco DNA Center gửi cảnh báo qua email/SMS khi phát hiện mối đe dọa (ví dụ: tấn công DDoS, truy cập trái phép).

#### – **Phản ứng:**

- + **Bước 1 - Cô lập:** Ngắt kết nối thiết bị hoặc VLAN bị tấn công (ví dụ: VLAN 40 bị xâm nhập sẽ bị chặn lưu lượng).
  - + **Bước 2 - Phân tích:** Sử dụng nhật ký từ Cisco DNA Center và Cisco ISE để xác định nguồn gốc tấn công.
  - + **Bước 3 - Khắc phục:** Vá lỗ hổng, thay đổi mật khẩu, và cập nhật firmware.
  - + **Bước 4 - Báo cáo:** Ghi lại chi tiết sự cố và báo cáo lên ban lãnh đạo.
- **Đào tạo:** Tổ chức đào tạo định kỳ (hàng quý) cho nhân viên về nhận thức bảo mật.
  - **Dự phòng:** Sao lưu dữ liệu trên Server hàng ngày, lưu trữ bản sao trên AWS S3.

### **3.5.10 Ứng dụng trong kịch bản Chooky**

- **Bảo vệ lưu lượng giữa HQ và chi nhánh:** VPN IPsec (R6-R7, R7-R8) đảm bảo dữ liệu của hơn 45 nhân viên và 15 thiết bị IoT được mã hóa an toàn.
- **Ngăn chặn truy cập trái phép:** VLAN 40 (GUEST) và VLAN 30 (IoT) bị cô lập, bảo vệ tài nguyên nội bộ như Server tại [12.0.4.194](#).
- **Quản lý an toàn:** [SSH](#) và chính sách mật khẩu mạnh giảm nguy cơ

tấn công từ bên trong.

- **Phát hiện và phản ứng:** Firewall và IDS/IPS tăng cường khả năng phát hiện và phản ứng với các mối đe dọa từ Internet.

## **Kết luận phần bảo mật**

Các giải pháp bảo mật được triển khai cho hệ thống mạng của công ty Chooky đảm bảo an toàn ở cả khía cạnh vật lý và kỹ thuật số. An ninh vật lý bảo vệ thiết bị và cơ sở hạ tầng, phân vùng mạng và kiểm soát truy cập ngăn chặn truy cập trái phép, bảo mật mạng không dây và VPN bảo vệ lưu lượng dữ liệu, quản lý người dùng kiểm soát quyền truy cập, và hệ thống giám sát/phản ứng sự cố giúp phát hiện và xử lý kịp thời các vấn đề. Các biện pháp này không chỉ bảo vệ dữ liệu và tài sản của công ty mà còn đảm bảo hoạt động liên tục, hiệu quả, và sẵn sàng cho các nhu cầu mở rộng trong tương lai.

## Chương 4

# Mô tả cấu hình hệ thống - IPv4

### 4.1 Cấu hình địa chỉ IPv4

Để triển khai hệ thống mạng IPv4, trước tiên cần gán địa chỉ IP cho các interface trên các router và switch theo sơ đồ địa chỉ đã được phân bổ. Dưới đây là các bước cấu hình chi tiết:

#### – Router R1 (Chi nhánh):

- + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `128.1.8.2/24` (`255.255.255.0`) để kết nối với mạng chi nhánh.
- + Interface `Loopback0`: Gán địa chỉ `128.1.0.1/23` (`255.255.254.0`) để mô phỏng mạng với 500 host.
- + Interface `Loopback1`: Gán địa chỉ `128.1.2.1/23` (`255.255.254.0`) để mô phỏng mạng với 300 host.
- + Bật các interface: `no shutdown`.

#### – Router R2 (Chi nhánh):

- + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `128.1.8.3/24` (`255.255.255.0`) để kết nối với mạng chi nhánh.
- + Interface `Loopback0`: Gán địa chỉ `128.1.4.1/25` (`255.255.255.128`) để mô phỏng mạng với 100 host.
- + Bật các interface: `no shutdown`.

#### – Router R3 (Chi nhánh):

- + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `128.1.8.4/24` (`255.255.255.0`) để kết nối với mạng chi nhánh.
- + Interface `Loopback0`: Gán địa chỉ `128.1.5.1/24` (`255.255.255.0`) để mô phỏng mạng với 200 host.
- + Interface `Loopback1`: Gán địa chỉ `128.1.6.1/25` (`255.255.255.128`) để mô phỏng mạng với 100 host.
- + Bật các interface: `no shutdown`.
- **Switch S0 (Chi nhánh):**
  - + Cấu hình thêm VLAN 1 để quản lý và kết nối giữa 3 router khu vực chi nhánh là R1, R2 và R3 với router R5.
  - + Interface `VLAN 1`: Gán địa chỉ `128.1.8.1/24` (`255.255.255.0`) để quản lý switch.
  - + Các interface `FastEthernet0/1`, `FastEthernet0/2`, `FastEthernet0/3`, và dải `FastEthernet0/4 - 24`: Đặt chế độ `switchport mode access`, gán vào `VLAN 1`.
  - + Interface `GigabitEthernet0/1`: Đặt chế độ `switchport mode trunk` để kết nối với router.
  - + Cấu hình gateway mặc định đến Router R5:  
`ip default-gateway 128.1.8.5`.
  - + Bật các interface: `no shutdown`.
- **Router R5 (HQ):**
  - + Interface `Serial0/1/0`: Gán địa chỉ `200.0.100.9/30` (`255.255.255.252`) để kết nối với router ACCESS.
  - + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `128.1.8.5/24` (`255.255.255.0`) để kết nối với mạng chi nhánh.
  - + Interface `GigabitEthernet0/0/1`: Gán địa chỉ `12.0.4.230/27` (`255.255.255.224`) để kết nối với mạng HQ.



- + Bật các interface: `no shutdown`.
- **Router R6 (HQ - LAN 6):**
  - + Interface `Serial0/1/0`: Gán địa chỉ `200.0.100.2/30` (`255.255.255.252`) để kết nối với R7.
  - + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `128.1.7.1/24` (`255.255.255.0`) để mô phỏng LAN 6.
  - + Bật các interface: `no shutdown`.
- **Router R7 (HQ):**
  - + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `12.0.4.231/27` (`255.255.255.224`) để kết nối với mạng HQ.
  - + Interface `Serial0/1/0`: Gán địa chỉ `200.0.100.1/30` (`255.255.255.252`) để kết nối với R6.
  - + Interface `Serial0/1/1`: Gán địa chỉ `200.0.100.5/30` (`255.255.255.252`) để kết nối với R8.
  - + Bật các interface: `no shutdown`.
- **Router R8 (HQ - LAN 8):**
  - + Interface `Serial0/1/0`: Gán địa chỉ `200.0.100.6/30` (`255.255.255.252`) để kết nối với R7.
  - + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `12.0.6.1/24` (`255.255.255.0`) để mô phỏng LAN 8.
  - + Bật các interface: `no shutdown`.
- **Router ACCESS (Internet):**
  - + Interface `Serial0/1/0`: Gán địa chỉ `200.0.100.10/30` (`255.255.255.252`) để kết nối với R5.
  - + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `203.0.113.1/24` (`255.255.255.0`) để mô phỏng kết nối Internet.
  - + Bật các interface: `no shutdown`.

Các địa chỉ IP được gán đảm bảo phù hợp với yêu cầu số lượng host cho từng mạng (Bảng 2.2 và Bảng 2.3) và sơ đồ địa chỉ point-to-point (Bảng 1). Việc bật các interface bằng lệnh `no shutdown` đảm bảo các kết nối vật lý sẵn sàng hoạt động.

## 4.2 Cấu hình xác thực PPP giữa các router

Yêu cầu cấu hình kết nối PPP giữa R7 và R6 với xác thực PAP, và giữa R7 và R8 với xác thực CHAP. Dưới đây là các bước cấu hình chi tiết:

### – Kết nối PPP giữa R7 và R6 (Xác thực PAP):

+ Trên R7, interface `Serial0/1/1`:

- Đã gán địa chỉ `200.0.100.5/30` (từ cấu hình trước).
- Bật PPP encapsulation: `encapsulation ppp`.
- Cấu hình thông tin xác thực: `username R6 password chooky`.

+ Trên R6, interface `Serial0/1/0`:

- Đã gán địa chỉ `200.0.100.2/30` (từ cấu hình trước).
- Bật PPP encapsulation: `encapsulation ppp`.
- Cấu hình xác thực PAP:  
`ppp pap sent-username R6 password chooky`.

### – Kết nối PPP giữa R7 và R8 (Xác thực CHAP):

+ Trên R7, interface `Serial0/1/0`:

- Đã gán địa chỉ `200.0.100.1/30` (từ cấu hình trước).
- Đặt hostname: `hostname R7`.
- Cấu hình thông tin xác thực: `username R8 password vmc`.
- Bật PPP encapsulation: `encapsulation ppp`.
- Kích hoạt xác thực CHAP: `ppp authentication chap`.
- Cấu hình CHAP:  
`ppp chap hostname R7, ppp chap password vmc`.

+ Trên R8, interface `Serial0/1/0`:

- Đã gán địa chỉ `200.0.100.6/30` (từ cấu hình trước).
- Đặt hostname: `hostname R8`.
- Cấu hình thông tin xác thực: `username R7 password vmc`.
- Bật PPP encapsulation: `encapsulation ppp`.
- Kích hoạt xác thực CHAP: `ppp authentication chap`.
- Cấu hình CHAP:  
`ppp chap hostname R8, ppp chap password vmc`.

Cấu hình PPP đảm bảo các kết nối point-to-point giữa các router hoạt động ổn định. PAP được sử dụng giữa R7 và R6 với tên người dùng/mật khẩu đơn giản, trong khi CHAP giữa R7 và R8 cung cấp bảo mật cao hơn nhờ cơ chế challenge-response.

### 4.3 Cấu hình GRE tunnel giữa R6 và R8

Yêu cầu cấu hình GRE tunnel giữa R6 và R8, sử dụng địa chỉ mạng `200.0.100.24/30` với yêu cầu 2 host. Dưới đây là các bước cấu hình chi tiết:

– Trên R6:

- + Tạo interface tunnel: `interface Tunnel 0`.
- + Gán địa chỉ IP cho tunnel:  
`ip address 200.0.100.25 255.255.255.252`.
- + Chỉ định nguồn: `tunnel source Serial0/1/0`  
(đã gán địa chỉ `200.0.100.2/30` từ cấu hình trước).
- + Chỉ định đích: `tunnel destination 200.0.100.6`  
(interface `Serial0/1/0` của R8).

– Trên R8:

- + Tạo interface tunnel: `interface Tunnel 0`.
- + Gán địa chỉ IP cho tunnel:  
`ip address 200.0.100.26 255.255.255.252`.

- + Chỉ định nguồn: `tunnel source Serial0/1/0`  
(đã gán địa chỉ `200.0.100.6/30` từ cấu hình trước).
- + Chỉ định đích: `tunnel destination 200.0.100.2`  
(interface `Serial0/1/0` của R6).

Cấu hình GRE tunnel được thiết lập thành công, cho phép giao tiếp giữa các mạng được kết nối qua R6 và R8 thông qua đường hầm. Tuy nhiên, GRE không mã hóa dữ liệu.

## 4.4 Cấu hình định tuyến EIGRP và OSPF

Yêu cầu cấu hình OSPF tại khu vực chi nhánh, EIGRP tại khu vực HQ, phân phối lại tuyến trên R5, và thiết lập tuyến mặc định. Ngoài ra, do R4, R5, và R7 không kết nối trực tiếp với nhau mà thông qua switch khu vực HQ (sử dụng VLAN 60), cần cấu hình các tuyến tĩnh để đảm bảo các router này có thể giao tiếp với nhau và với các mạng khác. Dưới đây là các bước cấu hình chi tiết:

### – OSPF tại khu vực chi nhánh:

- + Trên R1:
  - Kích hoạt OSPF: `router ospf 1`.
  - Thêm các mạng vào Area 0:  
`network 128.1.8.0 0.0.0.255 area 0` (mạng chi nhánh),  
`network 128.1.0.0 0.0.1.255 area 0` (Loopback0),  
`network 128.1.2.0 0.0.1.255 area 0` (Loopback1).
  - Đặt tất cả interface thành passive mặc định:  
`passive-interface default`.
  - Bật gửi bản cập nhật trên interface kết nối với chi nhánh:  
`no passive-interface GigabitEthernet0/0/0`.
- + Trên R2:
  - Kích hoạt OSPF: `router ospf 1`.
  - Thêm các mạng vào Area 0:

```
network 128.1.8.0 0.0.0.255 area 0 (mạng chi nhánh),  
network 128.1.4.0 0.0.0.127 area 0 (Loopback0).
```

- Đặt tất cả interface thành passive mặc định:

```
passive-interface default.
```

- Bật gửi bản cập nhật trên interface kết nối với chi nhánh:

```
no passive-interface GigabitEthernet0/0/0.
```

+ Trên R3:

- Kích hoạt OSPF: `router ospf 1`.

- Thêm các mạng vào Area 0:

```
network 128.1.8.0 0.0.0.255 area 0 (mạng chi nhánh),  
network 128.1.5.0 0.0.0.255 area 0 (Loopback0),  
network 128.1.6.0 0.0.0.127 area 0 (Loopback1).
```

- Đặt tất cả interface thành passive mặc định:

```
passive-interface default.
```

- Bật gửi bản cập nhật trên interface kết nối với chi nhánh:

```
no passive-interface GigabitEthernet0/0/0.
```

## – EIGRP tại khu vực HQ:

+ Trên R4:

- Kích hoạt EIGRP: `router eigrp 100`.

- Thêm các mạng VLAN:

```
network 12.0.1.0 0.0.0.255 (VLAN 10),  
network 12.0.2.0 0.0.1.255 (VLAN 20),  
network 12.0.4.0 0.0.0.127 (VLAN 30),  
network 12.0.4.128 0.0.0.63 (VLAN 40),  
network 12.0.4.192 0.0.0.15 (VLAN 50),  
network 12.0.4.224 0.0.0.31 (VLAN 60).
```

- Đặt tất cả interface thành passive mặc định:

```
passive-interface default.
```

- Bật gửi bản cập nhật trên interface kết nối với HQ:  
`no passive-interface GigabitEthernet0/0/0,`  
`no passive-interface GigabitEthernet0/0/1.`
- Tắt tự động tóm tắt: `no auto-summary.`

+ Trên R6:

- Kích hoạt EIGRP: `router eigrp 100.`
- Thêm các mạng:  
`network 128.1.7.0 0.0.0.255` (LAN 6),  
`network 200.0.100.0 0.0.0.3` (R7-R6),  
`network 200.0.100.24 0.0.0.3` (GRE tunnel).
- Đặt tất cả interface thành passive mặc định:  
`passive-interface default.`
- Bật gửi bản cập nhật trên interface kết nối với R7:  
`no passive-interface Serial0/1/0.`
- Tắt tự động tóm tắt: `no auto-summary.`

+ Trên R7:

- Kích hoạt EIGRP: `router eigrp 100.`
- Thêm các mạng:  
`network 12.0.4.224 0.0.0.31` (VLAN 60),  
`network 200.0.100.0 0.0.0.3` (R7-R6),  
`network 200.0.100.4 0.0.0.3` (R7-R8),  
`network 200.0.100.24 0.0.0.3` (GRE tunnel).
- Đặt tất cả interface thành passive mặc định:  
`passive-interface default.`
- Bật gửi bản cập nhật trên các interface kết nối:  
`no passive-interface Serial0/1/0,`  
`no passive-interface Serial0/1/1,`  
`no passive-interface GigabitEthernet0/0/0.`

- Tắt tự động tóm tắt: `no auto-summary`.
- **EIGRP và OSPF trên R5 (router biên giữa HQ và chi nhánh):**
  - + Cấu hình EIGRP:
    - Kích hoạt EIGRP: `router eigrp 100`.
    - Thêm các mạng:  
`network 128.1.8.0 0.0.0.255` (mạng chi nhánh),  
`network 12.0.4.224 0.0.0.31` (VLAN 60),  
`network 200.0.100.8 0.0.0.3` (R5-ACCESS).
    - Phân phối lại OSPF và tuyến tính:  
`redistribute ospf 1 metric 100000 100 255 1 1500`,  
`redistribute static metric 100000 100 255 1 1500`.
    - Phân phối tuyến mặc định: `default-information originate`.
    - Đặt tất cả interface thành passive mặc định:  
`passive-interface default`.
    - Bật gửi bản cập nhật trên các interface kết nối:  
`no passive-interface GigabitEthernet0/0/0`,  
`no passive-interface GigabitEthernet0/0/1`,  
`no passive-interface Serial0/1/0`.
    - Tắt tự động tóm tắt: `no auto-summary`.
  - + Cấu hình OSPF:
    - Kích hoạt OSPF: `router ospf 1`.
    - Thêm các mạng vào Area 0:  
`network 128.1.8.0 0.0.0.255 area 0` (mạng chi nhánh),  
`network 12.0.4.224 0.0.0.31 area 0` (VLAN 60).
    - Phân phối lại EIGRP:  
`redistribute eigrp 100 metric 100 subnets`.
    - Phân phối tuyến mặc định: `default-information originate`.
    - Đặt tất cả interface thành passive mặc định:

```
passive-interface default.
```

- Bật gửi bản cập nhật trên các interface kết nối:

```
no passive-interface GigabitEthernet0/0/0,  
no passive-interface GigabitEthernet0/0/1.
```

– **Tuyến mặc định trên R5:**

- + Cấu hình tuyến mặc định đến router ACCESS:

```
ip route 0.0.0.0 0.0.0.0 Serial0/1/0.
```

– **Cấu hình định tuyến tĩnh do R4, R5, R7 không kết nối trực tiếp:**

- + Tại khu vực HQ, R4, R5 và R7 được kết nối thông qua switch khu vực HQ trên VLAN 60 ([12.0.4.224/27](#)). Do switch không tham gia định tuyến động, các router không thể tự động khám phá nhau qua EIGRP. Vì vậy, cần cấu hình các tuyến tĩnh để định hướng lưu lượng giữa các router này và đến các mạng khác.

- + Trên R4:

- Tuyến đến R5:

```
ip route 12.0.4.230 255.255.255.255 12.0.4.230.
```

- Tuyến đến R7:

```
ip route 12.0.4.231 255.255.255.255 12.0.4.231.
```

- Tuyến đến các mạng qua R5:

```
ip route 200.0.100.8 255.255.255.252 12.0.4.230  
(R5-ACCESS),
```

```
ip route 128.1.8.0 255.255.255.0 12.0.4.230  
(mạng chi nhánh),
```

```
ip route 128.1.0.0 255.255.254.0 12.0.4.230,
```

```
ip route 128.1.2.0 255.255.254.0 12.0.4.230,
```

```
ip route 128.1.4.0 255.255.255.128 12.0.4.230,
```

```
ip route 128.1.5.0 255.255.255.0 12.0.4.230,
```

```
ip route 128.1.6.0 255.255.255.128 12.0.4.230
```



(các mạng chi nhánh),

```
ip route 203.0.113.0 255.255.255.0 12.0.4.230 (Internet).
```

- Tuyến đến các mạng qua R7:

```
ip route 200.0.100.0 255.255.255.252 12.0.4.231 (R7-R6),
```

```
ip route 200.0.100.4 255.255.255.252 12.0.4.231 (R7-R8),
```

```
ip route 200.0.100.24 255.255.255.252 12.0.4.231 (GRE  
tunnel),
```

```
ip route 128.1.7.0 255.255.255.0 12.0.4.231 (LAN 6),
```

```
ip route 12.0.6.0 255.255.255.0 12.0.4.231 (LAN 8).
```

+ Trên R5:

- Tuyến đến R4:

```
ip route 12.0.1.0 255.255.255.0 12.0.4.225,
```

```
ip route 12.0.2.0 255.255.254.0 12.0.4.225,
```

```
ip route 12.0.4.0 255.255.255.128 12.0.4.225,
```

```
ip route 12.0.4.128 255.255.255.192 12.0.4.225,
```

```
ip route 12.0.4.192 255.255.255.240 12.0.4.225,
```

```
ip route 12.0.4.225 255.255.255.255 12.0.4.225
```

(các mạng VLAN của R4).

- Tuyến đến R7:

```
ip route 12.0.4.231 255.255.255.255 12.0.4.231.
```

+ Trên R7:

- Tuyến đến R4:

```
ip route 12.0.1.0 255.255.255.0 12.0.4.225,
```

```
ip route 12.0.2.0 255.255.254.0 12.0.4.225,
```

```
ip route 12.0.4.0 255.255.255.128 12.0.4.225,
```

```
ip route 12.0.4.128 255.255.255.192 12.0.4.225,
```

```
ip route 12.0.4.192 255.255.255.240 12.0.4.225,
```

```
ip route 12.0.4.225 255.255.255.255 12.0.4.225
```

(các mạng VLAN của R4).

- Tuyến đến R5:

```
ip route 12.0.4.230 255.255.255.255 12.0.4.230.
```

- Tuyến đến các mạng qua R5:

```
ip route 128.1.8.0 255.255.255.0 12.0.4.230
```

(mạng chi nhánh),

```
ip route 128.1.0.0 255.255.254.0 12.0.4.230,
```

```
ip route 128.1.2.0 255.255.254.0 12.0.4.230,
```

```
ip route 128.1.4.0 255.255.255.128 12.0.4.230,
```

```
ip route 128.1.5.0 255.255.255.0 12.0.4.230,
```

```
ip route 128.1.6.0 255.255.255.128 12.0.4.230
```

(các mạng chi nhánh),

```
ip route 203.0.113.0 255.255.255.0 12.0.4.230 (Internet).
```

Cấu hình định tuyến đảm bảo các mạng tại HQ và chi nhánh có thể giao tiếp với nhau. Các tuyến tĩnh được thêm vào để khắc phục hạn chế do R4, R5, R7 không kết nối trực tiếp mà thông qua switch khu vực HQ. Tuyến mặc định trên R5 đảm bảo lưu lượng không xác định sẽ được chuyển đến router ACCESS.

## 4.5 Cấu hình chuyển mạch

Yêu cầu cấu hình VTP để quản lý VLAN, Rapid PVST+ và root bridge để tránh vòng lặp, EtherChannel để tăng băng thông, SSH để quản lý từ xa an toàn, và Inter-VLAN Routing trên R4 để định tuyến giữa các VLAN. Dưới đây là các bước cấu hình chi tiết:

### – VTP trên các switch:

+ Trên S1 (VTP Server):

- Đặt chế độ VTP Server: `vtp mode server`.
- Cấu hình domain VTP: `vtp domain HQ`.
- Tạo các VLAN:
  - `vlan 10`, tên `UNIT1`.

- `vlan 20`, tên `UNIT2`.
  - `vlan 30`, tên `UNIT3`.
  - `vlan 40`, tên `GUEST`.
  - `vlan 50`, tên `SERVERS`.
  - `vlan 60`, tên `Management`.
- + Trên S2, S3, S4 (VTP Client):
- Đặt chế độ VTP Client: `vtp mode client`.
  - Cấu hình domain VTP: `vtp domain HQ`.
- **Cấu hình VLAN và gán port trên các switch:**
- + Trên S1, S2, S3, S4:
- Interface `VLAN 60`: Gán địa chỉ IP để quản lý (`12.0.4.226/27` trên S1, `12.0.4.227/27` trên S2, `12.0.4.228/27` trên S3, `12.0.4.229-230/27` trên S4).
  - Các port `FastEthernet0/5 - 12`: Đặt chế độ `switchport mode access`, gán vào `VLAN 10`, bật: `no shutdown`.
  - Các port `FastEthernet0/13 - 20`: Đặt chế độ `switchport mode access`, gán vào `VLAN 20`, bật: `no shutdown`.
  - Các port `FastEthernet0/21 - 22`: Đặt chế độ `switchport mode access`, gán vào `VLAN 30`, bật: `no shutdown`.
  - Port `FastEthernet0/23`: Đặt chế độ `switchport mode access`, gán vào `VLAN 40`, bật: `no shutdown`.
  - Port `FastEthernet0/24`: Đặt chế độ `switchport mode access`, gán vào `VLAN 50`, bật: `no shutdown`.
  - Interface `GigabitEthernet0/1` (trên S1, S2): Đặt chế độ `switchport mode trunk`, đặt native VLAN là `VLAN 60`, bật: `no shutdown`.
  - Interface `GigabitEthernet0/2` (trên S1): Đặt chế độ `switchport mode trunk`, đặt native VLAN là `VLAN 60`, bật: `no shutdown`.

- Gateway mặc định: `ip default-gateway 12.0.4.225` (địa chỉ của R4 trên VLAN 60).
- **EtherChannel với LACP:**
  - + Trên S1, S2, S3, S4:
    - Dải port `FastEthernet0/1 - 2`: Đặt chế độ `switchport mode trunk`, native VLAN `VLAN 60`, thêm vào `channel-group 1 mode active`, bật: `no shutdown`.
    - Interface `Port-channel1`: Đặt chế độ `switchport mode trunk`, native VLAN `VLAN 60`, bật: `no shutdown`.
    - Dải port `FastEthernet0/3 - 4`: Đặt chế độ `switchport mode trunk`, native VLAN `VLAN 60`, thêm vào `channel-group 2 mode active`, bật: `no shutdown`.
    - Interface `Port-channel2`: Đặt chế độ `switchport mode trunk`, native VLAN `VLAN 60`, bật: `no shutdown`.
- **Rapid PVST+ và root bridge:**
  - + Trên S1, S2, S3, S4:
    - Bật chế độ Rapid PVST+: `spanning-tree mode rapid-pvst`.
  - + Trên S1:
    - Đặt làm root bridge cho VLAN 10, 20, 30:  
`spanning-tree vlan 10 root primary,`  
`spanning-tree vlan 20 root primary,`  
`spanning-tree vlan 30 root primary.`
  - + Trên S2:
    - Đặt làm root bridge cho VLAN 40, 50, 60:  
`spanning-tree vlan 40 root primary,`  
`spanning-tree vlan 50 root primary,`  
`spanning-tree vlan 60 root primary.`
- **SSH trên các switch:**

- + Trên S1, S2, S3, S4:
  - Cấu hình domain name: `ip domain-name hq.local`.
  - Tạo khóa RSA: `crypto key generate rsa`.
  - Tạo tài khoản:  
`username admin privilege 15 password chooky`.
  - Đặt mật khẩu enable: `enable password vmc`.
  - Cấu hình VTY lines:  
`line vty 0 15, login local, transport input ssh`.
- **Inter-VLAN Routing trên R4:**
  - + Tạo sub-interface cho mỗi VLAN:
    - GigabitEthernet0/0/0.10: `encapsulation dot1Q 10, ip address 12.0.1.1 255.255.255.0`, bật: `no shutdown`.
    - GigabitEthernet0/0/0.20: `encapsulation dot1Q 20, ip address 12.0.2.1 255.255.254.0`, bật: `no shutdown`.
    - GigabitEthernet0/0/0.30: `encapsulation dot1Q 30, ip address 12.0.4.1 255.255.255.128`, bật: `no shutdown`.
    - GigabitEthernet0/0/0.40: `encapsulation dot1Q 40, ip address 12.0.4.129 255.255.255.192`, bật: `no shutdown`.
    - GigabitEthernet0/0/0.50: `encapsulation dot1Q 50, ip address 12.0.4.193 255.255.255.240`, bật: `no shutdown`.
    - GigabitEthernet0/0/0.60: `encapsulation dot1Q 60 native, ip address 12.0.4.225 255.255.255.224`, bật: `no shutdown`.
  - + Interface chính: `GigabitEthernet0/0/0, GigabitEthernet0/0/1`, bật: `no shutdown`.

Cấu hình chuyển mạch đảm bảo các VLAN được quản lý tập trung qua VTP, tránh vòng lặp với Rapid PVST+, tăng băng thông với Ether-Channel, và hỗ trợ quản lý từ xa an toàn qua SSH. Inter-VLAN Routing trên R4 cho phép các VLAN giao tiếp với nhau và với các mạng khác.

## 4.6 Cấu hình NAT Overload, Port Forwarding và DHCP

Yêu cầu cấu hình NAT Overload và Port Forwarding trên router ACCESS để cho phép các mạng nội bộ truy cập Internet và định tuyến đến server cụ thể, đồng thời cấu hình DHCP trên R4 để tự động cấp địa chỉ IP cho các VLAN. Dưới đây là các bước cấu hình chi tiết:

### – NAT Overload và Port Forwarding trên router ACCESS:

#### + Cấu hình NAT Overload:

- Tạo ACL để xác định các mạng nội bộ:

```
access-list 1 permit 12.0.0.0 0.255.255.255 (mạng HQ),  
access-list 1 permit 128.1.0.0 0.0.255.255  
(mạng chi nhánh).
```

- Áp dụng NAT Overload trên interface ngoài:

```
ip nat inside source list 1 interface  
GigabitEthernet0/0/0 overload.
```

- Đánh dấu interface trong và ngoài:

```
ip nat inside trên Serial0/1/0, ip nat outside trên  
GigabitEthernet0/0/0.
```

#### + Cấu hình Port Forwarding:

- Chuyển tiếp cổng HTTP: `ip nat inside source static tcp 12.0.4.194 80 203.0.113.1 80`, ánh xạ từ server nội bộ 12.0.4.194 (VLAN 50) đến địa chỉ công cộng 203.0.113.1.

- Chuyển tiếp cổng HTTPS: `ip nat inside source static tcp 12.0.4.194 443 203.0.113.1 443`, ánh xạ từ server nội bộ 12.0.4.194 đến địa chỉ công cộng 203.0.113.1.

### – Giải thích chi tiết về NAT:

- + NAT Overload (PAT - Port Address Translation) cho phép nhiều thiết bị trong mạng nội bộ (12.0.0.0/8 và 128.1.0.0/16) chia sẻ một địa chỉ IP công cộng (203.0.113.1) bằng cách ánh xạ các cổng nguồn

khác nhau. Điều này tối ưu hóa việc sử dụng địa chỉ IP công cộng, đặc biệt khi số lượng địa chỉ IPv4 hạn chế.

- + Port Forwarding được sử dụng để định tuyến lưu lượng từ Internet (qua **203.0.113.1**) đến server nội bộ (**12.0.4.194**) trên các cổng **80** (HTTP) và **443** (HTTPS). Điều này cho phép truy cập dịch vụ từ bên ngoài mà không cần mở toàn bộ mạng nội bộ, tăng cường bảo mật.
- + NAT được áp dụng trên các interface **Serial0/1/0** (bên trong, kết nối với mạng nội bộ) và **GigabitEthernet0/0/0** (bên ngoài, kết nối với Internet), đảm bảo lưu lượng được chuyển đổi đúng cách.

#### – DHCP Server trên router R4:

- + Loại trừ các địa chỉ IP cố định:
  - `ip dhcp excluded-address 12.0.1.1, 12.0.2.1, 12.0.4.1, 12.0.4.129, 12.0.4.193, 12.0.4.225` (địa chỉ của router R4), `12.0.4.194` (server).
- + Tạo các DHCP pool:
  - Pool **VLAN10**: `network 12.0.1.0 255.255.255.0,`  
`default-router 12.0.1.1, dns-server 12.0.4.194.`
  - Pool **VLAN20**: `network 12.0.2.0 255.255.254.0,`  
`default-router 12.0.2.1, dns-server 12.0.4.194.`
  - Pool **VLAN30**: `network 12.0.4.0 255.255.255.128,`  
`default-router 12.0.4.1, dns-server 12.0.4.194.`
  - Pool **VLAN40**: `network 12.0.4.128 255.255.255.192,`  
`default-router 12.0.4.129, dns-server 12.0.4.194.`
  - Pool **VLAN50**: `network 12.0.4.192 255.255.255.240,`  
`default-router 12.0.4.193, dns-server 12.0.4.194.`
  - Pool **VLAN60**: `network 12.0.4.224 255.255.255.224,`  
`default-router 12.0.4.225, dns-server 12.0.4.194.`

+ Cấu hình IP Helper trên các sub-interface:

- `GigabitEthernet0/0/0.10: encapsulation dot1Q 10,  
ip address 12.0.1.1 255.255.255.0,  
ip helper-address 12.0.1.1.`
- `GigabitEthernet0/0/0.20: encapsulation dot1Q 20,  
ip address 12.0.2.1 255.255.254.0,  
ip helper-address 12.0.2.1.`
- `GigabitEthernet0/0/0.30: encapsulation dot1Q 30,  
ip address 12.0.4.1 255.255.255.128,  
ip helper-address 12.0.4.1.`
- `GigabitEthernet0/0/0.40: encapsulation dot1Q 40,  
ip address 12.0.4.129 255.255.255.192,  
ip helper-address 12.0.4.129.`
- `GigabitEthernet0/0/0.50: encapsulation dot1Q 50,  
ip address 12.0.4.193 255.255.255.240,  
ip helper-address 12.0.4.193.`
- `GigabitEthernet0/0/0.60: encapsulation dot1Q 60 native,  
ip address 12.0.4.225 255.255.255.224,  
ip helper-address 12.0.4.225.`

Cấu hình NAT Overload cho phép các mạng nội bộ truy cập Internet hiệu quả, Port Forwarding đảm bảo truy cập dịch vụ từ server trong VLAN 50, và DHCP tự động cấp IP cho các host trong các VLAN với cấu hình phù hợp.

## 4.7 Cấu hình ACL và các yêu cầu bổ sung

Yêu cầu cấu hình ACL để kiểm soát truy cập cho VLAN GUEST và VLAN SERVERS, đồng thời bổ sung cấu hình server Web và DNS nội bộ tại địa chỉ `12.0.4.194` trên interface `Fa0/24` của switch S1. Dưới đây là các bước cấu hình chi tiết:



– **Cấu hình ACL trên router R4:**

+ Tạo ACL mở rộng 101 cho VLAN 40:

- Cho phép DHCP:  
`permit udp any eq 68 any eq 67,`  
`permit udp any eq 67 any eq 68.`
- Cho phép DNS từ VLAN 40 (12.0.4.128/26) đến server: `permit`  
`udp 12.0.4.128 0.0.0.63 host 12.0.4.194 eq 53.`
- Cho phép HTTP và HTTPS từ VLAN 40 đến server 12.0.4.194:  
`permit tcp 12.0.4.128 0.0.0.63 host 12.0.4.194 eq 80,`  
`permit tcp 12.0.4.128 0.0.0.63 host 12.0.4.194 eq 443.`
- Cho phép truy cập Internet từ VLAN 40:  
`permit ip 12.0.4.128 0.0.0.63 203.0.113.0 0.0.0.255.`
- Từ chối truy cập vào các mạng nội bộ từ VLAN 40:  
`deny ip 12.0.4.128 0.0.0.63 12.0.0.0 0.255.255.255`  
(HQ),  
`deny ip 12.0.4.128 0.0.0.63 200.0.100.0 0.0.0.255`  
(mạng point-to-point),  
`deny ip 12.0.4.128 0.0.0.63 128.1.0.0 0.0.255.255`  
(mạng chi nhánh).
- Cho phép tất cả lưu lượng còn lại từ VLAN 40:  
`permit ip 12.0.4.128 0.0.0.63 any.`

+ Áp dụng ACL trên sub-interface:

```
interface GigabitEthernet0/0/0.40, ip access-group 101 in.
```

+ Tạo ACL mở rộng 102 cho VLAN 30:

- Cho phép DHCP:  
`permit udp any eq 68 any eq 67,`  
`permit udp any eq 67 any eq 68.`
- Cho phép DNS từ VLAN 30 (12.0.4.0/25) đến server:  
`permit udp 12.0.4.0 0.0.0.127 host 12.0.4.194 eq 53.`

- Cho phép truy cập Internet từ VLAN 30:  
`permit ip 12.0.4.0 0.0.0.127 203.0.113.0 0.0.0.255.`
  - Từ chối truy cập vào các mạng nội bộ từ VLAN 30:  
`deny ip 12.0.4.0 0.0.0.127 12.0.0.0 0.255.255.255` (HQ),  
`deny ip 12.0.4.0 0.0.0.127 200.0.100.0 0.0.0.255` (mạng point-to-point),  
`deny ip 12.0.4.0 0.0.0.127 128.1.0.0 0.0.255.255` (mạng chi nhánh).
  - Cho phép tất cả lưu lượng còn lại từ VLAN 30:  
`permit ip 12.0.4.0 0.0.0.127 any.`
- + Áp dụng ACL trên sub-interface VLAN 30:  
`interface GigabitEthernet0/0/0.30, ip access-group 102 in.`
- **Cấu hình ACL trên các switch (S1, S2, S3, S4):**
- + Tạo ACL **101** để kiểm soát truy cập VTY: `access-list 101 permit tcp 12.0.4.192 0.0.0.15 any eq 22`  
(cho phép VLAN 50 - SERVERS truy cập SSH).
- + Áp dụng ACL trên VTY: `line vty 0 15, access-class 101 in.`
- **Cấu hình bổ sung server Web và DNS nội bộ:**
- + Server Web và DNS nội bộ được cấu hình tại địa chỉ **12.0.4.194** trên interface **FastEthernet0/24** của switch S1, thuộc VLAN 50 (SERVERS). Địa chỉ này đã được sử dụng trong NAT Overload và Port Forwarding (section 3.6) để định tuyến cổng **80** (HTTP) và **443** (HTTPS) từ Internet đến server này.
- + Server này hoạt động như DNS nội bộ (cổng **53**) cho các VLAN, được cấu hình trong DHCP pool trên R4 với `dns-server 12.0.4.194`, và cũng là điểm đến cho các dịch vụ Web từ VLAN 40 (GUEST) theo ACL.

Cấu hình ACL đảm bảo VLAN GUEST (VLAN 40) chỉ truy cập

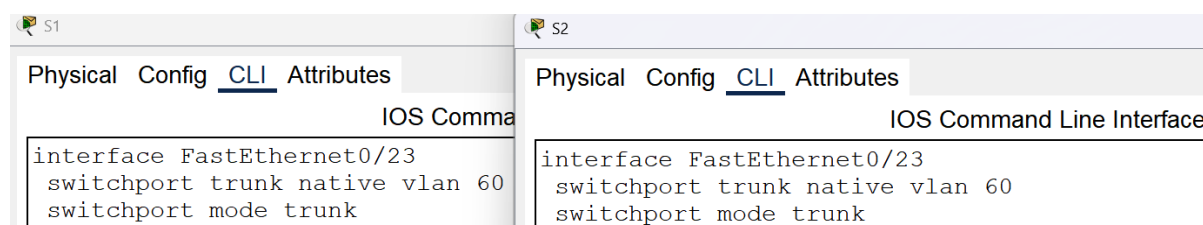
Internet và các dịch vụ cơ bản (DNS, HTTP, HTTPS) trên server nội bộ, trong khi VLAN SERVERS (VLAN 50) được phép quản lý switch qua SSH. Server Web và DNS nội bộ tại **12.0.4.194** hỗ trợ các dịch vụ nội bộ và liên kết với cấu hình NAT trước đó.

## Chương 5

# Mô tả cấu hình mạng không dây

### 5.1 Cấu hình chuẩn bị

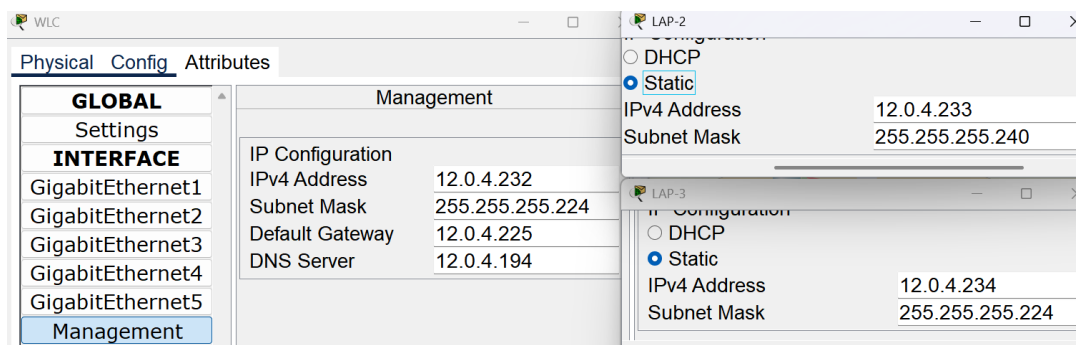
- **Mục tiêu:** Hỗ trợ wifi cho VLAN 10 - Marketing, VLAN 20 - Business, VLAN 30 - IoT và LAN 40 - GUEST.
- Cấu hình **mode trunk** trên các **interface** mà các Switch S1, S2, S3 và S4 kết nối với WLC và các LAP.
- Bật **Native VLAN 60** trên các interface này. Mục đích là dùng VLAN 60 để quản lí mạng không dây.



Hình 5.1: Minh họa cấu hình port trunk.

- Đấu nối các thiết bị vào các port đã cấu hình bên trên.
- **Cấu hình IP cho WLC và các LAP:**
  - + Do đã có DHCP trước đó nên chúng có thể nhận IP động.
  - + Tuy nhiên, để tiện quản lí, chúng nên được cấu hình IP tĩnh.
  - + IP của chúng lần lượt là:
    - WLC: 12.0.4.232
    - LAP-2: 12.0.4.233

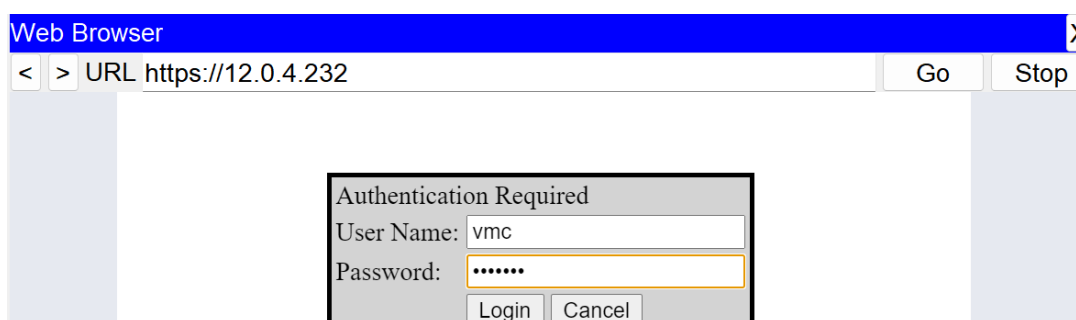
- LAP-3: 12.0.4.234
  - LAP-4: 12.0.4.235
- + Như đã nói, chúng đều thuộc VLAN 60 12.0.4.224/27.



Hình 5.2: Cấu hình IP cho WLC và LAP.

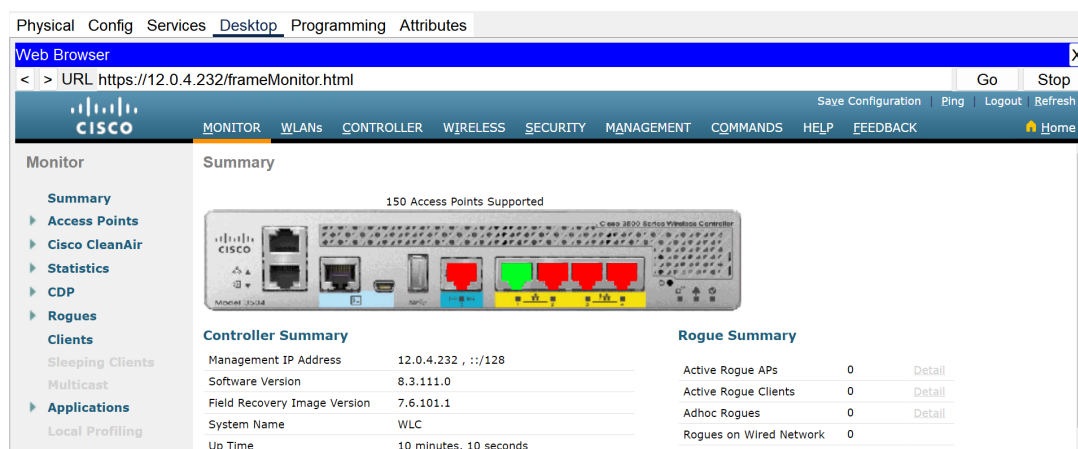
- Thực hiện một số cấu hình cơ bản với WLC.
- + Dùng một PC hay Laptop bất kỳ có thể truy cập mạng VLAN 60.
- + Mở giao diện web và gõ <http://12.0.4.232>.
- + Thực hiện một số cấu hình cơ bản, bao gồm việc thiết lập username và password cho WLC.
- + Thông tin đã thiết lập: username: **vmc**, password: **Vmc123!**.
- + Thông tin này hiện không có ảnh minh họa.
- + **Lưu ý:** Lần đầu tiên truy cập dùng <http>, nhưng kể từ sau khi thiết lập thì dùng <https>

## 5.2 Cấu hình mạng không dây



Hình 5.3: Đăng nhập vào WLC.

- **Đăng nhập:** truy cập WLC qua trình duyệt.
- Truy cập vào được giao diện web đồ họa của WLC.



Hình 5.4: Đăng nhập vào được WLC.

- **Kiểm tra:** Vào mục **Wireless** để kiểm tra các LAP đã thiết lập kết nối vào mạng với WLC qua giao thức **CAPWAP**.



Hình 5.5: Kiểm tra kết nối các LAP.

- **Thông tin cơ bản về các WLAN:**
  - + Marketing: VLAN 10 - 12.0.1.0/24 - 802.1
  - + Business: VLAN 20 - 12.0.2.0/23 - 802.1X.
  - + IoT: VLAN 30 - 12.0.4.0/25 - PSK.
  - + GUEST: VLAN 40 - 12.0.4.128/26 - Open.

### 5.2.1 Cấu hình Radius Server - Xác thực AAA

- Truy cập menu **SECURITY**, chọn **Authentication** ở mục **RADIUS**.
- Nhập thông tin của Server Radius.

- + Server IP Address: **12.0.4.194**.
- + Shared Secret: **cisco**.
- + Confirm Shared Secret: **cisco**.
- + Port Number: **1812**.

Hình 5.6: Cấu hình thông tin Radius AAA trên WLC.

- + **Lưu ý:** Thông tin này sẽ được nhập đồng bộ với Radius Server. Radius Server sẽ được triển khai chung với Server DNS, Web và Database.
- + Nhấn **Apply**.

Network User	Management	Server Index	Server Address (IPv4/IPv6)	Port	IPSec	Admin Sta
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	12.0.4.194	1812	Disabled	Enabled

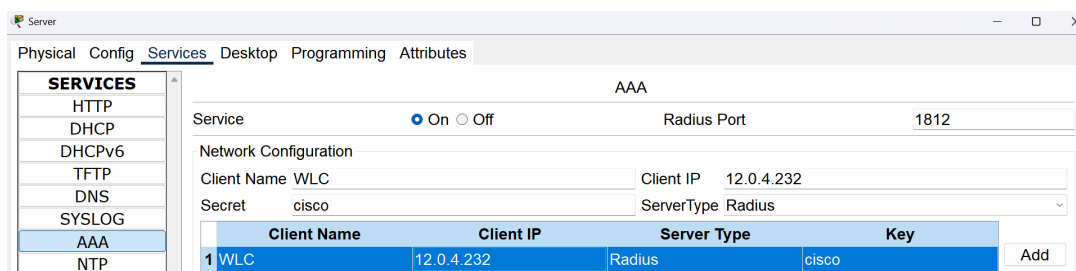
Hình 5.7: Hoàn tất cấu hình Radius trên WLC.

## – Cấu hình xác thực AAA trên Server:

- + Mở giao diện **Services** trên Server.
- + Chọn thẻ **RADIUS EAP**.
- + Bật tính năng **Allow EAP-MD5**.
- + Chọn thẻ **AAA**.
- + Phần Service, chọn **on**, phần Radius Port, nhập **1812**.
- + Client Name: Nhập tên tùy chọn, ở đây dùng **WLC**.

+ Client IP: Nhập IP của WLC là **12.0.4.232**.

+ Secret: **cisco**. ServerType: **Radius**.



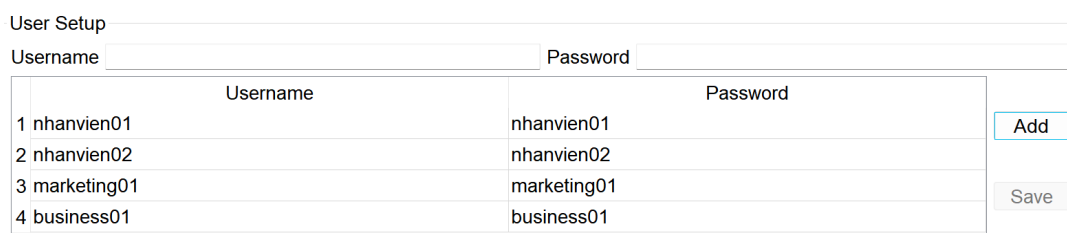
Hình 5.8: Cấu hình xác thực AAA trên Server.

+ Nhấn **Add**.

### – Cấu hình tài khoản truy cập:

+ Vẫn trong thẻ AAA của Server, tìm đến phần **User Setup**.

+ Nhập thông tin username và password, tùy chọn theo nhu cầu. Rồi nhấn **Add**

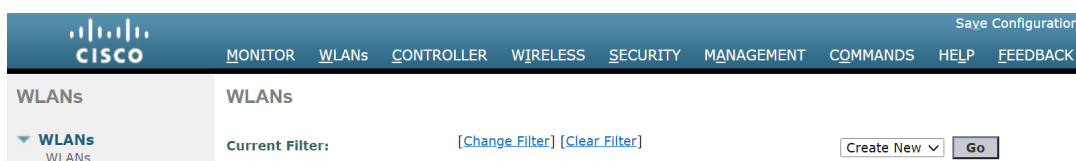


Hình 5.9: Cấu hình tài khoản truy cập.

+ Nhấn **Add**.

## 5.2.2 Cấu hình SSID WLANs

– Trên giao diện Web của WLC, truy cập menu **WLANs**.



Hình 5.10: Truy cập menu WLANs.

– Chọn **Create New**, chọn **Go**.



- Nhập các thông tin:
  - + Profile Name: Thông tin dùng để quản lí WLAN.
  - + SSID: Thông tin này sẽ là tên sóng Wifi.
  - + Nhấp **Apply**.

WLANs > New [< BACK](#) [Apply](#)

Type	WLAN ▾
Profile Name	Marketing
SSID	Marketing
ID	5 ▾

Hình 5.11: Tạo WLANs.

- Làm tương tự để tạo 4 WLANs.

## WLANs

Current Filter: [\[Change Filter\]](#) [\[Clear Filter\]](#) [Create New ▾](#)

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID
<input type="checkbox"/>	<a href="#">1</a>	WLAN	Marketing	Marketing
<input type="checkbox"/>	<a href="#">2</a>	WLAN	Business	Business
<input type="checkbox"/>	<a href="#">3</a>	WLAN	IoT	IoT
<input type="checkbox"/>	<a href="#">4</a>	WLAN	GUEST	GUEST

Hình 5.12: Tạo thành công 4 WLANs.

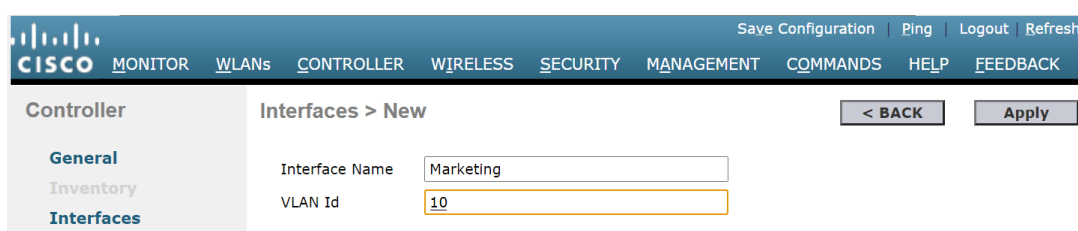
## 5.2.3 Cấu hình Interface WLANs

- Truy cập giao diện web của WLC, chọn menu **CONTROLLER**.
- Menu Controller hiện ra, chọn **Interfaces**.

Cisco						
MONITOR WLANs <b>CONTROLLER</b> WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK						
Save Configuration Ping Logout Refresh Home						
Controller Entries 1 - 6 of 6 <a href="#">New...</a>						
General	Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
Inventory		20	12.0.2.2	Dynamic	Disabled	<a href="#">Remove</a>
Interfaces		40	12.0.4.130	Dynamic	Disabled	<a href="#">Remove</a>
Interface Groups		30	12.0.4.2	Dynamic	Disabled	<a href="#">Remove</a>
Multicast		10	12.0.1.2	Dynamic	Disabled	<a href="#">Remove</a>
Internal DHCP Server		untagged	12.0.4.232	Static	Enabled	:::128
Mobility Management		N/A	192.0.2.1	Static	Not Supported	
Ports						

Hình 5.13: Truy cập Interfaces trong Controller.

- Khởi tạo Interface WLAN:
  - + Ở góc phải của trang này, chọn **New**.
  - + Interface Name: Nhập tên tùy chọn, nên đặt tên đồng bộ với Profile Name đã đặt trong phần tạo SSID.
  - + VLAN id: Nhập VLAN id muốn kết nối vào SSID.
  - + Chọn **Apply**.



Hình 5.14: Tạo interface WLANs.

- **Cấu hình thông tin cho Interface WLANs:**
  - + Port number: **1**. Thật ra có thể nhập con số khác, nhưng trong môi trường mô phỏng, chỉ cho phép port 1.
  - + VLAN Identifier: Mã của VLAN, ở đây là **10**.
  - + IP Address: Nhập địa chỉ IP cho WLAN, có thể xem như nó là một loại gateway nhưng trở về WLC.
  - + Ở đây nhập **12.0.1.2**. Có thể thấy IP gateway của mạng VLAN 10 nằm trên Router R4 là **12.0.1.1**.
  - + Net mask: Nhập subnet mask của đường mạng, ở đây nhập **255.255.255.0**.
  - + Gateway: Default gateway của đường mạng VLAN, chính là địa chỉ default gateway trên Router R4. Ở đây nhập **12.0.1.1**.
  - + Primary DHCP Server: Địa chỉ để yêu cầu IP động. Do R4 được cấu hình Stateful DHCP nên địa chỉ này trùng với địa chỉ Gateway, là **12.0.1.1**.
  - + Nhấn **Apply**.

The screenshot shows the Cisco Controller configuration page for a WLAN interface. The left sidebar contains a navigation menu with options like General, Inventory, Interfaces, Interface Groups, Multicast, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, Tunneling, IPv6, and mDNS. The main content area is titled 'Physical Information' and includes fields for Port Number (1), Backup Port (0), Active Port (1), and a checkbox for Enable Dynamic AP Management. Below this is the 'Interface Address' section with fields for VLAN Identifier (10), IP Address (12.0.1.2), Netmask (255.255.255.0), and Gateway (12.0.1.1). The 'DHCP Information' section has a field for Primary DHCP Server (12.0.1.1).

Hình 5.15: Cấu hình thông tin Interface WLAN.

## – Làm tương tự để tạo các Interfaces WLANs khác:

### + Interface Business:

- Port Number: 1.
- VLAN Identifier: 20.
- IP Address: 12.0.2.2.
- Net mask: 255.255.254.0.
- Gateway: 12.0.2.1.
- Primary DHCP Server: 12.0.2.1.

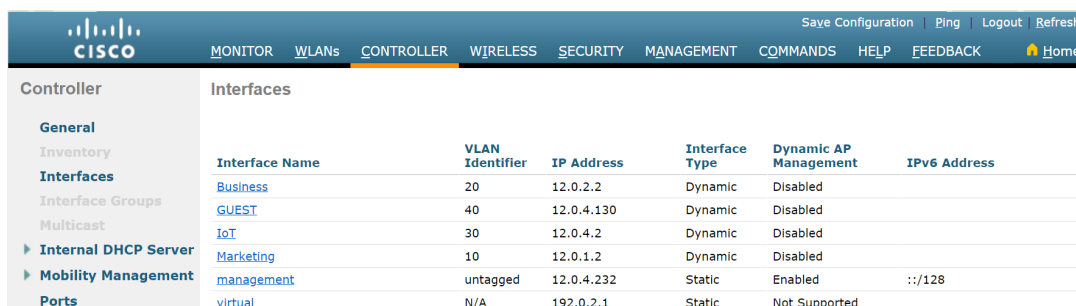
### + Interface IoT:

- Port Number: 1.
- VLAN Identifier: 30.
- IP Address: 12.0.4.2.
- Net mask: 255.255.255.128.
- Gateway: 12.0.4.1.
- Primary DHCP Server: 12.0.4.1.

### + Interface GUEST:

- Port Number: 1.
- VLAN Identifier: 40.
- IP Address: 12.0.4.130.

- Net mask: 255.255.255.192.
- Gateway: 12.0.4.129.
- Primary DHCP Server: 12.0.4.129.

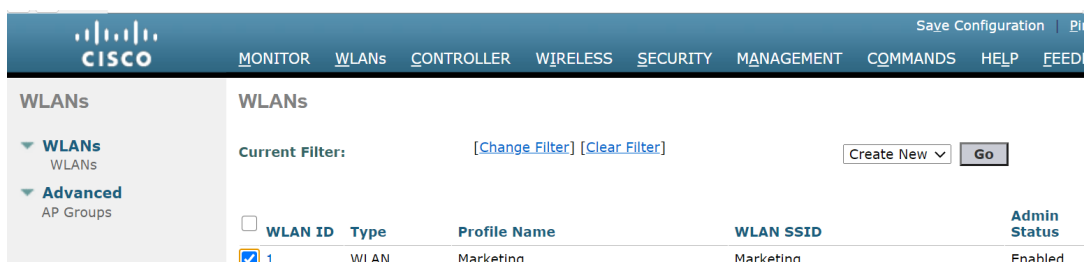


Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
Business	20	12.0.2.2	Dynamic	Disabled	
GUEST	40	12.0.4.130	Dynamic	Disabled	
IoT	30	12.0.4.2	Dynamic	Disabled	
Marketing	10	12.0.1.2	Dynamic	Disabled	
management	untagged	12.0.4.232	Static	Enabled	::128
virtual	N/A	192.0.2.1	Static	Not Supported	

Hình 5.16: Cấu hình hoàn tất các Interface WLAN.

## 5.2.4 Cấu hình bảo mật cho các SSID

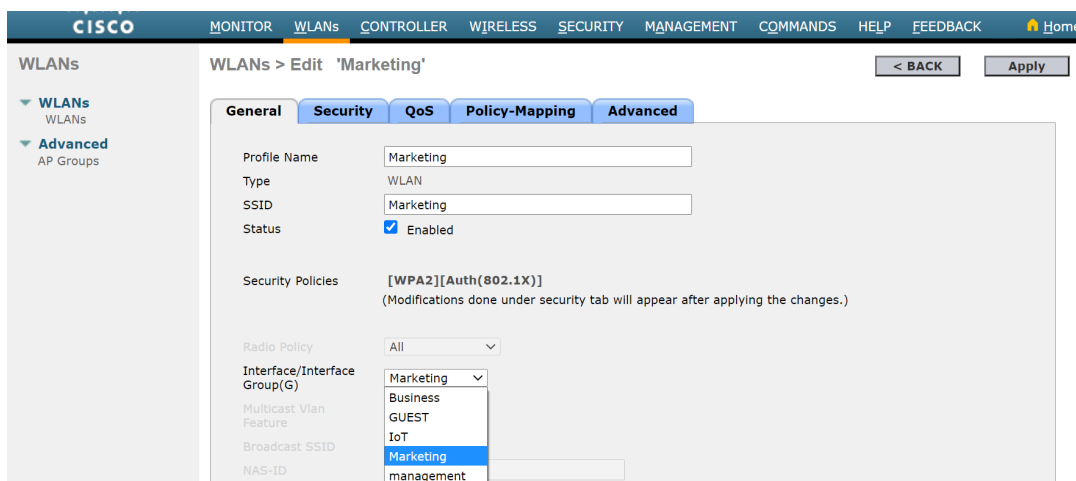
- Trên giao diện web của WLC, chọn menu **WLANs**.



WLAN ID	Type	Profile Name	WLAN SSID	Admin Status
1	WLAN	Marketing	Marketing	Enabled

Hình 5.17: Truy cập menu WLANs.

- Nhấn chọn WLAN ID cần cấu hình, ở đây đang cấu hình cho Marketing.



WLANs > Edit 'Marketing'

General Security QoS Policy-Mapping Advanced

Profile Name: Marketing

Type: WLAN

SSID: Marketing

Status: ☒ Enabled

Security Policies: [WPA2][Auth(802.1X)]  
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface/Interface Group(G): Marketing

Multicast Vlan Feature: Business

Broadcast SSID: GUEST

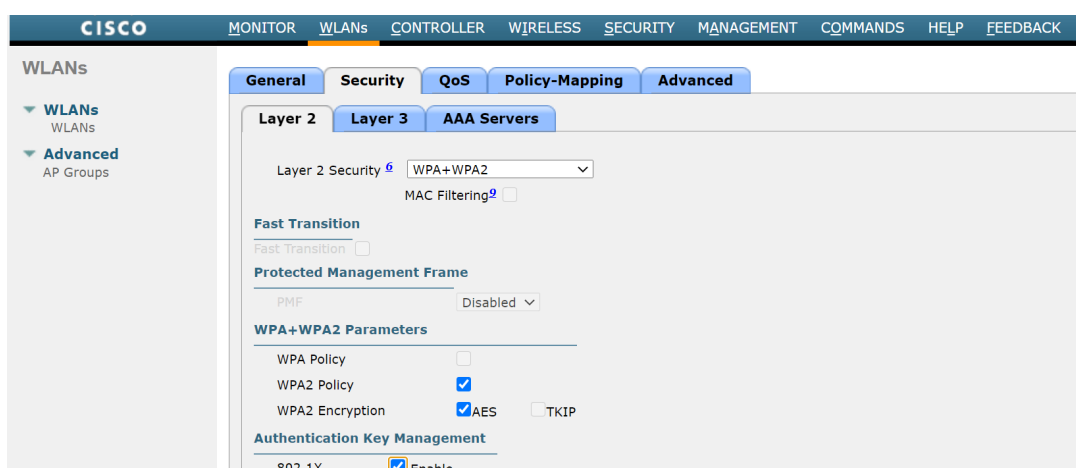
NAS-ID: IoT

Marketing

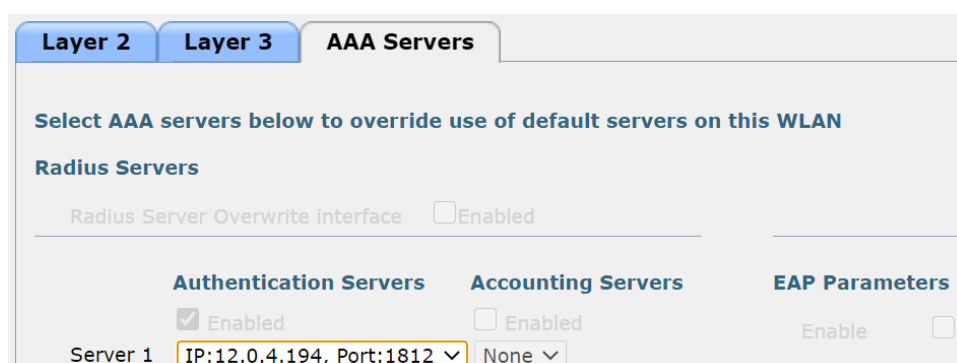
management

Hình 5.18: Cấu hình bảo mật cho Marketing.

- Mục Status: Chọn **Enabled**.
- Đến đây, phần Profile Name và SSID có thể thay đổi, tuy nhiên không khuyến khích thay đổi ở bước này.
- Ở mục Interface/Interface Group (G): Chọn Interface đã tạo, ở đây chọn interface **Marketing**.
- Chọn thẻ **Security**. Ở đây đang cấu hình bảo mật cho WLAN Marketing, dùng 802.1X.
  - + Ở thẻ Layer 2, mục Layer 2 Security, chọn **WPA+WPA2**. Giới hạn của chương trình mô phỏng không có WPA3.
  - + Tích chọn vào **WPA2 Policy**, **WPA2 Encrytion** và chọn chuẩn mã hóa nâng cao **AES**.
  - + Ở mục Authentication Key Management, chọn **Enable** chuẩn 802.1X.

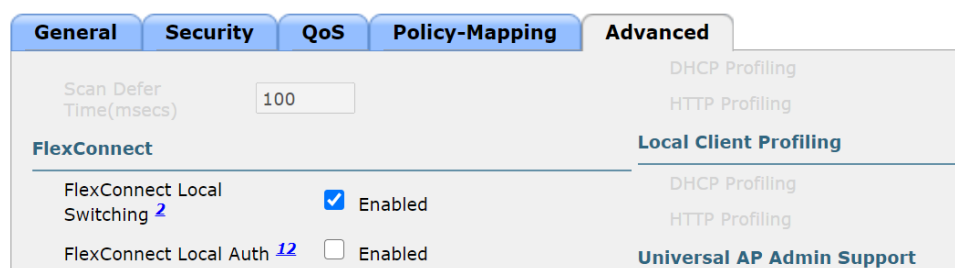


Hình 5.19: Cấu hình bảo mật cho Marketing.



Hình 5.20: Cấu hình bảo mật cho Marketing.

- Chuyển sang thẻ **AAA Servers**. Ở phần Authentication Servers, chọn Server đã cấu hình thông tin trước đó.
- Chuyển sang thẻ Advanced, ở mục FlexConnect, tích chọn **Enabled** vào mục Flex Connect Local Switching.
- **Lưu ý:** Nếu không tích chọn vào mục này, lưu lượng mạng sẽ chạy lên **WLC** rồi mới ra ngoài. Do đó, tích chọn vào, mạng sẽ đến Switch, Router và lưu thông bình thường.



Hình 5.21: Cấu hình bảo mật cho Marketing.

- Chọn **Apply**.
- Vừa rồi đã cấu hình bảo mật thành công cho mạng wifi Marketing với chuẩn **802.1X**.
- Do mạng Business cũng dùng chuẩn này nên chỉ cần thao tác lại tương tự.
- **Cấu hình bảo mật cho IoT:**
  - + Đối với mạng wifi IoT, dùng xác thực WPA2 + PSK thì các thao tác cũng tương tự như trên nhưng có điểm khác biệt sau:
    - Ở thẻ Security, thẻ con Layer 2, mục Authentication Key Management, tích chọn **PSK** thay vì **802.1X**.
    - Nhập mật khẩu vào ô trong ở mục PSK format chuẩn ASCII, ở đây mật khẩu dùng là **IoT2025!**.
    - Không cần cấu hình thẻ **AAA Servers**.

**Authentication Key Management**

802.1X ☐ Enable

CCKM ☐ Enable

PSK ☒ Enable

FT 802.1X ☐ Enable

FT PSK ☐ Enable

PSK Format ASCII ▾

WPA gtk-randomize State Disable ▾

Hình 5.22: Cấu hình bảo mật cho IoT.

- + Bật **Enabled** cho mục FlexConnect Local Switching và nhấn **Apply** là hoàn thành cấu hình.
- **Không bảo mật cho GUEST:**
  - + Đối với Wifi GUEST, sẽ để chế độ **Open**, nên phần Security, trong thẻ Layer 2, mục Layer 2 Security, chọn **None**.

**WLANs > Edit 'GUEST'**

**General** **Security** **QoS** **Policy-Mapping** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Layer 2 Security 6 None ▾

MAC Filtering 9 ☐

Hình 5.23: Không bảo mật cho wifi GUEST.

- + Bật **Enabled** cho mục FlexConnect Local Switching và nhấn **Apply** là hoàn thành cấu hình.

**WLANs** Entries 1 - 4 of 4

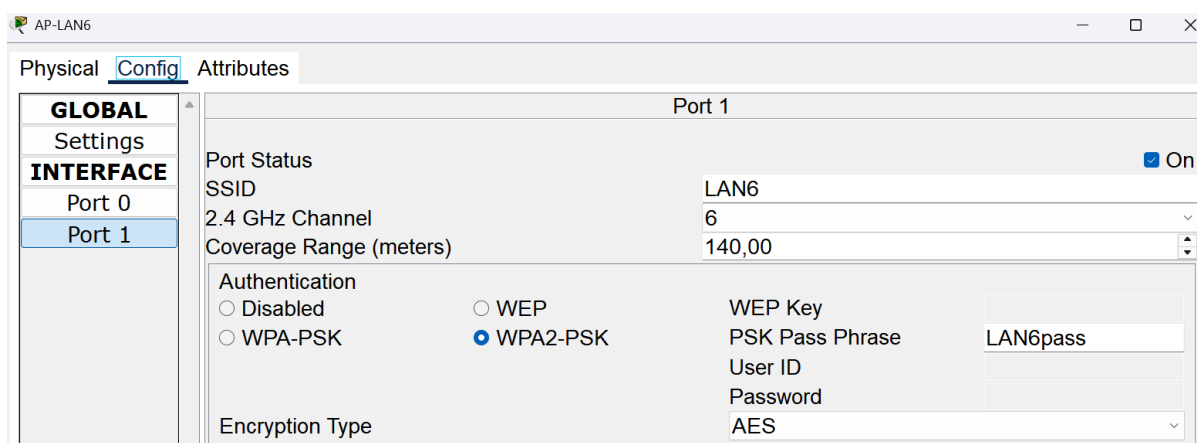
Current Filter: [\[Change Filter\]](#) [\[Clear Filter\]](#) Create New ▾ **Go**

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/>	<a href="#">1</a>	WLAN	Marketing	Marketing	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/>	<a href="#">2</a>	WLAN	Business	Business	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/>	<a href="#">3</a>	WLAN	IoT	IoT	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	<a href="#">4</a>	WLAN	GUEST	GUEST	Enabled	None

Hình 5.24: Hoàn thành cấu hình bảo mật WLANs.

## 5.2.5 Cấu hình mạng không dây khu vực REMOTE

- Cấu hình mạng không dây khu vực REMOTE khá đơn giản khi dùng Access Point - PT.
- Access Point này có 2 port là 0 và 1.
- Đầu nối port 0 vào Switch khu vực mạng của LAN6 và LAN8.
- Cấu hình mạng không dây trên Port 1.



Hình 5.25: Mô phỏng mạng không dây khu vực REMOTE.

- Làm tương tự cho khu vực LAN8.

## 5.3 Cấu hình VPN

Phần này trình bày chi tiết cấu hình VPN IPsec giữa R6 với R7 và giữa R7 với R8 trong khu vực REMOTE, nhằm đảm bảo an toàn cho lưu lượng dữ liệu giữa các chi nhánh và Trụ sở chính (HQ). VPN được triển khai sử dụng giao thức **ISAKMP/IKE** với chính sách bảo mật mạnh mẽ, mã hóa **AES 256**, và xác thực **SHA**.

- Tổng quan cấu hình VPN:
  - + VPN IPsec được thiết lập để mã hóa lưu lượng giữa các mạng nội bộ của chi nhánh và HQ, bao gồm các dải địa chỉ **12.0.0.0/16**, **128.1.0.0/16**, và **200.0.100.0/24**.
  - + VPN giữa R6 và R7 sử dụng chính sách ISAKMP 67, khóa chia sẻ



`VPNKeyR6R7!`, và transform-set `SET67`.

- + VPN giữa R7 và R8 sử dụng chính sách ISAKMP 78, khóa chia sẻ `VPNKeyR7R8!`, và transform-set `SET78`.
- + Các ACL được cấu hình để xác định lưu lượng cần mã hóa, áp dụng trên các interface `S0/1/0` và `S0/1/1`.
- Cấu hình VPN trên R6:
  - + Mô tả: R6 thiết lập VPN IPsec với R7 để mã hóa lưu lượng giữa mạng nội bộ `128.1.7.0/24` (chi nhánh R6) và các mạng tại HQ và chi nhánh khác.
  - + Các bước cấu hình:
    - Kích hoạt ISAKMP và định nghĩa chính sách 67:
      - `crypto isakmp enable`: Kích hoạt giao thức ISAKMP.
      - `crypto isakmp policy 67`: Tạo chính sách ISAKMP với độ ưu tiên 67.
      - `encryption aes 256`: Sử dụng mã hóa AES 256 bit.
      - `hash sha`: Sử dụng thuật toán SHA cho xác thực.
      - `authentication pre-share`: Sử dụng khóa chia sẻ trước.
      - `group 2`: Sử dụng nhóm Diffie-Hellman 2.
    - Cấu hình khóa chia sẻ:  
`crypto isakmp key VPNKeyR6R7! address 200.0.100.1`  
để xác thực với R7.
    - Cấu hình transform-set: `crypto ipsec transform-set SET67 esp-aes 256 esp-sha-hmac` để định nghĩa phương thức mã hóa và xác thực.
    - ACL xác định lưu lượng cần mã hóa: `access-list 110` cho phép các dải `128.1.7.0/24` kết nối với `12.0.0.0/16`, `128.1.0.0/16`, và `200.0.100.0/24`.
    - Ánh xạ VPN: `crypto map VPN-MAP 67 ipsec-isakmp` với peer

200.0.100.1, transform-set SET67, và ACL 110.

- Áp dụng trên interface:

`interface S0/1/0` với `crypto map VPN-MAP`.

– Cấu hình VPN trên R7 (với R6):

- + Mô tả: R7 đóng vai trò trung tâm, thiết lập VPN với cả R6 và R8. Phần này tập trung vào VPN với R6.

- + Các bước cấu hình:

- Kích hoạt ISAKMP và định nghĩa chính sách 67 (tương tự R6).

- Cấu hình khóa chia sẻ:

`crypto isakmp key VPNKeyR6R7! address 200.0.100.2`

để xác thực với R6.

- Cấu hình transform-set: `crypto ipsec transform-set SET67 esp-aes 256 esp-sha-hmac`.

- ACL 110: Tương tự R6, xác định lưu lượng cần mã hóa giữa các mạng.

- Ánh xạ VPN: `crypto map VPN-MAP 67 ipsec-isakmp` với peer `200.0.100.2`.

- Áp dụng trên interface:

`interface S0/1/1` với `crypto map VPN-MAP`.

- Lưu cấu hình: `wr`.

– Cấu hình VPN trên R7 (với R8):

- + Mô tả: R7 thiết lập VPN IPsec thứ hai với R8 để mã hóa lưu lượng giữa các mạng tại HQ và mạng nội bộ `12.0.6.0/24` (chi nhánh R8).

- + Các bước cấu hình:

- Kích hoạt ISAKMP và định nghĩa chính sách 78:

- `crypto isakmp policy 78`: Chính sách ISAKMP với độ ưu tiên 78.

- Các tham số tương tự: `encryption aes 256, hash sha, group`

## 2.

- Cấu hình khóa chia sẻ:  
`crypto isakmp key VPNKeyR7R8! address 200.0.100.6.`
  - Cấu hình transform-set: `crypto ipsec transform-set SET78 esp-aes 256 esp-sha-hmac.`
  - ACL 120: Cho phép lưu lượng giữa `12.0.6.0/24` với `12.0.0.0/16`, `128.1.0.0/16`, và `200.0.100.0/24`.
  - Ánh xạ VPN: `crypto map VPN-MAP2 78 ipsec-isakmp` với peer `200.0.100.6`.
  - Áp dụng trên interface:  
`interface S0/1/0` với `crypto map VPN-MAP2`.
  - Lưu cấu hình: `wr`.
- Cấu hình VPN trên R8:
- + Mô tả: R8 thiết lập VPN IPsec với R7 để bảo vệ lưu lượng giữa mạng nội bộ `12.0.6.0/24` và các mạng tại HQ.
  - + Các bước cấu hình:
    - Kích hoạt ISAKMP và định nghĩa chính sách 78 (tương tự R7).
    - Cấu hình khóa chia sẻ:  
`crypto isakmp key VPNKeyR7R8! address 200.0.100.5.`
    - Cấu hình transform-set: `crypto ipsec transform-set SET78 esp-aes 256 esp-sha-hmac.`
    - ACL 120: Tương tự R7, xác định lưu lượng cần mã hóa.
    - Ánh xạ VPN: `crypto map VPN-MAP2 78 ipsec-isakmp` với peer `200.0.100.5`.
    - Áp dụng trên interface:  
`interface S0/1/0` với `crypto map VPN-MAP2`.

Cấu hình VPN đảm bảo lưu lượng giữa các chi nhánh và HQ được mã hóa an toàn, phù hợp với yêu cầu bảo mật của doanh nghiệp Chooky.

## Chương 6

# Mô tả cấu hình hệ thống - IPv6

### 6.1 Cấu hình địa chỉ IPv6

Để triển khai hệ thống mạng IPv6, cần gán địa chỉ IPv6 cho các interface trên các router theo sơ đồ địa chỉ đã được phân bổ. Dưới đây là các bước cấu hình chi tiết:

#### – Router R4 (HQ):

- + Interface `GigabitEthernet0/0/0`: Bật IPv6: `ipv6 enable`.
- + Sub-interface `GigabitEthernet0/0/0.10`:
  - Gán địa chỉ global:  
`ipv6 address 2019:ABBA:CDDC:1000::1/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::4:10 link-local`.
  - Bật hỗ trợ cấu hình khác: `ipv6 nd other-config-flag`.
  - Bật interface: `no shutdown`.
- + Sub-interface `GigabitEthernet0/0/0.20`:
  - Gán địa chỉ global:  
`ipv6 address 2019:ABBA:CDDC:2000::1/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::4:20 link-local`.
  - Bật hỗ trợ cấu hình khác: `ipv6 nd other-config-flag`.
  - Bật interface: `no shutdown`.
- + Sub-interface `GigabitEthernet0/0/0.30`:

- Gán địa chỉ global: `ipv6 address 2019:ABBA:CDDC:3000::1/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::4:30 link-local`.
  - Bật hỗ trợ cấu hình khác: `ipv6 nd other-config-flag`.
  - Bật interface: `no shutdown`.
- + Sub-interface `GigabitEthernet0/0/0.40`:
- Gán địa chỉ global: `ipv6 address 2019:ABBA:CDDC:4000::1/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::4:40 link-local`.
  - Bật hỗ trợ cấu hình khác: `ipv6 nd other-config-flag`.
  - Bật interface: `no shutdown`.
- + Sub-interface `GigabitEthernet0/0/0.60`:
- Gán địa chỉ global: `ipv6 address 2019:ABBA:BBBB:1::2/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::4 link-local`.
  - Bật interface: `no shutdown`.
- **Router R5 (HQ/Branch):**
- + Interface `Serial0/1/0`:
- Bật IPv6: `ipv6 enable`.
  - Gán địa chỉ global: `ipv6 address 2019:ABBA:AAAA:1::1/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::5:1 link-local`.
- + Interface `GigabitEthernet0/0/1`:
- Bật IPv6: `ipv6 enable`.
  - Gán địa chỉ global: `ipv6 address 2019:ABBA:BBBB:1::1/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::5 link-local`.
- **Router R7 (HQ):**
- + Interface `GigabitEthernet0/0/0`:
- Bật IPv6: `ipv6 enable`.
  - Gán địa chỉ global: `ipv6 address 2019:ABBA:BBBB:1::3/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::7 link-local`.

- Bật interface: `no shutdown`.
- + Interface `Serial0/1/1`:
  - Bật IPv6: `ipv6 enable`.
  - Gán địa chỉ global: `ipv6 address 2019:ABBA:CCCC:1::1/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::7:1 link-local`.
  - Bật interface: `no shutdown`.
- + Interface `Serial0/1/0`:
  - Bật IPv6: `ipv6 enable`.
  - Gán địa chỉ global: `ipv6 address 2019:ABBA:DDDD:1::1/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::7:2 link-local`.
  - Bật interface: `no shutdown`.
- **Router R6 (HQ):**
  - + Interface `GigabitEthernet0/0/0`:
    - Bật IPv6: `ipv6 enable`.
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:EEEE:1::1/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::6:1 link-local`.
    - Bật interface: `no shutdown`.
  - + Interface `Serial0/1/0`:
    - Bật IPv6: `ipv6 enable`.
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:CCCC:1::2/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::6 link-local`.
    - Bật interface: `no shutdown`.
- **Router R8 (HQ):**
  - + Interface `GigabitEthernet0/0/0`:
    - Bật IPv6: `ipv6 enable`.
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:FFFF:1::1/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::8:1 link-local`.

- Bật interface: `no shutdown`.
- + Interface `Serial0/1/0`:
  - Bật IPv6: `ipv6 enable`.
  - Gán địa chỉ global: `ipv6 address 2019:ABBA:DDDD:1::2/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::8 link-local`.
  - Bật interface: `no shutdown`.

– **Router ACCESS:**

- + Interface `Serial0/1/0`:
  - Bật IPv6: `ipv6 enable`.
  - Gán địa chỉ global: `ipv6 address 2019:ABBA:AAAA:1::2/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::A link-local`.
  - Bật interface: `no shutdown`.

Cấu hình IPv6 đảm bảo các interface trên các router được gán địa chỉ global và link-local phù hợp, với hỗ trợ cấu hình khác (nd other-config-flag) trên các sub-interface của R4 để chuẩn bị cho việc phân phối địa chỉ tự động.

## 6.2 Định tuyến IPv6

Yêu cầu cấu hình giao thức EIGRPv6 và các tuyến tính để đảm bảo kết nối giữa các mạng IPv6. Dưới đây là các bước cấu hình chi tiết:

– **Router R4 (HQ):**

- + Bật định tuyến unicast IPv6: `ipv6 unicast-routing`.
- + Cấu hình EIGRPv6:
  - Kích hoạt EIGRP: `ipv6 router eigrp 100`.
  - Đặt router-id: `router-id 4.4.4.4`.
  - Bật EIGRP: `no shutdown`.
  - Đặt tất cả interface thành passive mặc định: `passive-interface default`.

- Bật gửi bản cập nhật trên interface chính: `no passive-interface GigabitEthernet0/0/0`.
- + Áp dụng EIGRP trên các sub-interface:
- `GigabitEthernet0/0/0.10: ipv6 eigrp 100`.
  - `GigabitEthernet0/0/0.20: ipv6 eigrp 100`.
  - `GigabitEthernet0/0/0.30: ipv6 eigrp 100`.
  - `GigabitEthernet0/0/0.40: ipv6 eigrp 100`.
- + Cấu hình tuyến tính:
- Đến mạng R5: `ipv6 route 2019:ABBA:AAAA:1::/64 2019:ABBA:BBBB:1::1 100`.
  - Đến mạng R7-R6: `ipv6 route 2019:ABBA:CCCC:1::/64 2019:ABBA:BBBB:1::3 100`.
  - Đến mạng R7-R8: `ipv6 route 2019:ABBA:DDDD:1::/64 2019:ABBA:BBBB:1::3 100`.
  - Đến mạng R6: `ipv6 route 2019:ABBA:EEEE:1::/64 2019:ABBA:BBBB:1::3 100`.
  - Đến mạng R8: `ipv6 route 2019:ABBA:FFFF:1::/64 2019:ABBA:BBBB:1::3 100`.
  - Tuyến mặc định: `ipv6 route ::/0 2019:ABBA:BBBB:1::1`.
- **Router R5 (HQ/Branch):**
- + Bật định tuyến unicast IPv6: `ipv6 unicast-routing`.
- + Cấu hình EIGRPv6:
- Kích hoạt EIGRP: `ipv6 router eigrp 100`.
  - Đặt router-id: `router-id 5.5.5.5`.
  - Bật EIGRP: `no shutdown`.
  - Đặt tất cả interface thành passive mặc định: `passive-interface default`.



- Bật gửi bản cập nhật trên các interface:  
`no passive-interface GigabitEthernet0/0/0,`  
`no passive-interface GigabitEthernet0/0/1,`  
`no passive-interface Serial0/1/0.`
  - Phân phối lại tuyến tĩnh: `redistribute static.`
- + Áp dụng EIGRP trên các interface:
- `Serial0/1/0: ipv6 eigrp 100.`
  - `GigabitEthernet0/0/0: ipv6 eigrp 100.`
  - `GigabitEthernet0/0/1: ipv6 eigrp 100.`
- + Cấu hình tuyến tĩnh:
- Đến các mạng R4:  
`ipv6 route 2019:ABBA:CDDC:1000::/64`  
`2019:ABBA:BBBB:1::2 100,`  
`ipv6 route 2019:ABBA:CDDC:2000::/64`  
`2019:ABBA:BBBB:1::2 100,`  
`ipv6 route 2019:ABBA:CDDC:3000::/64`  
`2019:ABBA:BBBB:1::2 100,`  
`ipv6 route 2019:ABBA:CDDC:4000::/64`  
`2019:ABBA:BBBB:1::2 100.`
  - Tuyến mặc định: `ipv6 route ::/0 Serial0/1/0.`
- **Router R7 (HQ):**
- + Bật định tuyến unicast IPv6: `ipv6 unicast-routing.`
- + Cấu hình EIGRPv6:
- Kích hoạt EIGRP: `ipv6 router eigrp 100.`
  - Đặt router-id: `router-id 7.7.7.7.`
  - Bật EIGRP: `no shutdown.`
  - Đặt tất cả interface thành passive mặc định:  
`passive-interface default.`

- Bật gửi bản cập nhật trên các interface:  
`no passive-interface GigabitEthernet0/0/0,`  
`no passive-interface Serial0/1/0,`  
`no passive-interface Serial0/1/1.`
  - Phân phối lại tuyến tĩnh: `redistribute static.`
- + Áp dụng EIGRP trên các interface:
- `Serial0/1/0: ipv6 eigrp 100.`
  - `GigabitEthernet0/0/0: ipv6 eigrp 100.`
  - `Serial0/1/1: ipv6 eigrp 100.`
- + Cấu hình tuyến tĩnh:
- Đến các mạng R4:  
`ipv6 route 2019:ABBA:CDDC:1000::/64`  
`2019:ABBA:BBBB:1::2 100,`  
`ipv6 route 2019:ABBA:CDDC:2000::/64`  
`2019:ABBA:BBBB:1::2 100,`  
`ipv6 route 2019:ABBA:CDDC:3000::/64`  
`2019:ABBA:BBBB:1::2 100,`  
`ipv6 route 2019:ABBA:CDDC:4000::/64`  
`2019:ABBA:BBBB:1::2 100.`
  - Tuyến mặc định: `ipv6 route ::/0 2019:ABBA:BBBB:1::1.`
- **Router R6 (HQ):**
- + Bật định tuyến unicast IPv6: `ipv6 unicast-routing.`
- + Cấu hình EIGRPv6:
- Kích hoạt EIGRP: `ipv6 router eigrp 100.`
  - Đặt router-id: `router-id 6.6.6.6.`
  - Bật EIGRP: `no shutdown.`
  - Đặt tất cả interface thành passive mặc định:  
`passive-interface default.`

- Bật gửi bản cập nhật trên các interface:  
`no passive-interface GigabitEthernet0/0/0,`  
`no passive-interface Serial0/1/0.`
  - Phân phối lại tuyến tĩnh: `redistribute static.`
- + Áp dụng EIGRP trên các interface:
- `Serial0/1/0: ipv6 eigrp 100.`
  - `GigabitEthernet0/0/0: ipv6 eigrp 100.`
- **Router R8 (HQ):**
- + Bật định tuyến unicast IPv6: `ipv6 unicast-routing.`
- + Cấu hình EIGRPv6:
- Kích hoạt EIGRP: `ipv6 router eigrp 100.`
  - Đặt router-id: `router-id 8.8.8.8.`
  - Bật EIGRP: `no shutdown.`
  - Đặt tất cả interface thành passive mặc định:  
`passive-interface default.`
  - Bật gửi bản cập nhật trên các interface:  
`no passive-interface GigabitEthernet0/0/0,`  
`no passive-interface Serial0/1/0.`
  - Phân phối lại tuyến tĩnh: `redistribute static.`
- + Áp dụng EIGRP trên các interface:
- `Serial0/1/0: ipv6 eigrp 100.`
  - `GigabitEthernet0/0/0: ipv6 eigrp 100.`
- **Router ACCESS:**
- + Bật định tuyến unicast IPv6: `ipv6 unicast-routing.`
- + Cấu hình tuyến tĩnh:
- Đến mạng R4:  
`ipv6 route 2019:ABBA:CDDC::/48 Serial0/1/0.`

- Đến mạng R5:  
`ipv6 route 2019:ABBA:AAAA:1::/64 Serial0/1/0.`
- Đến mạng R4-R7:  
`ipv6 route 2019:ABBA:BBBB:1::/64 Serial0/1/0.`
- Đến mạng R7-R6:  
`ipv6 route 2019:ABBA:CCCC:1::/64 Serial0/1/0.`
- Đến mạng R7-R8:  
`ipv6 route 2019:ABBA:DDDD:1::/64 Serial0/1/0.`
- Đến mạng R6:  
`ipv6 route 2019:ABBA:EEEE:1::/64 Serial0/1/0.`
- Đến mạng R8:  
`ipv6 route 2019:ABBA:FFFF:1::/64 Serial0/1/0.`

Cấu hình EIGRPv6 đảm bảo kết nối động giữa các mạng nội bộ, trong khi các tuyến tĩnh và tuyến mặc định hỗ trợ định tuyến đến các mạng khác và Internet thông qua router ACCESS.

## 6.3 Cấu hình DHCPv6

Yêu cầu cấu hình DHCPv6 trên router R4 để tự động cấp địa chỉ IPv6 cho các VLAN tại khu vực HQ (VLAN 10, 20, 30, 40). Dưới đây là các bước cấu hình chi tiết:

### – Router R4 (HQ):

- + Bật định tuyến unicast IPv6: `ipv6 unicast-routing`.
- + Cấu hình các DHCPv6 pool:
  - Pool **VLAN10**:
    - Gán prefix địa chỉ:  
`address prefix 2019:ABBA:CDDC:1000::/64.`
    - Cấu hình DNS server: `dns-server 2001:4860:4860::8888`  
(Google Public DNS).

- Pool **VLAN20**:
    - Gán prefix địa chỉ:  
`address prefix 2019:ABBA:CDDC:2000::/64.`
    - Cấu hình DNS server: `dns-server 2001:4860:4860::8888.`
  - Pool **VLAN30**:
    - Gán prefix địa chỉ:  
`address prefix 2019:ABBA:CDDC:3000::/64.`
    - Cấu hình DNS server: `dns-server 2001:4860:4860::8888.`
  - Pool **VLAN40**:
    - Gán prefix địa chỉ:  
`address prefix 2019:ABBA:CDDC:4000::/64.`
    - Cấu hình DNS server: `dns-server 2001:4860:4860::8888.`
- + Áp dụng DHCPv6 server trên các sub-interface:
- `GigabitEthernet0/0/0.10: ipv6 dhcp server VLAN10.`
  - `GigabitEthernet0/0/0.20: ipv6 dhcp server VLAN20.`
  - `GigabitEthernet0/0/0.30: ipv6 dhcp server VLAN30.`
  - `GigabitEthernet0/0/0.40: ipv6 dhcp server VLAN40.`

Cấu hình DHCPv6 đảm bảo các host trong VLAN 10, 20, 30, 40 nhận được địa chỉ IPv6 từ prefix tương ứng và sử dụng DNS server `2001:4860:4860::8888`. Điều này kết hợp với lệnh `ipv6 nd other-config-flag` (đã cấu hình trước đó) để thông báo host lấy thêm thông tin cấu hình qua DHCPv6.

## Chương 7

# Kết quả đạt được mạng có dây

### 7.1 Kết quả cấu hình kết nối PPP

Quá trình cấu hình **PPP PAP** giữa **R7** và **R6** trên interface **Serial0/1/1**, và **PPP CHAP** giữa **R7** và **R8** trên interface **Serial0/1/0** đã thành công. Kết quả kiểm tra bằng lệnh **show interface Serial0/1/1** trên **R7** cho thấy trạng thái **up/up**, với giao thức PPP hoạt động ổn định. Xác thực PAP và CHAP được thực hiện chính xác, không có lỗi đăng nhập. Lệnh **ping** từ **R7** đến **R6** (địa chỉ **200.0.100.1**) và **R8** (địa chỉ **200.0.100.5**) đều thành công với tỷ lệ 100%.

R7	R6
Physical Config <u>CLI</u> Attributes	Physical Config <u>CLI</u> Attributes
IOS Command Line Interface	IOS Command Line Interface
<pre>interface Serial0/1/1 ip address 200.0.100.1 255.255.255.252 encapsulation ppp ipv6 address FE80::7:1 link-local ipv6 address 2019:ABBA:CCCC:1::1/64 ipv6 eigrp 100</pre>	<pre>interface Serial0/1/0 ip address 200.0.100.2 255.255.255.252 encapsulation ppp ppp pap sent-username R6 password 0 chooky ipv6 address FE80::6 link-local ipv6 address 2019:ABBA:CCCC:1::2/64</pre>

Hình 7.1: Kết quả cấu hình PPP PAP trên R7 và R6.

R7	R8
Physical Config <u>CLI</u> Attributes	Physical Config <u>CLI</u> Attributes
IOS Command Line Interface	IOS Command Line Interface
<pre>interface Serial0/1/0 ip address 200.0.100.5 255.255.255.252 encapsulation ppp ppp authentication chap ppp chap hostname R7 ppp chap password vmc</pre>	<pre>interface Serial0/1/0 ip address 200.0.100.6 255.255.255.252 encapsulation ppp ppp authentication chap ppp chap hostname R8 ppp chap password vmc</pre>

Hình 7.2: Kết quả cấu hình PPP CHAP trên R7 và R8.

```

R7#ping 200.0.100.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.100.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/19/29 ms

R7#ping 200.0.100.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.100.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/20/34 ms

```

Hình 7.3: Thông mạng R7 đến R6 và R8.

## 7.2 Kết quả cấu hình GRE tunnel

Cấu hình **GRE tunnel** giữa **R6** và **R8** với địa chỉ tunnel **200.0.100.24/30** đã hoạt động hiệu quả. Kết quả kiểm tra bằng lệnh **show interface Tunnel0** trên **R6** và **R8** cho thấy trạng thái **up/up**, với lưu lượng dữ liệu được truyền qua tunnel mà không bị mất gói. Lệnh **ping** từ **200.0.100.25** (R6) đến **200.0.100.26** (R8) thành công với tỷ lệ 100% gói tin trả về, độ trễ trung bình khoảng 3ms. Giao thức **EIGRP** chạy trên tunnel cũng thiết lập quan hệ láng giềng thành công, được xác nhận qua lệnh **show ip eigrp neighbors**.

R8	R6
Physical Config <u>CLI</u> Attributes	Physical Config <u>CLI</u> Attributes
IOS Comm	IOS Command Line Interface
<pre> interface Tunnel0 ip address 200.0.100.26 255.255.255.252 mtu 1476 tunnel source Serial0/1/0 tunnel destination 200.0.100.2 </pre>	<pre> interface Tunnel0 ip address 200.0.100.25 255.255.255.252 mtu 1476 tunnel source Serial0/1/0 tunnel destination 200.0.100.6 </pre>

Hình 7.4: Kết quả trạng thái GRE tunnel trên R6 và R8.

<pre> R8#ping 200.0.100.25  Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 200.0.100.25, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 16/27/53 ms </pre>	<pre> R6#ping 200.0.100.26  Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 200.0.100.26, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 31/59/146 ms </pre>
--	---

Hình 7.5: Thông mạng R6 và R8 trên GRE Tunnel.

## 7.3 Kết quả cấu hình định tuyến

Cấu hình **OSPF** tại khu vực chi nhánh (**R1, R2, R3**) và **EIGRP** tại khu vực HQ (**R4, R5, R6, R7**), cùng tuyến tỉnh giữa **R4, R5, R7** qua **VLAN 60 (12.0.4.224/27)**, đã đảm bảo kết nối đầy đủ giữa các mạng. Bảng định tuyến trên các router hiển thị các tuyến chính xác, với độ trễ thấp và không có lỗi định tuyến.

Neighbor ID	Pri	State	Dead Time	Address	Interface
128.1.4.1	1	2WAY/DROTHER	00:00:34	128.1.8.3	GigabitEthernet0/0/0
200.0.100.9	1	FULL/DR	00:00:35	128.1.8.5	GigabitEthernet0/0/0
128.1.6.1	1	FULL/BDR	00:00:34	128.1.8.4	GigabitEthernet0/0/0

Neighbor ID	Pri	State	Dead Time	Address	Interface
200.0.100.9	1	FULL/DR	00:00:33	128.1.8.5	GigabitEthernet0/0/0
128.1.6.1	1	FULL/BDR	00:00:33	128.1.8.4	GigabitEthernet0/0/0
128.1.2.1	1	2WAY/DROTHER	00:00:32	128.1.8.2	GigabitEthernet0/0/0

Neighbor ID	Pri	State	Dead Time	Address	Interface
128.1.4.1	1	FULL/DROTHER	00:00:31	128.1.8.3	GigabitEthernet0/0/0
200.0.100.9	1	FULL/DR	00:00:32	128.1.8.5	GigabitEthernet0/0/0
128.1.2.1	1	FULL/DROTHER	00:00:30	128.1.8.2	GigabitEthernet0/0/0

Neighbor ID	Pri	State	Dead Time	Address	Interface
128.1.4.1	1	FULL/DROTHER	00:00:33	128.1.8.3	GigabitEthernet0/0/0
128.1.6.1	1	FULL/BDR	00:00:33	128.1.8.4	GigabitEthernet0/0/0
128.1.2.1	1	FULL/DROTHER	00:00:32	128.1.8.2	GigabitEthernet0/0/0

Hình 7.6: Miền OSPF trên R1, R2, R3 và R5.

```

12.0.0.0/8 is variably subnetted, 7 subnets, 7 masks
S    12.0.1.0/24 [1/0] via 12.0.4.225
S    12.0.2.0/23 [1/0] via 12.0.4.225
S    12.0.4.0/25 [1/0] via 12.0.4.225
S    12.0.4.128/26 [1/0] via 12.0.4.225
S    12.0.4.192/28 [1/0] via 12.0.4.225
C    12.0.4.224/27 is directly connected, GigabitEthernet0/0/1
L    12.0.4.230/32 is directly connected, GigabitEthernet0/0/1
128.1.0.0/16 is variably subnetted, 7 subnets, 2 masks
O    128.1.0.1/32 [110/2] via 128.1.8.2, 03:00:40, GigabitEthernet0/0/0
O    128.1.2.1/32 [110/2] via 128.1.8.2, 03:00:40, GigabitEthernet0/0/0
O    128.1.4.1/32 [110/2] via 128.1.8.3, 03:00:40, GigabitEthernet0/0/0
O    128.1.5.1/32 [110/2] via 128.1.8.4, 03:00:40, GigabitEthernet0/0/0
O    128.1.6.1/32 [110/2] via 128.1.8.4, 03:00:40, GigabitEthernet0/0/0
C    128.1.8.0/24 is directly connected, GigabitEthernet0/0/0
L    128.1.8.5/32 is directly connected, GigabitEthernet0/0/0
200.0.100.0/24 is variably subnetted, 5 subnets, 2 masks
D    200.0.100.0/30 [90/2170112] via 12.0.4.231, 01:06:57, GigabitEthernet0/0/1
D    200.0.100.4/30 [90/2170112] via 12.0.4.231, 01:06:57, GigabitEthernet0/0/1
C    200.0.100.8/30 is directly connected, Serial0/1/0
L    200.0.100.9/32 is directly connected, Serial0/1/0
D    200.0.100.24/30 [90/27392256] via 12.0.4.231, 00:11:22, GigabitEthernet0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/1/0

```

Hình 7.7: Bảng định tuyến trên Router R5.

Ping thành công từ một Router bất kỳ khu vực chi nhánh (Router R1) ra Internet thành công.



```
R1#ping 203.0.113.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/11/31 ms
```

```
R1#ping 203.0.113.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 203.0.113.2, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/22/48 ms
```

Hình 7.8: Kết quả thông mạng khu vực chi nhánh ra Internet

```
12.0.0.0/8 is variably subnetted, 13 subnets, 7 masks
C    12.0.1.0/24 is directly connected, GigabitEthernet0/0/0.10
L    12.0.1.1/32 is directly connected, GigabitEthernet0/0/0.10
C    12.0.2.0/23 is directly connected, GigabitEthernet0/0/0.20
L    12.0.2.1/32 is directly connected, GigabitEthernet0/0/0.20
C    12.0.4.0/25 is directly connected, GigabitEthernet0/0/0.30
L    12.0.4.1/32 is directly connected, GigabitEthernet0/0/0.30
C    12.0.4.128/26 is directly connected, GigabitEthernet0/0/0.40
L    12.0.4.129/32 is directly connected, GigabitEthernet0/0/0.40
C    12.0.4.192/28 is directly connected, GigabitEthernet0/0/0.50
L    12.0.4.193/32 is directly connected, GigabitEthernet0/0/0.50
C    12.0.4.224/27 is directly connected, GigabitEthernet0/0/0.60
L    12.0.4.225/32 is directly connected, GigabitEthernet0/0/0.60
S    12.0.6.0/24 [1/0] via 12.0.4.231
128.1.0.0/16 is variably subnetted, 7 subnets, 3 masks
S    128.1.0.0/23 [1/0] via 12.0.4.230
S    128.1.2.0/23 [1/0] via 12.0.4.230
S    128.1.4.0/25 [1/0] via 12.0.4.230
S    128.1.5.0/24 [1/0] via 12.0.4.230
S    128.1.6.0/25 [1/0] via 12.0.4.230
S    128.1.7.0/24 [1/0] via 12.0.4.231
S    128.1.8.0/24 [1/0] via 12.0.4.230
200.0.100.0/30 is subnetted, 4 subnets
S    200.0.100.0/30 [1/0] via 12.0.4.231
S    200.0.100.4/30 [1/0] via 12.0.4.231
S    200.0.100.8/30 [1/0] via 12.0.4.230
S    200.0.100.24/30 [1/0] via 12.0.4.231
S    203.0.113.0/24 [1/0] via 12.0.4.230
```

Hình 7.9: Bảng định tuyến trên Router R4.

Thực hiện ping thành công từ một PC trong VLAN 10 ra Internet.

```
UNIT1 C>:>ping 203.0.113.1
```

```
Pinging 203.0.113.1 with 32 bytes of data:
```

```
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
```

```
Reply from 203.0.113.1: bytes=32 time=3ms TTL=253
```

```
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
```

```
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
```

```

12.0.0.0/8 is variably subnetted, 7 subnets, 7 masks
S    12.0.1.0/24 [1/0] via 12.0.4.225
S    12.0.2.0/23 [1/0] via 12.0.4.225
S    12.0.4.0/25 [1/0] via 12.0.4.225
S    12.0.4.128/26 [1/0] via 12.0.4.225
S    12.0.4.192/28 [1/0] via 12.0.4.225
C    12.0.4.224/27 is directly connected, GigabitEthernet0/0/0
L    12.0.4.231/32 is directly connected, GigabitEthernet0/0/0
128.1.0.0/16 is variably subnetted, 11 subnets, 4 masks
S    128.1.0.0/23 [1/0] via 12.0.4.230
D EX 128.1.0.1/32 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
S    128.1.2.0/23 [1/0] via 12.0.4.230
D EX 128.1.2.1/32 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
S    128.1.4.0/25 [1/0] via 12.0.4.230
D EX 128.1.4.1/32 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
S    128.1.5.0/24 [1/0] via 12.0.4.230
D EX 128.1.5.1/32 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
S    128.1.6.0/25 [1/0] via 12.0.4.230
D EX 128.1.6.1/32 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
S    128.1.8.0/24 [1/0] via 12.0.4.230
200.0.100.0/24 is variably subnetted, 8 subnets, 2 masks
C    200.0.100.0/30 is directly connected, Serial0/1/1
L    200.0.100.1/32 is directly connected, Serial0/1/1
C    200.0.100.2/32 is directly connected, Serial0/1/1
C    200.0.100.4/30 is directly connected, Serial0/1/0
L    200.0.100.5/32 is directly connected, Serial0/1/0
C    200.0.100.6/32 is directly connected, Serial0/1/0
D    200.0.100.8/30 [90/2170112] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
D    200.0.100.24/30 [90/27392000] via 200.0.100.6, 00:17:21, Serial0/1/0
S    203.0.113.0/24 [1/0] via 12.0.4.230
D*EX 0.0.0.0/0 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0

```

Hình 7.10: Bảng định tuyến trên Router R7.

<pre> R6#ping 203.0.113.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 9/32/63 ms </pre>	<pre> R8#ping 203.0.113.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 23/44/77 ms </pre>
--	---

Hình 7.11: Thông mạng từ R6 và R8 ra Internet.

## 7.4 Kết quả cấu hình chuyển mạch

Cấu hình chuyển mạch trên **S1**, **S2**, **S3**, **S4** với **VTP domain HQ**, **Rapid PVST+**, và **EtherChannel** đã hoạt động hiệu quả. Lệnh **show vtp status** trên **S1** xác nhận **S1** là VTP Server, với các VLAN **10**, **20**, **30**, **40**, **50**, **60** được đồng bộ hóa trên **S2**, **S3**, **S4**. **Rapid PVST+** đảm bảo không có vòng lặp, với **S1** là root bridge cho **VLAN 10**, **20**, **30** và **S2** là root cho **VLAN 40**, **50**, **60**, được xác nhận qua **show spanning-tree**. **EtherChannel** trên các port **FastEthernet0/1-2** và **FastEthernet0/3-4** hoạt động ổn định, tăng băng thông (lệnh **show etherchannel summary**).

Inter-VLAN Routing trên R4 cho phép các VLAN giao tiếp, với ping từ 12.0.1.2 (VLAN 10) đến 12.0.2.2 (VLAN 20) thành công.

S1				S2			
Number of channel-groups in use: 2				Number of channel-groups in use: 2			
Number of aggregators: 2				Number of aggregators: 2			
Group	Port-channel	Protocol	Ports	Group	Port-channel	Protocol	Ports
1	Po1 (SU)	LACP	Fa0/1 (P) Fa0/2 (P)	1	Po1 (SU)	LACP	Fa0/1 (P) Fa0/2 (P)
2	Po2 (SU)	LACP	Fa0/3 (P) Fa0/4 (P)	2	Po2 (SU)	LACP	Fa0/3 (P) Fa0/4 (P)

S4				S3			
Number of channel-groups in use: 2				Number of channel-groups in use: 2			
Number of aggregators: 2				Number of aggregators: 2			
Group	Port-channel	Protocol	Ports	Group	Port-channel	Protocol	Ports
1	Po1 (SU)	LACP	Fa0/1 (P) Fa0/2 (P)	1	Po1 (SU)	LACP	Fa0/1 (P) Fa0/2 (P)
2	Po2 (SU)	LACP	Fa0/3 (P) Fa0/4 (P)	2	Po2 (SU)	LACP	Fa0/3 (P) Fa0/4 (P)

Hình 7.12: Kết quả cấu hình EtherChannel.

S1				S2			
Physical Config CLI Attributes				Physical Config CLI Attributes			
IOS Command Line Interface				IOS Command Line Interface			
S1#show spanning-tree summary				S2#show spanning-tree summary			
Switch is in rapid-pvst mode				Switch is in rapid-pvst mode			
Root bridge for: UNIT1 UNIT2 UNIT3				Root bridge for: default GUEST SERVERS Management			

Hình 7.13: Kết quả cấu hình Spanning-tree.

S1				S2			
Physical Config CLI Attributes				Physical Config CLI Attributes			
IOS Command Line Interface				IOS Command Line Interface			
S1#show vtp status				S2#show vtp status			
VTP Version capable : 1 to 2				VTP Version capable : 1 to 2			
VTP version running : 1				VTP version running : 1			
VTP Domain Name : HQ				VTP Domain Name : HQ			
VTP Pruning Mode : Disabled				VTP Pruning Mode : Disabled			
VTP Traps Generation : Disabled				VTP Traps Generation : Disabled			
Device ID : 000D.BD64.7ECC				Device ID : 000A.4116.1180			
Configuration last modified by 12.0.4.226 at 3-1-93 01:46:26				Configuration last modified by 12.0.4.226 at 3-1-93 01:46:26			
Local updater ID is 12.0.4.226 on interface V160							
Feature VLAN :				Feature VLAN :			
VTP Operating Mode : Server				VTP Operating Mode : Client			
Maximum VLANs supported locally : 255				Maximum VLANs supported locally : 255			
Number of existing VLANs : 11				Number of existing VLANs : 11			
Configuration Revision : 18				Configuration Revision : 18			

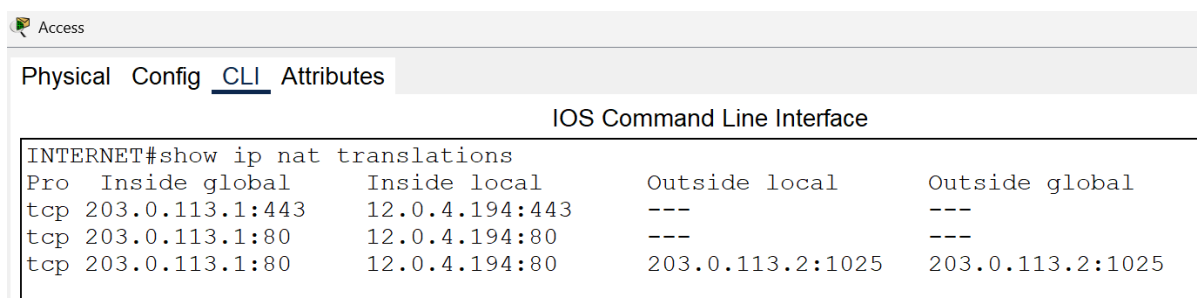
Hình 7.14: Kết quả cấu hình VTP Client-Server.

S1				S3				S2			
Physical Config CLI Attributes				Physical Config CLI Attributes				Physical Config CLI Attributes			
IOS Command Line Interface				IOS Command Line Interface				IOS Command Line Interface			
line vty 0 4				line vty 0 4				line vty 0 4			
access-class 101 in				access-class 101 in				access-class 101 in			
login local				login local				login local			
transport input ssh				transport input ssh				transport input ssh			
line vty 5 15				line vty 5 15				line vty 5 15			
access-class 101 in				access-class 101 in				access-class 101 in			
login local				login local				login local			
transport input ssh				transport input ssh				transport input ssh			
!				!				!			
!				!				!			

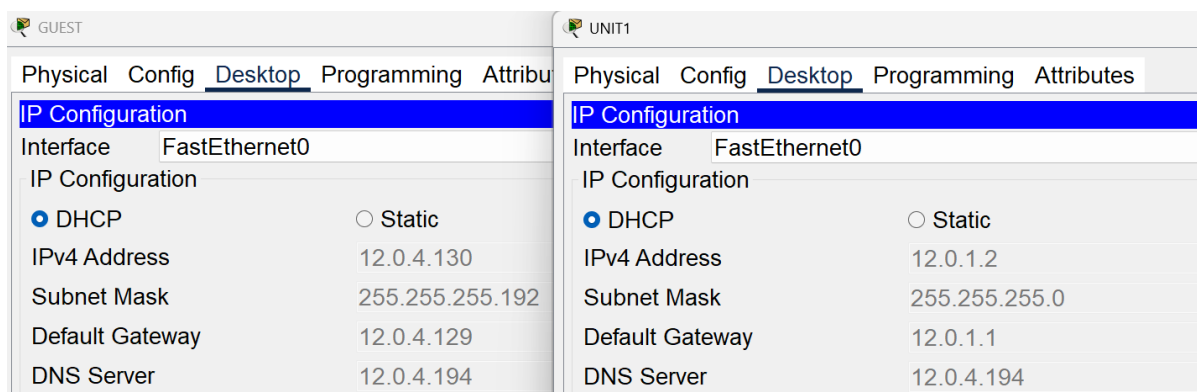
Hình 7.15: Kết quả cấu hình SSH.

## 7.5 Kết quả cấu hình NAT và DHCP

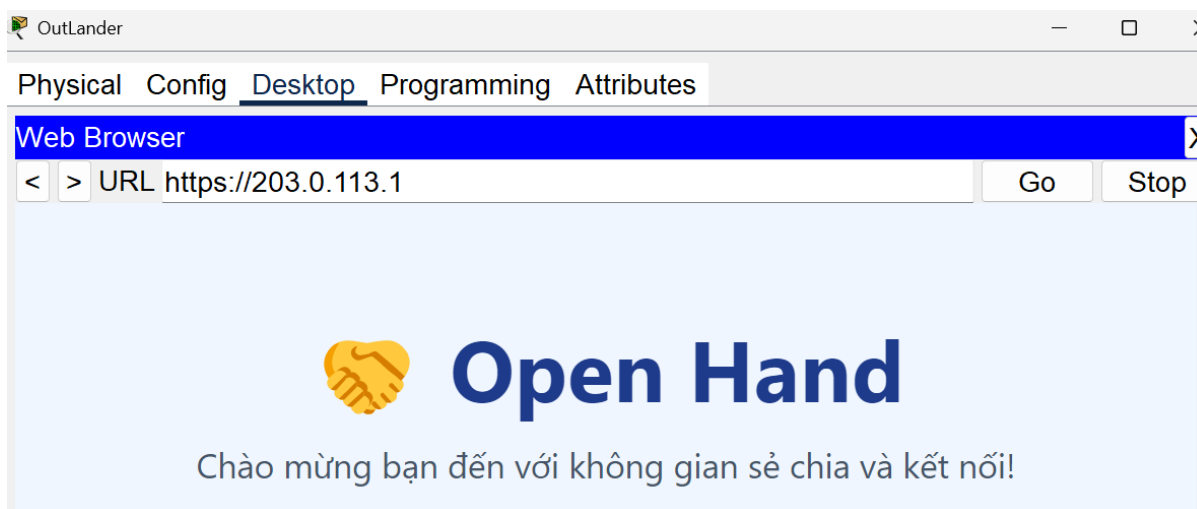
Cấu hình **NAT Overload** và **Port Forwarding** trên router **ACCESS** cho phép truy cập Internet từ các mạng nội bộ qua **203.0.113.1**, với server Web/DNS tại **12.0.4.194** hoạt động ổn định. **DHCP** trên **R4** đã cấp địa chỉ tự động cho các VLAN, với không có xung đột IP.



Hình 7.16: Kết quả cấu hình NAT.

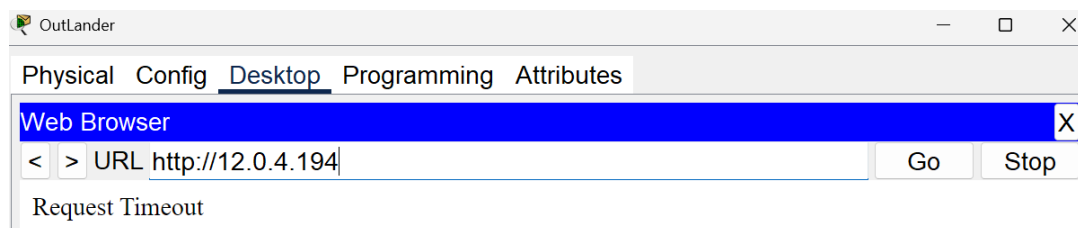


Hình 7.17: Kết quả cấu hình DHCPv4, host nhận IP động.



Hình 7.18: PC từ ngoài Internet truy cập web thành công.

Có thể thấy Outlander là PC ngoài Internet có thể truy cập web nội bộ bằng địa chỉ IP mặt ngoài của router ACCESS, nơi giao tiếp với Internet. Nhưng nếu Outlander dùng IP nội bộ của web server thì lại không thể ping được.



Hình 7.19: PC từ ngoài Internet truy cập web không thành công.

Lưu lượng ngoài được NAT thành IP mặt ngoài của router ACCESS.

```
C:>ping 12.0.4.194
Pinging 12.0.4.194 with 32 bytes of data:
Reply from 203.0.113.1: bytes=32 time=20ms TTL=125
Reply from 203.0.113.1: bytes=32 time=2ms TTL=125
Reply from 203.0.113.1: bytes=32 time=2ms TTL=125
Reply from 203.0.113.1: bytes=32 time=17ms TTL=125
Ping statistics for 12.0.4.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:>ping 12.0.1.1
Pinging 12.0.1.1 with 32 bytes of data:
Reply from 203.0.113.1: bytes=32 time=19ms TTL=253
Reply from 203.0.113.1: bytes=32 time=2ms TTL=253
Reply from 203.0.113.1: bytes=32 time=2ms TTL=253
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Ping statistics for 12.0.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 19ms, Average = 6ms

C:>ping 12.1.8.2
Pinging 12.1.8.2 with 32 bytes of data:
Reply from 203.0.113.1: bytes=32 time=29ms TTL=253
Reply from 203.0.113.1: bytes=32 time=20ms TTL=253
Reply from 203.0.113.1: bytes=32 time=47ms TTL=253
Reply from 203.0.113.1: bytes=32 time=41ms TTL=253
Ping statistics for 12.1.8.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

## 7.6 Kết quả cấu hình ACL

Cấu hình **ACL 101** trên **R4** cho **VLAN 40 (GUEST)** đã giới hạn truy cập hiệu quả. Lệnh **show ip access-lists** trên **R4** cho thấy các gói tin từ **12.0.4.128/26** chỉ được phép đến **12.0.4.194** trên cổng **53 (DNS)**, **80 (HTTP)**, **443 (HTTPS)**, và ra Internet qua **203.0.113.0/24**, trong khi truy cập đến các mạng nội bộ **12.0.0.0/8** và **128.1.0.0/16** bị từ chối. Trên các switch, **ACL 101** cho phép **VLAN 50 (12.0.4.192/28)** truy cập SSH, được xác nhận qua lệnh **show access-lists** trên **S1**.

Thực hiện lệnh ping từ máy PC GUEST thuộc VLAN 40 thì có thể ping ra Internet nhưng không ping đến mạng nội bộ được (mạng chi nhánh và trụ sở).

```
C:>ping 203.0.113.1
Pinging 203.0.113.1 with 32 bytes of data:
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Reply from 203.0.113.1: bytes=32 time=2ms TTL=253
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Ping statistics for 203.0.113.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:>ping 12.0.4.194
Pinging 12.0.4.194 with 32 bytes of data:
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
Ping statistics for 12.0.4.194:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:>ping 128.1.8.3
Pinging 128.1.8.3 with 32 bytes of data:
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
```

---

Thực hiện ping tương tự nhưng thành công trên PC UNIT1 thuộc VLAN 10.

```
C:>ping 203.0.113.1
Pinging 203.0.113.1 with 32 bytes of data:
Reply from 203.0.113.1: bytes=32 time=2ms TTL=253
Reply from 203.0.113.1: bytes=32 time=14ms TTL=253
Reply from 203.0.113.1: bytes=32 time=32ms TTL=253
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Ping statistics for 203.0.113.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 32ms, Average = 12ms
```

```
C:>ping 12.0.4.194
Pinging 12.0.4.194 with 32 bytes of data:
Reply from 12.0.4.194: bytes=32 time<1ms TTL=127
Reply from 12.0.4.194: bytes=32 time<1ms TTL=127
Reply from 12.0.4.194: bytes=32 time<1ms TTL=127
Reply from 12.0.4.194: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 12.0.4.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:>ping 128.1.8.3
Pinging 128.1.8.3 with 32 bytes of data:
Reply from 128.1.8.3: bytes=32 time<1ms TTL=253
Reply from 128.1.8.3: bytes=32 time<1ms TTL=253
Reply from 128.1.8.3: bytes=32 time<1ms TTL=253
Reply from 128.1.8.3: bytes=32 time=1ms TTL=253
Ping statistics for 128.1.8.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

---

Thực hiện ssh thành công trên VLAN 50 (từ Server ssh vào Switch).

---

```
C:>ssh -l admin 12.0.4.227
Password:
S2#exit
[Connection to 12.0.4.227 closed by foreign host] C:>ssh -l admin 12.0.4.228
Password:
S3#exit
[Connection to 12.0.4.228 closed by foreign host] C:>ssh -l admin 12.0.4.226
Password:
S1#exit
[Connection to 12.0.4.226 closed by foreign host] C:>ssh -l admin 12.0.4.229
Password:
S4#
```

Thực hiện ssh không thành công trên VLAN 10 (Từ PC UNIT1 ssh vào Switch thì bị từ chối).

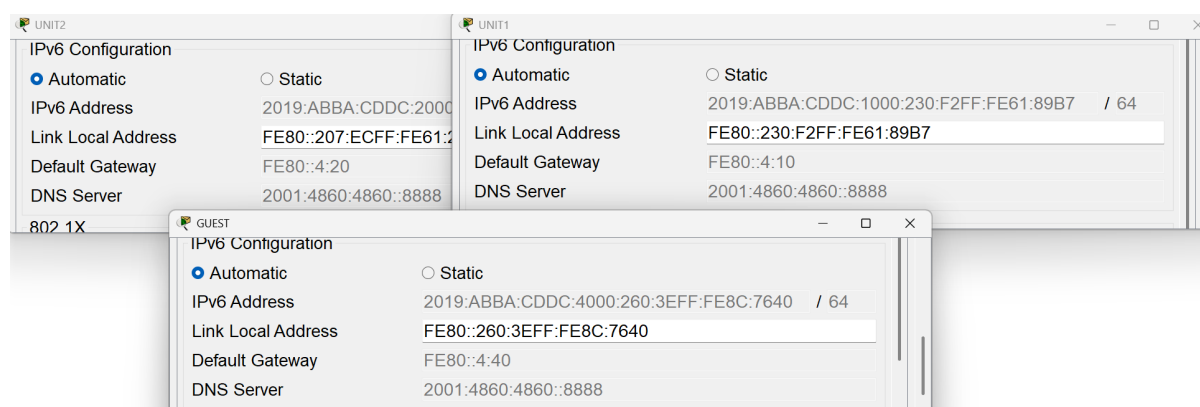
```
C:>ssh -l admin 12.0.4.226
% Connection refused by remote host
C:>ssh -l admin 12.0.4.227
% Connection refused by remote host
C:>ssh -l admin 12.0.4.228
% Connection refused by remote host
C:>ssh -l admin 12.0.4.229
% Connection refused by remote host
```

## 7.7 Kết quả cấu hình IPv6, định tuyến và DHCPv6

Cấu hình địa chỉ IPv6 với prefix như `2019:ABBA:CDDC:1000::/64` trên các router (`R4`, `R5`, `R6`, `R7`, `R8`, `ACCESS`) đã hoàn tất, với ping thành công giữa các mạng.

Cấu hình `EIGRPv6` với `router-id` như `4.4.4.4` trên `R4` và tuyến tính trên các router đã đảm bảo kết nối động và tính giữa các mạng. Bảng định tuyến IPv6 hiển thị đầy đủ các tuyến.

Cấu hình `DHCPv6` trên `R4` đã cấp địa chỉ tự động cho các VLAN (`10`, `20`, `30`, `40`) với DNS `2001:4860:4860::8888`, đảm bảo tất cả host nhận được cấu hình IPv6 chính xác.



Hình 7.20: Kết quả cấu hình DHCPv6, host nhận IP động.



R6								
IPv6-EIGRP neighbors for process 100								
H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	Link-local address: FE80::7:1	Se0/1/0	11	00:02:13	40	1000	0	21
R7								
0	Link-local address: FE80::6	Se0/1/1	13	00:01:58	40	1000	0	17
1	Link-local address: FE80::8	Se0/1/0	13	00:01:58	40	1000	0	17
2	Link-local address: FE80::5	Gig0/0/0	14	00:01:48	40	1000	0	10
R8								
0	Link-local address: FE80::7:2	Se0/1/0	13	00:01:47	40	1000	0	21
R5								
0	Link-local address: FE80::7	Gig0/0/1	14	00:03:20	40	1000	0	22

Hình 7.21: Thiết lập quan hệ láng giềng trong miền EIGRP

Thực hiện ping thông mạng từ máy PC UNIT2 ra toàn mạng và cả router ACCESS thành công.

```
C:>ping 2019:ABBA:AAAA:1::1
Pinging 2019:ABBA:AAAA:1::1 with 32 bytes of data:
Reply from 2019:ABBA:AAAA:1::1: bytes=32 time=1ms TTL=254
Reply from 2019:ABBA:AAAA:1::1: bytes=32 time<1ms TTL=254
Ping statistics for 2019:ABBA:AAAA:1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:>ping 2019:ABBA:BBBB:1::1
Pinging 2019:ABBA:BBBB:1::1 with 32 bytes of data:
Reply from 2019:ABBA:BBBB:1::1: bytes=32 time<1ms TTL=254
Ping statistics for 2019:ABBA:BBBB:1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:>ping 2019:ABBA:CCCC:1::1
Pinging 2019:ABBA:CCCC:1::1 with 32 bytes of data:
Reply from 2019:ABBA:CCCC:1::1: bytes=32 time<1ms TTL=254
Ping statistics for 2019:ABBA:CCCC:1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
C:>ping 2019:ABBA:DDDD:1::1
Pinging 2019:ABBA:DDDD:1::1 with 32 bytes of data:
Reply from 2019:ABBA:DDDD:1::1: bytes=32 time<1ms TTL=254
Ping statistics for 2019:ABBA:DDDD:1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

## Chương 8

# Kết quả đạt được mạng không dây

### 8.1 Kết quả mạng không dây khu vực HQ

- Kiểm tra các LAP đã có phát các WLANs (Wifi) hay chưa.
- Kết quả phải đảm bảo các LAP đều có 4 mạng Marketing, Business, IoT và GUEST.

Device Name: LAP-2  
Device Model: 3702i

Port	Link	IP Address	MAC Address
GigabitEthernet0	Up	12.0.4.233/28	000D.BD23.E501
Dot11Radio0	Up	<not set>	000D.BD23.E502

CAPWAP Status: Connected to 12.0.4.232

Providing WLANs:

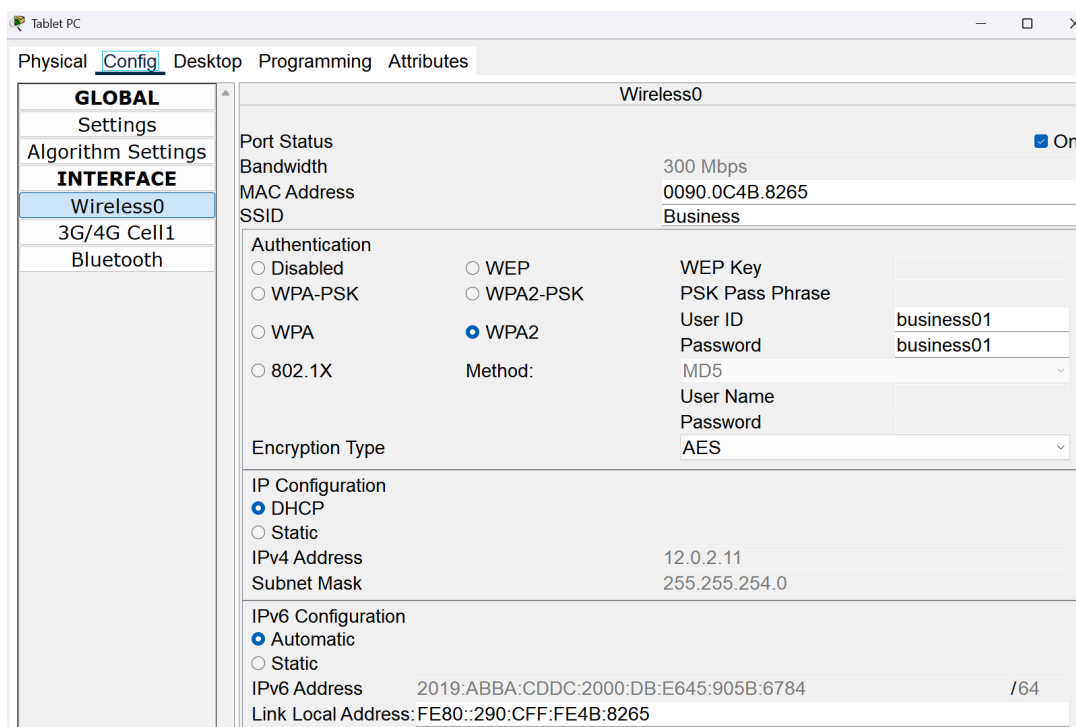
Marketing (Marketing)  
Business (Business)  
IoT (IoT)  
GUEST (GUEST)

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > LAP-2

Hình 8.1: Kiểm tra các LAP đều phát sóng Wifi.

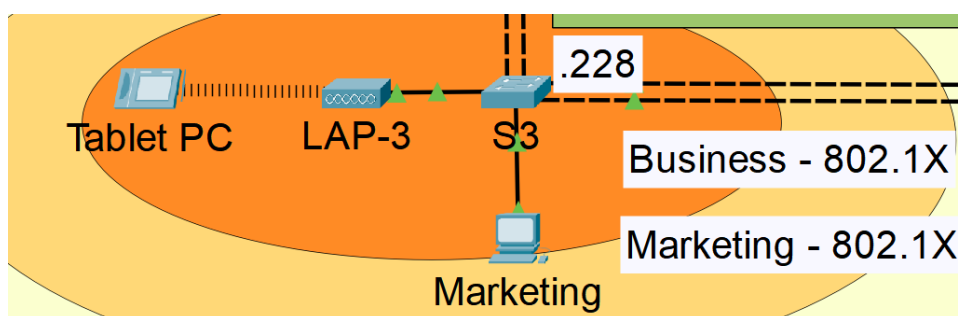
- Thiết lập card mạng trên thiết bị là laptop. Tắt nguồn máy, tháo card mạng mặc định ra. Chọn card mạng **PT-LAPTOP-NM-1W-AC**. Sau đó bật nguồn laptop lại.
- **Kết nối Wifi Business bằng Tablet PC**
  - + Truy cập thẻ **Config**. Chọn giao diện **Wireless0**.
  - + SSID: Nhập **Business**.
  - + Authentication: Chọn **WPA2**.
  - + Nhập user id và password là **business01**.

- + Phần Encryption Type: Chọn chuẩn **AES**.
- + Nhấn Enter hoặc chọn vào một vùng nào đó.
- + Kết nối thành công, IPv4 và IPv6 DHCP sẽ được cấp phát như hình bên dưới.



Hình 8.2: Kiểm tra kết nối wifi Business.

- + Sóng wifi kết nối sẽ xuất hiện kết nối với Tablet PC.

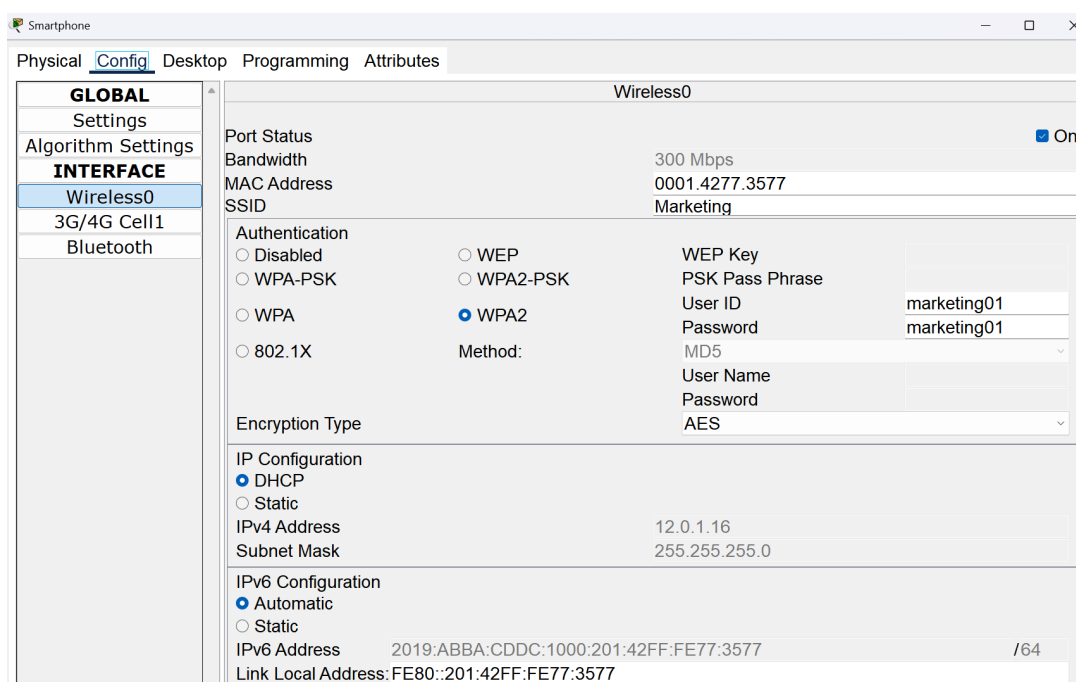


Hình 8.3: Kiểm tra kết nối wifi Business.

## – Kết nối Wifi Marketing bằng Smartphone

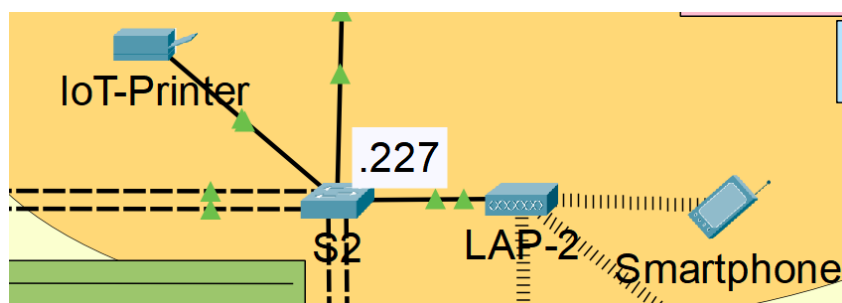
- + Truy cập thẻ **Config**. Chọn giao diện **Wireless0**.
- + SSID: Nhập **Marketing**.

- + Authentication: Chọn **WPA2**.
- + Nhập user id và password là **marketing01**.
- + Phần Encryption Type: Chọn chuẩn **AES**.
- + Nhấn Enter hoặc chọn vào một vùng nào đó.
- + Kết nối thành công, IPv4 và IPv6 DHCP sẽ được cấp phát như hình bên dưới.



Hình 8.4: Kiểm tra kết nối wifi Marketing.

- + Sóng wifi kết nối sẽ xuất hiện kết nối với Smartphone.

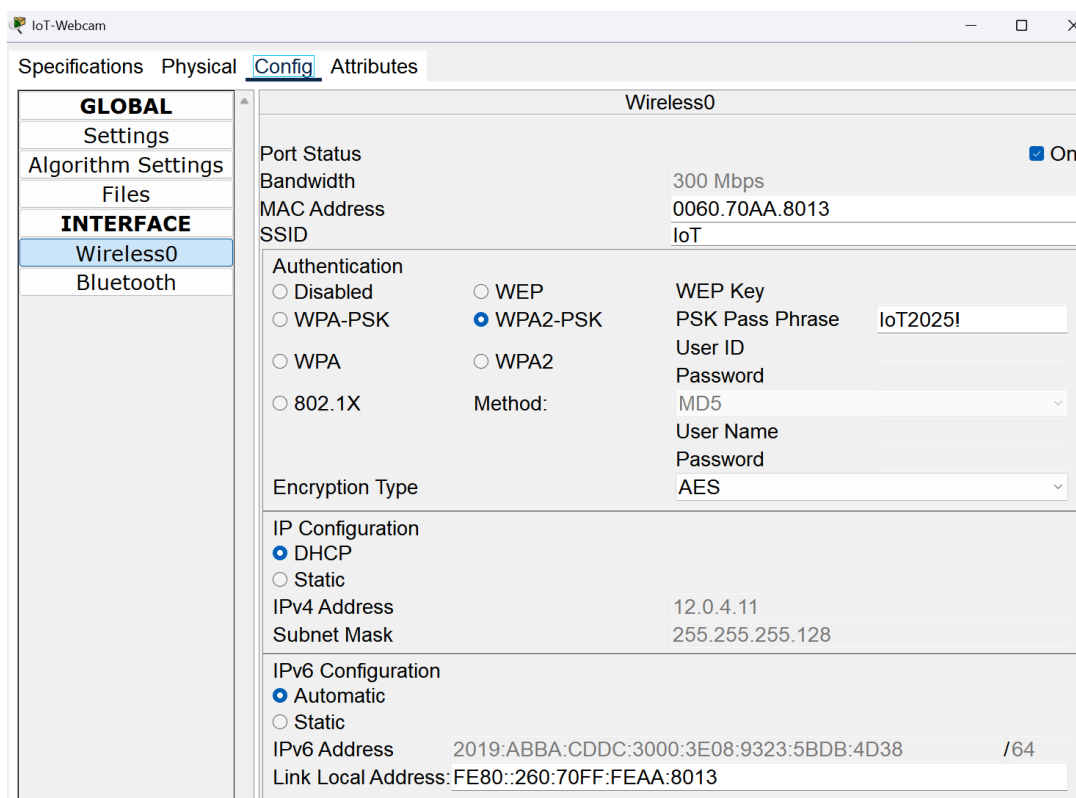


Hình 8.5: Kiểm tra kết nối wifi Marketing.

## – Kết nối Wifi IoT bằng WebCam

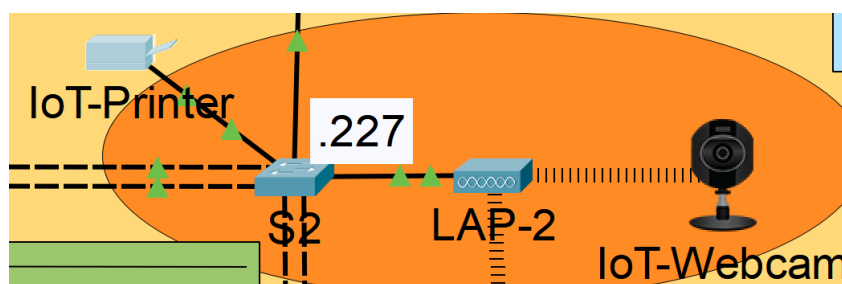
- + Truy cập thẻ **Config**. Chọn giao diện **Wireless0**.

- + SSID: Nhập IoT.
- + Authentication: Chọn WPA2-PSK.
- + Nhập PSK Pass Phrase là IoT2025!.
- + Phần Encryption Type: Chọn chuẩn AES.
- + Nhấn Enter hoặc chọn vào một vùng nào đó.
- + Kết nối thành công, IPv4 và IPv6 DHCP sẽ được cấp phát như hình bên dưới.



Hình 8.6: Kiểm tra kết nối wifi IoT.

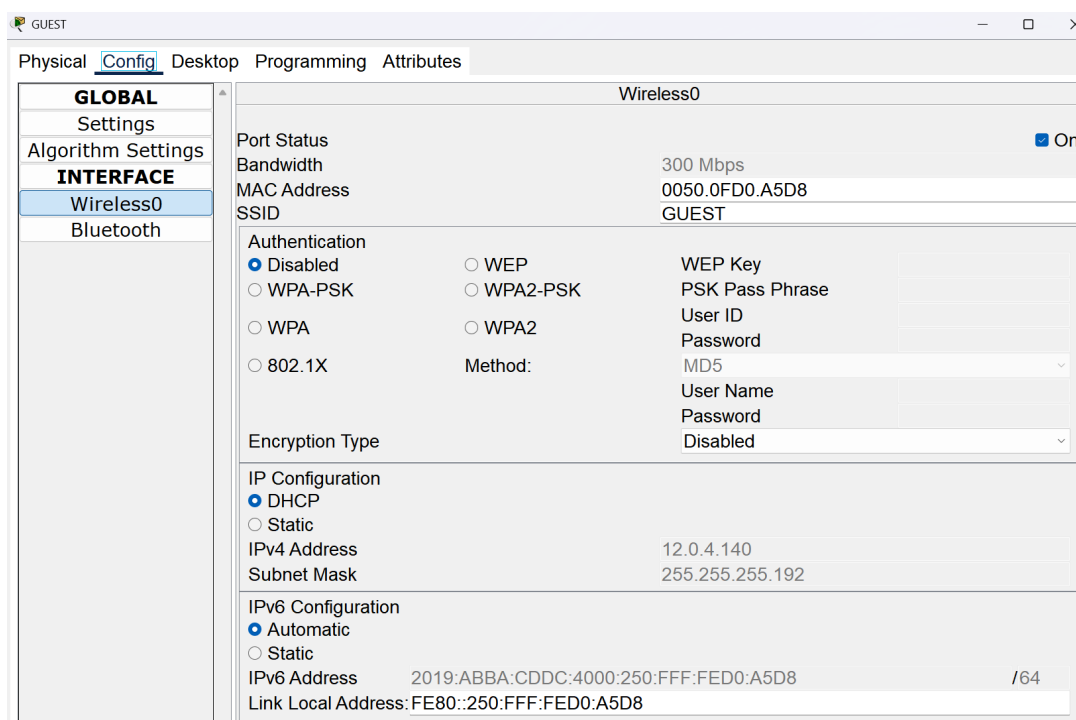
- + Sóng wifi kết nối sẽ xuất hiện kết nối với WebCam.



Hình 8.7: Kiểm tra kết nối wifi IoT.

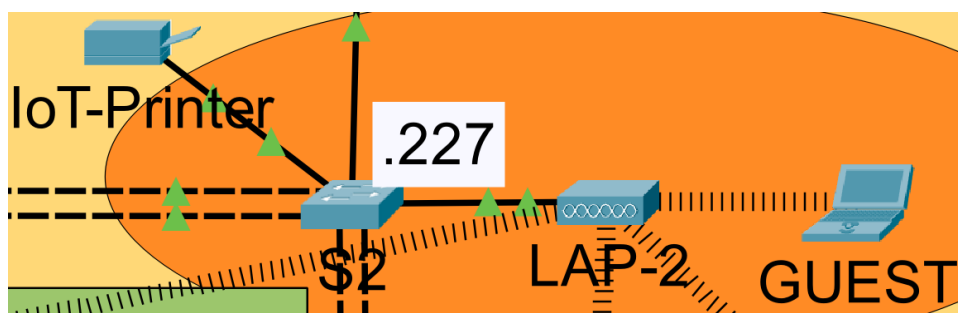
## – Kết nối Wifi GUEST bằng Laptop

- + Truy cập thẻ **Config**. Chọn giao diện **Wireless0**.
- + SSID: Nhập **GUEST**.
- + Authentication: Chọn **Disabled**.
- + Nhấn Enter hoặc chọn vào một vùng nào đó.
- + Kết nối thành công, IPv4 và IPv6 DHCP sẽ được cấp phát như hình bên dưới.



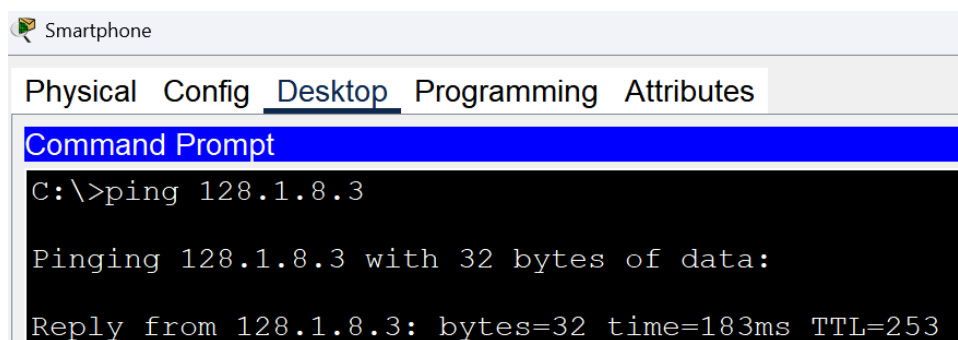
Hình 8.8: Kiểm tra kết nối wifi GUEST.

- + Sóng wifi kết nối sẽ xuất hiện kết nối với WebCam.

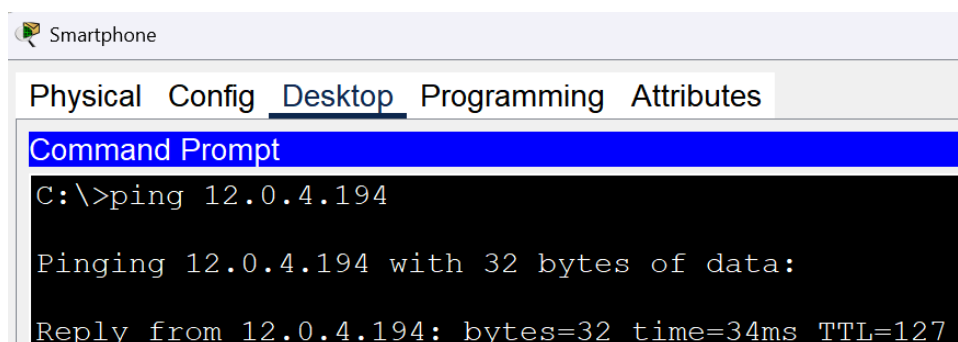


Hình 8.9: Kiểm tra kết nối wifi GUEST.

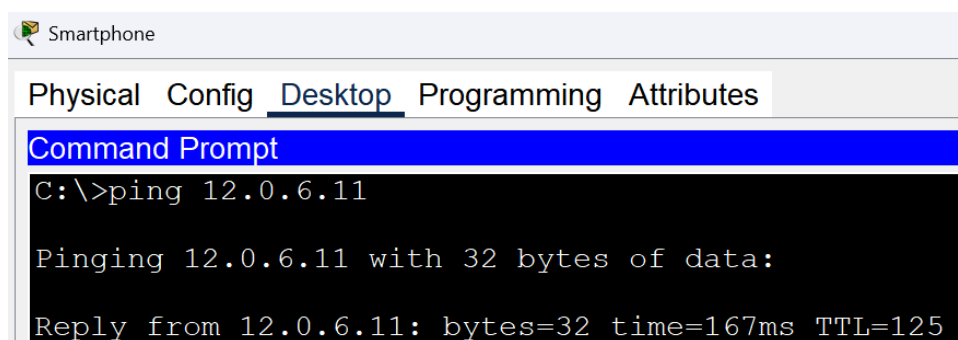
- **Kiểm tra thông mạng:** Chọn các mốc để kiểm tra lần lượt là:
  - + Khu vực Branch: 128.1.8.3 - IP R2.
  - + Khu vực HQ: 12.0.4.194 - IP Server.
  - + Khu vực REMOTE: 12.0.6.11 - IP Laptop LAN8.
  - + Internet: 203.0.113.1.
- + **Thông mạng Marketing:**



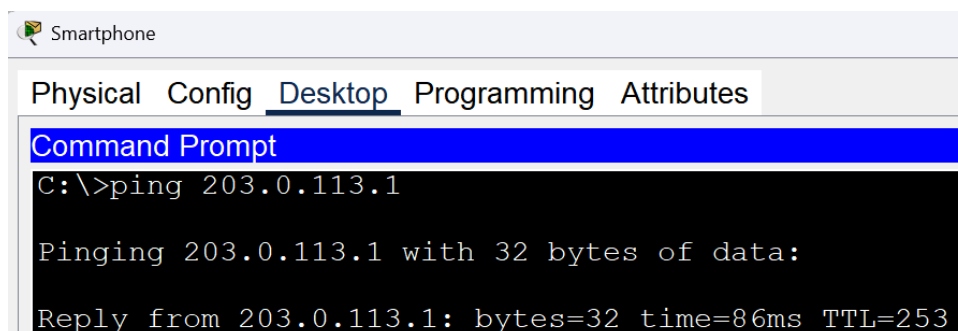
Hình 8.10: Marketing to Branch



Hình 8.11: Marketing to Server



Hình 8.12: Marketing to REMOTE

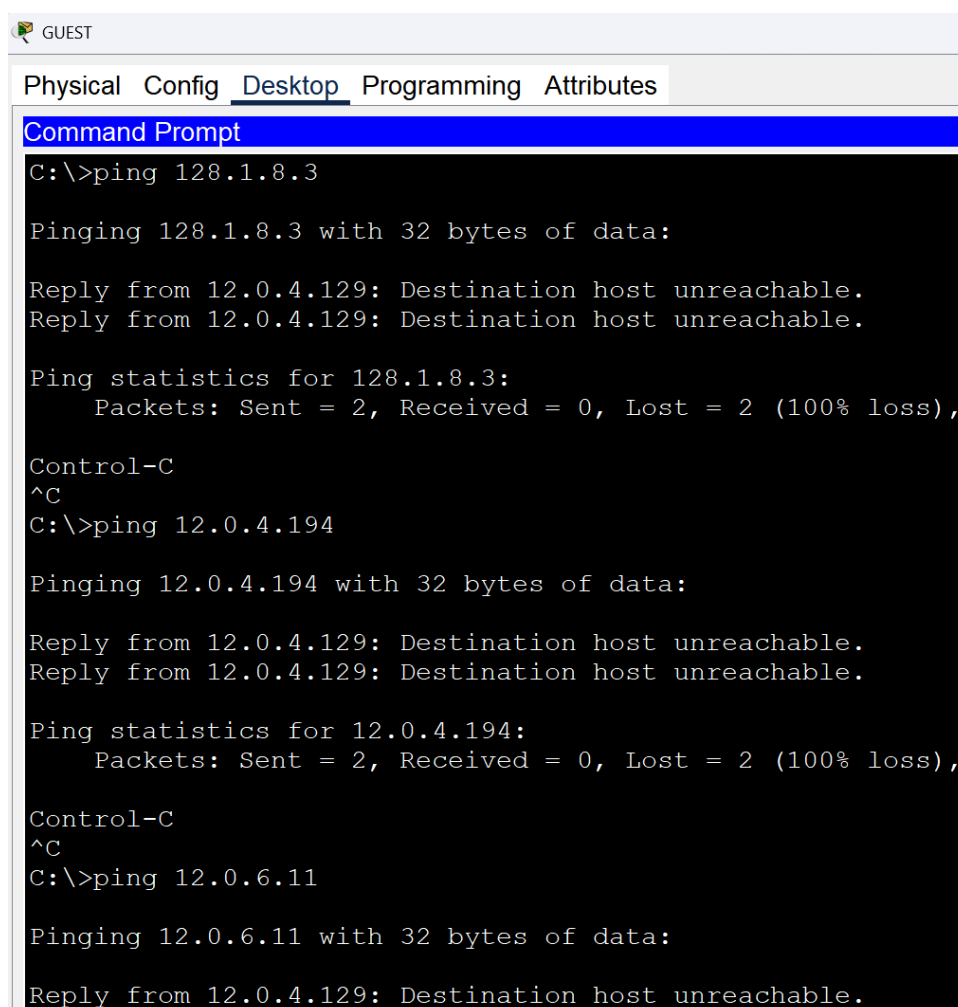


Hình 8.13: Marketing to Internet

+ Thông mạng Business cũng tương tự.

+ **Thông mạng IoT và GUEST:**

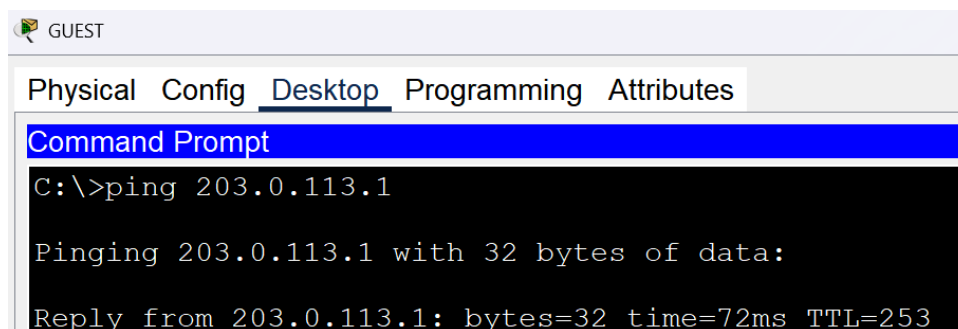
- IoT và GUEST đều bị chặn truy cập đến mạng nội bộ, chỉ thông mạng ra được Internet.



Hình 8.14: Marketing to Local Network

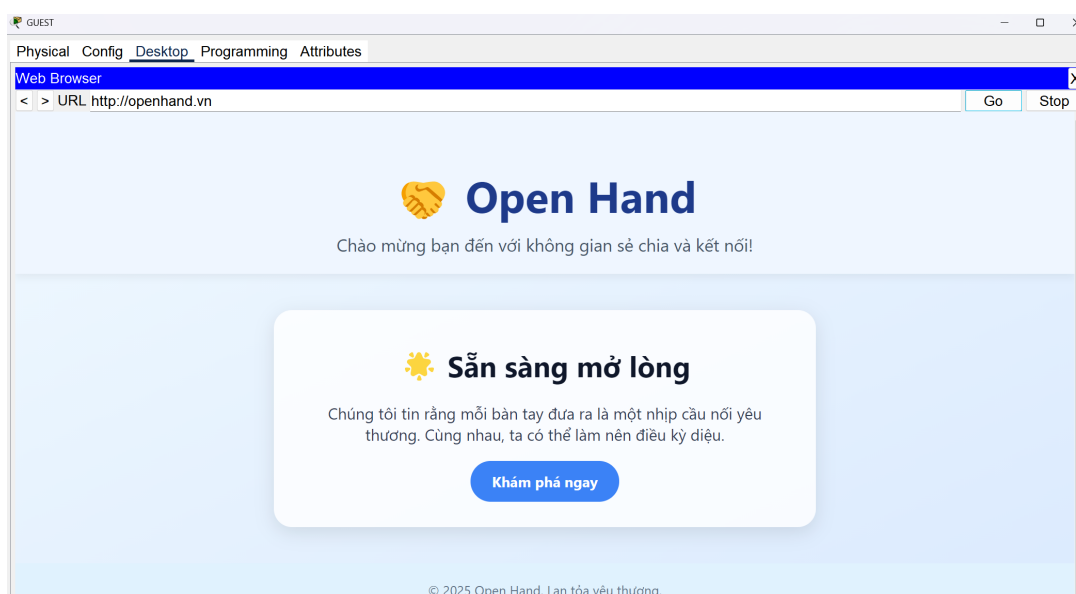


- GUEST và IoT có thể truy cập Internet.



Hình 8.15: Marketing to Internet

- Điều này tương tự như trên IoT nên sẽ không minh họa thêm. Có thể kiểm chứng trong mô hình.
- Điểm đặc biệt ở GUEST là vẫn có thể truy cập dịch vụ Web do ACL trên R4 vẫn cho phép dịch vụ http trên cổng 80 và https trên cổng 443, cho phép nhận DNS trên cổng 53, DHCP trên cổng 667, 68.



Hình 8.16: Guest truy cập Web bằng tên miền

## 8.2 Kết quả đạt được VPN

- Dùng lệnh `show crypto isakmp sa` để kiểm chứng source và destination.
- dùng lệnh `show crypto isakmp policy` để kiểm chứng mã hóa.

R6					
IPv4 Crypto ISAKMP SA					
dst	src	state	conn-id	slot	status
200.0.100.1	200.0.100.2	QM_IDLE	1022	0	ACTIVE
R7					
IPv4 Crypto ISAKMP SA					
dst	src	state	conn-id	slot	status
200.0.100.2	200.0.100.1	QM_IDLE	1043	0	ACTIVE
R8					
IPv4 Crypto ISAKMP SA					
dst	src	state	conn-id	slot	status
200.0.100.5	200.0.100.6	QM_IDLE	1076	0	ACTIVE

Hình 8.17: Kiểm tra cấu hình VPN

R6	
Global IKE policy	
Protection suite of priority 67	
encryption algorithm:	AES - Advanced Encryption Standard (256 bit keys).
hash algorithm:	Secure Hash Standard
authentication method:	Pre-Shared Key
Diffie-Hellman group:	#2 (1024 bit)
lifetime:	86400 seconds, no volume limit
R7	
Protection suite of priority 67	
encryption algorithm:	AES - Advanced Encryption Standard (256 bit keys).
hash algorithm:	Secure Hash Standard
authentication method:	Pre-Shared Key
Diffie-Hellman group:	#2 (1024 bit)
lifetime:	86400 seconds, no volume limit
Protection suite of priority 78	
encryption algorithm:	AES - Advanced Encryption Standard (256 bit keys).
hash algorithm:	Secure Hash Standard
authentication method:	Pre-Shared Key
Diffie-Hellman group:	#2 (1024 bit)
lifetime:	86400 seconds, no volume limit
R8	
Global IKE policy	
Protection suite of priority 78	
encryption algorithm:	AES - Advanced Encryption Standard (256 bit keys).
hash algorithm:	Secure Hash Standard
authentication method:	Pre-Shared Key
Diffie-Hellman group:	#2 (1024 bit)
lifetime:	86400 seconds, no volume limit

Hình 8.18: Kiểm tra cấu hình mã hóa IPsec VPN

Laptop-LAN6	Laptop-LAN8
Physical Config Desktop Programming Attributes	Physical Config Desktop Programming Attributes
Command Prompt	Command Prompt
Cisco Packet Tracer PC Command Line 1.0	
C:\>ping openhand.vn	C:\>ping
Pinging 12.0.4.194 with 32 bytes of data:	C:\>ping 203.0.113.1
Reply from 12.0.4.194: bytes=32 time=23ms	Pinging 203.0.113.1 with 32 bytes of data:
Reply from 12.0.4.194: bytes=32 time=10ms	Reply from 203.0.113.1: bytes=32 time=13ms TTL=252
Reply from 12.0.4.194: bytes=32 time=385ms	Reply from 203.0.113.1: bytes=32 time=816ms TTL=252

Hình 8.19: Kiểm tra thông mạng REMOTE

## KẾT LUẬN

Báo cáo đã trình bày chi tiết quá trình thiết kế và triển khai hệ thống mạng doanh nghiệp cho công ty Chooky, tích hợp đồng thời giao thức **IPv4** và **IPv6**, đáp ứng các yêu cầu về kết nối, định tuyến, chuyển mạch, cấp phát địa chỉ và bảo mật.

Hệ thống **IPv4** được cấu hình với các kết nối **PPP** (sử dụng **PAP** và **CHAP**), **GRE tunnel** giữa **R6** và **R8**, cùng định tuyến động **OSPF** tại chi nhánh và **EIGRP** tại trụ sở. Các tuyến tĩnh đảm bảo giao tiếp thông suốt qua **VLAN 60**. Các switch triển khai **VTP**, **Rapid PVST+** và **EtherChannel**, hỗ trợ **Inter-VLAN Routing** trên **R4**. Truy cập Internet được thực hiện qua **NAT Overload** và **Port Forwarding** tại router **ACCESS**, với **DHCP** trên **R4** cấp phát địa chỉ tự động cho các VLAN. Chính sách **ACL** kiểm soát hiệu quả truy cập từ **VLAN 40 (GUEST)** và quản lý **SSH** từ **VLAN 50 (SERVERS)** đến server Web/DNS tại **12.0.4.194**. Đối với **IPv6**, địa chỉ được gán với tiền tố **2019:ABBA:CDDC:1000::/64**, sử dụng **EIGRPv6** và tuyến tĩnh để kết nối Internet qua **ACCESS**. **DHCPv6** trên **R4** cấp phát địa chỉ và DNS (**2001:4860:4860::8888**) cho các VLAN, đảm bảo tương thích và hiệu quả.

Hệ thống mạng vận hành ổn định, cung cấp kết nối thông suốt giữa trụ sở, chi nhánh và khu vực từ xa, đồng thời bảo vệ dữ liệu nhạy cảm thông qua **WPA2/WPA3**, **802.1X**, **VPN** và **IDS/IPS**. Các biện pháp bảo mật như **RADIUS** và **ACL** đảm bảo kiểm soát truy cập chặt chẽ, với kết quả kiểm tra cho thấy ping thành công từ các VLAN nội bộ đến server và Internet, trong khi **VLAN 40 (GUEST)** bị giới hạn đúng yêu cầu. Tuy nhiên, hệ thống còn một số hạn chế: thiếu tích hợp **IPsec** cho **GRE tunnel** làm giảm độ an toàn của dữ liệu truyền qua Internet; việc triển khai **IPv6** chưa tối ưu cho các thiết bị IoT do hạn chế về hỗ trợ phần cứng; và chưa có cơ chế giám sát thời gian thực toàn diện để phát hiện các cuộc tấn công tinh vi.

**Đánh giá:** Hệ thống đáp ứng tốt các yêu cầu cơ bản của Chooky,

với độ trễ thấp (ping dưới 1ms trong nội bộ), khả năng phân vùng mạng hiệu quả qua **VLAN**, và bảo mật cơ bản được đảm bảo qua **ACL** và **RADIUS**. Kết quả kiểm tra WiFi cho thấy các WLAN (**Business**, **Marketing**, **IoT**, **GUEST**) hoạt động ổn định, hỗ trợ đồng thời 50–70 thiết bị. Tuy nhiên, hiệu suất mạng không dây có thể bị ảnh hưởng ở khu vực đông người dùng do số lượng **AP** giới hạn, và việc thiếu **NAT64** gây khó khăn trong giao tiếp giữa các thiết bị chỉ hỗ trợ **IPv4** và **IPv6**.

**Hướng phát triển:** Trong tương lai, cần tích hợp **IPsec** vào **GRE tunnel** để mã hóa dữ liệu, tăng cường bảo mật cho kết nối giữa các khu vực. Triển khai **NAT64** sẽ cải thiện tương thích **IPv4/IPv6**, đặc biệt cho các ứng dụng kế thừa. Nâng cấp **AP** hỗ trợ **WiFi 6E** và tăng số lượng **AP** sẽ cải thiện độ phủ sóng và hiệu suất mạng không dây ở khu vực đông người dùng. Ngoài ra, nên triển khai hệ thống giám sát thời gian thực với **SIEM** (Security Information and Event Management) để phát hiện và phản ứng nhanh với các mối đe dọa, cùng với việc áp dụng **AI** để tối ưu hóa định tuyến và quản lý lưu lượng. Các cải tiến này sẽ giúp hệ thống mạng trở thành nền tảng linh hoạt, an toàn và sẵn sàng cho các nhu cầu mở rộng của Chooky.

# Tài liệu tham khảo

- [1] Trường Đại học Tôn Đức Thắng, TS. Bùi Quy Anh. (2025). *An toàn mạng không dây và di động*.
- [2] Cisco Systems. (n.d.). *IPv6 Implementation Guide, Cisco IOS Release 15.2S*. Cisco Press. <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2s/ipv6-15-2s-book.html>
- [3] Forouzan, B. A. (2013). *Data Communications and Networking* (5th ed.). McGraw-Hill Education.
- [4] Droms, R. (2003). *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. IETF. <https://doi.org/10.17487/RFC3315>
- [5] Cisco Systems. (n.d.). *Configuring and Troubleshooting PPP Password Authentication Protocol (PAP)*. <https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/10313-config-pap.html>
- [6] Cisco Systems. (n.d.). *Configuring GRE Tunnels*. [https://www.cisco.com/c/en/us/td/docs/iosxr/ncs560/interfaces/710x/b-interfaces-hardware-component-cg-710x-ncs560/configuring\\_gre\\_tunnels.html](https://www.cisco.com/c/en/us/td/docs/iosxr/ncs560/interfaces/710x/b-interfaces-hardware-component-cg-710x-ncs560/configuring_gre_tunnels.html)
- [7] Cisco Systems. (n.d.). *Configure Network Address Translation*. <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html>
- [8] Cisco Systems. (n.d.). *Configuring the Cisco IOS DHCP Server*. [https://www.cisco.com/en/US/docs/ios/12\\_4t/ip\\_addr/](https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/)

- configuration/guide/htdhcpsv.html
- [9] Cisco Systems. (n.d.). *Configuring VLAN Trunks*. [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0\\_2\\_EX/vlan/configuration\\_guide/b\\_vlan\\_152ex\\_2960-x\\_cg/b\\_vlan\\_152ex\\_2960-x\\_cg\\_chapter\\_0100.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/vlan/configuration_guide/b_vlan_152ex_2960-x_cg/b_vlan_152ex_2960-x_cg_chapter_0100.pdf)
  - [10] Odom, W. (2020). *CCNA 200-301 Official Cert Guide, Volume 1* (1st ed.). Cisco Press.
  - [11] Moy, J. (1998). *OSPF Version 2*. IETF. <https://doi.org/10.17487/RFC2328>
  - [12] Lindem, A., Mirtorabi, S., Roy, A., Barnes, M., & Jethanandani, M. (2016). *OSPFv3 for IPv4-IPv6 Address Families*. IETF. <https://doi.org/10.17487/RFC7868>
  - [13] Zhang, J., & Lindem, A. (2016). *OSPFv3 Authentication Trailer for OSPFv3*. IETF. <https://doi.org/10.17487/RFC7869>
  - [14] Cisco Systems. (n.d.). *Configuring Rapid PVST+*. [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503\\_n1\\_1/Cisco\\_n5k\\_layer2\\_config\\_gd\\_rel\\_503\\_N1\\_1\\_chapter9.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html)
  - [15] Cisco Systems. (n.d.). *Configuring EtherChannels*. [https://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli\\_rel\\_4\\_1/Cisco\\_Nexus\\_5000\\_Series\\_Switch\\_CLI\\_Software\\_Configuration\\_Guide\\_chapter9.pdf](https://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_1/Cisco_Nexus_5000_Series_Switch_CLI_Software_Configuration_Guide_chapter9.pdf)
  - [16] Cisco Systems. (n.d.). *Configuring EIGRP*. [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_eigrp/configuration/15-mt/ire-15-mt-book/ire-eigrp.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-mt/ire-15-mt-book/ire-eigrp.html)
  - [17] IEEE. (2020). *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Con-*

- trol (MAC) and Physical Layer (PHY) Specifications.*  
<https://doi.org/10.1109/IEEESTD.2020.9264788>
- [18] Rigney, C., Willens, S., Rubens, A., & Simpson, W. (2000). *Remote Authentication Dial In User Service (RADIUS)*. IETF. <https://doi.org/10.17487/RFC2865>
- [19] Cisco Systems. (n.d.). *Configuring IPsec VPNs*. [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_vpnips/configuration/15-mt/sec-ipsec-vpn-15-mt-book/sec-cfg-vpn-ipsec.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-mt/sec-ipsec-vpn-15-mt-book/sec-cfg-vpn-ipsec.html)
- [20] Wi-Fi Alliance. (2020). *WPA3 Specification Version 2.0*. <https://www.wi-fi.org/file/wpa3-specification-v2-0>
- [21] Bagnulo, M., Sullivan, A., Matthews, P., & van Beijnum, I. (2011). *DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*. IETF. <https://doi.org/10.17487/RFC6147>
- [22] Lammle, T. (2021). *CCNA Cisco Certified Network Associate Study Guide* (8th ed.). Sybex.
- [23] OpenAI. (2025). *ChatGPT: AI Language Model for Technical Assistance*. <https://www.openai.com/chatgpt>
- [24] xAI. (2025). *Grok 3: AI Assistant for Network Design and Analysis*. <https://x.ai/grok>