TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CUỐI KỲ MÔN AN TOÀN**

**MẠNG KHÔNG DÂY VÀ DI ĐỘNG**

**XÂY DỰNG VÀ BẢO MẬT HỆ THỐNG MẠNG KHÔNG DÂY CHO CÔNG TY CỔ PHẦN BÁNH KẸO HẢI HÀ**

*Người hướng dẫn*: **T.S BÙI QUY ANH**

*Người thực hiện*: **TRẦN NGUYÊN LINH – 52000569**

Lớp **: 20050401**

Khoá  **: 24**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

LỜI CẢM ƠN

Lời đầu tiên em xin dành lời cảm ơn chân thành đến thầy Bùi Quy Anh - giáo viên giảng dạy môn An toàn mạng không dây và di động của em vì đã dành hết tâm huyết để dạy những bài học hay nhất cho em. Bên cạnh đó em cũng xin gửi lời cảm ơn sâu sắc đến các thầy cô trong khoa Công nghệ thông tin vì đã hết mình hỗ trợ và tạo điều kiện cho em hoàn thành bài báo cáo cuối kỳ này.

Lời cuối cùng em xin chúc tất cả quý thầy cô hiện đang công tác ở ngôi trường đại học Tôn Đức Thắng lời chúc sức khỏe và luôn thành công trong sự nghiệp giảng dạy của mình.

**BÁO CÁO ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của riêng tôi và được sự hướng dẫn của T.S Bùi Quý 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 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 tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày 10 tháng 12 năm 2022*

*Tác giả*

 *(ký tên và ghi rõ họ tên)*

*Trần Nguyên Linh*

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

TÓM TẮT

Xây dựng hệ thống mạng theo yêu cầu của công ty cổ phần bánh kẹo Hải Hà. Để giải quyết các yêu cầu mà công ty đưa ra nhóm đã có các giải pháp như sau: quy hoạch địa chỉ IP để dễ dàng mở rộng mạng nội bộ về sau; cấu hình HSRP; cấu hình Trunk; cấu hình VLAN, interface và port chanel, cấu hình dịch vụ DHCP, cấu hình các dịch vụ cơ bản như: DNS server, Mail server, FTP server, Web server; định tuyến động OSPF; cấu hình DHCP Replay, cấu hình DHCP Snooping, cấu hình WLAN, cấu hình console, cấu hình SSH, cấu hình ACLs.

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc29571)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc4598)

[TÓM TẮT iv](#_Toc4356)

[MỤC LỤC 1](#_Toc14683)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 3](#_Toc29126)

[CHƯƠNG 1 – PHÂN TÍCH YÊU CẦU KHÁCH HÀNG 5](#_Toc3682)

[1.1 Thu thập và phân tích yêu cầu của khách hàng 5](#_Toc6246)

[1.2 Đề xuất 5](#_Toc1669)

[1.3 Thiết bị và giá thành 6](#_Toc21655)

[CHƯƠNG 2 – CƠ SỞ LÝ THUYẾT 7](#_Toc10815)

[2.1 Mạng máy tính 7](#_Toc3613)

[2.2 Mạng wifi 8](#_Toc1715)

[2.3 Bảo mật wifi 9](#_Toc30798)

[2.4 DHCP 11](#_Toc31128)

[2.5 VLAN 12](#_Toc31450)

[2.6 STP 12](#_Toc4455)

[2.7 HSRP 13](#_Toc16819)

[2.8 SSH 13](#_Toc19492)

[2.9 Bảo mật cổng 13](#_Toc13638)

[2.10 DHCP Snooping 13](#_Toc4403)

[2.11 ACLs 13](#_Toc25955)

[CHƯƠNG 3 – THỰC NGHIỆM 15](#_Toc26395)

[3.1 Mô hình hệ thống mạng 15](#_Toc1162)

[3.1.1 Mô hình luận lý 15](#_Toc11305)

[3.1.2 Mô hình vật lý 15](#_Toc15990)

[3.2 Bảng địa chỉ, bảng Vlan, bảng Port 16](#_Toc4424)

[3.2.1 Bảng địa chỉ 16](#_Toc19477)

[3.2.2 Bảng VLan 17](#_Toc20626)

[3.2.3 Bảng Port 18](#_Toc30814)

[3.3 Cấu hình hạ tầng 19](#_Toc9568)

[3.3.1 Cấu hình Vlan, interface, port channel 19](#_Toc9369)

[3.3.2 Cấu hình các dịch vụ 22](#_Toc31203)

[3.3.3 Cấu hình OSPF 35](#_Toc4114)

[3.3.4 Cấu hình DHCP Replay 37](#_Toc7826)

[3.3.5 Cấu hình DHCP Snooping 38](#_Toc1623)

[3.3.6 Cấu hình HSRP 39](#_Toc16876)

[3.3.7 Cấu hình WLAN 41](#_Toc28781)

[3.3.8 Cấu hình Console 61](#_Toc21343)

[3.3.9 Cấu hình SSH, ACLs 62](#_Toc26781)

[CHƯƠNG 4 – KẾT LUẬN 65](#_Toc4691)

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

**DANH MỤC HÌNH**

[Hình 2. 1 Mạng máy tính 9](#_Toc3363)

[Hình 2. 2 Mạng wifi 10](#_Toc20954)

[Hình 2. 3 Bảo mật wifi 12](#_Toc3041)

[Hình 2. 4 DHCP 13](#_Toc14004)

[Hình 3. 1 Mô hình luận lý 16](#_Toc5942)

[Hình 3. 2 Mô hình vật lý 17](#_Toc20399)

[Hình 3. 3 Tạo pool Quản Lý 24](#_Toc3596)

[Hình 3. 4 Tạo pool Hành chính 24](#_Toc32713)

[Hình 3. 5 Tạo pool Kế toán 25](#_Toc27573)

[Hình 3. 6 Tạo pool Kinh doanh 26](#_Toc26487)

[Hình 3. 7 Tạo pool Giám đốc 26](#_Toc27859)

[Hình 3. 8 DNS Server 27](#_Toc3396)

[Hình 3. 9 Web Server 28](#_Toc2834)

[Hình 3. 10 Dịch vụ web 29](#_Toc25136)

[Hình 3. 11 FTP Server 30](#_Toc24944)

[Hình 3. 12 Mail Server 31](#_Toc13143)

[Hình 3. 13 Mail Server 32](#_Toc30302)

[Hình 3. 14 Tạo tài khoản mail trên PC6 33](#_Toc19458)

[Hình 3. 15 Tạo tài khoản mail trên PC7 34](#_Toc21534)

[Hình 3. 16 Tạo Mail và gửi Mail 35](#_Toc12575)

[Hình 3. 17 Nhận Mail thành công 36](#_Toc18640)

[Hình 3. 18 Kiểm tra DHCP Snooping 40](#_Toc2450)

[Hình 3. 19 Đăng nhập vào WLC 43](#_Toc13313)

[Hình 3. 20 VLAN10 44](#_Toc8704)

[Hình 3. 21 VLAN10 45](#_Toc13772)

[Hình 3. 22 VLAN20 46](#_Toc12291)

[Hình 3. 23 VLAN20 47](#_Toc29627)

[Hình 3. 24 VLAN30 48](#_Toc22505)

[Hình 3. 25 VLAN30 49](#_Toc2580)

[Hình 3. 26 VLAN40 50](#_Toc20834)

[Hình 3. 27 VLAN40 51](#_Toc13370)

[Hình 3. 28 WLAN10 52](#_Toc10969)

[Hình 3. 29 WLAN10 52](#_Toc19772)

[Hình 3. 30 WLAN20 53](#_Toc26690)

[Hình 3. 31 WLAN20 54](#_Toc4563)

[Hình 3. 32 WLAN30 54](#_Toc24994)

[Hình 3. 33 WLAN30 55](#_Toc5982)

[Hình 3. 34 WLAN40 55](#_Toc9891)

[Hình 3. 35 WLAN40 56](#_Toc18325)

[Hình 3. 36 Cấu hình bảo mật WLAN 56](#_Toc6125)

[Hình 3. 39 Kết nối wifi Laptop0 59](#_Toc7383)

[Hình 3. 40 Kết nối wifi Laptop0 60](#_Toc17790)

[Hình 3. 41 Kết nối wifi Smartphone0 61](#_Toc17299)

[Hình 3. 42 Kết nối wifi Tablet PC0 62](#_Toc26410)

[Hình 3. 43 Test Console trên BR-Router 63](#_Toc20756)

**DANH MỤC BẢNG**

[Bảng 1.1 Thiết bị và giá thành 9](#_Toc24865)

[Bảng 3. 1 Bảng địa chỉ phòng ban 19](#_Toc3458)

[Bảng 3. 2 Bảng địa chỉ thiết bị 20](#_Toc1740)

[Bảng 3. 3 Bảng VLAN 21](#_Toc14787)

[Bảng 3. 4 Bảng Port 22](#_Toc31311)

CHƯƠNG 1 – PHÂN TÍCH YÊU CẦU KHÁCH HÀNG

1.1 Thu thập và phân tích yêu cầu của khách hàng

**- Khảo sát thực tế:**

* **Trụ sở chính TP.Hồ Chí Minh:** - Địa chỉ: Lô số 27 Khu Công Nghiệp Tân Tạo, đường Tân Tạo, Phường Tân Tạo A, Quận Bình Tân, Thành phố Hồ Chí Minh, Việt Nam.
* **Chi nhánh Đà Nẵng:** - Địa chỉ: 134 Phan Thanh, Phường Thạc Gián, Quận Thanh Khê, Thành phố Đà Nẵng, Việt Nam.

**- Yêu cầu của khách hàng:**

* Quy hoạch địa chỉ IP cho mạng nội bộ đảm bảo tính dễ dàng mở rộng về sau.
* Mỗi phòng ban (mỗi tầng) phải được cấu hình VLAN tương ứng với phòng ban đó.
* Cấu hình bảo mật cơ bản cho các thiết bị mạng.
* Hệ thống phải đảm bảo tính dự phòng.
* Sử dụng giao thức định tuyến động OSPF.
* Cấu hình dịch vụ DHCP để cấp địa chỉ IP cho toàn bộ các thiết bị trong hệ thống mạng (bao gồm cả các thiết bị có dây và không dây).
* Mỗi tầng có một WLAN khác nhau với xác thực WPA-2 Enterprise.
* Cấu hình SSH để có thể truy cập cấu hình các thiết bị từ xa và không cho phép truy cập từ xa bằng SSH trừ các thiết bị ở phòng Hành chính.
* Cấu hình các dịch vụ cần thiết như: DNS Server, Mail Server, FTP server, Web Server.
* Đảm bảo các thiết bị trong mạng có thể nhìn thấy nhau và kết nối thành công đến các chi nhánh khác.

1.2 Đề xuất

**- Chi nhánh Hồ Chí Minh:**

* **Router Gateway:** sử dụng 2 Switch Layer 3 3650-24PS
* **SW-CORE:** 2 Router Cisco ISR4331
* **Tầng 1 (phòng Hành chính):** 1 Switch 2960, 1 Light Weight Access Point
* **Tầng 2 (phòng Kế toán):** 1 Switch 2960
* **Tầng 3 (phòng Kinh doanh):** 1 Switch 2960
* **Tầng 4 (phòng Giám đốc):** 1 Switch 2960
* **Tầng 5 (phòng Quản lý):** 1 Switch 2960, 1 thùng server

**- Chi nhánh Đà Nẵng:**

* **Router Gateway:** 1 Router Cisco ISR4331
* **Tầng 1:** 1 Switch 2960
* **Tầng 2:** 1 Switch 2960

1.3 Thiết bị và giá thành

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Tên thiết bị** | **SL** | **Giá thành(VNĐ)** | **Tổng chi phí** |
| **1** | Access Point Cisco 37021-C-K9 | 1 | 12.700.000 | 12.700.000 |
| **2** | WLC Cisco AIR-CT3504-K9 | 1 | 58.000.000 | 58.000.000 |
| **3** | Switch Cisco 2960 WS-C2960 | 7 | 8.300.000 | 58.100.000 |
| **4** | Switch Cisco 3650 WS-C3650-24TS-S | 2 | 41.500.000 | 83.000.000 |
| **5** | Router Cisco ISR 4331K9 | 4 | 25.000.000 | 100.000.000 |
| **6** | Wifi Cisco AIR-AP1852E-S-K9 | 1 | 12.000.000 | 12.000.000 |
| **7** | Server - Z240 Workstation | 1 | 25.000.000 | 25.000.000 |
| **8** | Máy bộ I3-10100/RAM 8GB/SSD 128GB | 300 | 10.050.000 | 3 tỷ 0 trăm 15 triệu |
| **Tổng cộng** |  |  |  | 3 tỷ 338 triệu 800 nghìn |

Bảng 1.1 Thiết bị và giá thành

CHƯƠNG 2 – CƠ SỞ LÝ THUYẾT

2.1 Mạng máy tính

- Mạng máy tính (Computer network hay network system) là một hệ thống gồm nhiều máy tính và các thiết bị được kết nối với nhau. Chúng được kết nối bởi các thiết bị nối kết mạng và phương tiện truyền thông (giao thức mạng, môi trường truyền dẫn) theo một cấu trúc nào đó.

- Mục đích của hệ thống mạng là thu thập, trao đổi dữ liệu và chia sẽ tài nguyên cho nhiều người sử dụng. Các máy tính được kết nối với nhau có thể trong cùng một phòng, một tòa nhà, một thành phố hoặc trên phạm vi toàn cầu.

- Trong các mạng máy tính, các thiết bị máy tính trao đổi dữ liệu với nhau bằng các kết nối (liên kết dữ liệu) giữa các nút. Các liên kết dữ liệu này được thiết lập qua cáp mạng như dây, cáp quang hoặc phương tiện không dây như Wifi.

- Mạng máy tính nổi tiếng nhất hiện nay là Internet.

- Các thành phần của mạng bao gồm:

* Thiết bị đầu cuối (máy tính, máy in,…) kết nối với nhau tạo thành mạng.
* Môi trường truyền dẫn (dây cáp, cáp quang, sóng điện từ, wifi,…).
* Các thiết bị kết nối mạng (hay gọi là thiết bị mạng: router, hub, switch,…) cùng môi trường truyền dẫn có nhiệm vụ kết nối các thiết bị đầu cuối trong phạm vi mạng.
* Giao thức truyền thông (protocol) là tập hợp các quy tắc quy định cách trao đổi thông tin giữa các thiết bị gửi và nhận dữ liệu trên mạng.



Hình 2. 1 Mạng máy tính

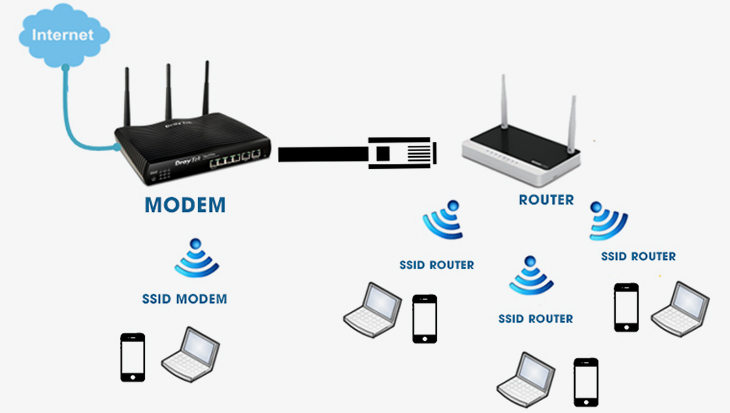
2.2 Mạng wifi

- Wifi là công nghệ mạng cho phép bạn kết nối không dây với [Internet](https://quantrimang.com/cong-nghe/internet-va-www-khac-nhau-nhu-the-nao-127708" \o "Internet là gì? Internet và WWW khác nhau như thế nào?). Nó còn được gọi là 802.11, là tiêu chuẩn IEEE của [mạng cục bộ không dây (WLAN)](https://quantrimang.com/cong-nghe/mang-wlan-hoat-dong-nhu-the-nao-172931" \o "Mạng WLAN hoạt động như thế nào?).

- Về bản chất kỹ thuật, tín hiệu WiFi hoạt động gửi và nhận dữ liệu ở tần số 2.5GHz đến 5GHz, cao hơn khá nhiều so với tần số của điện thoại di động, radio... do vậy tín hiệu Wifi có thể chứa nhiều dữ liệu nhưng lại bị hạn chế ở phạm vi truyền - khoảng cách.

- Sóng Wifi sử dụng chuẩn kết nối 802.11 trong thư viện IEEE (Institute of Electrical and Electronics Engineers), chuẩn này bao gồm 4 chuẩn nhỏ hơn là a/b/g/n.

* Chuẩn 802.11b là phiên bản đầu tiên trên thị trường. Đây là chuẩn chậm nhất và rẻ tiền nhất, và nó trở nên ít phổ biến hơn so với các chuẩn khác. 802.11b phát tín hiệu ở tần số 2.4 GHz, nó có thể xử lý đến 11 megabit/giây, và nó sử dụng mã CCK (complimentary code keying).
* Chuẩn 802.11g cũng phát ở tần số 2.4 GHz, nhưng nhanh hơn so với chuẩn 802.11b, tốc độ xử lý đạt 54 megabit/giây. Chuẩn 802.11g nhanh hơn vì nó sử dụng mã OFDM (orthogonal frequency-division multiplexing), một công nghệ mã hóa hiệu quả hơn.
* Chuẩn 802.11a phát ở tần số 5 GHz và có thể đạt đến 54 megabit/ giây. Nó cũng sử dụng mã OFDM. Những chuẩn mới hơn sau này như 802.11n còn nhanh hơn chuẩn 802.11a, nhưng 802.11n vẫn chưa phải là chuẩn cuối cùng.
* Chuẩn 802.11n cũng phát ở tần số 2.4 GHz, nhưng nhanh hơn so với chuẩn 802.11a, tốc độ truyền dữ liệu tối đa đạt 450 megabit/giây.
* Chuẩn 802.11ac phát ở tần số 5 GHz nhanh hơn so với chuẩn 802.11n, tốc độ truyền dữ liệu tối đa đạt đến 1.3 Gigabit/giây
* Chuẩn 802.11ad phát ở tần số 60 GHz nhanh hơn so với chuẩn 802.11ac, tốc độ truyền dữ liệu tối đa đạt đến 4,6 Gigabit/giây



Hình 2. 2 Mạng wifi

2.3 Bảo mật wifi

- Các loại bảo mật wifi phổ biến là WEP, WPA và WPA2.

* WEP (Wired Equivalent Privacy) là chuẩn bảo mật wifi lâu đời nhất, ra đời vào năm 1997. Đây được xem là phương thức bảo mật wifi kém an toàn nhất. Vào năm 2004, chuẩn bảo mật WEP đã bị loại bỏ.
* WPA (Wi-Fi Protected Access) là chuẩn bảo mật được phát triển để thay thế WEP do mã hóa WEP đã lỗi thời và dễ dàng bị phá vỡ.. WPA có nhiều cải tiến so với WEP như hỗ trợ TKIP (Temporal Key Integrity Protocol) để ngăn chặn việc đánh cắp các gói tin truyền trong wifi và MIC (Message Integrity Check) nhằm đảm bảo dữ liệu không bị giả mạo. Tuy vậy, WAP vẫn còn tồn đọng một vài lỗ hổng từ WEP.
* WPA2 là chuẩn bảo mật thay thế cho WPA kể từ năm 2006. WPA2 còn thay thế TKIP bằng giao thức CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol). Có hai loại hình: WPA2-Personal (bảo vệ truy cập mạng trái phép bằng cách sử dụng mật khẩu đã thiết lập) và WPA2-Enterprise xác minh người dùng mạng thông qua một server. WPA2 tương thích ngược với WPA.
* WPA3 là chuẩn bảo mật wifi mới nhất hiện nay và được áp dụng trên một số bộ định tuyến sản xuất trong năm 2019. WPA3 mang đến khả năng bảo mật trên các mạng wifi công cộng, ngăn chặn việc hacker có thể xem trộm hay đánh cắp thông tin khi bạn kết nối với wifi công cộng như ở sân bay, nhà hàng,…



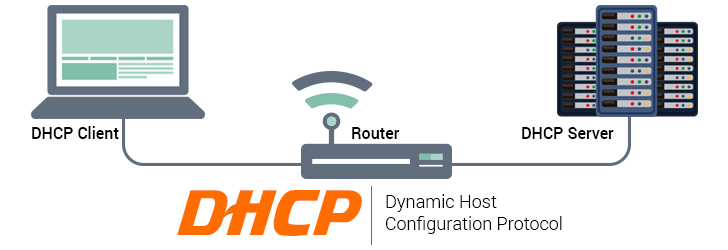
Hình 2. 3 Bảo mật wifi

2.4 DHCP

- DHCP (Dynamic Host Configuration Protocol) là Giao thức cấu hình máy chủ. DHCP có nhiệm vụ giúp quản lý nhanh, tự động và tập trung việc phân phối địa chỉ IP bên trong một mạng. Ngoài ra DHCP còn giúp đưa thông tin đến các thiết bị hợp lý hơn cũng như việc cấu hình subnet mask hay cổng mặc định.

- Cách thức hoạt động của DHCP:

* Khi một thiết bị muốn kết nối với mạng thì nó sẽ gửi một yêu cầu tới máy chủ, yêu cầu này gọi là DHCP DISCOVER. Sau khi yêu cầu này đến máy chủ DHCP thì ngay tại đó máy chủ sẽ tìm một địa chỉ IP có thể sử dụng trên thiết bị đó tồi cung cấp cho thiết bị địa chỉ cùng với gói DHCPOFFER.
* Khi nhận được IP thì thiết bị tiếp tục phản hồi lại máy chủ DHCP gói mang tên DHCPREQUEST. Lúc này là lúc chấp nhận yêu cầu thì máy chủ sẽ gửi tin báo nhận (ACK) để xác định thiết bị đó đã có IP, đồng thời xác định rõ thời gian sử dụng IP vừa cấp đến khi có địa chỉ IP mới.



Hình 2. 4 DHCP

2.5 VLAN

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

- Phân loại VLAN:

* Port - based VLAN: là cách cấu hình VLAN đơn giản và phổ biến. Mỗi cổng của Switch được gắn với một VLAN xác định (mặc định là VLAN 1), do vậy bất cứ thiết bị host nào gắn vào cổng đó đều thuộc một VLAN nào đó.
* MAC address based VLAN: Cách cấu hình này ít được sử dụng do có nhiều bất tiện trong việc quản lý. Mỗi địa chỉ MAC được đánh dấu với một VLAN xác định.
* Protocol – based VLAN: Cách cấu hình này gần giống như MAC Address based, nhưng sử dụng một địa chỉ logic hay địa chỉ IP thay thế cho địa chỉ MAC. Cách cấu hình không còn thông dụng nhờ sử dụng giao thức DHCP.

2.6 STP

- STP ([Spanning Tree Protocol](https://en.wikipedia.org/wiki/Spanning_Tree_Protocol)) là một giao thức dùng để ngăn chặn sự lặp vòng. Giao thức này cho phép các bridge truyền thông với nhau từ đó để phát hiện vòng lặp vật lý trong mạng. Sau đó STP sẽ tạo một cấu trúc cây của free-loop gồm các lá và các nhánh nối toàn bộ layer 2.

2.7 HSRP

- HSRP (Hot Standby Router Protocol) là một giao thức chuẩn của Cisco cung cấp tính sẵn sàng cho hệ thống mạng. HSRP hoạt động dựa trên việc tạo ra một gateway ảo. Gateway ảo đóng vai trò làm gateway cho các PC trong hệ thống mạng LAN.

2.8 SSH

- SSH (Secure Shell) đây là một giao thức hỗ trợ các nhà quản trị mạng truy cập vào máy chủ từ xa thông qua mạng internet không bảo mật. Ngoài ra, SSH còn cung cấp các bộ tiện ích phục vụ phát triển chính giao thức SSH.

- Chức năng:

* Hỗ trợ truy cập từ xa vào những hệ thống, thiết bị ứng dụng giao thức SSH.
* Cho phép dịch chuyển file an toàn.
* Thực thi lệnh bảo mật, an toàn trên hệ thống điều khiển từ xa.
* Quản lý an toàn và hiệu quả thành phần hạ tầng mạng.

2.9 Bảo mật cổng

- Là tính năng security layer 2 trên switch. Port security thường được triển khai trên các switch Cisco layer 2 để ngăn chặn người lạ xâm nhập vào thống mạng nội bộ. Port security dựa vào địa chỉ MAC của thiết bị để bảo vệ port.

- Một số nguyên tắc khi cấu hình port security:

* Không thể cấu hình port security trên các port trunk.
* Không thể cấu hình port security trên Destination port SPAN.
* Không thể cấu hình port security trên interface port-channel.

2.10 DHCP Snooping

- DHCP Snooping (chống giả mạo DHCP): là tính năng chỉ cho phép những DHCP Server được sự cho phép của Admin mới có quyền cấp DHCP cho các máy tính trong mạng.

2.11 ACLs

- ACL (Access Control List) là danh sách tuần tự các câu lệnh dùng để quản lý lưu lượng truy cập đến hoặc đi, xác định cách chuyển tiếp hoặc ngăn chặn một gói tin (packet) trên một thiết bị, được áp dụng trên một Interface nào đó, và trên bộ đệm vào hoặc ra, điều khiển Router thực hiện các hành động tương ứng là cho phép (allow) hoặc từ chối (deny). Khi bạn xác định ACL trên thiết bị định tuyến cho một interface cụ thể, tất cả lưu lượng chạy qua sẽ được câu lệnh ACL xem xét và quyết định sẽ ngăn chặn hay cho phép nó đi qua.

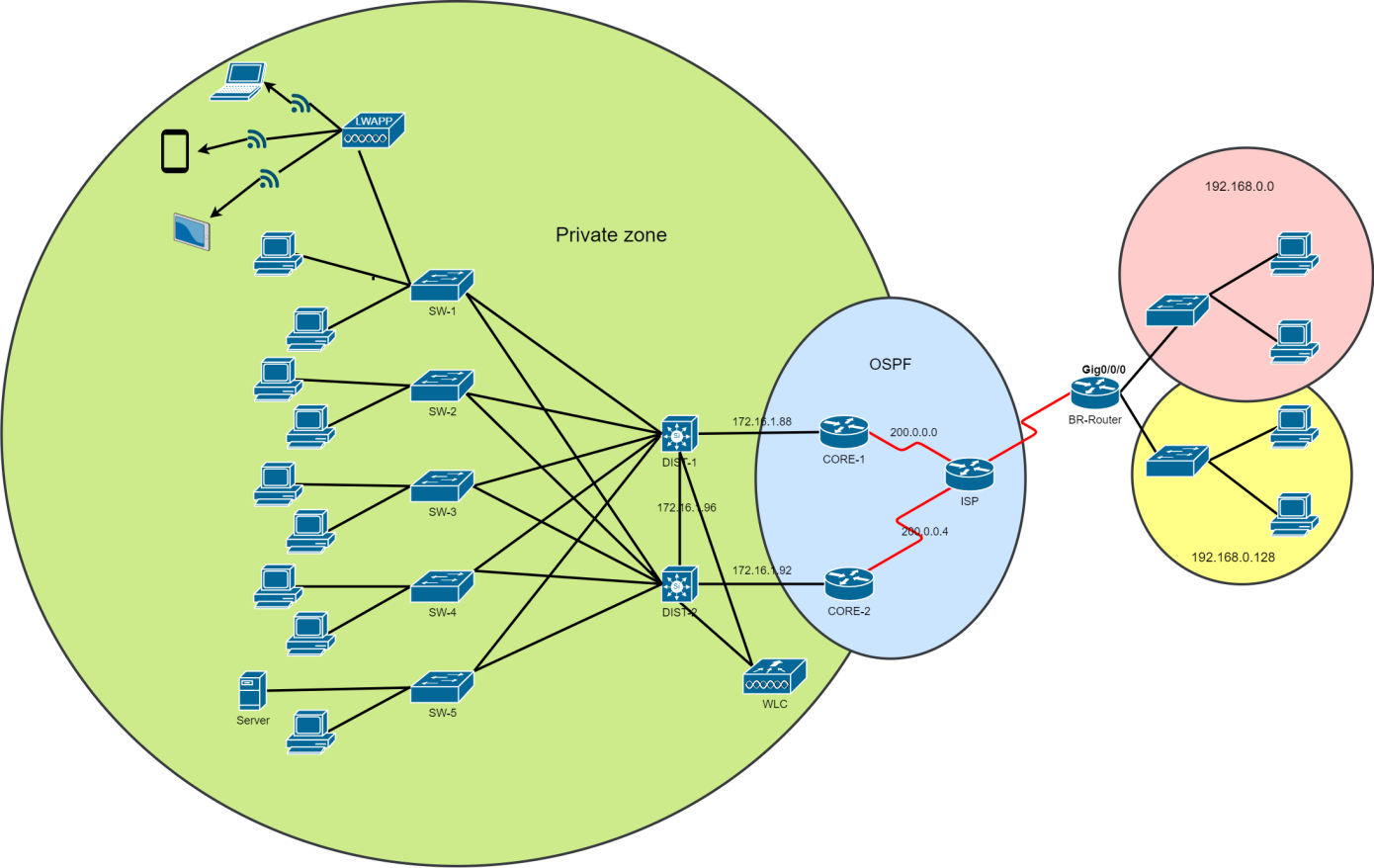
- Có hai loại hệ thống thực hiện ACL:

* Hệ thống tập tin ACL ━ là một cấu trúc dữ liệu (thường là một bảng) chứa các mục kiểm soát truy cập (ACE), có tác dụng chỉ định quyền của một người dùng riêng lẻ hoặc một nhóm đối với các đối tượng hệ thống cụ thể như các ứng dụng, tiến trình, hoặc các tập tin. Nhìn chung, hệ thống tập tin ACL cho hệ điều hành biết người dùng nào có thể truy cập vào hệ thống và những đặc quyền nào mà người dùng được phép.
* Networking ACL cho các thiết bị mạng ━ bộ lọc truy cập vào mạng. Các networking ACL nói cho các bộ định tuyến và thiết bị chuyển mạch (switch) biết loại lưu lượng nào có thể truy cập vào mạng và hoạt động nào được phép.

CHƯƠNG 3 – THỰC NGHIỆM

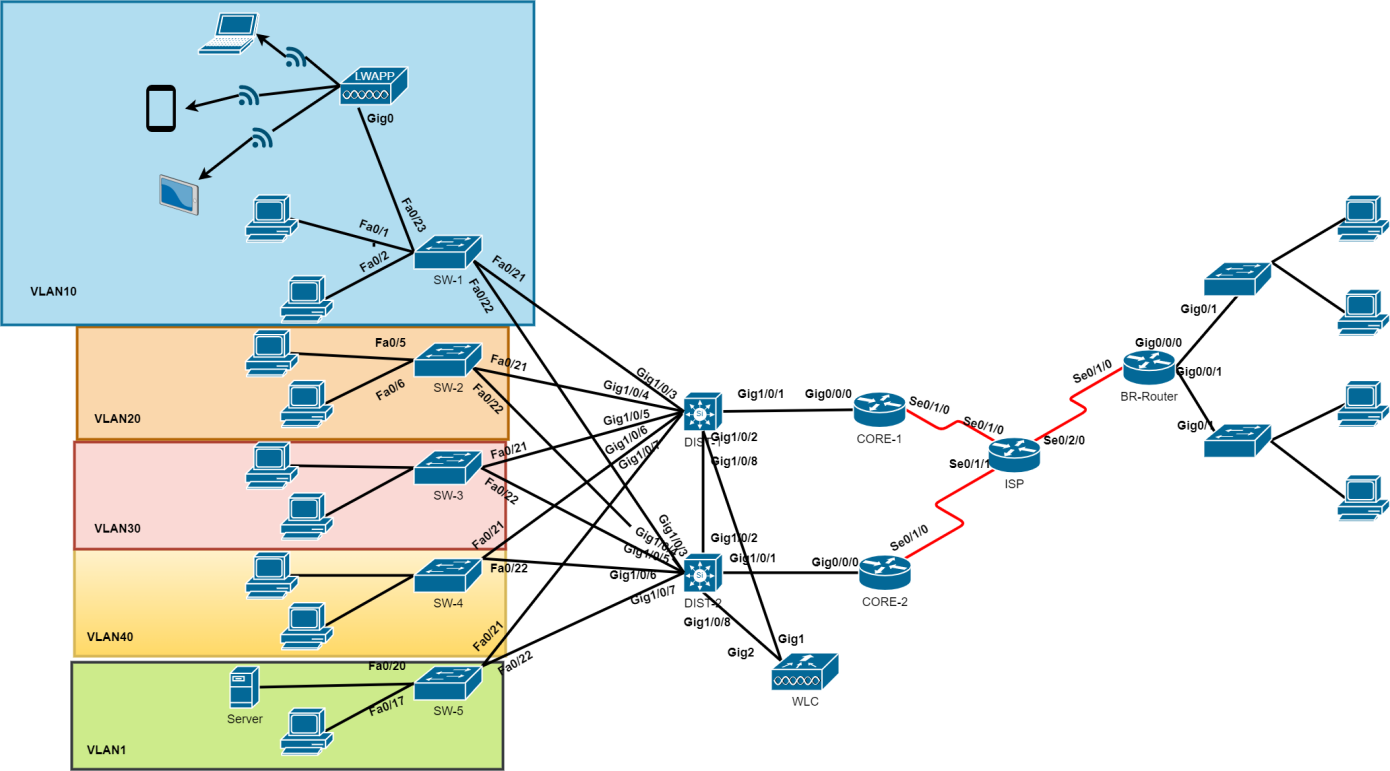
3.1 Mô hình hệ thống mạng

3.1.1 Mô hình luận lý



Hình 3. 1 Mô hình luận lý

3.1.2 Mô hình vật lý



Hình 3. 2 Mô hình vật lý

3.2 Bảng địa chỉ, bảng Vlan, bảng Port

3.2.1 Bảng địa chỉ

|  |  |  |
| --- | --- | --- |
| **Khu vực/đường mạng** | **Host** | **IPv4/IPv6** |
| Phòng Hành chính | 120 | 172.16.0.0/25 |
| Phòng Kế toán | 60 | 172.16.0.128/26 |
| Phòng Kinh doanh | 60 | 172.16.0.192/26 |
| Phòng Quản lý | 50 | 172.16.1.0/26 |
| Phòng Giám đốc | 10 | 172.16.1.64/28 |
| ISP to CORE-1 | 2 | 172.16.1.80/30 |
| ISP to CORE-2 | 2 | 172.16.1.84/30 |
| CORE-1 to Distribution-1 | 2 | 172.16.1.88/30 |
| CORE-2 to Distribution-2 | 2 | 172.16.1.92/30 |
| Distribution-1 to Distribution-2 | 2 | 172.16.1.96/30 |

Bảng 3. 1 Bảng địa chỉ phòng ban

|  |  |  |  |
| --- | --- | --- | --- |
| **Khu vực/ Thiết bị** | **Interface** | **IPv4 Address** | **Gateway** |
| Server | Fa0 | 172.16.1.4 | 172.16.1.1 |
| ISP | G0/0/0 | 172.16.1.81 |  |
| G0/0/1 | 172.16.1.85 |  |
| CORE-1 | G0/0/0 | 172.16.1.89 |  |
| G0/0/1 | 172.16.1.82 |  |
| CORE-2 | G0/0/0 | 172.16.1.93 |  |
| G0/0/1 | 172.16.1.86 |  |
| Distribution-1 | G1/0/1 | 172.16.1.90 |  |
| G1/0/2 | 172.16.1.97 |  |
| Distribution-2 | G1/0/1 | 172.16.1.94 |  |
| G1/0/2 | 172.16.1.98 |  |
| Phòng Hành chính | Fa0 | DHCP | DHCP |
| Phòng Kế toán | Fa0 | DHCP | DHCP |
| Phòng Kinh doanh | Fa0 | DHCP | DHCP |
| Phòng Quản lý | Fa0 | DHCP | DHCP |
| Phòng Giám đốc | Fa0 | DHCP | DHCP |

Bảng 3. 2 Bảng địa chỉ thiết bị

3.2.2 Bảng VLan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Tên VLAN** | **ID VLAN** | **Subnet** | **Default Gateway** |
| 1 | Hành chính | 10 | /25 | 172.16.0.3 |
| 2 | Kế toán | 20 | /26 | 172.16.0.131 |
| 3 | Kinh doanh | 30 | /26 | 172.16.0.195 |
| 4 | Quản lý | 1 | /26 | 172.16.1.3 |
| 5 | Giám đốc | 40 | /28 | 172.16.1.67 |

Bảng 3. 3 Bảng VLAN

3.2.3 Bảng Port

|  |  |  |  |
| --- | --- | --- | --- |
| **Thiết bị** | **Port** | **Thiết bị kết nối** | **Trunking/ VLAN** |
| Phòng hành chính - Tầng 1 | Fa0 | SW-1 | VLAN 10 |
| Phòng kế toán - Tầng 2 | Fa0 | SW-2 | VLAN 20 |
| Phòng kinh doanh - Tầng 3 | Fa0 | SW-3 | VLAN 30 |
| Phòng giám đốc - Tầng 4 | Fa0 | SW-4 | VLAN40 |
| Phòng quản lý - Tầng 5 | Fa0 | SW-5 | VLAN1 |
| DNS Server | Fa0/1 | SW-5 | VLAN 1 |
| Mail Server | Fa0/1 | SW-5 | VLAN 1 |
| FTP Server | Fa0/1 | SW-5 | VLAN 1 |
| Web Server | Fa0/1 | SW-5 | VLAN 1 |
| SW-1 | Fa0/17 | PC0 | VLAN 1 |
| Fa0/21 | Distribution-1 | Trunking |
| Fa0/22 | Distribution-2 |
| SW-2 | Fa0/12 | PC1 | VLAN 30 |
| Fa0/21 | Distribution-1 | Trunking |
| Fa0/22 | Distribution-2 |
| SW-3 | Fa0/21 | Distribution-1 | Trunking |
| Fa0/22 | Distribution-2 |
| SW-4 | Fa0/21 | Distribution-1 | Trunking |
| Fa0/22 | Distribution-2 |
| SW-5 | Fa0/21 | Distribution-1 | Trunking |
| Fa0/22 | Distribution-2 |
| Distribution-1 | G1/0/3 | SW-1 | Trunking |
| G1/0/4 | SW-2 |
| G1/0/5 | SW-3 |
| G1/0/6 | SW-4 |
| G1/0/7 | SW-7 |
| Distribution-2 | G1/0/3 | SW-1 | Trunking |
| G1/0/4 | SW-2 |
| G1/0/5 | SW-3 |
| G1/0/6 | SW-4 |
| G1/0/7 | SW-7 |
| CORE-1 | G0/0/0 | Distribution-1 | Trunking |
| G0/0/1 | ISP |
| CORE-2 | G0/0/0 | Distribution-2 | Trunking |
| G0/0/1 | ISP |
| ISP | G0/0/0 | CORE-1 | Trunking |
| G0/0/1 | CORE-2 |

Bảng 3. 4 Bảng Port

3.3 Cấu hình hạ tầng

3.3.1 Cấu hình Vlan, interface, port channel

**- Cấu hình Vlan:**

* **Distribution-1, Distribution-2:**

Switch(config)#vlan 10

Switch(config-vlan)#name HANH\_CHINH

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name KE\_TOAN

Switch(config-vlan)#vlan 30

Switch(config-vlan)#name KINH\_DOANH

Switch(config-vlan)#vlan 40

Switch(config-vlan)#name GIAM\_DOC

**- Gán địa chỉ cho port vlan:**

* **Distribution-1**

Switch(config)#int vlan 10

Switch(config-if)#ip add 172.16.0.1 255.255.255.128

Switch(config-if)#no sh

Switch(config-if)#int vlan 20

Switch(config-if)#ip add 172.16.0.129 255.255.255.192

Switch(config-if)#no sh

Switch(config-if)#int vlan 30

Switch(config-if)#ip add 172.16.0.193 255.255.255.192

Switch(config-if)#no sh

Switch(config-if)#int vlan 1

Switch(config-if)#ip add 172.16.1.1 255.255.255.192

Switch(config-if)#no sh

Switch(config-if)#int vlan 40

Switch(config-if)#ip add 172.16.1.65 255.255.255.240

Switch(config-if)#no sh

* **Distribution-2**

Switch(config)#int vlan 10

Switch(config-if)#ip add 172.16.0.2 255.255.255.128

Switch(config-if)#no sh

Switch(config-if)#int vlan 20

Switch(config-if)#ip add 172.16.0.130 255.255.255.192

Switch(config-if)#no sh

Switch(config-if)#int vlan 30

Switch(config-if)#ip add 172.16.0.194 255.255.255.192

Switch(config-if)#no sh

Switch(config-if)#int vlan 1

Switch(config-if)#ip add 172.16.1.2 255.255.255.192

Switch(config-if)#no sh

Switch(config-if)#int vlan 40

Switch(config-if)#ip add 172.16.1.66 255.255.255.240

Switch(config-if)#no sh

**- Cấu hình Port access vlan:**

* **SW-1, SW-2, SW-3, SW-4, SW-5:**

Switch (config)#interface range f0/1-4

Switch (config-if)#switchport access vlan 10

Switch (config)#interface range f0/5-8

Switch (config-if)#switchport access vlan 20

Switch (config)#interface range f0/9-12

Switch (config-if)#switchport access vlan 30

Switch (config)#interface range f0/13-16

Switch (config-if)#switchport access vlan 40

* **Distribution-1, Distribution-2:**

Switch#config t

Switch(config)#int r f0/1-4

Switch(config-if)#sw mo ac

Switch(config-if)#sw ac vlan 10

Switch(config-if)#int r f0/5-8

Switch(config-if)#sw mo ac

Switch(config-if)#sw ac vlan 20

Switch(config-if)#int r f0/9-12

Switch(config-if)#sw mo ac

Switch(config-if)#sw ac vlan 30

Switch(config-if)#int r f0/13-16

Switch(config-if)#sw mo ac

Switch(config-if)#sw ac vlan 40

Switch(config-if)#end

**- Cấu hình Port Trunk:**

* **Distribution-1, Distribution-2:**

Switch (config)#interface range f0/3-7

Switch (config-if)#switchport trunk encapsulation dot1q

Switch (config-if)#switchport mode trunk

* **SW-1, SW-2, SW-3, SW-4, SW-5:**

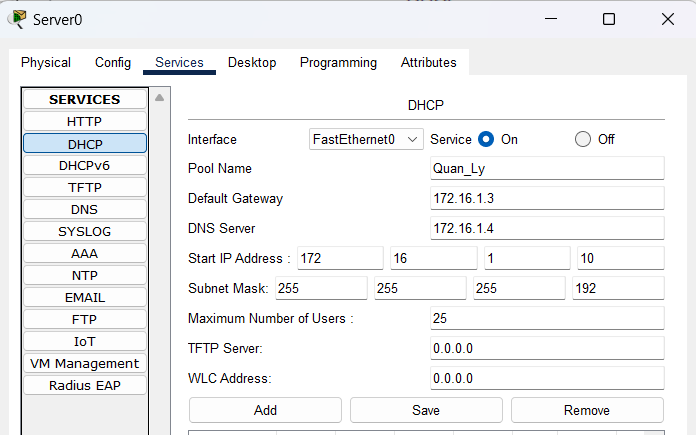
Switch (config)#interface range f0/21-22

Switch (config-if)#switchport mode trunk

3.3.2 Cấu hình các dịch vụ

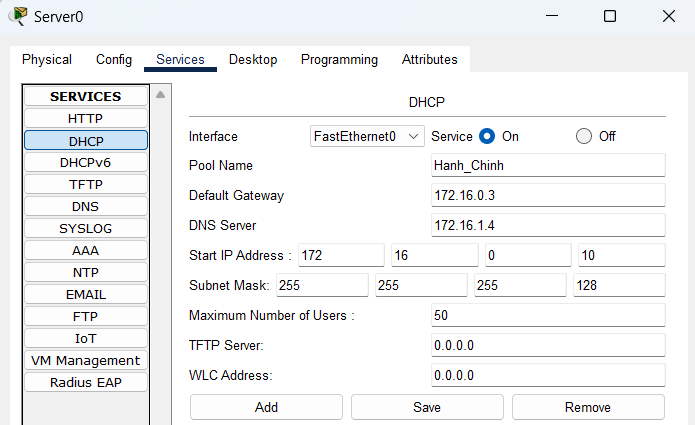
**- DHCP Server: tạo pool**

* **Phòng Quản lý:**



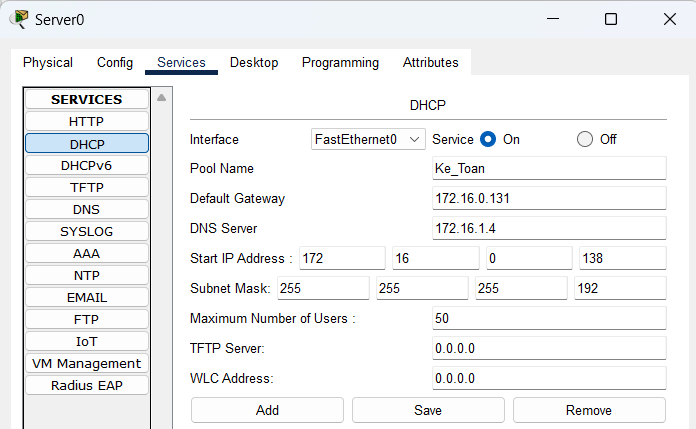
Hình 3. 3 Tạo pool Quản Lý

* **Phòng Hành chính:**



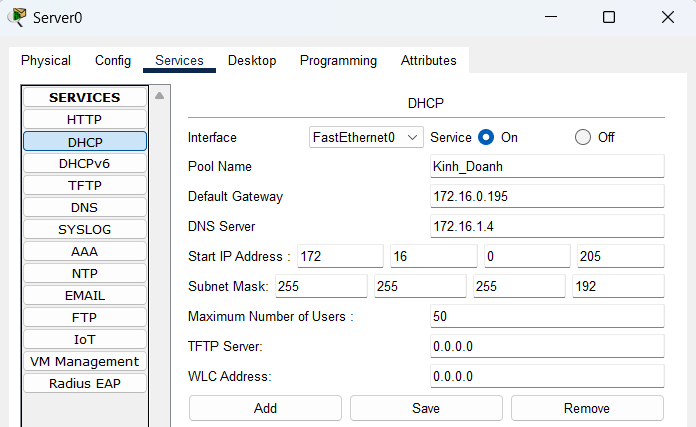
Hình 3. 4 Tạo pool Hành chính

* **Phòng Kế toán:**



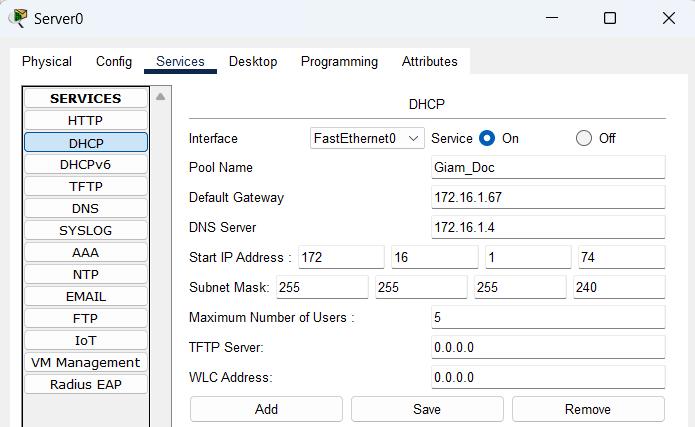
Hình 3. 5 Tạo pool Kế toán

* **Phòng Kinh doanh:**



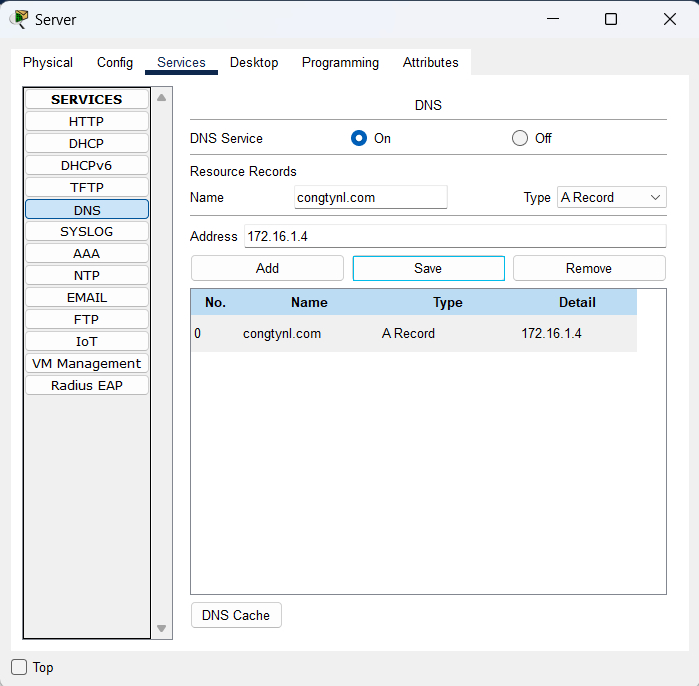
Hình 3. 6 Tạo pool Kinh doanh

* **Phòng Giám đốc:**



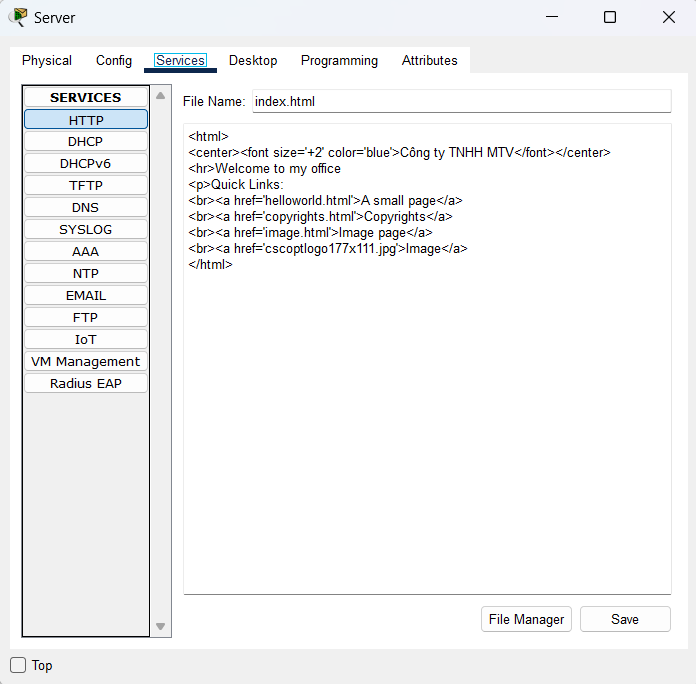
Hình 3. 7 Tạo pool Giám đốc

**- DNS Server:**



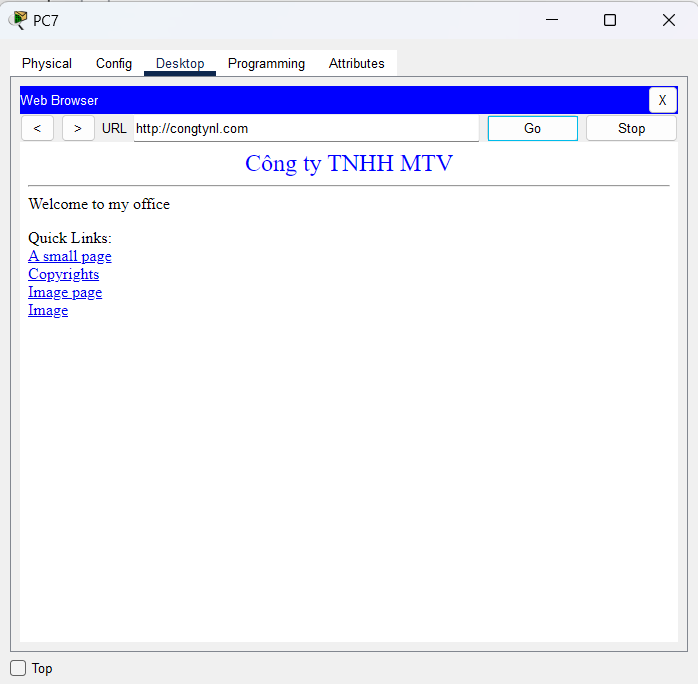
Hình 3. 8 DNS Server

**- Web Server:**



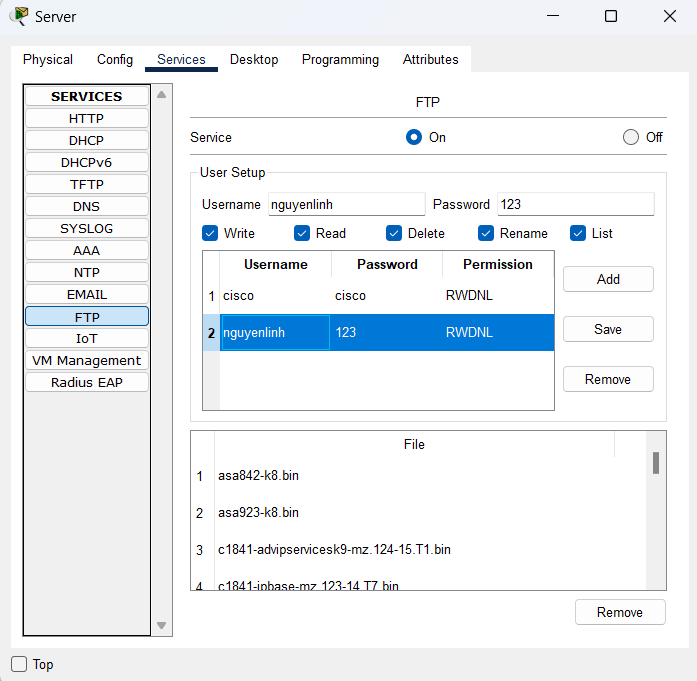
Hình 3. 9 Web Server

* **Dịch vụ web:**



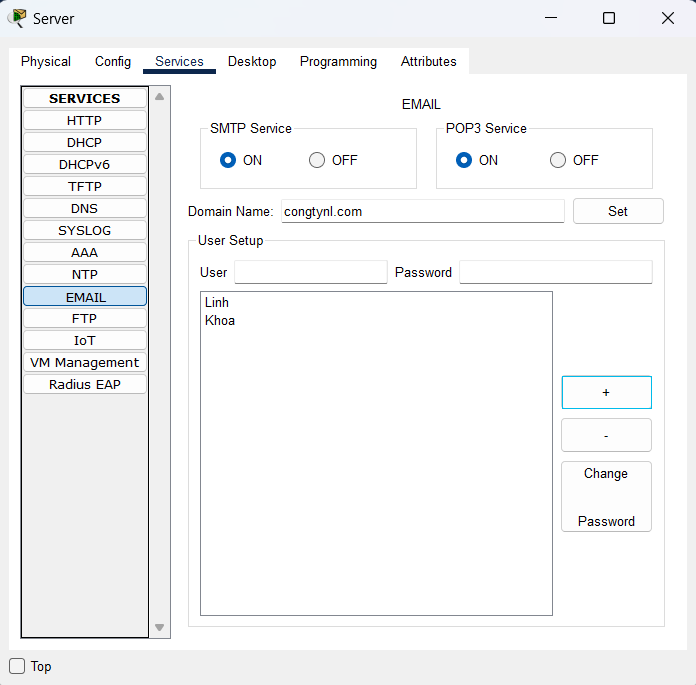
Hình 3. 10 Dịch vụ web

**- FTP Server:**

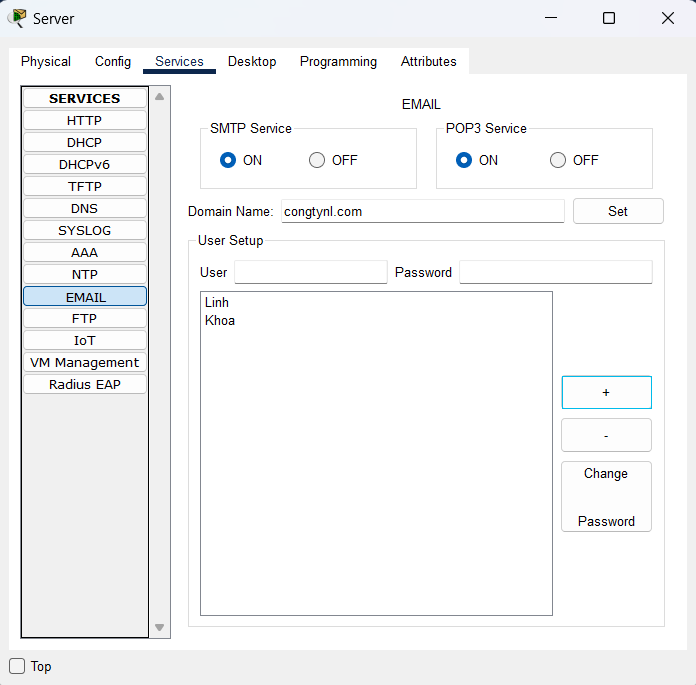


Hình 3. 11 FTP Server

**- Mail Server:**

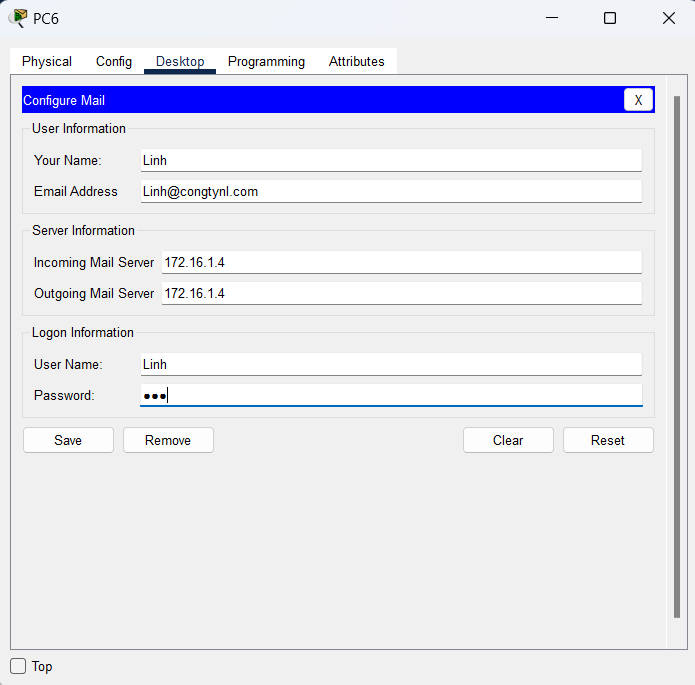


Hình 3. 12 Mail Server

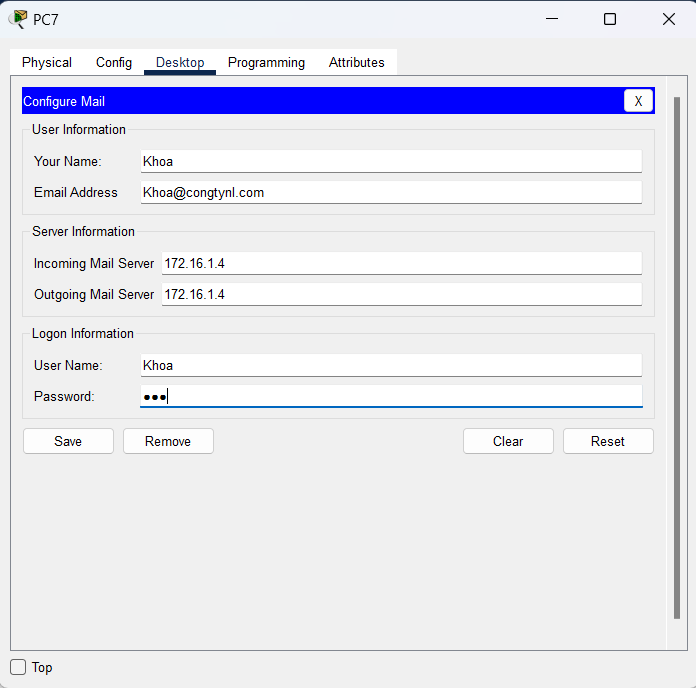


Hình 3. 13 Mail Server

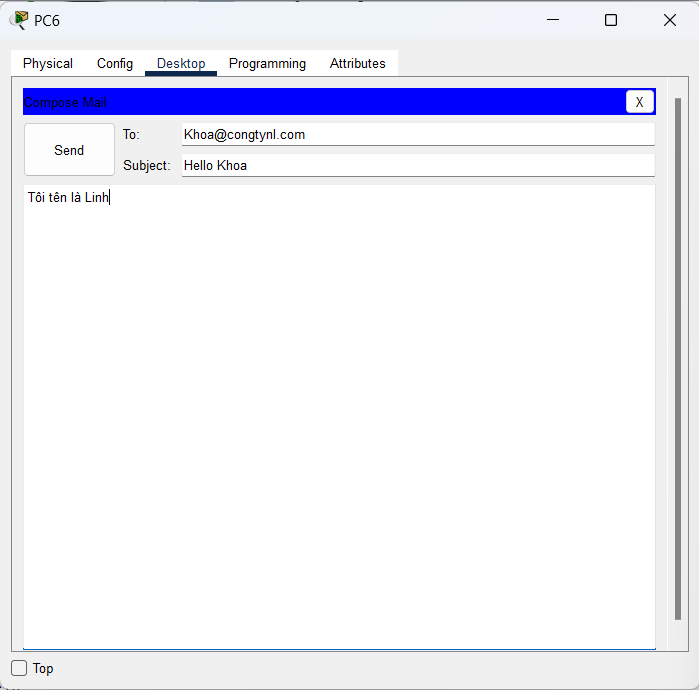
* **Test Mail Server:**



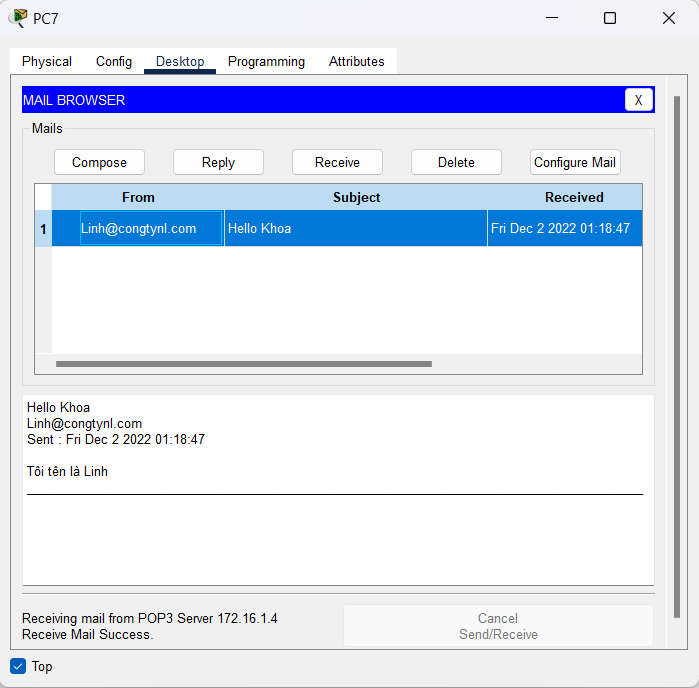
Hình 3. 14 Tạo tài khoản mail trên PC6



Hình 3. 15 Tạo tài khoản mail trên PC7



Hình 3. 16 Tạo Mail và gửi Mail



Hình 3. 17 Nhận Mail thành công

3.3.3 Cấu hình OSPF

* **Distribution-1:**

Switch(config)#ip routing

Switch(config)#router ospf 10

Switch(config-router)#network 172.16.1.88 0.0.0.3 area 0

Switch(config-router)#network 172.16.1.96 0.0.0.3 area 0

Switch(config-router)#network 172.16.0.0 0.0.0.127 area 0

Switch(config-router)#network 172.16.0.128 0.0.0.63 area 0

Switch(config-router)#network 172.16.0.192 0.0.0.63 area 0

Switch(config-router)#network 172.16.1.0 0.0.0.63 area 0

Switch(config-router)#network 172.16.1.0 0.0.0.15 area 0

Switch(config-router)#end

* **Distribution-2:**

Switch(config)#ip routing

Switch(config)#router ospf 10

Switch(config-router)#network 172.16.1.92 0.0.0.3 area 0

Switch(config-router)#network 172.16.1.96 0.0.0.3 area 0

Switch(config-router)#network 172.16.0.0 0.0.0.127 area 0

Switch(config-router)#network 172.16.0.128 0.0.0.63 area 0

Switch(config-router)#network 172.16.0.192 0.0.0.63 area 0

Switch(config-router)#network 172.16.1.0 0.0.0.63 area 0

Switch(config-router)#network 172.16.1.0 0.0.0.15 area 0

Switch(config-router)#end

* **CORE-1:**

Router(config)#router ospf 10

Router(config-router)#network 200.0.0.0 0.0.0.3 area 0

Router(config-router)#network 172.16.1.88 0.0.0.3 area 0

Router(config-router)#network 172.16.0.0 0.0.0.127 area 0

Router(config-router)#network 172.16.0.128 0.0.0.63 area 0

Router(config-router)#network 172.16.0.192 0.0.0.63 area 0

Router(config-router)#network 172.16.1.0 0.0.0.63 area 0

Router(config-router)#network 172.16.1.0 0.0.0.15 area 0

Router(config-router)#end

* **CORE-2:**

Router(config)#router ospf 10

Router(config-router)#network 200.0.0.4 0.0.0.3 area 0

Router(config-router)#network 172.16.1.92 0.0.0.3 area 0

Router(config-router)#network 172.16.0.0 0.0.0.127 area 0

Router(config-router)#network 172.16.0.128 0.0.0.63 area 0

Router(config-router)#network 172.16.0.192 0.0.0.63 area 0

Router(config-router)#network 172.16.1.0 0.0.0.63 area 0

Router(config-router)#network 172.16.1.0 0.0.0.15 area 0

Router(config-router)#end

* **ISP:**

Router(config)#router ospf 10

Router(config-router)#network 200.0.0.0 0.0.0.3 area 0

Router(config-router)#network 200.0.0.4 0.0.0.3 area 0

Router(config-router)#network 200.0.0.8 0.0.0.3 area 0

Router(config-router)#network 172.16.0.0 0.0.0.127 area 0

Router(config-router)#network 172.16.0.128 0.0.0.63 area 0

Router(config-router)#network 172.16.0.192 0.0.0.63 area 0

Router(config-router)#network 172.16.1.0 0.0.0.63 area 0

Router(config-router)#network 172.16.1.0 0.0.0.15 area 0

Router(config-router)#end

3.3.4 Cấu hình DHCP Replay

* **Distribution 1 và Distribution-2:**

Switch(config)#int vlan 1

Switch(config-if)#ip help

Switch(config-if)#ip helper-address 172.16.1.4

Switch(config-if)#int vlan 10

Switch(config-if)#ip helper-address 172.16.1.4

Switch(config-if)#int vlan 20

Switch(config-if)#ip helper-address 172.16.1.4

Switch(config-if)#int vlan 30

Switch(config-if)#ip helper-address 172.16.1.4

Switch(config-if)#int vlan 40

Switch(config-if)#ip helper-address 172.16.1.4

3.3.5 Cấu hình DHCP Snooping

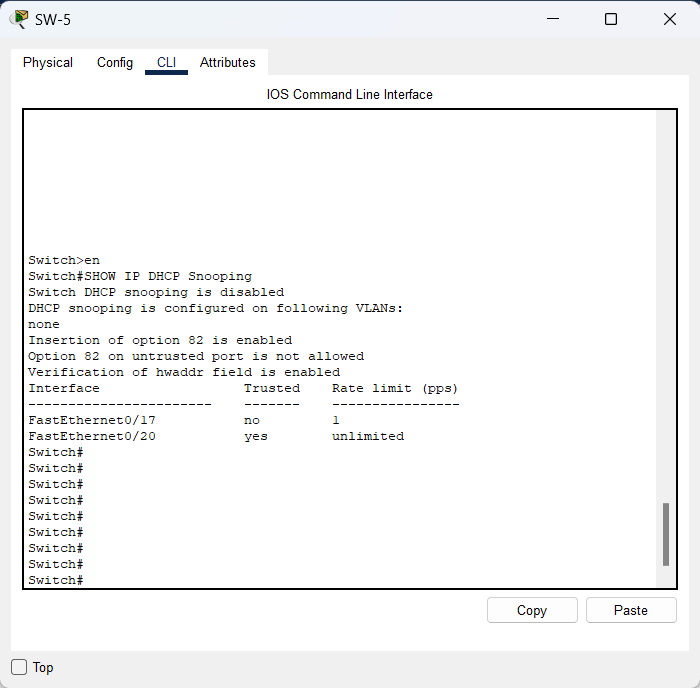
**- SW-5:**

Switch#conf t

Switch(config)#int fa0/20

Switch(config-if)#ip dhcp snooping trust

**- Kiểm tra DHCP Snooping:**



Hình 3. 18 Kiểm tra DHCP Snooping

3.3.6 Cấu hình HSRP

* **Distribution-1:**

Switch#config t

Switch(config)#int vlan 1

Switch(config-if)#standby version 2

Switch(config-if)#standby 1 ip 172.16.1.3

Switch(config-if)#standby 1 priority 150

Switch(config-if)#standby 1 preempt

Switch(config-if)#exit

Switch(config)#int vlan 10

Switch(config-if)#standby version 2

Switch(config-if)#standby 1 ip 172.16.0.3

Switch(config-if)#standby 1 priority 150

Switch(config-if)#standby 1 preempt

Switch(config-if)#exit

Switch(config)#int vlan 20

Switch(config-if)#standby version 2

Switch(config-if)#standby 1 ip 172.16.0.131

Switch(config-if)#standby 1 priority 150

Switch(config-if)#standby 1 preempt

Switch(config-if)#exit

Switch(config)#int vlan 30

Switch(config-if)#standby version 2

Switch(config-if)#standby 1 ip 172.16.0.195

Switch(config-if)#standby 1 priority 150

Switch(config-if)#standby 1 preempt

Switch(config-if)#exit

Switch(config)#int vlan 40

Switch(config-if)#standby version 2

Switch(config-if)#standby 1 ip 172.16.1.67

Switch(config-if)#standby 1 priority 150

Switch(config-if)#standby 1 preempt

Switch(config-if)#end

* **Distribution-2:**

Switch#config t

Switch(config)#int vlan 1

Switch(config-if)#standby version 2

Switch(config-if)#standby 1 ip 172.16.1.3

Switch(config-if)#exit

Switch(config)#int vlan 10

Switch(config-if)#standby version 2

Switch(config-if)#standby 1 ip 172.16.0.3

Switch(config-if)#exit

Switch(config)#int vlan 20

Switch(config-if)#standby version 2

Switch(config-if)#standby 1 ip 172.16.0.131

Switch(config-if)#exit

Switch(config)#int vlan 30

Switch(config-if)#standby version 2

Switch(config-if)#standby 1 ip 172.16.0.195

Switch(config-if)#exit

Switch(config)#int vlan 40

Switch(config-if)#standby version 2

Switch(config-if)#standby 1 ip 172.16.1.67

Switch(config-if)#end

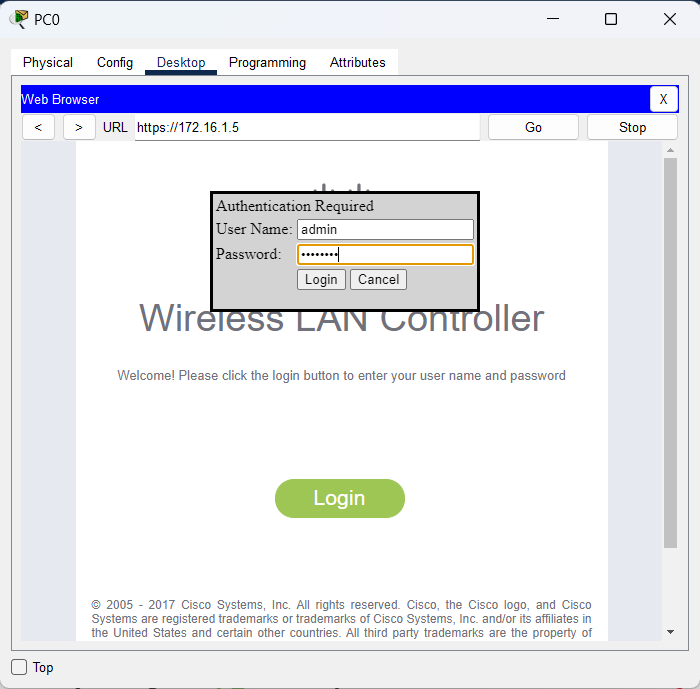
3.3.7 Cấu hình WLAN

**- Tạo một giao diện VLAN mới:**

* Đăng nhập vào WLC:

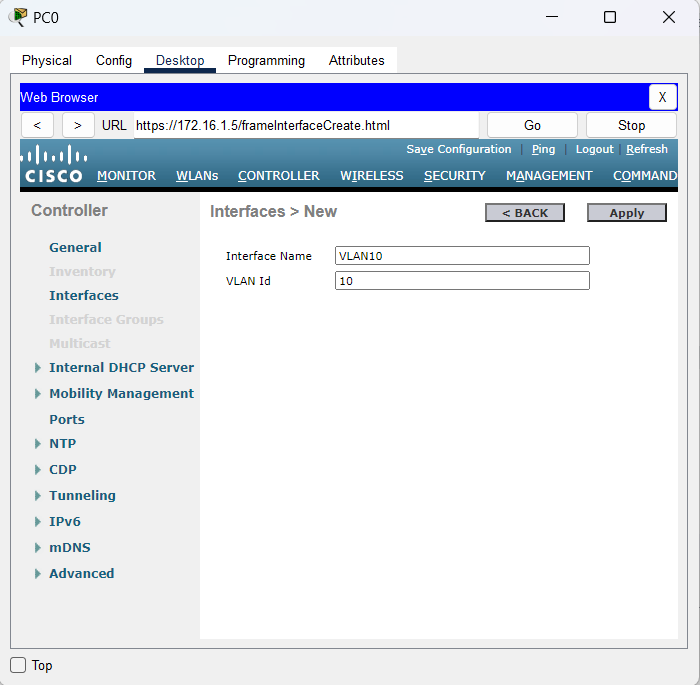
**+** User Name: **admin**

+ Password: **Cisco123**

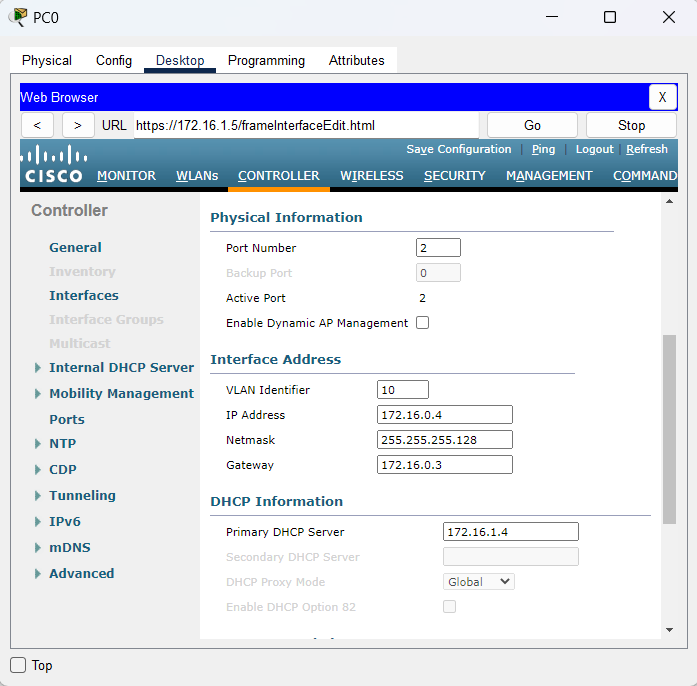


Hình 3. 19 Đăng nhập vào WLC

* **Tạo VLAN10:**

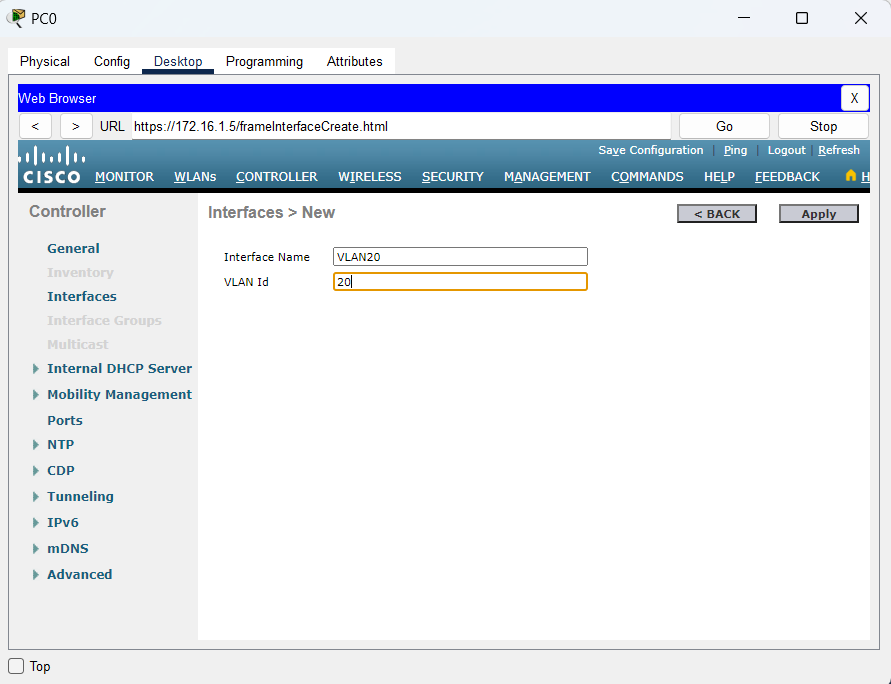


Hình 3. 20 VLAN10

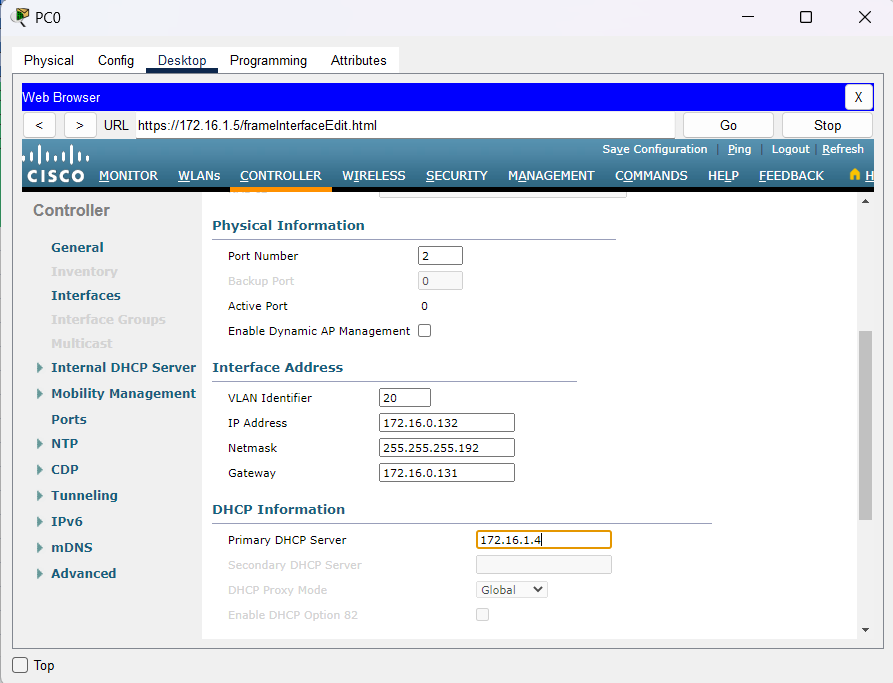


Hình 3. 21 VLAN10

* **Tạo VLAN20:**

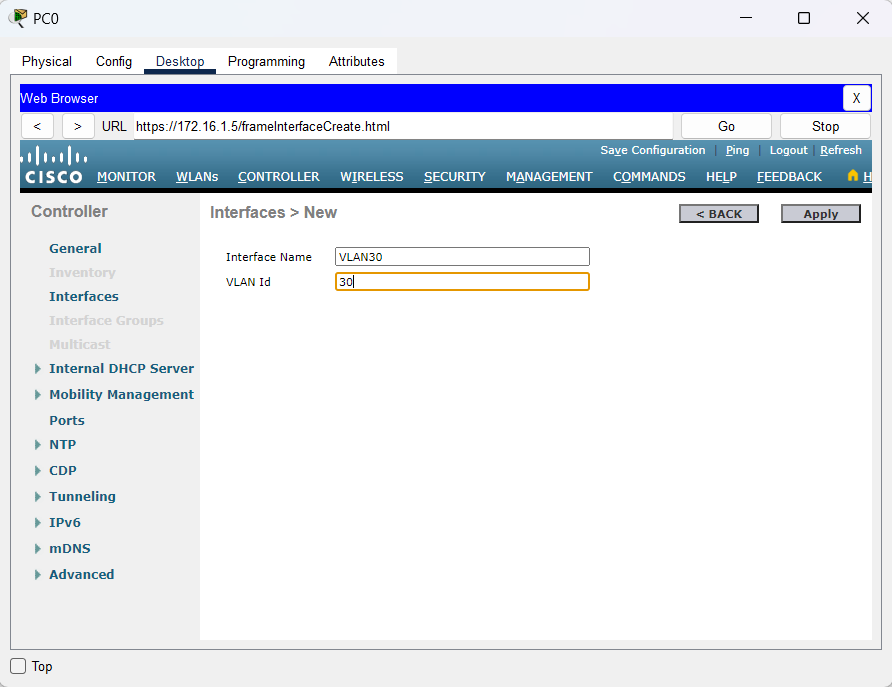


Hình 3. 22 VLAN20

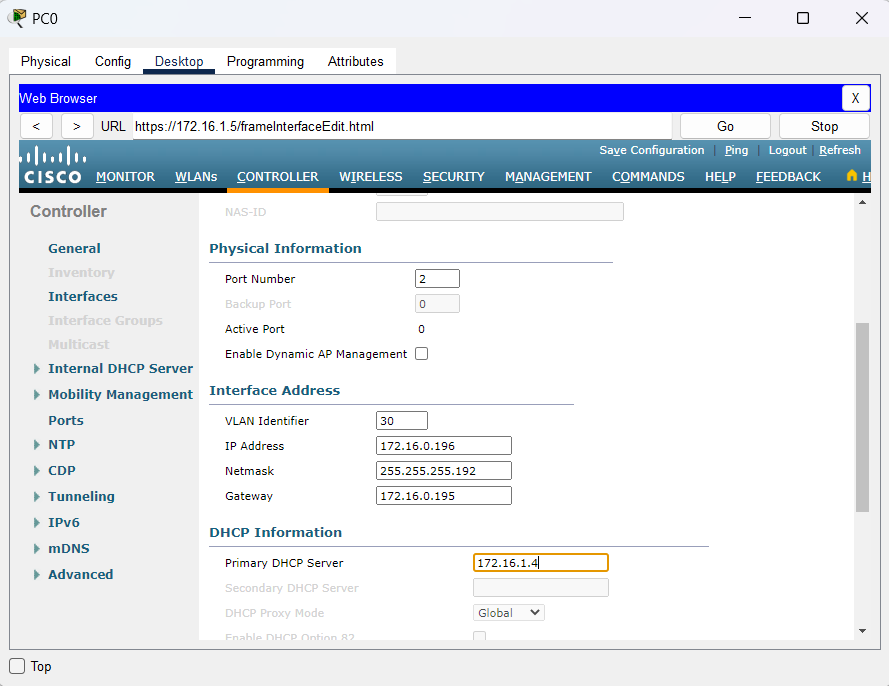


Hình 3. 23 VLAN20

* **Tạo VLAN30:**

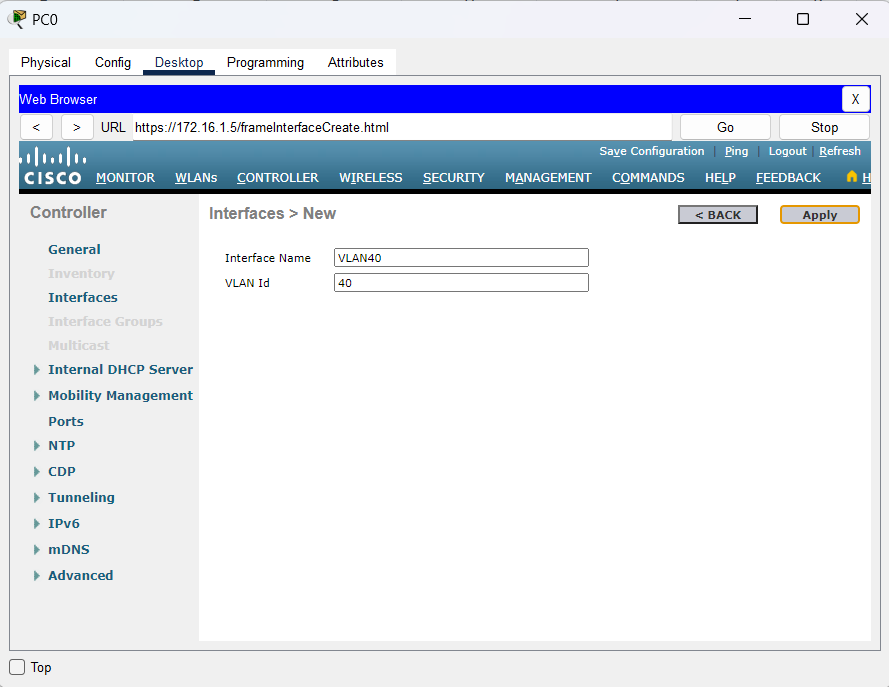


Hình 3. 24 VLAN30

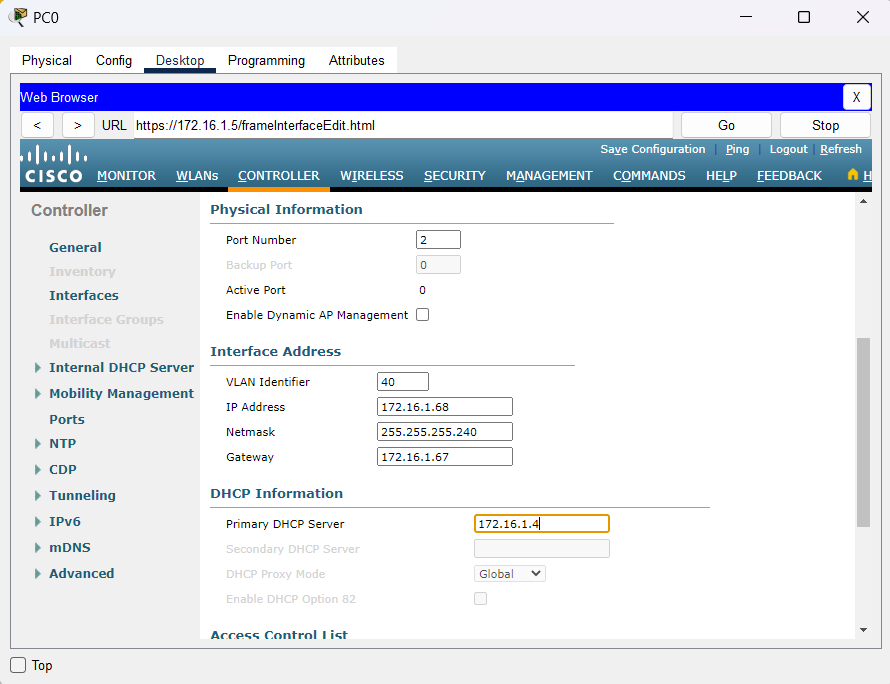


Hình 3. 25 VLAN30

* **Tạo VLAN40:**



Hình 3. 26 VLAN40



Hình 3. 27 VLAN40

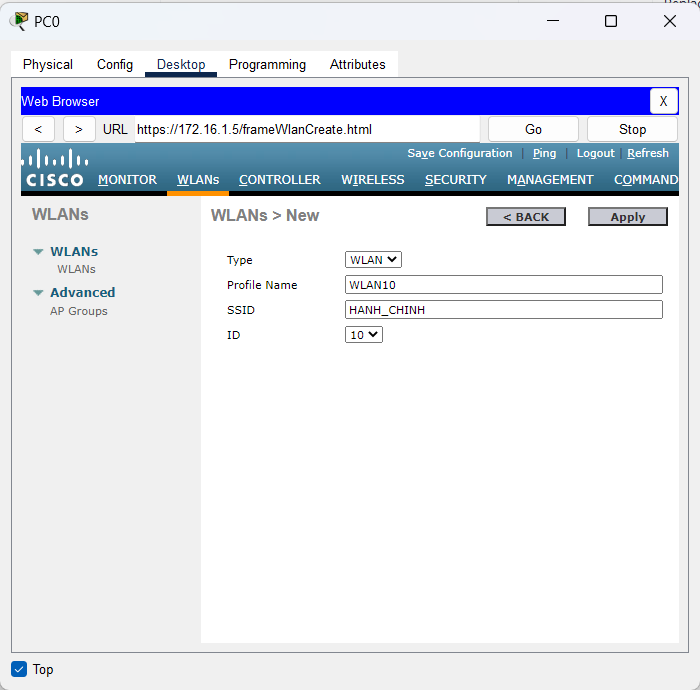
**- Tạo WLAN:**

* **WLAN10:**

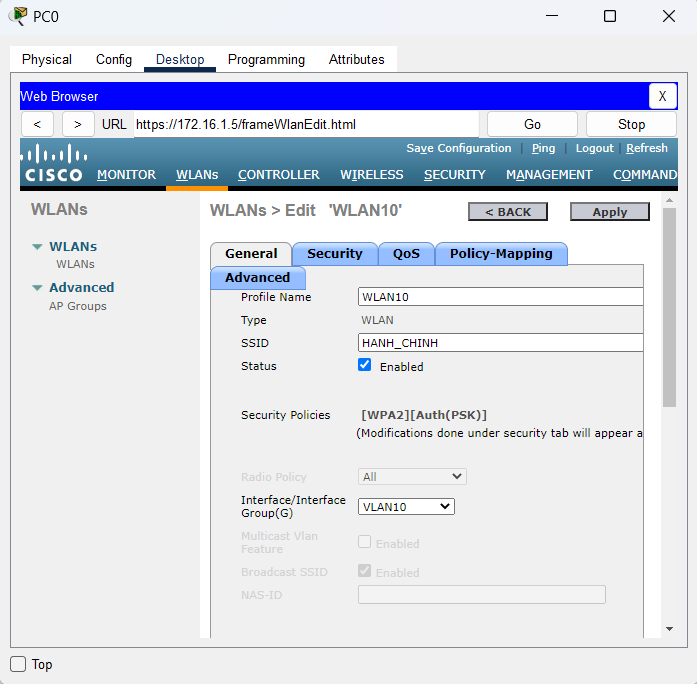
+ Profile Name: **WLAN10**

+ SSID: **HANH\_CHINH**

+ ID: **1**

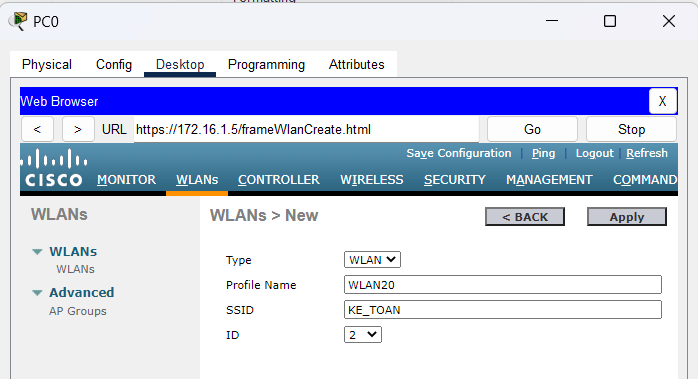


Hình 3. 28 WLAN10

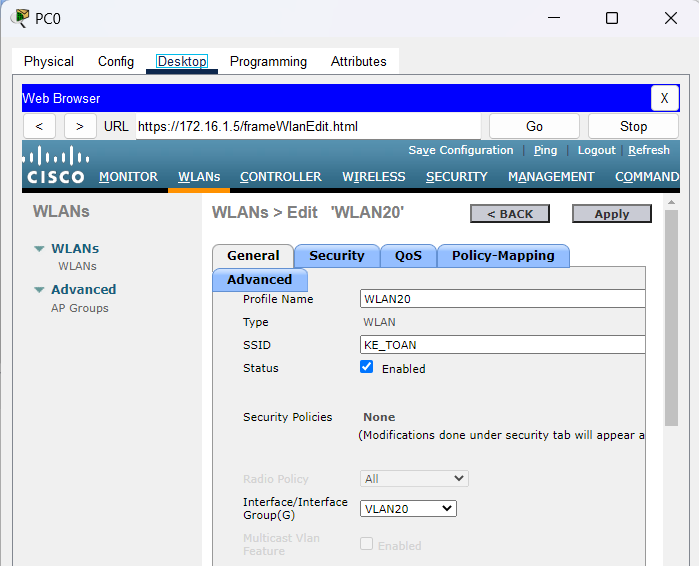


Hình 3. 29 WLAN10

* **WLAN20:**

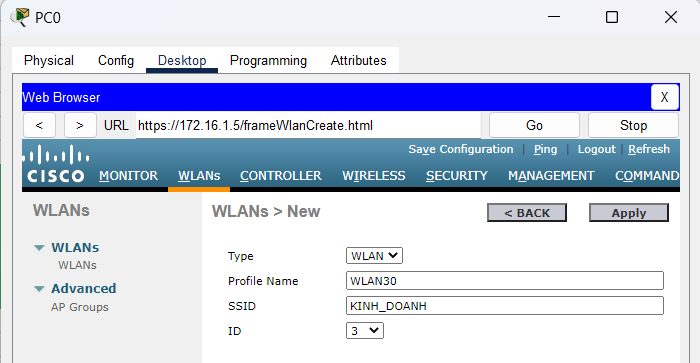


Hình 3. 30 WLAN20

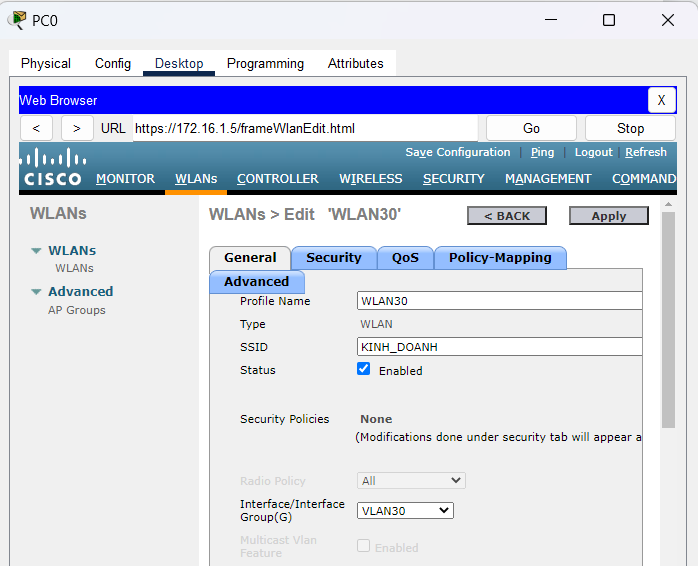


Hình 3. 31 WLAN20

* **WLAN30:**

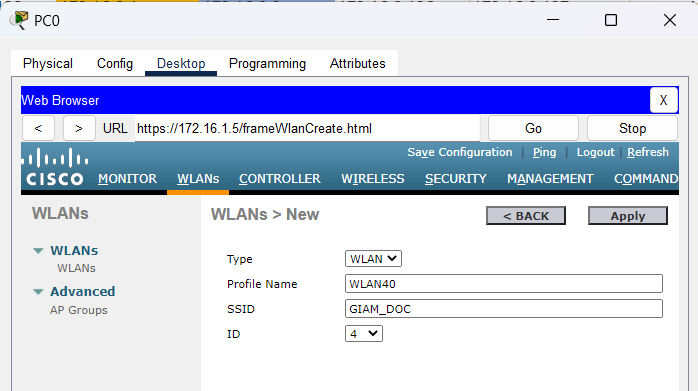


Hình 3. 32 WLAN30

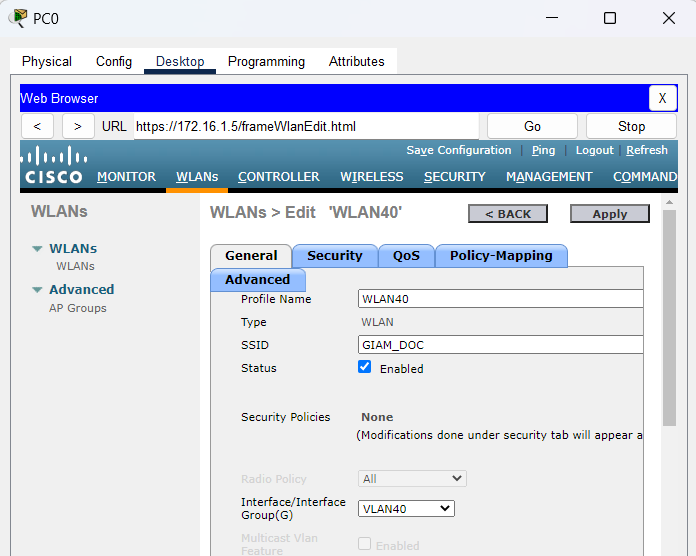


Hình 3. 33 WLAN30

* **WLAN40:**



Hình 3. 34 WLAN40



Hình 3. 35 WLAN40

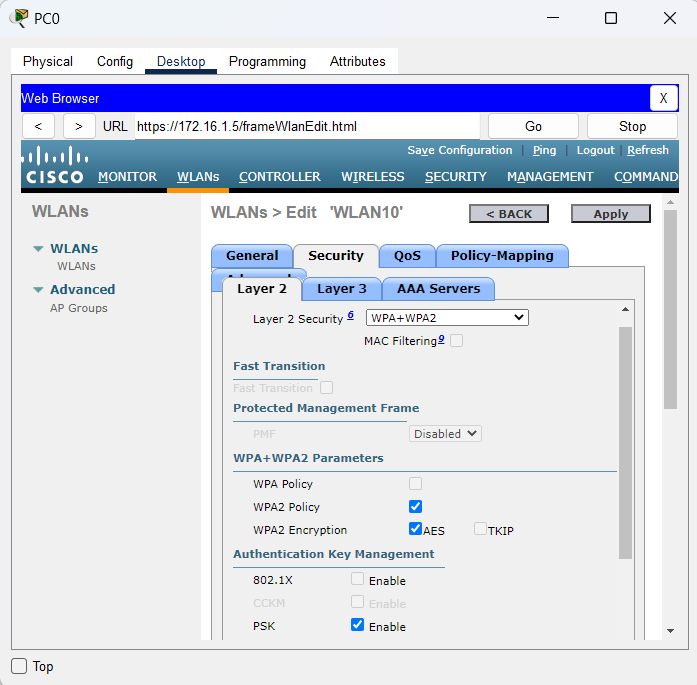
**- Cấu hình bảo mật WLAN:**

+ Layer 2 Security: **WPA + WPA2**

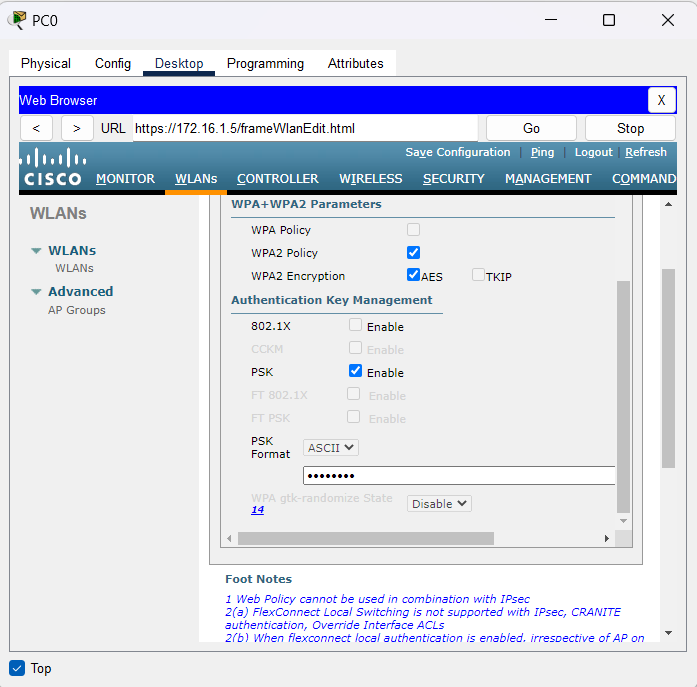
+ WPA + WPA2 Parameters: WPA2 Policy **Enable**

WPA2 Encryption **Enable AES**

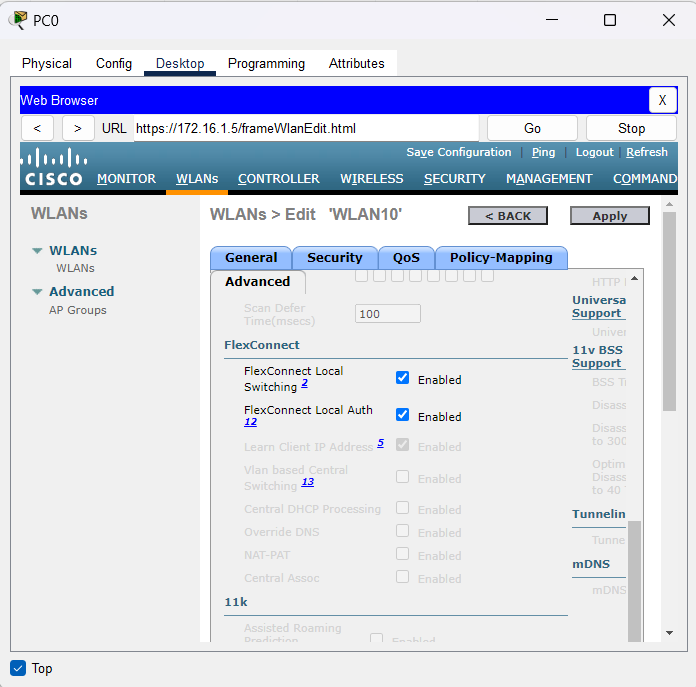
+ Password: **12345678**



Hình 3. 36 Cấu hình bảo mật WLAN



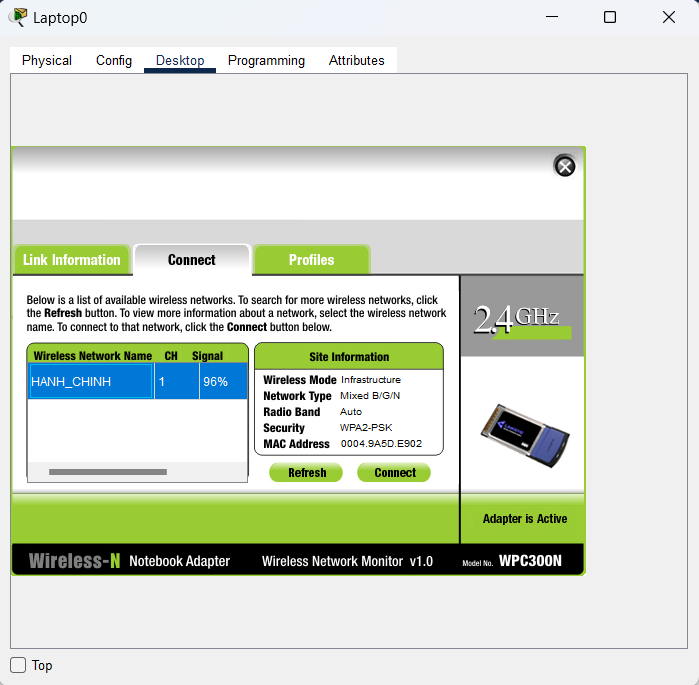
Hình 3. 37 Cấu hình bảo mật WLAN



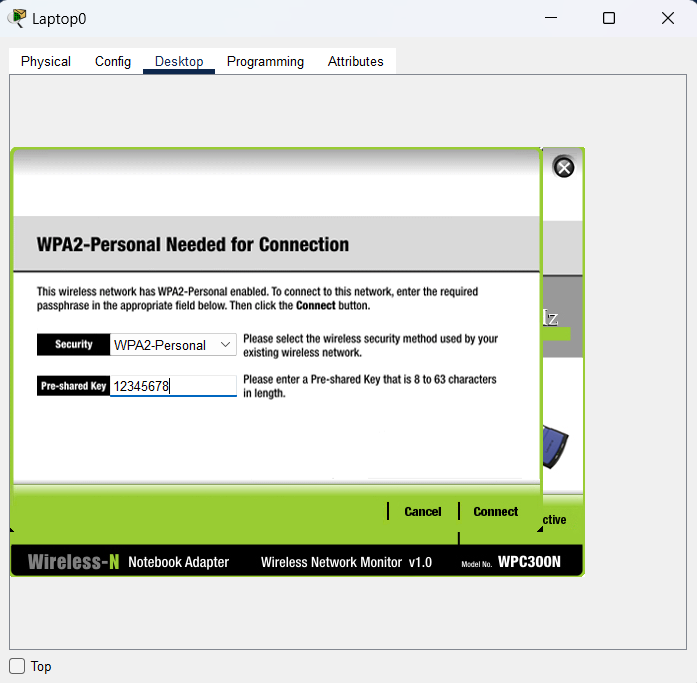
Hình 3. 38 Cấu hình bảo mật WLAN

**- Kết nối các thiết bị không dây:**

* **Laptop0:**

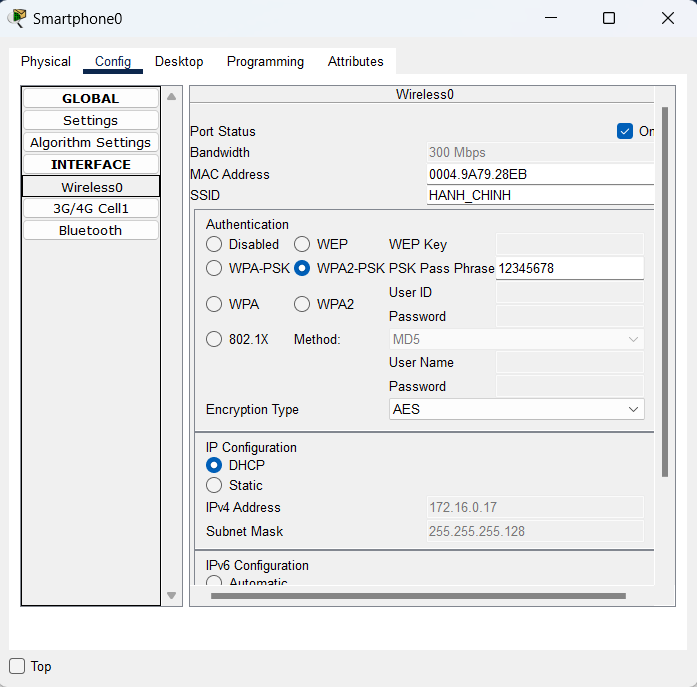


Hình 3. 39 Kết nối wifi Laptop0



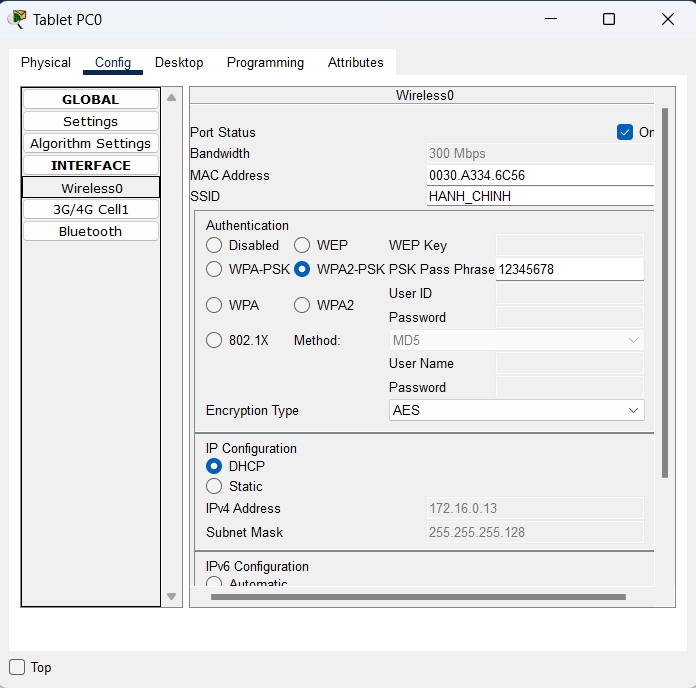
Hình 3. 40 Kết nối wifi Laptop0

* **Smartphone0:**



Hình 3. 41 Kết nối wifi Smartphone0

* **Tablet PC0:**



Hình 3. 42 Kết nối wifi Tablet PC0

3.3.8 Cấu hình Console

**- Distribution-1:**

DIST-1(config)#line console 0

DIST-1(config-line)#login local

DIST-1(config-line)#end

**- Distribution-2**

DIST-2(config)#line console 0

DIST-2(config-line)#login local

DIST-2(config-line)#end

**- CORE-1:**

CORE-1(config)#line console 0

CORE-1(config-line)#login local

CORE-1(config-line)#end

**- CORE-2:**

CORE-2(config)#line console 0

CORE-2(config-line)#login local

CORE-2(config-line)#end

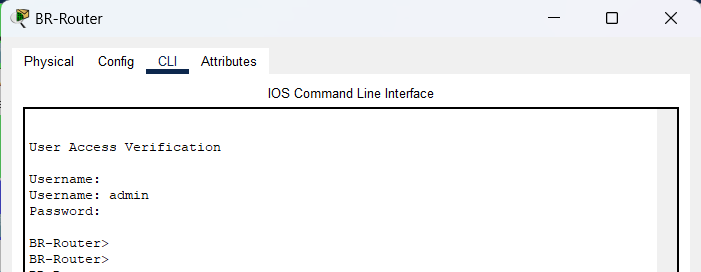
**- BR-Router:**

BR-Router(config)#line console 0

BR-Router(config-line)#login local

BR-Router(config-line)#end

* **Test Console trên BR-Router:**



Hình 3. 43 Test Console trên BR-Router

3.3.9 Cấu hình SSH, ACLs

**- Distribution-1, Distribution-2, CORE-1, CORE-2, BR-Router:**

config t

hostname BR-Router

ip domain-name nguyenlinh.vn

crypto key generate rsa

1024

username admin password admin

enable secret admin

line vty 0 4

login local

transport input ssh

exit

**- Cấu hình ACLs chỉ cho các máy thuộc VLAN1 truy cập SSH:**

* **Distribution-1:**

DIST-1(config)#ip access-list standard DIEU\_KHIEN\_SSH

DIST-1(config-std-nacl)#!Only vlan 1 access SSH

DIST-1(config-std-nacl)#permit 172.16.1.0 0.0.0.63

DIST-1(config-std-nacl)#exit

DIST-1(config)#line vty 0 4

DIST-1(config-line)#access-class DIEU\_KHIEN\_SSH in

DIST-1(config-line)#end

* **Distribution-2:**

DIST-2(config)#ip access-list standard DIEU\_KHIEN\_SSH

DIST-2(config-std-nacl)#!Only vlan 1 access SSH

DIST-2(config-std-nacl)#permit 172.16.1.0 0.0.0.63

DIST-2(config-std-nacl)#exit

DIST-2(config)#line vty 0 4

DIST-2(config-line)#access-class DIEU\_KHIEN\_SSH in

DIST-2(config-line)#end

* **CORE-1:**

CORE-1(config)#ip access-list standard DIEU\_KHIEN\_SSH

CORE-1(config-std-nacl)#!Only vlan 1 access SSH

CORE-1(config-std-nacl)#permit 172.16.1.0 0.0.0.63

CORE-1(config-std-nacl)#exit

CORE-1(config)#line vty 0 4

CORE-1(config-line)#access-class DIEU\_KHIEN\_SSH in

CORE-1(config-line)#end

* **CORE-2:**

CORE-2(config)#ip access-list standard DIEU\_KHIEN\_SSH

CORE-2(config-std-nacl)#!Only vlan 1 access SSH

CORE-2(config-std-nacl)#permit 172.16.1.0 0.0.0.63

CORE-2(config-std-nacl)#exit

CORE-2(config)#line vty 0 4

CORE-2(config-line)#access-class DIEU\_KHIEN\_SSH in

CORE-2(config-line)#end

* **BR-Router:**

BR-Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

BR-Router(config)#ip access-list standard DIEU\_KHIEN\_SSH

BR-Router(config-std-nacl)#!Only vlan 1 access SSH

BR-Router(config-std-nacl)#permit 172.16.1.0 0.0.0.63

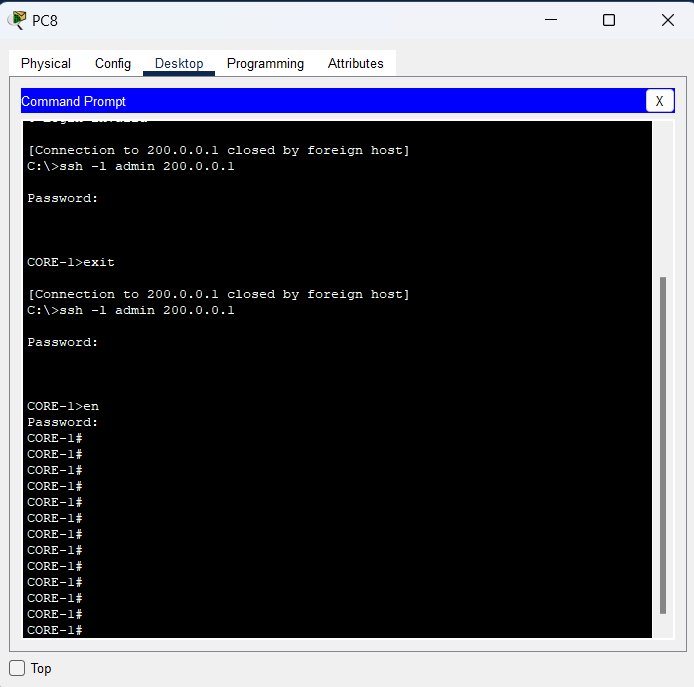
BR-Router(config-std-nacl)#exit

BR-Router(config)#line vty 0 4

BR-Router(config-line)#access-class DIEU\_KHIEN\_SSH in

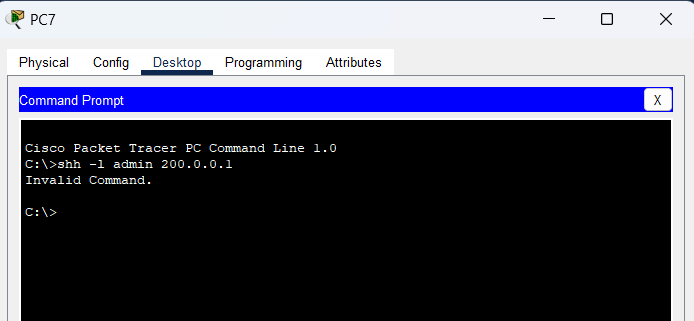
BR-Router(config-line)#end

- Kiểm tra xem thiết bị VLAN 1 có thể truy cập vào CORE-1 để cấu hình chưa:



Hình 3. 44 PC8 thuộc VLAN 1 có thể sử dụng SSH

- Những thiết bị ở VLAN khác không thể sử dụng SSH.



Hình 3. 45 PC7 thuộc VLAN 40 không thể sử dụng SSH

CHƯƠNG 4 – KẾT LUẬN

- Nhóm đã đạt được 95% các yêu cầu mà công ty cổ phần bánh kẹo Hải Hà đưa ra. Để giải quyết các yêu cầu mà công ty đưa ra nhóm đã có các giải pháp như sau: quy hoạch địa chỉ IP theo lớp B để dễ dàng mở rộng mạng nội bộ về sau; giải quyết dự phòng bằng STP sử dụng hai thiết bị Distribution và hai Core và cấu hình HSRP;cấu hình trunk để tránh vòng lặp; cấu hình VLAN theo từng ban, interface và port chanel để dễ dàng quản lý; cấu hình dịch vụ DHCP để cấp IP tự động; cấu hình các dịch vụ cơ bản như: DNS server, Mail server, FTP server, Web server; định tuyến động OSPF; cấu hình DHCP Replay trên hai con Distribution để nó gián tiếp cấp địa chỉ IP cho các thiết bị thuộc VLAN khác; cấu hình DHCP Snooping để nhận đường mạng tin cậy nhằm tránh các trường hợp hacker tấn công bằng cách sử dụng một máy server khác; cấu hình WLAN để quản lý các thiết bị trong mạng không dây; cấu hình console để đặt password và username nâng cao bảo mật cho các router quản lý; cấu hình SSH để các thiết bị ở chi nhánh có thể điều khiển từ xa; cấu hình ACLs chỉ cho phép các thiết bị thuộc VLAN 1 truy cập điều khiển bằng SSH.

**TÀI LIỆU THAM KHẢO**

**Tiếng Việt**

1. <https://cnttshop.vn/blogs/cisco/cau-hinh-vpn-client-to-site-cisco>

**Tiếng Anh**

1. <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html>
2. <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Medium_Enterprise_Design_Profile/MEDP/chap2.html>
3. [https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA\_campus\_DG/hacampusdg.html#wp1108924](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html" \l "wp1108924)
4. <https://www.arubanetworks.com/resource/mobile-first-campus-for-midsize-networks-design-and-deployment-guide/>
5. [https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html#DesignFundamentalsCampusWirelessLAN](https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html" \l "DesignFundamentalsCampusWirelessLAN)
6. <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_6.html>
7. <https://support.huawei.com/enterprise/en/doc/EDOC1100055102/9465df90/example-for-configuring-hybrid-vlan-based-layer-2-protocol-tunneling>