TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CUỐI KỲ**

**GIAO THỨC VÀ MẠNG MÁY TÍNH**

**THIẾT KẾ HỆ THỐNG MẠNG DOANH NGHIỆP CÓ HAI CHI NHÁNH**

*Người hướng dẫn*: **THẦY TS. TRƯƠNG ĐÌNH TÚ**

*Người thực hiện*: **Ngô Hữu Lễ - 51800571**

**Phạm Nhật Anh - 51900646**

*Khóa*    **:  22, 23**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023**

**LỜI CẢM ƠN**

Đầu tiên, tập thể nhóm chúng em xin gửi lời cảm ơn đến Khoa Công nghệ thông tin trường đại học Tôn Đức Thắng đã tạo điều kiện cho chúng em được tham gia học tập môn học này. Ngoài ra khoa còn tạo điều kiện để chúng em có cơ hội hoàn thành môn học một cách tốt nhất.

Tiếp theo, chúng em xin gửi lời cảm ơn đến thầy Trương Đình Tú, giảng viên bộ môn Công nghệ phần mềm đã hướng dẫn, chỉ dạy chúng em trong suốt quá trình học và hoàn thành bài báo cáo này. Và bên cạnh đó, chúng em cũng xin cảm ơn đến thầy cô giảng viên tại trường, đặt biệt là các giảng viên trong trong khoa Công Nghệ Thông Tin đã dạy chúng em nhiều kiến thức cơ bản, thiết yếu và trang bị cho chúng em một lượng tri thức trong suốt quá trình học cũng như trong quá trình làm bài báo cáo.

Cuối cùng em xin chúc khoa Công nghệ thông tin trường đại học Tôn Đức Thắng và thầy Trương Đình Tú có thật nhiều sức khỏe để có thể góp phần cống hiến cho sự phát triển khoa Công nghệ thông tin trường đại học Tôn Đức Thắng cũng như truyền đạt thật nhiều kiến thức đến sinh viên chúng em.

Nhóm chúng em xin chân thành cảm ơn!

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

#### Chúng tôi xin cam đoan đây là báo cáo nghiên cứu của riêng tôi và được sự hướng dẫn khoa học của thầy Trương Đình Tú. 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 13 tháng 4 năm 2023*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Phạm Nhật Anh*

*Ngô Hữu Lễ*

| **Mục lục** |  |
| --- | --- |
| [**DANH MỤC CHỮ VIẾT TẮT**](#_heading=h.375fbgg) | **i** |
| [**DANH MỤC HÌNH VẼ**](#_heading=h.375fbgg) | **iv** |
| [**DANH MỤC BẢNG BIỂU**](#_heading=h.375fbgg) | **v** |
| [**TÓM TẮT**](#_heading=h.375fbgg) | **vi** |
| [**CHƯƠNG 1 - GIỚI THIỆU VÀ KHẢO SÁT**](#_heading=h.375fbgg) | **1** |
| [1.1 Giới thiệu đề tài](#_heading=h.2s8eyo1) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 1 |
| [1.2 Mô tả đề tài](#_heading=h.1maplo9) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 1 |
| [1.3 Khảo sát thực tế](#_heading=h.46ad4c2) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
| [**CHƯƠNG 2 - MÔ HÌNH HỆ THỐNG**](#_heading=h.2lfnejv) | **4** |
| [2.1 Sơ đồ luận lý](#_heading=h.3rdcrjn) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 4 |
| [2.2 Sơ đồ vật lý](#_heading=h.35nkun2) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 5 |
| [2.3 Sơ đồ lắp đặt tủ Rack](#_heading=h.2jxsxqh) . . . . . . . . . . . . . . . . . . . . . . . . . . . | 6 |
| [**CHƯƠNG 3 - THÔNG TIN CÀI ĐẶT CẤU HÌNH HỆ THỐNG**](#_heading=h.3j2qqm3) | **7** |
| [3.1 Thông tin kết nối port trong hệ thống](#_heading=h.4i7ojhp) . . . . . . . . . . . . . . . . . . . | 7 |
| [3.2 Thông tin VLAN, Interface VLAN trong hệ thống](#_heading=h.1ci93xb) . . . . . . . . . . . . | 21 |
| [3.3 Thông tin thiết kế quy hoạch địa chỉ IP Planning](#_heading=h.3as4poj) . . . . . . . . . . . . . | 22 |
| [**CHƯƠNG 4 - CẤU HÌNH HẠ TẦNG**](#_heading=h.3as4poj) | **30** |
| [4.1 Cấu hình Interface](#_heading=h.2p2csry) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 30 |
| [4.1.1 Khu vực Router biên và Internet](#_heading=h.2p2csry) . . . . . . . . . . . . . . . . . | 30 |
| [4.1.2 Khu vực Quận 7](#_heading=h.23ckvvd) . . . . . . . . . . . . . . . . . . . . . . . . . | 33 |
| [4.1.3 Khu vực Thủ Đức](#_heading=h.32hioqz) . . . . . . . . . . . . . . . . . . . . . . . . | 35 |

* 1. [Định tuyến động IPv4 và IPv6](#_heading=h.41mghml) 37
     1. [Router biên và Internet](#_heading=h.vx1227) 37
     2. [Khu vực Quận 7](#_heading=h.1v1yuxt) 43
     3. [Khu vực Thủ Đức](#_heading=h.2u6wntf) 50
  2. [Cấu hình khu vực DMZ](#_heading=h.3tbugp1) 55
     1. [DNS Server](#_heading=h.nmf14n) 55
     2. [WEB Server](#_heading=h.46r0co2) 57
     3. [Mail Server](#_heading=h.4k668n3) 60
     4. [FTP Server](#_heading=h.4bvk7pj) 62
     5. [RADIUS Server](#_heading=h.43ky6rz) 65
     6. [NTP Server](#_heading=h.4h042r0) 69
     7. [Syslog Server](#_heading=h.2afmg28) 70
  3. [Cấu hình VLAN VÀ VTP](#_heading=h.1opuj5n) 70
     1. [Khu vực Quận 7](#_heading=h.1opuj5n) 70
     2. [Khu vực Thủ Đức](#_heading=h.48pi1tg) 74
  4. [Cấu hình WLC và Light Access Point](#_heading=h.1302m92) 77
  5. [Cấu hình DHCPv4 và DHCPv6](#_heading=h.1tuee74) 83
     1. [Khu vực Quận 7](#_heading=h.4du1wux) 83
     2. [Khu vực Thủ Đức](#_heading=h.184mhaj) 87
  6. [Cấu hình DHCP Snooping](#_heading=h.meukdy) 90
     1. [Khu vực Quận 7](#_heading=h.meukdy) 90
     2. [Khu vực Thủ Đức](#_heading=h.36ei31r) 95
  7. [Cấu hình Ethernet-Channel](#_heading=h.45jfvxd) 97
     1. [Khu vực Quận 7](#_heading=h.2koq656) 97
     2. [Khu vực Thủ Đức](#_heading=h.zu0gcz) 100
  8. [Cấu hình Spanning Tree](#_heading=h.1yyy98l) 102
     1. [Khu vực Quận 7](#_heading=h.1yyy98l) 102
     2. [Khu vực Thủ Đức](#_heading=h.4iylrwe) 103
  9. [Cấu hình HSRP](#_heading=h.1d96cc0) 104
     1. [Khu vực Quận 7](#_heading=h.1d96cc0) 104
     2. [Khu vực Thủ Đức](#_heading=h.3x8tuzt) 107
  10. [Cấu hình Firewall ASA](#_heading=h.rjefff) 108
      1. [Khu vực Quận 7](#_heading=h.rjefff) 108
      2. [Khu vực Thủ Đức](#_heading=h.3bj1y38) 112
  11. [Cấu hình Access Control List](#_heading=h.2pta16n) 114
      1. [Khu vực Quận 7](#_heading=h.2pta16n) 114
      2. [Khu vực Thủ Đức](#_heading=h.1qoc8b1) 115
  12. [Cấu hình Port Security](#_heading=h.3oy7u29) 115
      1. [Khu vực Quận 7](#_heading=h.3oy7u29) 115
      2. [Khu vực Thủ Đức](#_heading=h.243i4a2) 119
  13. [Cấu hình SSH access](#_heading=h.338fx5o) 122
      1. [Khu vực Quận 7](#_heading=h.1idq7dh) 122
      2. [Khu vực Thủ Đức](#_heading=h.42ddq1a) 124
  14. [Cấu hình NTP, Syslog](#_heading=h.wnyagw) 126
  15. [Cấu hình VPN-IPSec](#_heading=h.1vsw3ci) 126
  16. [Cấu hình NAT](#_heading=h.2uxtw84) 132
  17. [Qos Concept](#_heading=h.3u2rp3q) 135
  18. [Chương trình demo](#_heading=h.38czs75) 137
      1. [Kiểm tra DHCP](#_heading=h.38czs75) 137
      2. [Kiểm tra gửi gói tin](#_heading=h.2mn7vak) 138
      3. [Kiểm tra ACL](#_heading=h.4kx3h1s) 140
      4. [Kiểm tra dịch vụ NTP và Syslog](#_heading=h.1smtxgf) 145
      5. [Kiểm tra backup](#_heading=h.16x20ju) 146
      6. [Kiểm tra Wifi](#_heading=h.2jh5peh) 149
      7. [Kiểm tra Port Security](#_heading=h.4hr1b5p) 151
      8. [Kiểm tra SSH Access](#_heading=h.2b6jogx) 152
      9. [Kiểm tra VPN-IPsec](#_heading=h.1pgrrkc) 154
      10. [Kiểm tra NAT](#_heading=h.320vgez) 154
      11. [Kiểm tra QoS Concept](#_heading=h.3fg1ce0) 157

[**CHƯƠNG 5 - KẾT LUẬN**](#_heading=h.n5rssn) **159**

[**TÀI LIỆU THAM KHẢO**](#_heading=h.n5rssn) **160**

[**PHỤ LỤC**](#_heading=h.n5rssn) **161**

**DANH MỤC CHỮ VIẾT TẮT**

#### WLAN Wireless Local Area Network VLAN Virtual Local Area Network WLC Wireless Lan Controller

#### DNS Domain Name System HTTP Hypertext Transfer Protocol IP Internet Protocol

#### OSPF Open Shortest Path First HSRP Hot Standby Router Protocol

#### DHCP Dynamic Host Configuration Protocol ACL Access Control List

#### FTP File Transfer Protocol

#### STP Spanning Tree Protocol

#### NTP Network Time Protocol

#### VC Virtual Circuit

#### PVC Permanent Virtual Circuit

**Danh sách hình vẽ**

#### [Hình 2.1 Sơ đồ luận lý](#_heading=h.26in1rg) . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

#### [Hình 2.2 Sơ đồ vật lý](#_heading=h.1ksv4uv) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

#### [Hình 2.3 Sơ đồ tủ Rack](#_heading=h.3j2qqm3) . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6

#### [Hình 4.1 Khu vực Router biên và Internet](#_heading=h.147n2zr) 30

#### [Hình 4.2 Đăng ký 2 tên miền cho hai trụ sở](#_heading=h.37m2jsg) 55

#### [Hình 4.3 Cấu hình địa chỉ Ipv4 và Ipv6 cho DNS Server](#_heading=h.2lwamvv) 56

#### [Hình 4.4 Cấu hình địa chỉ Ipv4 và Ipv6 cho Web Server trụ sở Quận 7](#_heading=h.111kx3o) 57

#### [Hình 4.5 Bật dịch vụ HTTP](#_heading=h.3l18frh) 58

#### [Hình 4.6 Truy cập đến trang web thành công.](#_heading=h.2zbgiuw) 59

#### [Hình 4.7 Đăng ký tên miền bằng địa chỉ public](#_heading=h.1egqt2p) 59

#### [Hình 4.8 Bật dịch vụ Mail Server](#_heading=h.3ygebqi) 60

#### [Hình 4.9 Cấu hình email cho máy phòng Hành chính.](#_heading=h.2dlolyb) 60

#### [Hình 4.10 Cấu hình email cho máy phòng Du lịch nội địa](#_heading=h.sqyw64) 61

#### [Hình 4.11 Gửi email từ phòng du lịch nội địa đến phòng hành chính thành công](#_heading=h.3cqmetx) 61 [Hình 4.12 Cấu hình Ipv4 và Ipv6 cho FTP Server](#_heading=h.2r0uhxc) 62

#### [Hình 4.13 Bật dịch vụ FTP và tạo tài khoản cho các phòng chức năng](#_heading=h.1664s55) 63

#### [Hình 4.14 File test.txt vừa tạo tồn tại trên ổ C của máy](#_heading=h.3q5sasy) 63

#### [Hình 4.15 Tải file lên server FTP](#_heading=h.25b2l0r) 64

#### [Hình 4.16 Các phòng chức năng có thể tải file về máy](#_heading=h.kgcv8k) 64

#### [Hình 4.17 Các phòng chức năng ở chi nhánh Thủ Đức cũng có thể đăng nhập](#_heading=h.34g0dwd)

#### [vào ftp](#_heading=h.34g0dwd) 65

#### [Hình 4.18 Cấu hình Ipv4 và Ipv6 trên Server quận 7.](#_heading=h.2iq8gzs) 65

#### [Hình 4.19 Bật dịch vụ AAA và tạo các account cho các phòng chức năng](#_heading=h.xvir7l) 66

#### [Hình 4.20 Cấu hình Ipv4 và Ipv6 trên Server Thủ Đức](#_heading=h.3hv69ve) 67

#### [Hình 4.21 Bật dịch vụ AAA và tạo các account cho các phòng chức năng](#_heading=h.2w5ecyt) 68

#### [Hình 4.22 Khởi động và cài đặt dịch vụ NTP](#_heading=h.1baon6m) 69

#### [Hình 4.23 Khởi động dịch vụ Syslog](#_heading=h.pkwqa1) 70

#### [Hình 4.24 Tạo tài khoản](#_heading=h.3mzq4wv) 77

#### [Hình 4.25 Thông tin sau khi tạo](#_heading=h.2250f4o) 78

#### [Hình 4.26 Tạo Interface cho các WLAN](#_heading=h.haapch) 79

#### [Hình 4.27 Tạo WLAN ID](#_heading=h.319y80a) 80

#### [Hình 4.28 Chọn dải IP Radius phù hợp](#_heading=h.1gf8i83) 80

#### [Hình 4.29 Tạo AP Group](#_heading=h.40ew0vw) 81

#### [Hình 4.30 Cấu hình các LAP phát Wifi cho WLAN](#_heading=h.2fk6b3p) 82

#### [Hình 4.31 Các PC kết nối wifi thành công](#_heading=h.upglbi) 83

#### [Hình 4.32 Tạo các Pool DHCP trên Server](#_heading=h.2szc72q) 84

#### [Hình 4.33 Tạo các Pool DHCP trên Server](#_heading=h.3s49zyc) 88

#### [Hình 4.34 Các PC lấy DHCPv4 và DHCPv6 thành công](#_heading=h.1nia2ey) 137

#### [Hình 4.35 Các VLAN ping với nhau bằng IPv4 thành công](#_heading=h.11si5id) 138

#### [Hình 4.36 Các VLAN ping với nhau bằng IPv6 thành công](#_heading=h.3ls5o66) 139

#### [Hình 4.37 Khách hàng truy cập được web](#_heading=h.302dr9l) 140

#### [Hình 4.38 Khách hàng không truy cập dịch vụ FTP](#_heading=h.1f7o1he) 141

#### [Hình 4.39 Khách hàng không thể Telnet/SSH đến các thiết bị trong công ti](#_heading=h.3z7bk57) . 142 [Hình 4.40 Khi ping đến OUTSIDE thì cho phép OUTSIDE reply](#_heading=h.2eclud0) 143

#### [Hình 4.41 Nhưng OUTSIDE không thể ping vào trong công ty](#_heading=h.thw4kt) 144

#### [Hình 4.42 Syslog Server ghi lại nhật ký đăng nhập vào các thiết bị](#_heading=h.4cmhg48) 145

#### [Hình 4.43 Cấu hình HSRP trên Distribution 1 ở trạng thái acitve](#_heading=h.3qwpj7n) 146

#### [Hình 4.44 Cấu hình HSRP trên Distribution 1 ở trạng thái stanby](#_heading=h.261ztfg) 147

#### [Hình 4.45 Khi Switch Distribution 1 hoạt động bình thường, nó sẽ chiếm](#_heading=h.l7a3n9) [quyền gửi gói tin](#_heading=h.l7a3n9) 148

#### [Hình 4.46 Khi Distribution 1 bị hư, Distribution 2 sẽ đứng lên chiếm quyền](#_heading=h.356xmb2) . 148 [Hình 4.47 Khi này các gói tin gửi đi sẽ đi qua Distribution 2](#_heading=h.1kc7wiv) 148

#### [Hình 4.48 Các thiết bị không dây kết nối wifi thành công](#_heading=h.ymfzma) 149

| [Hình 4.49](#_heading=h.3im3ia3) | [Thiết bị kết nối với WLAN nào thì sẽ nhận DHCP tương ứng](#_heading=h.3im3ia3) . . . | 150 |
| --- | --- | --- |
| [Hình 4.50](#_heading=h.2wwbldi) | [Port F0/1 mặc định của máy Lễ tân](#_heading=h.2wwbldi) . . . . . . . . . . . . . . . . . | 151 |
| [Hình 4.51](#_heading=h.1c1lvlb) | [Port F0/1 khi nối thiết bị khác](#_heading=h.1c1lvlb) . . . . . . . . . . . . . . . . . . . | 152 |
| [Hình 4.52](#_heading=h.qbtyoq) | [Phòng Kỹ thuật ở quận 7 có thể truy cập SSH vào các thiết bị ở](#_heading=h.qbtyoq) |  |

#### [quận 7](#_heading=h.qbtyoq) 152

#### [Hình 4.53 Phòng Kỹ thuật ở quận 7 có thể truy cập SSH vào các thiết bị ở](#_heading=h.49gfa85)

#### [Thủ Đức](#_heading=h.49gfa85) 153

#### [Hình 4.54 Phòng Kỹ thuật ở Thủ Đức có thể truy cập SSH vào các thiết bị ở](#_heading=h.2olpkfy)

#### [Thủ Đức](#_heading=h.2olpkfy) 153

#### [Hình 4.55 Phòng Kỹ thuật ở Thủ Đức không thể truy cập SSH vào các thiết](#_heading=h.13qzunr)

| [bị ở](#_heading=h.13qzunr) | [quận 7](#_heading=h.13qzunr) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 153 |
| --- | --- | --- |
| [Hình 4.56](#_heading=h.3nqndbk) | [Hai VLAN hai chi nhánh ping thành công](#_heading=h.3nqndbk) . . . . . . . . . . . . . | 154 |
| [Hình 4.57](#_heading=h.22vxnjd) | [Mạng VLAN đi qua tunnel](#_heading=h.22vxnjd) . . . . . . . . . . . . . . . . . . . . . | 154 |
| [Hình 4.58](#_heading=h.1h65qms) | [VLAN đi ra OUTSIDE thành công](#_heading=h.1h65qms) . . . . . . . . . . . . . . . . . | 154 |
| [Hình 4.59](#_heading=h.415t9al) | [Kiểm tra NAT trên R1](#_heading=h.415t9al) . . . . . . . . . . . . . . . . . . . . . . . | 155 |
| [Hình 4.60](#_heading=h.2gb3jie) | [Kiểm tra NAT trên R2](#_heading=h.2gb3jie) . . . . . . . . . . . . . . . . . . . . . . . | 155 |
| [Hình 4.61](#_heading=h.1ulbmlt) | [Kiểm tra NAT trên R3](#_heading=h.1ulbmlt) . . . . . . . . . . . . . . . . . . . . . . . | 156 |
| [Hình 4.62](#_heading=h.4ekz59m) | [Kiểm tra NAT trên R4](#_heading=h.4ekz59m) . . . . . . . . . . . . . . . . . . . . . . . | 156 |
| [Hình 4.63](#_heading=h.2tq9fhf) | [kiểm tra QoS của các traffic](#_heading=h.2tq9fhf) . . . . . . . . . . . . . . . . . . . . | 157 |
| [Hình 4.64](#_heading=h.n5rssn) | [kiểm tra QoS của các traffic](#_heading=h.n5rssn) . . . . . . . . . . . . . . . . . . . . | 158 |

**Danh sách bảng**

#### [Bảng 1.1 Các thiết bị được sử dụng trong mô hình](#_heading=h.2lfnejv) . . . . . . . . . . . . . . 3 [Bảng 3.1 Thông tin kết nối port trong hệ thống](#_heading=h.4i7ojhp) 20

| [Bảng 3.2](#_heading=h.3whwml4) | [Thông tin VLAN, interface VLAN trong hệ thống](#_heading=h.3whwml4) . . . . . . . . . | 22 |
| --- | --- | --- |
| [Bảng 3.3](#_heading=h.3as4poj) | [Thông tin thiết kế quy hoạch địa chỉ IP planning](#_heading=h.3as4poj) . . . . . . . . . . | 29 |

**TÓM TẮT**

Mô hình hệ thống mạng máy tính được thiết kế cho một Doanh nghiệp, cụ thể cho công ty du lịch có trụ sở chính ở TPHCM và hai chi nhánh, một tại Đà Nẵng và một tại Hà Nội. Thiết kế mạng được phân chia thành ba khu riêng biệt, với trụ sở chính bao gồm đầy đủ các phòng chức năng, trong khi hai chi nhánh khác chỉ có một số phòng chức năng cần thiết.

#### Doanh nghiệp có trụ sở chính ở thành phố Hồ Chí Minh bao gồm:

#### • Tầng 1 bao gồm khu lễ tân và nơi phục vụ khách hàng

#### • Tầng 2 bao gồm các phòng: phòng giám đốc, phó giám đốc, phòng hành chính.

#### • Tầng 3 bao gồm các phòng: phòng kinh doanh, phòng kế toán.

#### • Tầng 4 bao gồm các phòng: phòng nhân sự, phòng kỹ thuật, phòng marketing online.

#### Chi nhánh ở Đà Nẵng và Hà Nội giống nhau gồm có 2 tầng (1-2).

#### • Tầng 1 bao gồm các phòng: phòng tiếp tân, phòng kinh doanh, phòng kế toán

#### • Tầng 2 bao gồm các phòng: phòng kỹ thuật, phòng hành chính.

#### Khu vực Server được cấu hình IP tĩnh toàn bộ. Dựa vào quy mô văn phòng, nhóm em triển khai phân vùng địa chỉ IP thông qua kĩ thuật chia VLSM đảm bảo tiết kiệm và có khả năng mở rộng. Mỗi phòng chức năng sẽ gán với một vlan để dễ quản trị. Mọi client đều được cấp phát IPv4 và IPv6 động thông qua Switch Layer 3.

#### Mỗi chi nhánh sẽ được lắp đặt một Light Access Point tại các tầng trệt để phát mạng không dây. Các tầng chức năng sẽ được cấp các account được cấp riêng để kết nối tới mạng.

#### Toàn bộ Switch được bảo mật thông qua port security. Trên các Router, cài đặt các lớp bảo mật và cơ chế Access List kết hợp với Firewall. Áp dụng các phương pháp bảo mật đã được học để bảo vệ hệ thống của công ti du lịch.

**CHƯƠNG 1 - GIỚI THIỆU VÀ KHẢO SÁT**

* 1. **Giới thiệu đề tài**

Hệ thống mạng máy tính là yếu tố then chốt cho sự phát triển kinh doanh. Công nghệ ngày càng tiên tiến đòi hỏi hệ thống mạng máy tính phải đảm nhiệm nhiều chức năng như liên lạc, chia sẻ tài liệu, quản lý dữ liệu và tăng hiệu suất làm việc.

Bao gồm quá trình lên kế hoạch và triển khai một hệ thống mạng máy tính trong doanh nghiệp để kết nối các thiết bị, người dùng và tài nguyên mạng, và cung cấp một môi trường an toàn và bảo mật để truyền tải dữ liệu và thông tin giữa các thành viên trong doanh nghiệp. Một hệ thống mạng máy tính hiệu quả sẽ giúp tăng năng suất làm việc, tối ưu hóa tài nguyên mạng và giảm thiểu các rủi ro an ninh mạng. Quá trình thiết kế mạng máy tính cho doanh nghiệp thường bao gồm việc phân tích yêu cầu, thiết kế mô hình mạng, lựa chọn và cấu hình thiết bị mạng, triển khai và kiểm tra hệ thống.

Đề tài “Thiết kế và triển khai hệ thống mạng máy tính cho một Doanh nghiệp có trụ sở chính ở TPHCM và 2 chi nhánh (Một ở Đà Nẵng và một ở Hà Nội)” sẽ giúp doanh nghiệp xây dựng một hệ thống mạng máy tính hiệu quả, phù hợp với nhu cầu kinh doanh và bảo mật thông tin.

* 1. **Mô tả đề tài**

Một Doanh nghiệp có 1 trụ sở chính ở TPHCM và 2 chi nhánh bao gồm 1 chi nhánh nằm ở Đà Nẵng và 1 chi nhánh nằm ở Hà Nội.

Trụ sở chính ở TPHCM gồm có:

* Phòng ban tiếp tân và nơi phục vụ khách hàng.
* Phòng kinh doanh.
* Phòng kế toán.
* Phòng nhân sự.
* Phòng kỹ thuật.
* Phòng marketing online.
* Phòng hành chính, phòng giám đốc, phó giám đốc.

Hai chi nhánh ở Đà Nẵng và Hà Nội có các phòng tiếp tân, phòng hành chính, phòng kinh doanh, phòng kỹ thuật và nơi phục vụ khách hàng.

Thiết kế một mạng cho công ty để phân chia các nhóm làm việc thành các VLAN khác nhau. Tạo một website riêng cho công ti và cho phép nhân viên liên lạc với nhau qua email.

Cần phải đảm bảo những điều sau: Kết nối các máy tính thành một mạng nội bộ và chia sẻ dữ liệu. Bảo vệ an ninh và an toàn mạng. Thiết kế gọn gàng để đảm bảo tính thẩm mỹ, dễ dàng di chuyển, lắp đặt và bảo trì hệ thống. Có thể nâng cấp và thiết lập khi cần thiết bằng cách truy cập từ xa. Có thêm một Access Point cho khách sử dụng wifi công cộng, còn lại sẽ là mạng nội bộ.

Để đáp ứng các yêu cầu trên, nhóm em dùng Access Point để khách có thể kết nối wifi với độ bảo mật là PSK. Các phòng chức năng, nhóm em sẽ dùng cùng lúc mạng VLAN và WLAN. Nhóm em sẽ phân chia VLAN thành 20 VLAN tương ứng với 20 chức năng trong doanh nghiệp, bên cạnh đó nhóm em sẽ tạo thêm 3 VLAN để quản lý các Lightweight Access Point ở 3 trụ sở.

Nhóm em sẽ đặt một máy chủ DHCP và cấp một địa chỉ động cho các VALN này. Cấu hình mạng không dây với WPA2 Enterprise để bảo đảm tính bảo mật cho công ty. Ngoài ra, nhóm em còn dùng tường lửa để ngăn chặn truy cập internet bên ngoài vào mạng nội bộ. Access List cấu hình cho phép các host thuộc phòng kỹ thuật và Admin được phép telnet/SSH vào thiết bị Router, ngoài ra khách hàng ngoài công ty chỉ được phép sử dụng dịch vụ truy cập website. Trên các switch của các chi nhánh thông qua port kết nối đến switch Distribution sẽ được cấu hình DHCP Snooping để ngăn chặn tấn công DHCP.

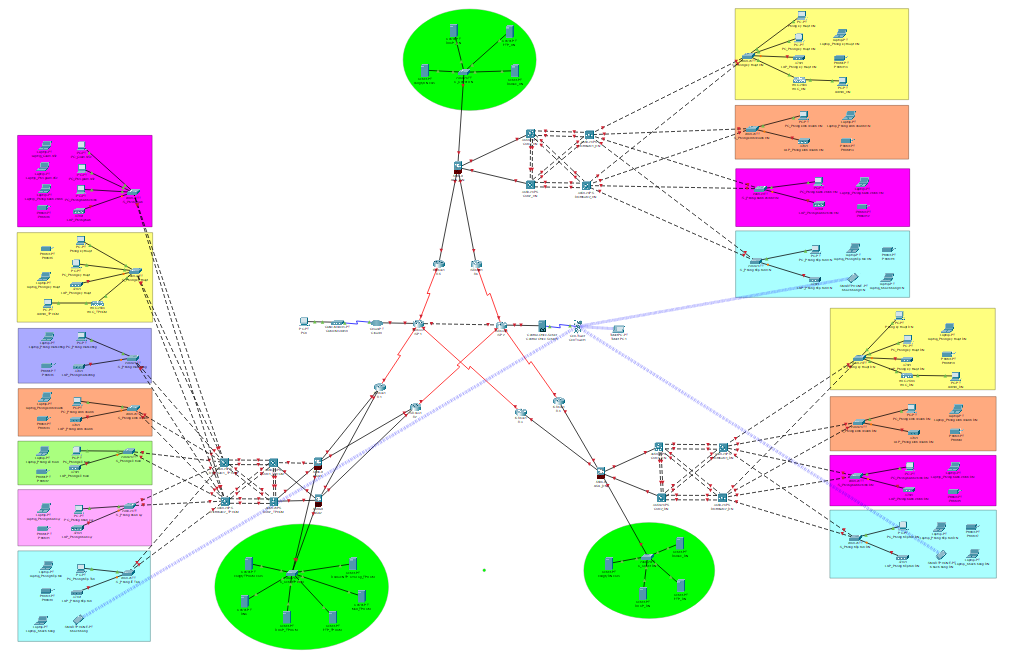
Các trụ sở sẽ được chia 10 IP cho VLAN lễ tân, 50 IP cho VLAN hành chính, 6 IP cho VLAN phó giám đốc, 6 IP cho VLAN giám đốc, 14 IP cho VLAN kế toán, 50 IP cho VLAN kinh doanh, 40 IP cho VLAN nhân sự, 20 IP cho VLAN kỹ thuật, 50 IP cho VLAN marketing, 10 IP cho VLAN lễ tân và 25 IP cho VLAN kinh doanh ở Đà Nẵng, 10 IP cho VLAN kỹ thuật ở Đà Nẵng, 20 IP cho VLAN hành chính Đà Nẵng, 10 IP cho VLAN lễ tân và 25 IP cho VLAN kinh doanh ở Hà Nội, 10 IP cho VLAN kỹ thuật ở Hà Nội, 20 IP cho VLAN hành chính Hà Nội, 10 IP cho vlan WLC\_TPHCM, 10 IP của WLC\_DN, 10 IP của WLC\_HN. Để bảo đảm đường truyền, nhóm em cấu hình thêm ethernet channel, spanning tree, HSRP để backup phòng khi các dây nối bị đứt sẽ có các dây khác dự phòng , đảm bảo gói tin luôn được truyền đi

* 1. **Khảo sát thực tế**

| STT | Thiết bị | Mã thiết bị | Số lượng | Giá tiền | Tổng |
| --- | --- | --- | --- | --- | --- |
| 1 | Router [link](https://netsystem.com.vn/router-cisco/) | ISR4221/K9 | 6 | 38.280.786 | 229684716 |
| 2 | Tường lửa ASA [link](https://netsystem.com.vn/firewall-cisco/cisco-asa5508k9.html) | 5508-K9 | 4 | 84.273.990 | 337095960 |
| 3 | Multilayer Switch [link](https://netsystem.com.vn/switch-cisco/switch-cisco-wsc365048tss.html) | WS-C3650-48TS-S | 12 | 86.100.000 | 1033200000 |
| 4 | Switch Access [link](https://netsystem.com.vn/switch-cisco/) | WS-C2960+24PC-S | 18 | 16.600.000 | 298800000 |
| 5 | Light weight Access Point [link](https://phatsongwifi.com/thiet-bi/thiet-bi-cong-nghe/thiet-bi-phat-song-wifi-cisco-3702i-c-k9.html) | 3702I-C-K9 | 15 | 12.700.000 | 190500000 |
| 6 | Wireless LAN Control [link](https://www.sieuthimaychu.vn/index.php/Thong_Tin_San_Pham/11676/Thiet-bi-Wifi-Cisco-2504-AIR-CT2504-25-K9) | AIR-CT2504-25-K9 | 3 | 56.827.000 | 170481000 |
| 7 | Server [link](https://vatgia.com/846/1278753/thong_so_ky_thuat/hp-blc3000-twr-2-ac-4-fan-full-ice-469500-b21-intel-2-0ghz-ram-1gb-hdd-120gb-1200w.html) | Server HP | 14 | 163.350.000 | 2286900000 |
| Tổng | 4546661676 VNĐ | | | | |

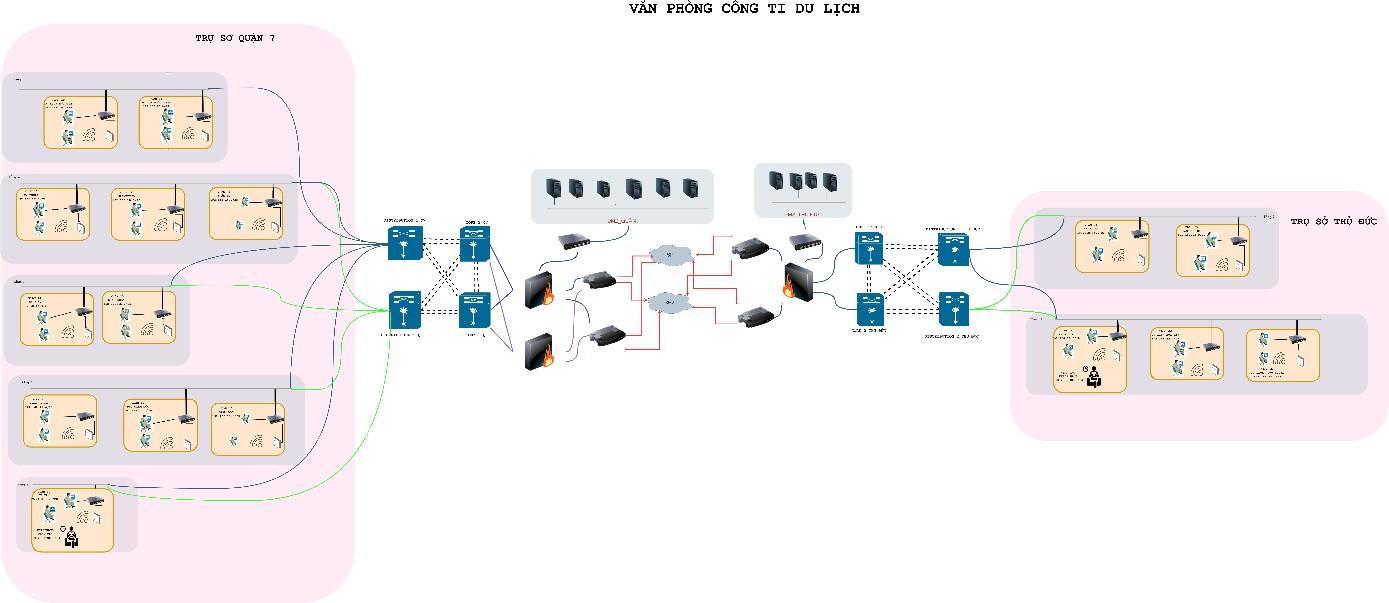
**CHƯƠNG 2 - MÔ HÌNH HỆ THỐNG**

* 1. **Sơ đồ luận lý**

****

#### Hình 2.1 Sơ đồ luận lý

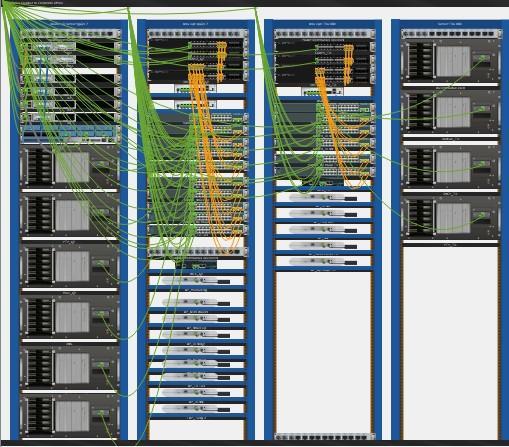
* 1. **Sơ đồ vật lý**



#### Hình 2.2 Sơ đồ vật lý

#### 

* 1. **Sơ đồ lắp đặt tủ Rack**



#### Hình 2.3 Sơ đồ tủ Rack

**CHƯƠNG 3 - THÔNG TIN CÀI ĐẶT CẤU HÌNH HỆ THỐNG**

* 1. **Thông tin kết nối port trong hệ thống**

Link bảng sheet: [Cisco command](https://docs.google.com/spreadsheets/d/1iLqWYop3Xt41jlRl28sLoc2psB6N3lT6g9EnR4xXKS0/edit?usp=sharing)

* 1. **Thông tin VLAN, Interface VLAN trong hệ thống**

Link sheet vlan: [Cisco command](https://docs.google.com/spreadsheets/d/1iLqWYop3Xt41jlRl28sLoc2psB6N3lT6g9EnR4xXKS0/edit?usp=sharing)

* 1. **Thông tin thiết kế quy hoạch địa chỉ IP Planning**

| **STT** | **DEVICES** | **INTER FACE** | **IPv4 AD- DRESS** | **Mask** | **NET** | **IPV6** |
| --- | --- | --- | --- | --- | --- | --- |
| I/QUẬN 7 | | | | | | |
| 1 | ASA1\_Q7 | G1/1 | 172.16.0.2 | /30 | 172.16.0.0 | 2001:db8:acad:172::2/64 |
| 2 | ASA1\_Q7 | G1/2 | 172.16.0.6 | /30 | 172.16.0.4 | 2001:db8:acad:173::2/64 |
| 3 | ASA1\_Q7 | G1/3 | 10.10.10.1 | /28 | 10.10.10.0 | 2001:DB8:BADC:A::1/64 |
| 4 | ASA1\_Q7 | G1/4 | 172.16.0.9 | /30 | 172.16.0.8 | 2001:db8:acad:174::1/64 |
| 5 | ASA1\_Q7 | G1/5 | 172.16.0.13 | /30 | 172.16.0.12 | 2001:db8:acad:175::1/64 |
| 6 | ASA2\_Q7 | G1/1 | 172.16.0.78 | /30 | 172.16.0.76 | 2001:db8:acad:178::2/64 |
| 7 | ASA2\_Q7 | G1/2 | 172.16.0.74 | /30 | 172.16.0.72 | 2001:db8:acad:177::2/64 |
| 8 | ASA2\_Q7 | G1/3 | 10.10.10.1 | /28 | 10.10.10.0 | 2001:DB8:BADC:A::1/64 |
| 9 | ASA2\_Q7 | G1/4 | 172.16.0.81 | /30 | 172.16.0.80 | 2001:db8:acad:180::1/64 |
| 10 | ASA2\_Q7 | G1/5 | 172.16.0.85 | /30 | 172.16.0.84 | 2001:db8:acad:179::1/64 |
| 11 | CORE1\_Q7 | G1/0/1 | 172.16.0.10 | /30 | 172.16.0.8 | 2001:db8:acad:174::2/64 |
| 12 | CORE1\_Q7 | G1/0/2 | 172.16.0.86 | /30 | 172.16.0.84 | 2001:db8:acad:179::2/64 |
| 13 | CORE1\_Q7 | G1/0/23-  24(Port 1) | 172.16.0.65 | /30 | 172.16.0.64 | 2001:db8:acad:185::1/64 |

| **STT** | **DEVICES** | **INTER FACE** | **IPv4 AD- DRESS** | **Mask** | **NET** | **IPV6** |
| --- | --- | --- | --- | --- | --- | --- |
| 14 | CORE1\_Q7 | G1/0/21- 22  (Port 2) | 172.16.0.17 | /30 | 172.16.0.16 | 2001:db8:acad:181::1/64 |
| 15 | CORE1\_Q7 | G1/0/19- 20  (Port 3) | 172.16.0.21 | /30 | 172.16.0.20 | 2001:db8:acad:182::1/64 |
| 16 | CORE2\_Q7 | G1/0/1 | 172.16.0.82 | /30 | 172.16.0.80 | 2001:db8:acad:180::2/64 |
| 17 | CORE2\_Q7 | G1/0/2 | 172.16.0.14 | /30 | 172.16.0.12 | 2001:db8:acad:175::2/64 |
| 18 | CORE2\_Q7 | G1/0/23-  24(Port 1) | 172.16.0.66 | /30 | 172.16.0.64 | 2001:db8:acad:185::2/64 |
| 19 | CORE2\_Q7 | G1/0/21- 22  (Port 2) | 172.16.0.29 | /30 | 172.16.0.28 | 2001:db8:acad:184::1/64 |
| 20 | CORE2\_Q7 | G1/0/19- 20  (Port 3) | 172.16.0.25 | /30 | 172.16.0.24 | 2001:db8:acad:183::1/64 |
| 21 | Distributed 1\_Q7 | G1/0/21- 22  (Port 2) | 172.16.0.18 | /30 | 172.16.0.16 | 2001:db8:acad:181::2/64 |

| **STT** | **DEVICES** | **INTER FACE** | **IPv4 AD- DRESS** | **Mask** | **NET** | **IPV6** |
| --- | --- | --- | --- | --- | --- | --- |
| 22 | Distributed 1\_Q7 | G1/0/19- 20  (Port 3) | 172.16.0.26 | /30 | 172.16.0.24 | 2001:db8:acad:183::2/64 |
| 23 | Distributed 1\_Q7 | G1/0/1- 9 | Trunking/Passive Interface | | | |
| 24 | Distributed 2\_Q7 | G1/0/21- 22  (Port 2) | 172.16.0.30 | /30 | 172.16.0.28 | 2001:db8:acad:184::2/64 |
| 25 | Distributed 2\_Q7 | G1/0/19- 20  (Port 3) | 172.16.0.22 | /30 | 172.16.0.20 | 2001:db8:acad:182::2/64 |
| 26 | Distributed 2\_Q7 | G1/0/1- 9 | Trunking/Passive Interface | | | |
| II/THỦ ĐỨC | | | | | | |
| 1 | ASA\_TD | G1/1 | 172.16.0.34 | /30 | 172.16.0.32 | 2001:db8:acad:186::2/64 |
| 2 | ASA\_TD | G1/2 | 172.16.0.38 | /30 | 172.16.0.36 | 2001:db8:acad:187::2/64 |
| 3 | ASA\_TD | G1/3 | 10.10.11.1 | /28 | 10.10.11.0 | 2001:DB8:BADC:B::1/64 |
| 4 | ASA\_TD | G1/4 | 172.16.0.41 | /30 | 172.16.0.40 | 2001:db8:acad:188::1/64 |
| 5 | ASA\_TD | G1/5 | 172.16.0.45 | /30 | 172.16.0.44 | 2001:db8:acad:189::1/64 |

| **STT** | **DEVICES** | **INTER FACE** | **IPv4 AD- DRESS** | **Mask** | **NET** | **IPV6** |
| --- | --- | --- | --- | --- | --- | --- |
| 6 | CORE1\_TD | G1/0/1 | 172.16.0.42 | /30 | 172.16.0.40 | 2001:db8:acad:188::2/64 |
| 7 | CORE1\_TD | G1/0/23-  24(Port 1) | 172.16.0.69 | /30 | 172.16.0.68 | 2001:db8:acad:194::1/64 |
| 8 | CORE1\_TD | G1/0/21- 22  (Port 2) | 172.16.0.49 | /30 | 172.16.0.48 | 2001:db8:acad:190::1/64 |
| 9 | CORE1\_TD | G1/0/19- 20  (Port 3) | 172.16.0.53 | /30 | 172.16.0.52 | 2001:db8:acad:191::1/64 |
| 10 | CORE2\_TD | G1/0/1 | 172.16.0.46 | /30 | 172.16.0.44 | 2001:db8:acad:189::2/64 |
| 11 | CORE2\_TD | G1/0/23-  24(Port 1) | 172.16.0.70 | /30 | 172.16.0.68 | 2001:db8:acad:194::2/64 |
| 12 | CORE2\_TD | G1/0/21- 22  (Port 2) | 172.16.0.61 | /30 | 172.16.0.60 | 2001:db8:acad:193::1/64 |
| 13 | CORE2\_TD | G1/0/19- 20  (Port 3) | 172.16.0.57 | /30 | 172.16.0.56 | 2001:db8:acad:192::1/64 |

| **STT** | **DEVICES** | **INTER FACE** | **IPv4 AD- DRESS** | **Mask** | **NET** | **IPV6** |
| --- | --- | --- | --- | --- | --- | --- |
| 14 | Distributed 1\_TD | G1/0/21- 22  (Port 2) | 172.16.0.50 | /30 | 172.16.0.48 | 2001:db8:acad:190::2/64 |
| 15 | Distributed 1\_TD | G1/0/19- 20  (Port 3) | 172.16.0.58 | /30 | 172.16.0.56 | 2001:db8:acad:192::1/64 |
| 16 | Distributed 1\_TD | G1/0/1- 5 | Trunking/Passive Interface | | | |
| 17 | Distributed 2\_TD | G1/0/21- 22  (Port 2) | 172.16.0.62 | /30 | 172.16.0.60 | 2001:db8:acad:193::2/64 |
| 18 | Distributed 2\_TD | G1/0/19- 20  (Port 3) | 172.16.0.54 | /30 | 172.16.0.52 | 2001:db8:acad:191::2/64 |
| 19 | Distributed 2\_TD | G1/0/1- 5 | Trunking/Passive Interface | | | |
| III/ROUTER BIÊN VÀ INTERNET | | | | | | |
| 1 | ISP1 | S0/1/0 | 209.165  .100.1 | /30 | 209.165  .100.0 | 2001:db8:acad:209::1/64 |
| S0/1/1 | 209.165  .100.9 | /30 | 209.165  .100.0 | 2001:db8:acad:210::1/64 |

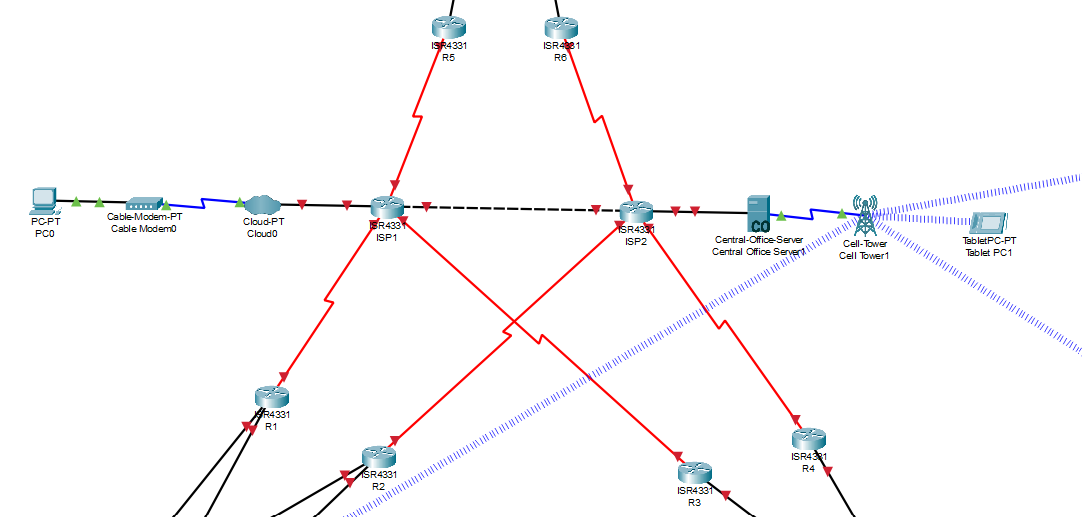
| **STT** | **DEVICES** | **INTER FACE** | **IPv4 AD- DRESS** | **Mask** | **NET** | **IPV6** |
| --- | --- | --- | --- | --- | --- | --- |
| 2 | ISP2 | S0/1/0 | 209.165  .100.5 | /30 | 209.165  .100.0 | 2001:db8:acad:211::1/64 |
| S0/1/1 | 209.165  .100.13 | /30 | 209.165  .100.0 | 2001:db8:acad:212::1/64 |
| 3 | R1 | G0/0/0 | 172.16.0.1 | /30 | 172.16.0.0 | 2001:db8:acad:172::1/64 |
| G0/0/1 | 172.16.0.73 | /30 | 172.16.0.72 | 2001:db8:acad:177::1/64 |
| S0/1/0 | 209.165  .100.2 | /30 | 209.165  .100.0 | 2001:db8:acad:209::2/64 |
| 4 | R2 | G0/0/0 | 172.16.0.77 | /30 | 172.16.0.76 | 2001:db8:acad:178::1/64 |
| G0/0/1 | 172.16.0.5 | /30 | 172.16.0.4 | 2001:db8:acad:173::1/64 |
| S0/1/0 | 209.165  .100.6 | /30 | 209.165  .100.0 | 2001:db8:acad:211::2/64 |
| 5 | R3 | G0/0/0 | 172.16.0.33 | /30 | 172.16.0.32 | 2001:db8:acad:186::1/64 |
| S0/1/0 | 209.165  .100.10 | /30 | 209.165  .100.0 | 2001:db8:acad:210::2/64 |
| 6 | R4 | G0/0/0 | 172.16.0.37 | /30 | 172.16.0.36 | 2001:db8:acad:187::1/64 |
| S0/1/0 | 209.165.  100.14 | /30 | 209.165  .100.0 | 2001:db8:acad:212::2/64 |

| **STT** | **DEVICES** | **INTER FACE** | **IPv4 AD- DRESS** | **Mask** | **NET** | **IPV6** |
| --- | --- | --- | --- | --- | --- | --- |

#### Bảng 3.3 Thông tin thiết kế quy hoạch địa chỉ IP planning

**CHƯƠNG 4 - CẤU HÌNH HẠ TẦNG**

* 1. **Cấu hình Interface**
     1. ***Khu vực Router biên và Internet***

******

#### Hình 4.1 Khu vực Router biên và Internet

* + - 1. **Router**

**R1**

*hostname R1*

*interface G0/0/0*

*ip address 172.16.0.89 255.255.255.252*

*ipv6 address 2001:db8:acad:172::1/64*

*ip nat in*

*no shutdown*

*interface G0/0/1*

*ip address 172.16.0.73 255.255.255.252*

*ipv6 address 2001:db8:acad:177::1/64*

*ip nat in*

*no shutdown*

*interface S0/1/0*

*ip address 209.165.100.2 255.255.255.252*

*ipv6 address 2001:db8:acad:209::2/64*

*ip nat out*

*clock rate 2000000*

*no shutdown*

*interface S0/1/1*

*ip address 209.165.100.25 255.255.255.252*

*ipv6 address 2001:db8:acad:226::2/64*

*ip nat out*

*no shutdown*

*interface Tunnel 1*

*ip address 192.168.1.1 255.255.255.252*

*tunnel mode gre ip*

*tunnel source S0/1/0*

*tunnel destination 209.165.100.10*

*no shutdown*

*interface Tunnel 2*

*ip address 192.168.1.5 255.255.255.252*

*tunnel mode gre ip*

*tunnel source S0/1/1*

*tunnel destination 209.165.100.18*

*no shutdown*

**b.Router R2**

*hostname R2*

*interface G0/0/0*

*ip address 172.16.0.5 255.255.255.252*

*ipv6 address 2001:db8:acad:173::1/64*

*ip nat in*

*no shutdown*

*interface G0/0/1*

*ip address 172.16.0.77 255.255.255.252*

*ipv6 address 2001:db8:acad:178::1/64*

*ip nat in*

*no shutdown*

*interface S0/1/0*

*ip address 209.165.100.6 255.255.255.252*

*ipv6 address 2001:db8:acad:211::2/64*

*ip nat out*

*clock rate 2000000*

*no shutdown*

*interface S0/1/1*

*ip address 209.165.100.29 255.255.255.252*

*ipv6 address 2001:db8:acad:225::2/64*

*ip nat out*

*no shutdown*

*interface Tunnel 1*

*ip address 192.168.2.1 255.255.255.252*

*tunnel mode gre ip*

*tunnel source S0/1/0*

*tunnel destination 209.165.100.14*

*no shutdown*

*interface Tunnel 2*

*ip address 192.168.2.5 255.255.255.252*

*tunnel mode gre ip*

*tunnel source S0/1/1*

*tunnel destination 209.165.100.22*

*no shutdown*

**c.Router R3**

*hostname R3*

*interface G0/0/0*

*ip address 172.16.0.33 255.255.255.252*

*ipv6 address 2001:db8:acad:186::1/64*

*ip nat in*

*no shutdown*

*interface S0/1/0*

*ip address 209.165.100.10 255.255.255.252*

*ipv6 address 2001:db8:acad:210::2/64*

*ip nat out*

*ip ospf 1 area 0*

*no shutdown*

*interface Tunnel 1*

*ip address 192.168.1.2 255.255.255.252*

*tunnel mode gre ip*

*tunnel source S0/1/0*

*tunnel destination 209.165.100.2*

*no shutdown*

**d.Router R4**

*hostname R4*

*interface G0/0/0*

*ip address 172.16.0.37 255.255.255.252*

*ipv6 address 2001:db8:acad:187::1/64*

*ip nat in*

*no shutdown*

*interface S0/1/0*

*ip address 209.165.100.14 255.255.255.252*

*ipv6 address 2001:db8:acad:212::2/64*

*ip nat out*

*clock rate 2000000*

*no shutdown*

*interface Tunnel 1*

*ip address 192.168.2.2 255.255.255.252*

*tunnel mode gre ip*

*tunnel source S0/1/0*

*tunnel destination 209.165.100.6*

*no shutdown*

**Router R5**

*hostname R5*

*interface G0/0/0*

*ip address 172.16.0.93 255.255.255.252*

*ipv6 address 2001:db8:acad:217::1/64*

*ip nat in*

*no shutdown*

*interface S0/1/0*

*ip address 209.165.100.18 255.255.255.252*

*ipv6 address 2001:db8:acad:213::2/64*

*ip nat out*

*ip ospf 2 area 1*

*no shutdown*

*interface Tunnel 1*

*ip address 192.168.1.6 255.255.255.252*

*tunnel mode gre ip*

*tunnel source S0/1/0*

*tunnel destination 209.165.100.25*

*no shutdown*

**Router R6**

*hostname R6*

*interface G0/0/0*

*ip address 172.16.0.97 255.255.255.252*

*ipv6 address 2001:db8:acad:218::1/64*

*ip nat in*

*no shutdown*

*interface S0/1/0*

*ip address 209.165.100.22 255.255.255.252*

*ipv6 address 2001:db8:acad:214::2/64*

*ip nat out*

*clock rate 2000000*

*no shutdown*

*interface Tunnel 1*

*ip address 192.168.2.6 255.255.255.252*

*tunnel mode gre ip*

*tunnel source S0/1/0*

*tunnel destination 209.165.100.29*

*no shutdown*

**e.Router ISP 1**

*hostname ISP1*

*interface G0/0/0*

*ip address 209.100.100.100 255.255.255.0*

*ipv6 address 2001:db8:acad:227::1/64*

*no shutdown*

*interface G0/0/1*

*ip address 209.165.200.100 255.255.255.0*

*ipv6 address 2001:db8:acad:228::1/64*

*ip ospf priority 0*

*no shutdown*

*interface S0/1/0*

*ip address 209.165.100.1 255.255.255.252*

*ipv6 address 2001:db8:acad:209::1/64*

*no shutdown*

*interface S0/1/1*

*ip address 209.165.100.9 255.255.255.252*

*ipv6 address 2001:db8:acad:210::1/64*

*no shutdown*

*interface S0/2/0*

*ip address 209.165.100.21 255.255.255.252*

*ipv6 address 2001:db8:acad:214::1/64*

*no shutdown*

*interface S0/2/1*

*ip address 209.165.100.30 255.255.255.252*

*ipv6 address 2001:db8:acad:225::1/64*

*no shutdown*

**f.Router ISP 2**

*hostname ISP2*

*interface G0/0/0*

*ip address 209.100.100.200 255.255.255.0*

*ipv6 address 2001:db8:acad:227::2/64*

*no shutdown*

*interface G0/0/1*

*ip address 209.100.200.200 255.255.255.0*

*ipv6 address 2001:db8:acad:229::1/64*

*no shutdown*

*interface S0/1/0*

*ip address 209.165.100.5 255.255.255.252*

*ipv6 address 2001:db8:acad:211::1/64*

*no shutdown*

*interface S0/1/1*

*ip address 209.165.100.13 255.255.255.252*

*ipv6 address 2001:db8:acad:212::1/64*

*no shutdown*

*interface S0/2/0*

*ip address 209.165.100.17 255.255.255.252*

*ipv6 address 2001:db8:acad:213::1/64*

*no shutdown*

*interface S0/2/1*

*ip address 209.165.100.26 255.255.255.252*

*ipv6 address 2001:db8:acad:226::1/64*

*no shutdown*

* + 1. ***Khu vực TPHCM***
       1. **Tường lửa ASA 1**

*hostname ASA1*

*interface G1/1*

*nameif INSIDE1*

*security-level 100*

*ip address 172.16.0.9 255.255.255.252*

*ipv6 address 2001:db8:acad:174::1/64*

*no shutdown*

*interface G1/2*

*nameif INSIDE2*

*security-level 100*

*ip address 172.16.0.13 255.255.255.252*

*ipv6 address 2001:db8:acad:175::1/64*

*no shutdown*

*interface G1/3*

*nameif DMZ*

*security-level 60*

*ip address 10.10.10.1 255.255.255.240*

*ipv6 address 2001:db8:badc:a::1/64*

*no shutdown*

*interface G1/4*

*nameif OUTSIDE1*

*security-level 20*

*ip address 172.16.0.90 255.255.255.252*

*ipv6 address 2001:db8:acad:172::2/64*

*no shutdown*

*interface G1/5*

*nameif OUTSIDE2*

*security-level 20*

*ip address 172.16.0.6 255.255.255.252*

*ipv6 address 2001:db8:acad:173::2/64*

*no shutdown*

* + - 1. **Tường lửa ASA 2**

*hostname ASA2*

*interface G1/1*

*nameif INSIDE1*

*security-level 100*

*ip address 172.16.0.81 255.255.255.252*

*ipv6 address 2001:db8:acad:180::1/64*

*no shutdown*

*interface G1/2*

*nameif INSIDE2*

*security-level 100*

*ip address 172.16.0.85 255.255.255.252*

*ipv6 address 2001:db8:acad:179::1/64*

*no shutdown*

*interface G1/3*

*nameif DMZ*

*security-level 60*

*ip address 10.10.10.1 255.255.255.240*

*ipv6 address 2001:db8:badc:a::1/64*

*no shutdown*

*interface G1/4*

*nameif OUTSIDE1*

*security-level 20*

*ip address 172.16.0.74 255.255.255.252*

*ipv6 address 2001:db8:acad:177::2/64*

*no shutdown*

*interface G1/5*

*nameif OUTSIDE2*

*security-level 20*

*ip address 172.16.0.78 255.255.255.252*

*ipv6 address 2001:db8:acad:178::2/64*

*no shutdown*

* + - 1. **Switch Core 1**

*hostname CORE1\_TPHCM*

*interface G1/0/1*

*no sw*

*ip address 172.16.0.10 255.255.255.252*

*ipv6 address 2001:db8:acad:174::2/64*

*no shutdown*

*interface G1/0/2*

*no sw*

*ip address 172.16.0.86 255.255.255.252*

*ipv6 address 2001:db8:acad:179::2/64*

*no shutdown*

* + - 1. **Switch Core 2**

*hostname CORE2\_TPHCM*

*interface G1/0/1*

*no sw*

*ip address 172.16.0.82 255.255.255.252*

*ipv6 address 2001:db8:acad:180::2/64*

*no shutdown*

*interface G1/0/2*

*no sw*

*ip address 172.16.0.14 255.255.255.252*

*ipv6 address 2001:db8:acad:175::2/64*

*no shutdown*

* + 1. ***Khu vực Đà Nẵng***
       1. **Tường lửa ASA\_DN**

*hostname ASA\_DN*

*interface G1/1*

*nameif INSIDE\_DN1*

*security-level 100*

*ip address 172.16.0.41 255.255.255.252*

*ipv6 address 2001:db8:acad:188::1/64*

*no shutdown*

*interface G1/2*

*nameif INSIDE\_DN2*

*security-level 100*

*ip address 172.16.0.45 255.255.255.252*

*ipv6 address 2001:db8:acad:189::1/64*

*no shutdown*

*interface G1/3*

*nameif OUTSIDE\_DN1*

*security-level 40*

*ip address 172.16.0.34 255.255.255.252*

*ipv6 address 2001:db8:acad:186::2/64*

*no shutdown*

*interface G1/4*

*nameif OUTSIDE\_DN2*

*security-level 40*

*ip address 172.16.0.38 255.255.255.252*

*ipv6 address 2001:db8:acad:187::2/64*

*no shutdown*

*interface G1/5*

*nameif DMZ\_DN*

*security-level 60*

*ip address 10.10.11.1 255.255.255.240*

*ipv6 address 2001:db8:badc:b::1/64*

*no shutdown*

* + - 1. **Switch Core 1**

*hostname CORE1\_DN*

*interface G1/0/1*

*no sw*

*ip address 172.16.0.42 255.255.255.252*

*ipv6 address 2001:db8:acad:188::2/64*

*no shutdown*

* + - 1. **Switch Core 2**

*hostname CORE2\_DN*

*interface G1/0/1*

*no sw*

*ip address 172.16.0.46 255.255.255.252*

*ipv6 address 2001:db8:acad:189::2/64*

*no shutdown*

* + 1. ***Khu vực Hà Nội***
       1. **Tường lửa ASA\_HN**

*hostname ASA\_HN*

*interface G1/1*

*nameif INSIDE\_HN1*

*security-level 100*

*ip address 172.16.0.101 255.255.255.252*

*ipv6 address 2001:db8:acad:215::1/64*

*no shutdown*

*interface G1/2*

*nameif INSIDE\_HN2*

*security-level 100*

*ip address 172.16.0.105 255.255.255.252*

*ipv6 address 2001:db8:acad:216::1/64*

*no shutdown*

*interface G1/3*

*nameif OUTSIDE\_HN1*

*security-level 40*

*ip address 172.16.0.94 255.255.255.252*

*ipv6 address 2001:db8:acad:217::2/64*

*no shutdown*

*interface G1/4*

*nameif OUTSIDE\_HN2*

*security-level 40*

*ip address 172.16.0.98 255.255.255.252*

*ipv6 address 2001:db8:acad:218::2/64*

*no shutdown*

*interface G1/5*

*nameif DMZ\_HN*

*security-level 60*

*ip address 10.10.12.1 255.255.255.240*

*ipv6 address 2001:db8:badc:c::1/64*

*no shutdown*

* + - 1. **Switch Core 1**

*hostname CORE1\_HN*

*interface G1/0/1*

*no sw*

*ip address 172.16.0.102 255.255.255.252*

*ipv6 address 2001:db8:acad:215::2/64*

*no shutdown*

* + - 1. **Switch Core 2**

*hostname CORE2\_HN*

*interface G1/0/1*

*no sw*

*ip address 172.16.0.106 255.255.255.252*

*ipv6 address 2001:db8:acad:216::2/64*

*no shutdown*

## Định tuyến động IPv4 và IPv6

#### Để các Router và Switch có thể gửi gói tin cho nhau, chúng em sẽ sử dụng hai loại định tuyến động là OSPF và EIGRP.

### *Router biên và Internet*

**Định tuyến IPv4**

#### ∇ Router ISP 1

*router eigrp 10*

*passive-interface G0/0/1*

*network 209.165.100.0 0.0.0.3*

*network 209.165.100.8 0.0.0.3*

*network 209.165.100.16 0.0.0.3*

*network 209.165.200.0*

*network 209.100.100.0*

#### ∇ Router ISP 2

*router eigrp 10*

*passive-interface G0/0/1*

*network 209.165.100.4 0.0.0.3*

*network 209.165.100.12 0.0.0.3*

*network 209.165.100.20 0.0.0.3*

*network 209.100.200.0*

*network 209.100.100.0*

#### ∇ Router R1

*ip routing*

*router eigrp 10*

*network 172.16.0.72 0.0.0.3*

*network 172.16.0.88 0.0.0.3*

*network 209.165.100.0 0.0.0.3*

*network 209.165.100.24 0.0.0.3*

*redistribute static metric 1000000 10 255 1 1500*

*exit*

*ip route 192.168.19.0 255.255.255.0 192.168.1.2*

*ip route 192.168.20.0 255.255.255.0 192.168.1.2*

*ip route 192.168.21.0 255.255.255.0 192.168.1.2*

*ip route 192.168.22.0 255.255.255.0 192.168.1.2*

*ip route 200.200.150.0 255.255.255.0 192.168.1.2*

*ip route 10.10.11.0 255.255.255.240 192.168.1.2*

*ip route 172.16.0.32 255.255.255.252 192.168.1.2*

*ip route 172.16.0.40 255.255.255.252 192.168.1.2*

*ip route 172.16.0.44 255.255.255.252 192.168.1.2*

*ip route 172.16.0.48 255.255.255.252 192.168.1.2*

*ip route 172.16.0.52 255.255.255.252 192.168.1.2*

*ip route 172.16.0.56 255.255.255.252 192.168.1.2*

*ip route 172.16.0.60 255.255.255.252 192.168.1.2*

*ip route 192.168.23.0 255.255.255.0 192.168.1.6*

*ip route 192.168.24.0 255.255.255.0 192.168.1.6*

*ip route 192.168.25.0 255.255.255.0 192.168.1.6*

*ip route 192.168.26.0 255.255.255.0 192.168.1.6*

*ip route 200.200.200.0 255.255.255.0 192.168.1.6*

*ip route 10.10.12.0 255.255.255.240 192.168.1.6*

*ip route 172.16.0.92 255.255.255.252 192.168.1.6*

*ip route 172.16.0.100 255.255.255.252 192.168.1.6*

*ip route 172.16.0.104 255.255.255.252 192.168.1.6*

*ip route 172.16.0.112 255.255.255.252 192.168.1.6*

*ip route 172.16.0.116 255.255.255.252 192.168.1.6*

*ip route 172.16.0.120 255.255.255.252 192.168.1.6*

*ip route 172.16.0.124 255.255.255.252 192.168.1.6*

#### ∇ Router R2

*ip routing*

*router eigrp 10*

*network 172.16.0.4 0.0.0.3*

*network 172.16.0.76 0.0.0.3*

*network 209.165.100.4 0.0.0.3*

*network 209.165.100.28 0.0.0.3*

*redistribute static metric 1000000 10 255 1 1500*

*exit*

*ip route 192.168.19.0 255.255.255.0 192.168.2.2*

*ip route 192.168.20.0 255.255.255.0 192.168.2.2*

*ip route 192.168.21.0 255.255.255.0 192.168.2.2*

*ip route 192.168.22.0 255.255.255.0 192.168.2.2*

*ip route 200.200.150.0 255.255.255.0 192.168.2.2*

*ip route 10.10.11.0 255.255.255.240 192.168.2.2*

*ip route 172.16.0.32 255.255.255.252 192.168.2.2*

*ip route 172.16.0.40 255.255.255.252 192.168.2.2*

*ip route 172.16.0.44 255.255.255.252 192.168.2.2*

*ip route 172.16.0.48 255.255.255.252 192.168.2.2*

*ip route 172.16.0.52 255.255.255.252 192.168.2.2*

*ip route 172.16.0.56 255.255.255.252 192.168.2.2*

*ip route 172.16.0.60 255.255.255.252 192.168.2.2*

*ip route 192.168.23.0 255.255.255.0 192.168.2.6*

*ip route 192.168.24.0 255.255.255.0 192.168.2.6*

*ip route 192.168.25.0 255.255.255.0 192.168.2.6*

*ip route 192.168.26.0 255.255.255.0 192.168.2.6*

*ip route 200.200.200.0 255.255.255.0 192.168.2.6*

*ip route 10.10.12.0 255.255.255.240 192.168.2.6*

*ip route 172.16.0.92 255.255.255.252 192.168.2.6*

*ip route 172.16.0.100 255.255.255.252 192.168.2.6*

*ip route 172.16.0.104 255.255.255.252 192.168.2.6*

*ip route 172.16.0.112 255.255.255.252 192.168.2.6*

*ip route 172.16.0.116 255.255.255.252 192.168.2.6*

*ip route 172.16.0.120 255.255.255.252 192.168.2.6*

*ip route 172.16.0.124 255.255.255.252 192.168.2.6*

#### ∇ Router R3

*ip routing*

*router eigrp 10*

*network 172.16.0.32 0.0.0.3*

*network 209.165.100.8 0.0.0.3*

*redistribute static metric 1000000 10 255 1 1500*

*exit*

*ip route 192.168.10.0 255.255.255.0 192.168.1.1*

*ip route 192.168.11.0 255.255.255.0 192.168.1.1*

*ip route 192.168.12.0 255.255.255.0 192.168.1.1*

*ip route 192.168.13.0 255.255.255.0 192.168.1.1*

*ip route 192.168.14.0 255.255.255.0 192.168.1.1*

*ip route 192.168.15.0 255.255.255.0 192.168.1.1*

*ip route 192.168.16.0 255.255.255.0 192.168.1.1*

*ip route 192.168.17.0 255.255.255.0 192.168.1.1*

*ip route 192.168.18.0 255.255.255.0 192.168.1.1*

*ip route 200.200.100.0 255.255.255.0 192.168.1.1*

*ip route 10.10.10.0 255.255.255.240 192.168.1.1*

#### ∇ Router R4

*ip routing*

*router eigrp 10*

*network 172.16.0.36 0.0.0.3*

*network 209.165.100.12 0.0.0.3*

*redistribute static metric 1000000 10 255 1 1500*

*exit*

*ip route 192.168.10.0 255.255.255.0 192.168.2.1*

*ip route 192.168.11.0 255.255.255.0 192.168.2.1*

*ip route 192.168.12.0 255.255.255.0 192.168.2.1*

*ip route 192.168.13.0 255.255.255.0 192.168.2.1*

*ip route 192.168.14.0 255.255.255.0 192.168.2.1*

*ip route 192.168.15.0 255.255.255.0 192.168.2.1*

*ip route 192.168.16.0 255.255.255.0 192.168.2.1*

*ip route 192.168.17.0 255.255.255.0 192.168.2.1*

*ip route 192.168.18.0 255.255.255.0 192.168.2.1*

*ip route 200.200.100.0 255.255.255.0 192.168.2.1*

*ip route 10.10.10.0 255.255.255.240 192.168.2.1*

#### ∇ Router R5

*ip routing*

*router eigrp 10*

*network 172.16.0.92 0.0.0.3*

*network 209.165.100.16 0.0.0.3*

*redistribute static metric 1000000 10 255 1 1500*

*exit*

*ip route 192.168.10.0 255.255.255.0 192.168.1.5*

*ip route 192.168.11.0 255.255.255.0 192.168.1.5*

*ip route 192.168.12.0 255.255.255.0 192.168.1.5*

*ip route 192.168.13.0 255.255.255.0 192.168.1.5*

*ip route 192.168.14.0 255.255.255.0 192.168.1.5*

*ip route 192.168.15.0 255.255.255.0 192.168.1.5*

*ip route 192.168.16.0 255.255.255.0 192.168.1.5*

*ip route 192.168.17.0 255.255.255.0 192.168.1.5*

*ip route 192.168.18.0 255.255.255.0 192.168.1.5*

*ip route 200.200.100.0 255.255.255.0 192.168.1.5*

*ip route 10.10.10.0 255.255.255.240 192.168.1.5*

#### Router R6

*ip routing*

*router eigrp 10*

*network 172.16.0.96 0.0.0.3*

*network 209.165.100.20 0.0.0.3*

*redistribute static metric 1000000 10 255 1 1500*

*exit*

*ip route 192.168.10.0 255.255.255.0 192.168.2.5*

*ip route 192.168.11.0 255.255.255.0 192.168.2.5*

*ip route 192.168.12.0 255.255.255.0 192.168.2.5*

*ip route 192.168.13.0 255.255.255.0 192.168.2.5*

*ip route 192.168.14.0 255.255.255.0 192.168.2.5*

*ip route 192.168.15.0 255.255.255.0 192.168.2.5*

*ip route 192.168.16.0 255.255.255.0 192.168.2.5*

*ip route 192.168.17.0 255.255.255.0 192.168.2.5*

*ip route 192.168.18.0 255.255.255.0 192.168.2.5*

*ip route 200.200.100.0 255.255.255.0 192.168.2.5*

*ip route 10.10.10.0 255.255.255.240 192.168.2.5*

#### Trên Router ISP 1 và 2, nhóm em sẽ sử dụng EIGRP để định tuyến Ipv4, sử dụng process-id là 10 và thêm các đường mạng xung quanh nó.

**Định tuyến IPv6**

#### ∇ Router ISP 1

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 2.2.2.1*

*interface G0/0/0*

*ipv6 ospf 20 area 0*

*interface G0/0/1*

*ipv6 ospf 20 area 0*

*interface S0/1/0*

*ipv6 ospf 20 area 0*

*interface S0/1/1*

*ipv6 ospf 20 area 0*

*interface S0/2/0*

*ipv6 ospf 20 area 0*

*interface S0/2/1*

*ipv6 ospf 20 area 0*

#### ∇ Router ISP 2

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 2.2.2.2*

*interface G0/0/0*

*ipv6 ospf 20 area 0*

*interface G0/0/1*

*ipv6 ospf 20 area 0*

*interface S0/1/0*

*ipv6 ospf 20 area 0*

*interface S0/1/1*

*ipv6 ospf 20 area 0*

*interface S0/2/0*

*ipv6 ospf 20 area 0*

*interface S0/2/1*

*ipv6 ospf 20 area 0*

#### ∇ Router R1

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 1.1.1.1*

*interface G0/0/0*

*ipv6 ospf 20 area 0*

*interface G0/0/1*

*ipv6 ospf 20 area 0*

*interface S0/1/0*

*ipv6 ospf 20 area 0*

*interface S0/1/1*

*ipv6 ospf 20 area 0*

#### ∇ Router R2

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 1.1.1.2*

*interface G0/0/0*

*ipv6 ospf 20 area 0*

*interface G0/0/1*

*ipv6 ospf 20 area 0*

*interface S0/1/0*

*ipv6 ospf 20 area 0*

*interface S0/1/1*

*ipv6 ospf 20 area 0*

#### ∇ Router R3

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 1.1.1.3*

*interface G0/0/0*

*ipv6 ospf 20 area 0*

*interface S0/1/0*

*ipv6 ospf 20 area 0*

#### ∇ Router R4

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 1.1.1.4*

*interface G0/0/0*

*ipv6 ospf 20 area 0*

*interface S0/1/0*

*ipv6 ospf 20 area 0*

#### Router R5

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 1.1.1.5*

*interface G0/0/0*

*ipv6 ospf 20 area 0*

*interface S0/1/0*

*ipv6 ospf 20 area 0*

#### Router R6

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 1.1.1.6*

*interface G0/0/0*

*ipv6 ospf 20 area 0*

*interface S0/1/0*

*ipv6 ospf 20 area 0*

#### Ở Router R1, nhóm em sẽ sử dụng định tuyến EIGRP để định tuyến cho Ipv4 và OSPFv3 cho Ipv6, tương tự, cấu hình ở R2, R3, R4, R5 và R6.

### *Khu vực* TPHCM

**Định tuyến IPv4**

#### ∇ Tường lửa ASA 1

*router eigrp 10*

*network 172.16.0.4 0.0.0.3*

*network 172.16.0.8 0.0.0.3*

*network 172.16.0.12 0.0.0.3*

*network 172.16.0.88 0.0.0.3*

*network 10.10.10.0 0.0.0.15*

*passive-interface DMZ*

#### ∇ Tường lửa ASA 2

*router eigrp 10*

*network 172.16.0.72 0.0.0.3*

*network 172.16.0.76 0.0.0.3*

*network 172.16.0.80 0.0.0.3*

*network 172.16.0.84 0.0.0.3*

*network 10.10.10.0 0.0.0.15*

*passive-interface DMZ*

#### ∇ Switch Core 1

*ip routing*

*router eigrp 10*

*network 172.16.0.8 0.0.0.3*

*network 172.16.0.16 0.0.0.3*

*network 172.16.0.20 0.0.0.3*

*network 172.16.0.64 0.0.0.3*

*network 172.16.0.84 0.0.0.3*

#### ∇ Switch Core 2

*ip routing*

*router eigrp 10*

*network 172.16.0.12 0.0.0.3*

*network 172.16.0.24 0.0.0.3*

*network 172.16.0.28 0.0.0.3*

*network 172.16.0.64 0.0.0.3*

*network 172.16.0.80 0.0.0.3*

∇ Switch Distribute 1

*ip routing*

*router eigrp 10*

*network 192.168.15.0 0.0.0.255*

*end*

*copy running-config startup-config*

*network 192.168.0.0 0.0.255.255*

*network 172.16.0.16 0.0.0.3*

*network 172.16.0.24 0.0.0.3*

*network 200.200.100.0 0.0.0.255*

*passive-interface GigabitEthernet1/0/1*

*passive-interface GigabitEthernet1/0/2*

*passive-interface GigabitEthernet1/0/3*

*passive-interface GigabitEthernet1/0/4*

*passive-interface GigabitEthernet1/0/5*

*passive-interface GigabitEthernet1/0/6*

*passive-interface GigabitEthernet1/0/7*

∇ Switch Distribute 2

*ip routing*

*router eigrp 10*

*network 172.16.0.20 0.0.0.3*

*network 172.16.0.28 0.0.0.3*

*network 192.168.0.0 0.0.255.255*

*network 200.200.200.0 0.0.0.255*

*passive-interface GigabitEthernet1/0/1*

*passive-interface GigabitEthernet1/0/2*

*passive-interface GigabitEthernet1/0/3*

*passive-interface GigabitEthernet1/0/4*

*passive-interface GigabitEthernet1/0/5*

*passive-interface GigabitEthernet1/0/6*

*passive-interface GigabitEthernet1/0/7*

**Định tuyến IPv6**

#### ∇ Tường lửa ASA 1

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*passive-interface DMZ*

*interface G1/1*

*ipv6 ospf 20 area 0*

*interface G1/2*

*ipv6 ospf 20 area 0*

*interface G1/3*

*ipv6 ospf 20 area 0*

*interface G1/4*

*ipv6 ospf 20 area 0*

*interface G1/5*

*ipv6 ospf 20 area 0*

#### ∇ Tường lửa ASA 2

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*passive-interface DMZ*

*interface G1/1*

*ipv6 ospf 20 area 0*

*interface G1/2*

*ipv6 ospf 20 area 0*

*interface G1/3*

*ipv6 ospf 20 area 0*

*interface G1/4*

*ipv6 ospf 20 area 0*

*interface G1/5*

*ipv6 ospf 20 area 0*

#### ∇ Switch Core 1

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.10*

*interface G1/0/1*

*ipv6 ospf 20 area 0*

*interface G1/0/2*

*ipv6 ospf 20 area 0*

*int po 1*

*ipv6 ospf 20 area 0*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

#### ∇ Switch Core 2

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.82*

*interface G1/0/1*

*ipv6 ospf 20 area 0*

*interface G1/0/2*

*ipv6 ospf 20 area 0*

*int po 1*

*ipv6 ospf 20 area 0*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

#### ∇ Switch Distribute 1

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.18*

*passive-interface G1/0/1*

*passive-interface G1/0/2*

*passive-interface G1/0/3*

*passive-interface G1/0/4*

*passive-interface G1/0/5*

*passive-interface G1/0/6*

*passive-interface G1/0/7*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

*int vlan 10*

*ipv6 ospf 20 area 0*

*int vlan 11*

*ipv6 ospf 20 area 0*

*int vlan 12*

*ipv6 ospf 20 area 0*

*int vlan 13*

*ipv6 ospf 20 area 0*

*int vlan 14*

*ipv6 ospf 20 area 0*

*int vlan 15*

*ipv6 ospf 20 area 0*

*int vlan 16*

*ipv6 ospf 20 area 0*

*int vlan 17*

*ipv6 ospf 20 area 0*

*int vlan 18*

*int vlan 100*

*ipv6 ospf 20 area 0*

*int vlan 110*

*ipv6 ospf 20 area 0*

#### ∇ Switch Distribute 2

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.30*

*passive-interface G1/0/1*

*passive-interface G1/0/2*

*passive-interface G1/0/3*

*passive-interface G1/0/4*

*passive-interface G1/0/5*

*passive-interface G1/0/6*

*passive-interface G1/0/7*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

*int vlan 10*

*ipv6 ospf 20 area 0*

*int vlan 11*

*ipv6 ospf 20 area 0*

*int vlan 12*

*ipv6 ospf 20 area 0*

*int vlan 13*

*ipv6 ospf 20 area 0*

*int vlan 14*

*ipv6 ospf 20 area 0*

*int vlan 15*

*ipv6 ospf 20 area 0*

*int vlan 16*

*ipv6 ospf 20 area 0*

*int vlan 17*

*ipv6 ospf 20 area 0*

*int vlan 18*

*int vlan 100*

*ipv6 ospf 20 area 0*

*int vlan 110*

*ipv6 ospf 20 area 0*

### *Khu vực* Đà Nẵng

**Định tuyến IPv4**

#### ∇ Tường lửa ASA

*router eigrp 10*

*network 172.16.0.32 0.0.0.3*

*network 172.16.0.36 0.0.0.3*

*network 172.16.0.40 0.0.0.3*

*network 172.16.0.44 0.0.0.3*

*network 10.10.11.0 0.0.0.15*

*passive-interface DMZ\_DN*

#### ∇ Switch Core 1

*ip routing*

*router eigrp 10*

*network 172.16.0.40 0.0.0.3*

*network 172.16.0.48 0.0.0.3*

*network 172.16.0.52 0.0.0.3*

*network 172.16.0.68 0.0.0.3*

#### ∇ Switch Core 2

*ip routing*

*router eigrp 10*

*network 172.16.0.44 0.0.0.3*

*network 172.16.0.56 0.0.0.3*

*network 172.16.0.60 0.0.0.3*

*network 172.16.0.68 0.0.0.3*

∇ Switch Distribute 1

*ip routing*

*router eigrp 10*

*network 172.16.0.48 0.0.0.3*

*network 172.16.0.56 0.0.0.3*

*network 192.168.0.0 0.0.255.255*

*network 200.200.150.0 0.0.0.255*

*passive-interface G1/0/1*

*passive-interface G1/0/2*

*passive-interface G1/0/3*

*passive-interface G1/0/4*

∇ Switch Distribute 2

*ip routing*

*router eigrp 10*

*network 172.16.0.52 0.0.0.3*

*network 172.16.0.60 0.0.0.3*

*network 192.168.0.0 0.0.255.255*

*network 200.200.150.0 0.0.0.255*

*passive-interface G1/0/1*

*passive-interface G1/0/2*

*passive-interface G1/0/3*

*passive-interface G1/0/4*

**Định tuyến IPv6**

#### ∇ Tường lửa ASA

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*passive-interface DMZ\_DN*

*interface G1/1*

*ipv6 ospf 20 area 0*

*interface G1/2*

*ipv6 ospf 20 area 0*

*interface G1/3*

*ipv6 ospf 20 area 0*

*interface G1/4*

*ipv6 ospf 20 area 0*

*interface G1/5*

*ipv6 ospf 20 area 0*

#### ∇ Switch Core 1

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.42*

*interface G1/0/1*

*ipv6 ospf 20 area 0*

*int po 1*

*ipv6 ospf 20 area 0*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

#### ∇ Switch Core 2

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.46*

*interface G1/0/1*

*ipv6 ospf 20 area 0*

*int po 1*

*ipv6 ospf 20 area 0*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

#### ∇ Switch Distribute 1

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.50*

*passive-interface G1/0/1*

*passive-interface G1/0/2*

*passive-interface G1/0/3*

*passive-interface G1/0/4*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

*int vlan 19*

*ipv6 ospf 20 area 0*

*int vlan 20*

*ipv6 ospf 20 area 0*

*int vlan 21*

*ipv6 ospf 20 area 0*

*int vlan 22*

*ipv6 ospf 20 area 0*

*int vlan 111*

*ipv6 ospf 20 area 0*

*int vlan 150*

#### ∇ Switch Distribute 2

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.62*

*passive-interface G1/0/1*

*passive-interface G1/0/2*

*passive-interface G1/0/3*

*passive-interface G1/0/4*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

*int vlan 19*

*ipv6 ospf 20 area 0*

*int vlan 20*

*ipv6 ospf 20 area 0*

*int vlan 21*

*ipv6 ospf 20 area 0*

*int vlan 22*

*ipv6 ospf 20 area 0*

*int vlan 111*

*ipv6 ospf 20 area 0*

*int vlan 150*

*ipv6 ospf 20 area 0*

### Khu vực Hà Nội

**Định tuyến IPv4**

#### ∇ Tường lửa ASA

*router eigrp 10*

*network 172.16.0.92 0.0.0.3*

*network 172.16.0.96 0.0.0.3*

*network 172.16.0.100 0.0.0.3*

*network 172.16.0.104 0.0.0.3*

*network 10.10.12.0 0.0.0.15*

*passive-interface DMZ\_HN*

#### ∇ Switch Core 1

*ip routing*

*router eigrp 10*

*network 172.16.0.100 0.0.0.3*

*network 172.16.0.108 0.0.0.3*

*network 172.16.0.112 0.0.0.3*

*network 172.16.0.116 0.0.0.3*

#### ∇ Switch Core 2

*ip routing*

*router eigrp 10*

*network 172.16.0.104 0.0.0.3*

*network 172.16.0.108 0.0.0.3*

*network 172.16.0.120 0.0.0.3*

*network 172.16.0.124 0.0.0.3*

∇ Switch Distribute 1

*ip routing*

*router eigrp 10*

*network 172.16.0.112 0.0.0.3*

*network 172.16.0.124 0.0.0.3*

*network 192.168.0.0 0.0.255.255*

*network 200.200.200.0 0.0.0.255*

*passive-interface G1/0/1*

*passive-interface G1/0/2*

*passive-interface G1/0/3*

*passive-interface G1/0/4*

∇ Switch Distribute 2

*ip routing*

*router eigrp 10*

*network 172.16.0.116 0.0.0.3*

*network 172.16.0.120 0.0.0.3*

*network 192.168.0.0 0.0.255.255*

*network 200.200.200.0 0.0.0.255*

*passive-interface G1/0/1*

*passive-interface G1/0/2*

*passive-interface G1/0/3*

*passive-interface G1/0/4*

**Định tuyến IPv6**

#### ∇ Tường lửa ASA

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*passive-interface DMZ\_HN*

*interface G1/1*

*ipv6 ospf 20 area 0*

*interface G1/2*

*ipv6 ospf 20 area 0*

*interface G1/3*

*ipv6 ospf 20 area 0*

*interface G1/4*

*ipv6 ospf 20 area 0*

*interface G1/5*

*ipv6 ospf 20 area 0*

#### ∇ Switch Core 1

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.102*

*interface G1/0/1*

*ipv6 ospf 20 area 0*

*int po 1*

*ipv6 ospf 20 area 0*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

#### ∇ Switch Core 2

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.106*

*interface G1/0/1*

*ipv6 ospf 20 area 0*

*int po 1*

*ipv6 ospf 20 area 0*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

#### ∇ Switch Distribute 1

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.114*

*passive-interface G1/0/1*

*passive-interface G1/0/2*

*passive-interface G1/0/3*

*passive-interface G1/0/4*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

*int vlan 23*

*ipv6 ospf 20 area 0*

*int vlan 24*

*ipv6 ospf 20 area 0*

*int vlan 25*

*ipv6 ospf 20 area 0*

*int vlan 26*

*ipv6 ospf 20 area 0*

*int vlan 112*

*ipv6 ospf 20 area 0*

*int vlan 200*

#### ∇ Switch Distribute 2

*ipv6 unicast-routing*

*ipv6 router ospf 20*

*router-id 172.16.0.122*

*passive-interface G1/0/1*

*passive-interface G1/0/2*

*passive-interface G1/0/3*

*passive-interface G1/0/4*

*int po 2*

*ipv6 ospf 20 area 0*

*int po 3*

*ipv6 ospf 20 area 0*

*int vlan 23*

*ipv6 ospf 20 area 0*

*int vlan 24*

*ipv6 ospf 20 area 0*

*int vlan 25*

*ipv6 ospf 20 area 0*

*int vlan 26*

*ipv6 ospf 20 area 0*

*int vlan 112*

*ipv6 ospf 20 area 0*

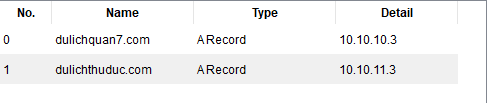
*int vlan 200*

*ipv6 ospf 20 area 0*

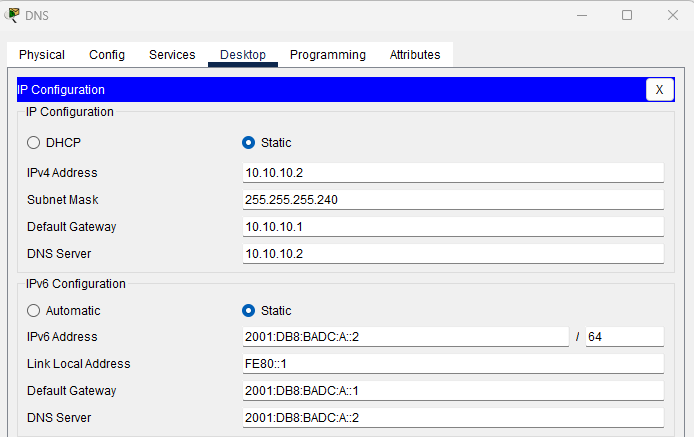
## Cấu hình khu vực DMZ

### *DNS Server*

#### Chúng ta sẽ sử dụng Server DNS để đăng ký tên miền cho cả hai chi nhánh là quận 7 và Thủ Đức.

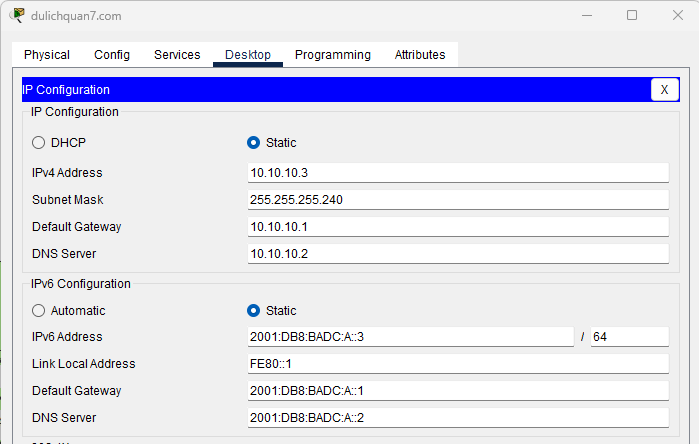


#### Hình 4.2 Đăng ký 2 tên miền cho hai trụ sở

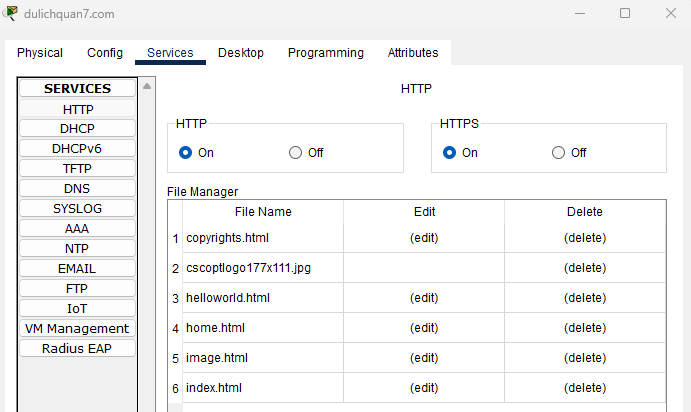


#### Hình 4.3 Cấu hình địa chỉ Ipv4 và Ipv6 cho DNS Server

### *WEB Server*

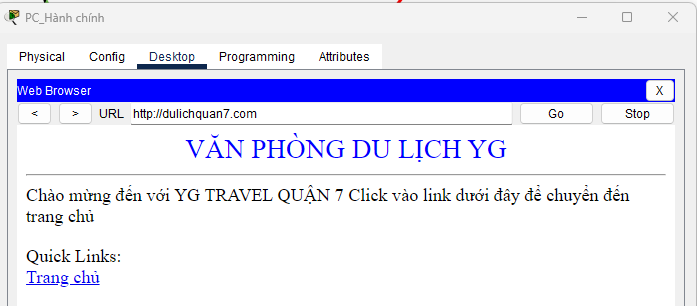


#### Hình 4.4 Cấu hình địa chỉ Ipv4 và Ipv6 cho Web Server trụ sở Quận 7



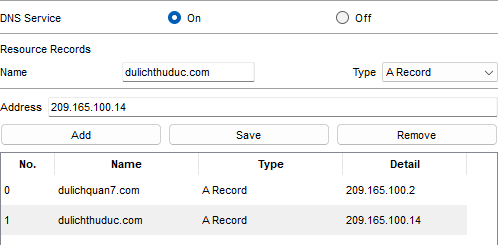
#### Hình 4.5 Bật dịch vụ HTTP

#### Truy cập trang web đã tạo tên miền:



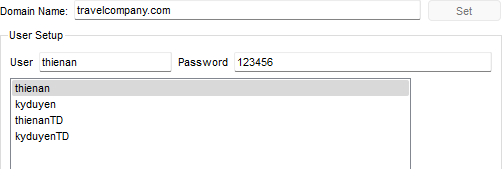
#### Hình 4.6 Truy cập đến trang web thành công.

#### Ngoài ra, ở máy chủ Web, chúng ta sẽ cài đặt tên miền với địa chỉ public, để các địa chỉ ngoài LAN có thể truy cập vào web.

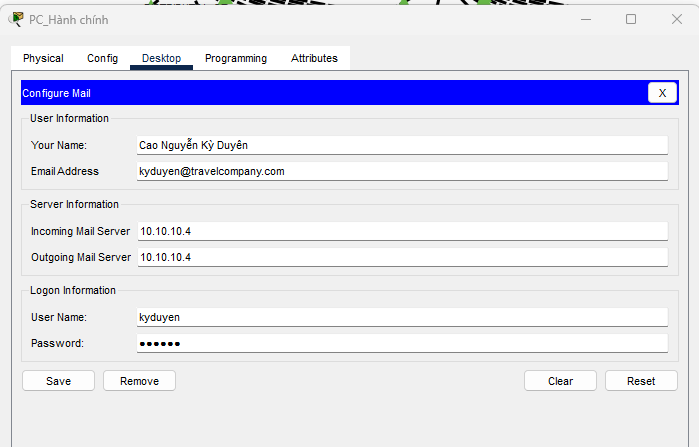


#### Hình 4.7 Đăng ký tên miền bằng địa chỉ public

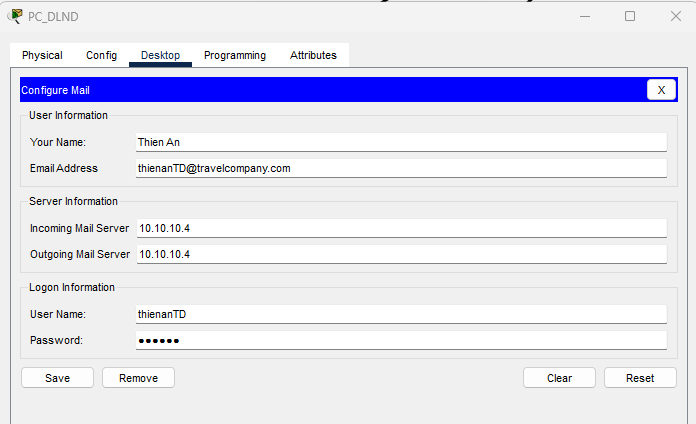
### *Mail Server*



#### Hình 4.8 Bật dịch vụ Mail Server



#### Hình 4.9 Cấu hình email cho máy phòng Hành chính.

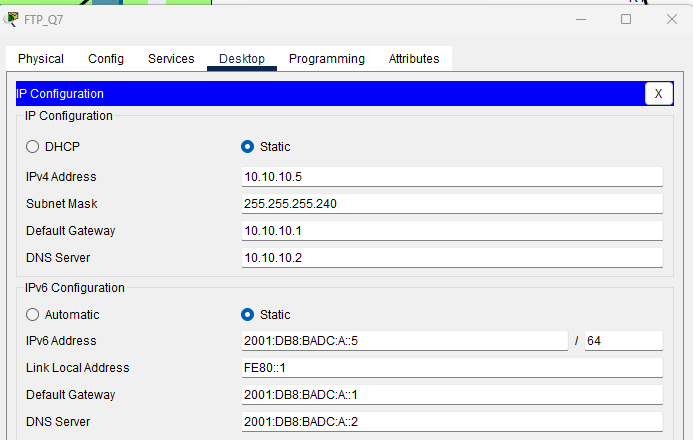


#### Hình 4.10 Cấu hình email cho máy phòng Du lịch nội địa

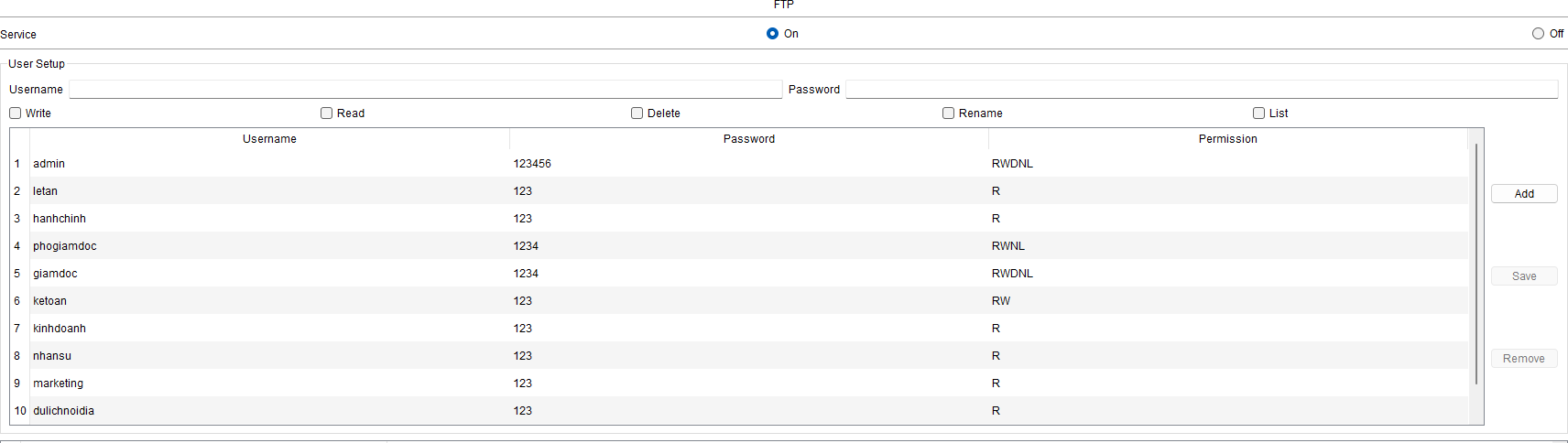


#### Hình 4.11 Gửi email từ phòng du lịch nội địa đến phòng hành chính thành công

### *FTP Server*

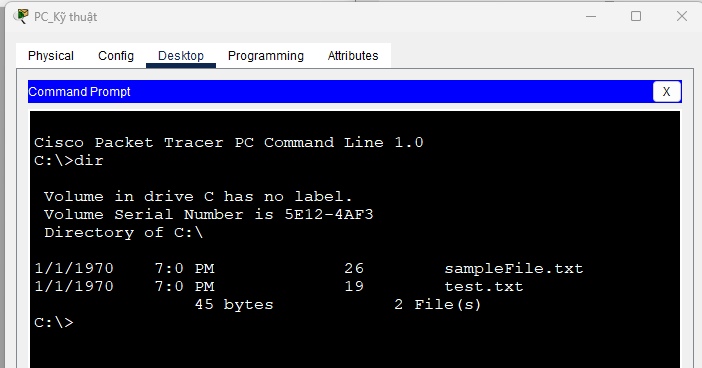


#### Hình 4.12 Cấu hình Ipv4 và Ipv6 cho FTP Server



#### Hình 4.13 Bật dịch vụ FTP và tạo tài khoản cho các phòng chức năng

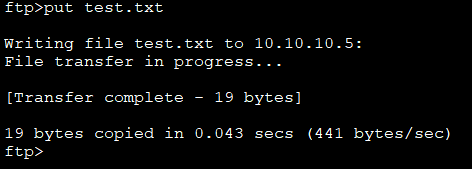
#### Để kiểm tra chức năng FTP, ta sẽ tạo một file txt ở một máy của phòng kỹ thuật, sau đó gửi lên Server FTP. Để kiểm tra file vừa tạo có tồn tại ở ổ đĩa đó hay không, ta sẽ mở CMD nhập lệnh dir.



#### Hình 4.14 File test.txt vừa tạo tồn tại trên ổ C của máy

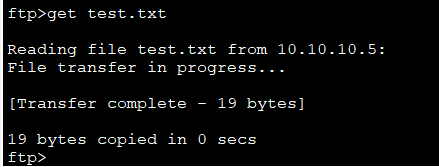
#### Khi xác định file có tồn tại trong máy, ta sẽ đăng nhập vào ftp và đưa file lên Server

#### FTP bằng lệnh put [file].

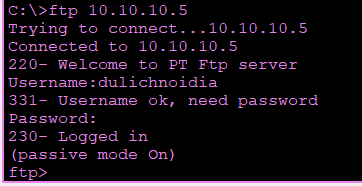


#### Hình 4.15 Tải file lên server FTP

#### Sau khi đã tải file thành công, các phòng chức năng khác có thể đăng nhập vào FTP để tải file về bằng câu lệnh get [file]

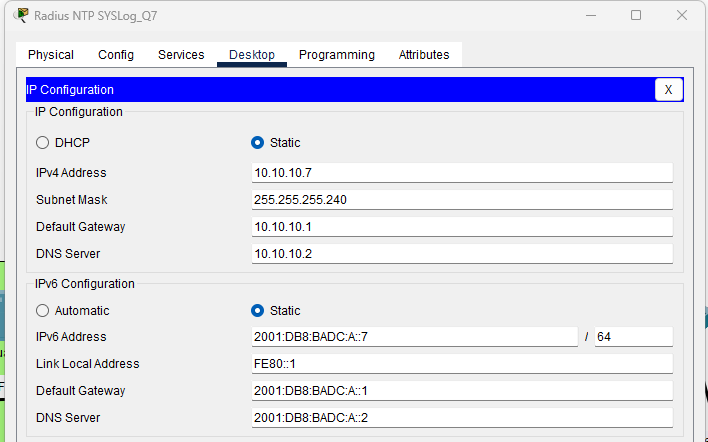


#### Hình 4.16 Các phòng chức năng có thể tải file về máy

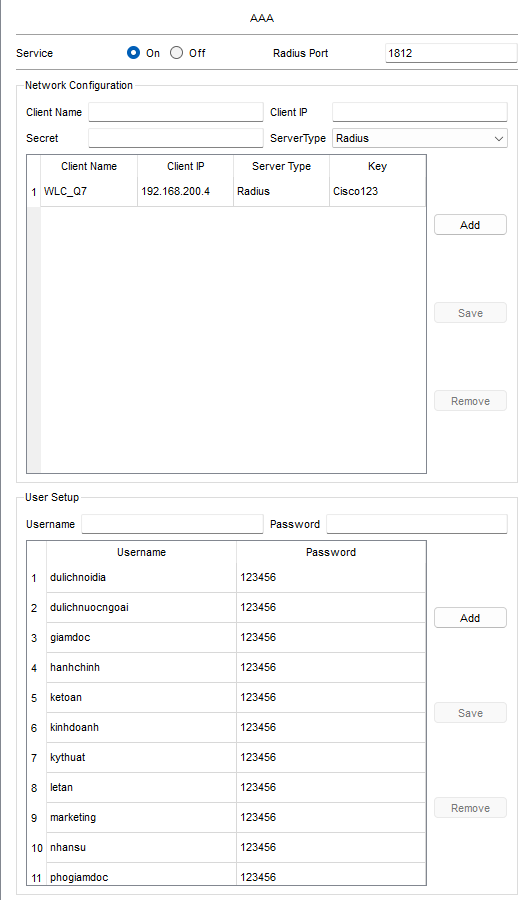


#### Hình 4.17 Các phòng chức năng ở chi nhánh Thủ Đức cũng có thể đăng nhập vào ftp

### *RADIUS Server*

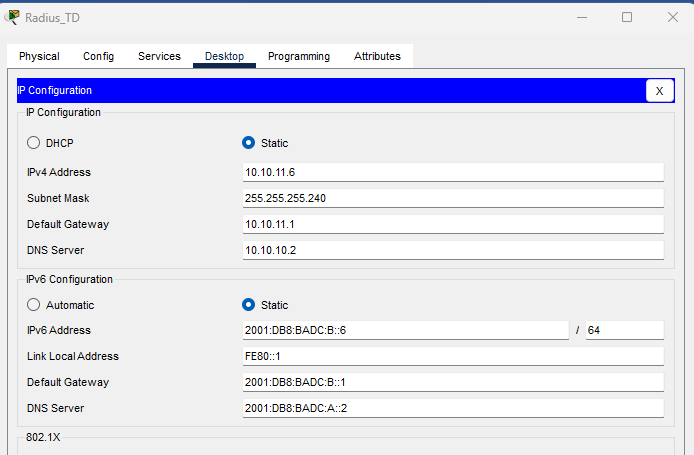


#### Hình 4.18 Cấu hình Ipv4 và Ipv6 trên Server quận 7.

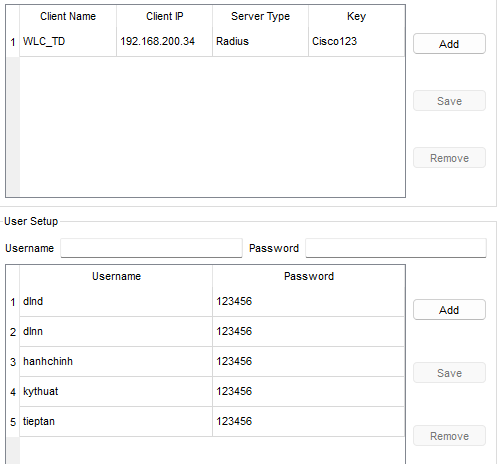


#### Hình 4.19 Bật dịch vụ AAA và tạo các account cho các phòng chức năng

#### Tương tự cấu hình tương tự ở Server Radius ở Thủ Đức

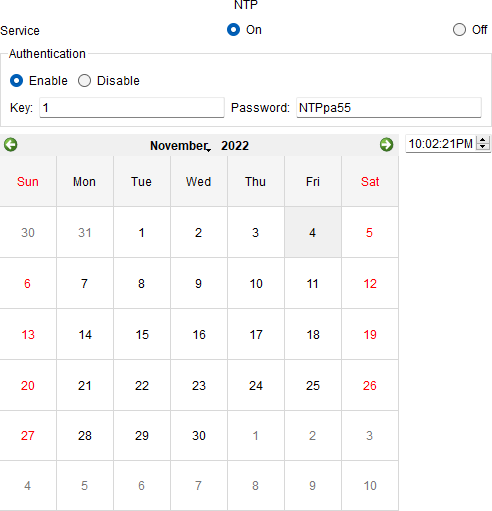


#### Hình 4.20 Cấu hình Ipv4 và Ipv6 trên Server Thủ Đức



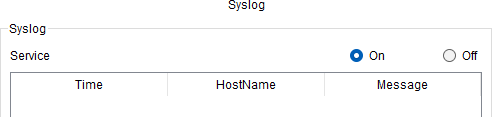
#### Hình 4.21 Bật dịch vụ AAA và tạo các account cho các phòng chức năng

### *NTP Server*



#### Hình 4.22 Khởi động và cài đặt dịch vụ NTP.

### *Syslog Server*



#### Hình 4.23 Khởi động dịch vụ Syslog

## Cấu hình VLAN VÀ VTP

### *Khu vực* TPHCM

#### Chúng ta sẽ cấu hình các VLAN trên các Switch Layer 3, ở trụ sở TPHCM sẽ có tổng cộng 10 VLAN, bao gồm: VLAN 10 cho phòng Tiếp tân, 11 cho phòng Nhân sự, 12 cho phòng Kế toán, 13 cho phòng Kinh doanh, 14 cho phòng Marketing, 15 cho phòng Kỹ thuật, 16 cho phòng Hành chính, 17 cho phòng Giám đốc, 18 cho phòng Phó giám đốc và 100 cho Khách hàng.

#### Tạo VLAN Database trên Switch Distribute 1 và 2:

*vlan 10*

*name TIEPTAN*

*vlan 11*

*name NHANSU*

*vlan 12*

*name KETOAN*

*vlan 13*

*name KINHDOANH*

*vlan 14*

*name MARKETING*

*vlan 15*

*name KYTHUAT*

*vlan 16*

*name HANHCHINH*

*vlan 17*

*name GIAMDOC*

*vlan 18*

*name PHOGIAMDOC*

*vlan 100*

*name KHACHHANG*

*vlan 110*

*name WLC\_TPHCM*

#### Sau khi tạo các VLAN Database, ta sẽ cấu hình giao thức VTP cho các Switch, trong đó, Switch Distribute 1 sẽ là mode Server, Distribute 2 ở mode transparent. Switch Distribute 1 ở mode server sẽ dùng để tạo bản tin VTP, lắng nghe bản tin, thêm xóa sửa VLAN. Switch Distribute 2 sẽ ở mode transparent để backup, dùng để thêm xóa sửa VLAN nhưng chỉ có tác dụng nội bộ trên switch cấu hình Transparent.

**Switch Distribution**

#### ∇ Switch Distribute 1

*vtp domain congtytphcm.com*

*vtp version 2*

*vtp mode server*

*vtp pass congtytphcm*

#### ∇ Switch Distribute 2

*vtp domain congtytphcm.com*

*vtp version 2*

*vtp mode transparent*

*vtp pass congtytphcm*

#### Trunking các đường Switch Distribute 1 và 2 nối với các Switch Access

∇ Switch Distribute 1 và 2 *interface range G1/0/1-7*

*switchport mode trunk*

**Switch Access**

#### Ở các Switch Access, nó sẽ ở mode client, có nhiệm vụ tạo và lắng nghe bản tin VTP

*vtp domain congtytphcm.com*

*vtp version 2*

*vtp mode client*

*vtp pass congtytphcm*

#### Các Switch Access nối với Switch Distribute 1 và 2 bằng các cổng Gigabit Ethernet 0/1 và 0/2, cho nên ta sẽ trunking các đường này.

*interface range G0/1-2 switchport mode trunk*

#### Đối với các port nối với các PC, ta sẽ gán port acces cho từng VLAN đã định sẵn

∇ **Switch Access Phòng Tiếp Tân**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 10*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 110*

∇ **Switch Access Phòng Nhân Sự**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 11*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 110*

∇ **Switch Access Phòng Kế Toán**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 12*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 110*

∇ **Switch Access Phòng Kinh Doanh**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 13*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 110*

∇ **Switch Access Phòng Marketing**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 14*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 110*

∇ **Switch Access Phòng Kỹ Thuật**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 15*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 110*

*interface Fa0/3*

*switchport mode trunk*

*switchport trunk native vlan 110*

*interface Fa0/4*

*switchport mode access*

*switchport access vlan 15*

∇ **Switch Access Phòng Ban**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 17*

*interface Fa0/2*

*switchport mode access*

*switchport access vlan 18*

*interface Fa0/3*

*switchport mode access*

*switchport access vlan 16*

*interface Fa0/4*

*switchport mode trunk*

*switchport trunk native vlan 110*

### *Khu vực* Đà Nẵng

#### Chúng ta sẽ cấu hình các VLAN trên các Switch Layer 3, ở chi nhánh Đà Nẵng sẽ có tổng cộng 6 VLAN, bao gồm : VLAN 19 cho phòng Tiếp Tân, 20 cho phòng Hành chính, VLAN 21 cho phòng Kinh doanh, VLAN 22 cho phòng Kỹ thuật, VLAN 111 cho WLC quản lý và 150 cho Khách hàng.

#### Tạo VLAN Database trên Switch Distribute 1 và 2:

*vlan 19*

*name TIEPTAN\_DN*

*vlan 20*

*name HANHCHINH\_DN*

*vlan 21*

*name KINHDOANH\_DN*

*vlan 22*

*name KYTHUAT\_DN*

*vlan 111*

*name WLC\_DN*

*vlan 150*

*name KHACHHANG\_DN*

#### Sau khi tạo các VLAN Database, ta sẽ cấu hình giao thức VTP cho các Switch, tương tự như khu vực TPHCM.

**Switch Distribution**

#### ∇ Switch Distribute 1

*vtp domain congtydn.com*

*vtp version 2*

*vtp mode server*

*vtp pass congtydn*

#### ∇ Switch Distribute 2

*vtp domain congtydn.com*

*vtp version 2*

*vtp mode transparent*

*vtp pass congtydn*

#### Trunking các đường Switch Distribute 1 và 2 nối với các Switch Access

∇ Switch Distribute 1 và 2 *interface range G1/0/1-4*

*switchport mode trunk*

**Switch Access**

#### Ở các Switch Access, nó sẽ ở mode client, có nhiệm vụ tạo và lắng nghe bản tin VTP

*vtp domain congtydn.com*

*vtp version 2*

*vtp mode client*

*vtp pass congtydn*

#### Các Switch Access nối với Switch Distribute 1 và 2 bằng các cổng Gigabit Ethernet 0/1 và 0/2, cho nên ta sẽ trunking các đường này.

*interface range G0/1-2*

*switchport mode trunk*

#### Đối với các port nối với các PC, ta sẽ gán port acces cho từng VLAN đã định sẵn

∇ **Switch Access Tiếp Tân**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 19*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 111*

∇ **Switch Access Hành Chính**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 20*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 111*

∇ **witch Access Kinh Doanh**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 21*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 111*

∇ **Switch Access Kỹ thuật**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 22*

*interface Fa0/2*

*switchport mode access*

*switchport access vlan 22*

*interface Fa0/3*

*switchport mode trunk*

*switchport trunk native vlan 111*

*interface Fa0/4*

*switchport mode trunk*

*switchport trunk native vlan 111*

### Khu vực Hà Nội

#### Chúng ta sẽ cấu hình các VLAN trên các Switch Layer 3, ở chi nhánh Hà Nội sẽ có tổng cộng 6 VLAN, bao gồm : VLAN 23 cho phòng Tiếp Tân, 24 cho phòng Hành chính, VLAN 25 cho phòng Kinh doanh, VLAN 26 cho phòng Kỹ thuật, VLAN 112 cho WLC quản lý và 200 cho Khách hàng.

#### Tạo VLAN Database trên Switch Distribute 1 và 2:

*vlan 23*

*name TIEPTAN\_HN*

*vlan 24*

*name HANHCHINH\_HN*

*vlan 25*

*name KINHDOANH\_HN*

*vlan 26*

*name KYTHUAT\_HN*

*vlan 112*

*name WLC\_HN*

*vlan 200*

*name KHACHHANG\_HN*

#### Sau khi tạo các VLAN Database, ta sẽ cấu hình giao thức VTP cho các Switch, tương tự như khu vực TPHCM.

**Switch Distribution**

#### ∇ Switch Distribute 1

*vtp domain congtyhn.com*

*vtp version 2*

*vtp mode server*

*vtp pass congtyhn*

#### ∇ Switch Distribute 2

*vtp domain congtyhn.com*

*vtp version 2*

*vtp mode transparent*

*vtp pass congtyhn*

#### Trunking các đường Switch Distribute 1 và 2 nối với các Switch Access

∇ Switch Distribute 1 và 2 *interface range G1/0/1-4*

*switchport mode trunk*

**Switch Access**

#### Ở các Switch Access, nó sẽ ở mode client, có nhiệm vụ tạo và lắng nghe bản tin VTP

*vtp domain congtyhn.com*

*vtp version 2*

*vtp mode client*

*vtp pass congtyhn*

#### Các Switch Access nối với Switch Distribute 1 và 2 bằng các cổng Gigabit Ethernet 0/1 và 0/2, cho nên ta sẽ trunking các đường này.

*interface range G0/1-2*

*switchport mode trunk*

#### Đối với các port nối với các PC, ta sẽ gán port acces cho từng VLAN đã định sẵn

∇ **Switch Access Tiếp Tân**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 23*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 112*

∇ **Switch Access Hành Chính**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 24*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 112*

∇ **witch Access Kinh Doanh**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 25*

*interface Fa0/2*

*switchport mode trunk*

*switchport trunk native vlan 112*

∇ **Switch Access Kỹ thuật**

*interface Fa0/1*

*switchport mode access*

*switchport access vlan 26*

*interface Fa0/2*

*switchport mode access*

*switchport access vlan 26*

*interface Fa0/3*

*switchport mode trunk*

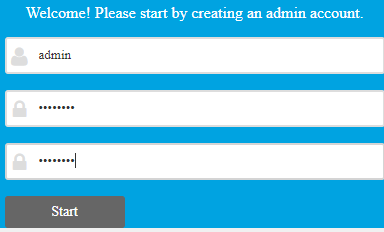
*switchport trunk native vlan 112*

*interface Fa0/4*

*switchport mode trunk*

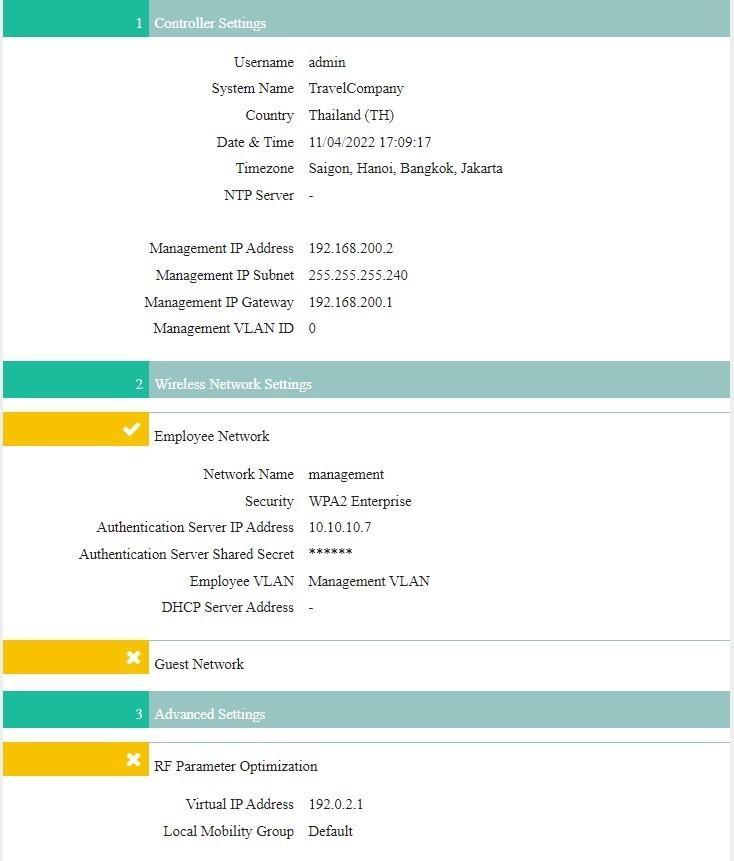
*switchport trunk native vlan 112*

## Cấu hình WLC và Light Access Point



#### Hình 4.24 Tạo tài khoản

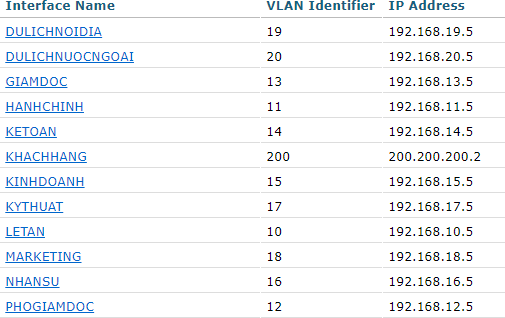
#### Truy cập vào địa chỉ IP đã đặt trên WLC để tạo tài khoản đăng nhập, sau đó tiến hành tạo các Interface và WLAN phù hợp. Sau khi tạo xong, chọn apply để tạo.



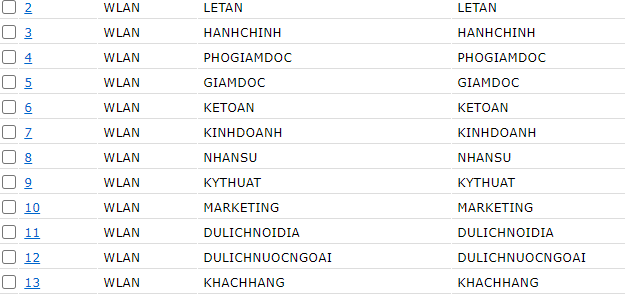
#### Hình 4.25 Thông tin sau khi tạo

#### Sau khi tạo tài khoản, truy cập địa chỉ: https://192.168.200.4 để đăng nhập vào giao diện WLC. Đăng nhập với tài khoản admin và mật khẩu Cisco123. Sau khi hiển thị

#### giao diện WLC, chúng ta sẽ tiến hành tạo các Interface và các WLAN ID.

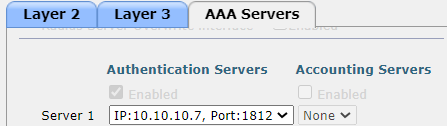


#### Hình 4.26 Tạo Interface cho các WLAN



#### Hình 4.27 Tạo WLAN ID

#### Tạo WLAN, ở Layer 2 Security , chọn WPA +WPA2 với thông số mã hóa WPA2 là AES và khóa xác thực là 802.1X. Sau đó, ở phần cấu hình AAA, chọn Server Radius với số port khớp với Server mà chúng ta đã tạo ở hệ thống.

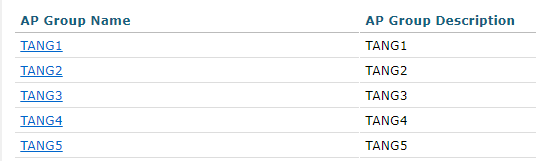


#### Hình 4.28 Chọn dải IP Radius phù hợp

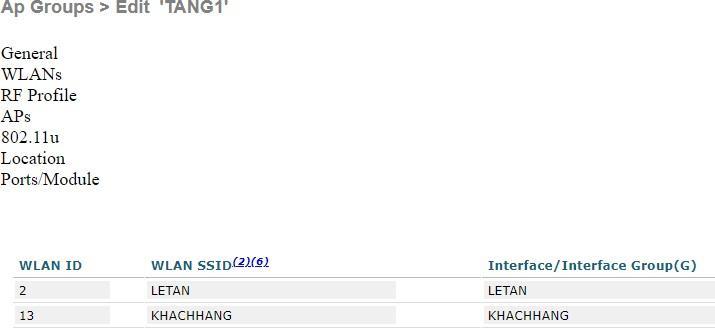
#### Ở phần Flex Connect, chúng ta sẽ chọn hai thông số là Flex Connect Switching

#### và Local Auth để tạo đường hầm CAPWAP đến WLC, một là để quản lý, còn lại là lưu lượng dữ liệu.

#### Sau khi đã tạo các WLAN và các Light Access Point đã kết nối được, lúc này chúng ta sẽ chia các Light Access Point ở các tầng để phát cố định các Wifi cần thiết. Ở tầng 1, chúng ta sẽ cho LAP chỉ phát một wifi cho phòng lễ tân, còn ở tầng 2, LAP sẽ phát wifi cho ba phòng hành chính, phó giám đốc và giám đốc, 3 tầng còn lại mỗi LAP sẽ phát wifi cho các phòng chức năng tương ứng.

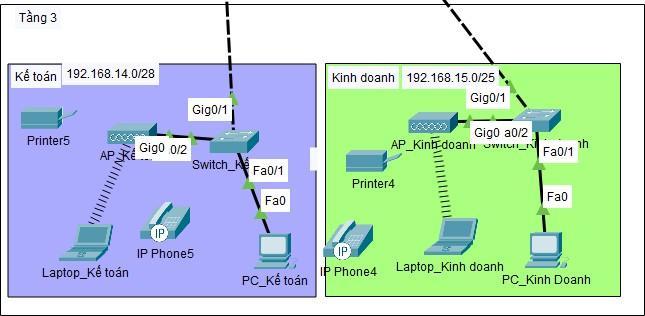


#### Hình 4.29 Tạo AP Group



#### Hình 4.30 Cấu hình các LAP phát Wifi cho WLAN

#### Sau khi đã cấu hình xong , vào các PC tạo profile để kết nối.



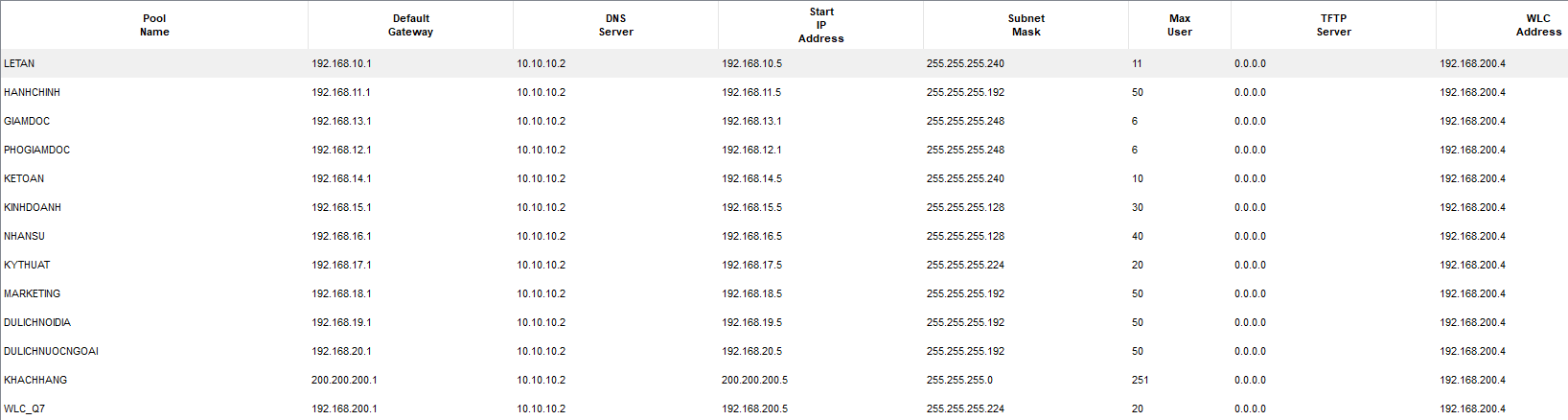
#### Hình 4.31 Các PC kết nối wifi thành công

#### Cấu hình tương tự ở chi nhánh Thủ Đức.

## Cấu hình DHCPv4 và DHCPv6

### *Khu vực* TPHCM

#### Tạo các pool DHCP cho các VLAN, bao gồm ipv4 và ipv6. Cấu hình của chức năng này sẽ được cấu hình trên DHCP server, cấp phát các IP động xuống cho các VLAN.



#### Hình 4.32 Tạo các Pool DHCP trên Server

#### Sau khi tạo pool trên Server, cấu hình inter-vlan trên hai switch Distribution như

**witch Distribution 1**

*int vlan 10*

*ip add 192.168.10.3 255.255.255.240*

*ipv6 add 2001:db8:acad:a::3/64*

*ip help 10.10.10.4*

*int vlan 11*

*ip add 192.168.11.3 255.255.255.128*

*ipv6 add 2001:db8:acad:b::3/64*

*ip help 10.10.10.4*

*int vlan 12*

*ip add 192.168.12.3 255.255.255.240*

*ipv6 add 2001:db8:acad:c::3/64*

*ip help 10.10.10.4*

*int vlan 13*

*ip add 192.168.13.3 255.255.255.192*

*ipv6 add 2001:db8:acad:d::3/64*

*ip help 10.10.10.4*

*int vlan 14*

*ip add 192.168.14.3 255.255.255.192*

*ipv6 add 2001:db8:acad:e::3/64*

*ip help 10.10.10.4*

*int vlan 15*

*ip add 192.168.15.3 255.255.255.224*

*ipv6 add 2001:db8:acad:f::3/64*

*ip help 10.10.10.4*

*int vlan 16*

*ip add 192.168.16.3 255.255.255.192*

*ipv6 add 2001:db8:acad:16::3/64*

*ip help 10.10.10.4*

*int vlan 17*

*ip add 192.168.17.3 255.255.255.248*

*ipv6 add 2001:db8:acad:17::3/64*

*ip help 10.10.10.4*

*int vlan 18*

*ip add 192.168.18.3 255.255.255.248*

*ipv6 add 2001:db8:acad:18::3/64*

*ip help 10.10.10.4*

*int vlan 100*

*ip add 200.200.100.3 255.255.255.0*

*ipv6 add 2001:db8:acad:100::3/64*

*ip help 10.10.10.4*

*int vlan 110*

*ip add 192.168.200.3 255.255.255.224*

*ipv6 add 2001:db8:acad:110::3/64*

*ip help 10.10.10.4*

**Switch Distribution 2**

*int vlan 10*

*ip add 192.168.10.2 255.255.255.240*

*ipv6 add 2001:db8:acad:a::2/64*

*ip help 10.10.10.4*

*int vlan 11*

*ip add 192.168.11.2 255.255.255.128*

*ipv6 add 2001:db8:acad:b::2/64*

*ip help 10.10.10.4*

*int vlan 12*

*ip add 192.168.12.2 255.255.255.240*

*ipv6 add 2001:db8:acad:c::2/64*

*ip help 10.10.10.4*

*int vlan 13*

*ip add 192.168.13.2 255.255.255.192*

*ipv6 add 2001:db8:acad:d::2/64*

*ip help 10.10.10.4*

*int vlan 14*

*ip add 192.168.14.2 255.255.255.192*

*ipv6 add 2001:db8:acad:e::2/64*

*ip help 10.10.10.4*

*int vlan 15*

*ip add 192.168.15.2 255.255.255.224*

*ipv6 add 2001:db8:acad:f::2/64*

*ip help 10.10.10.4*

*int vlan 16*

*ip add 192.168.16.2 255.255.255.192*

*ipv6 add 2001:db8:acad:16::2/64*

*ip help 10.10.10.4*

*int vlan 17*

*ip add 192.168.17.2 255.255.255.248*

*ipv6 add 2001:db8:acad:17::2/64*

*ip help 10.10.10.4*

*int vlan 18*

*ip add 192.168.18.2 255.255.255.248*

*ipv6 add 2001:db8:acad:18::2/64*

*ip help 10.10.10.4*

*int vlan 100*

*ip add 200.200.100.2 255.255.255.0*

*ipv6 add 2001:db8:acad:100::2/64*

*ip help 10.10.10.4*

*int vlan 110*

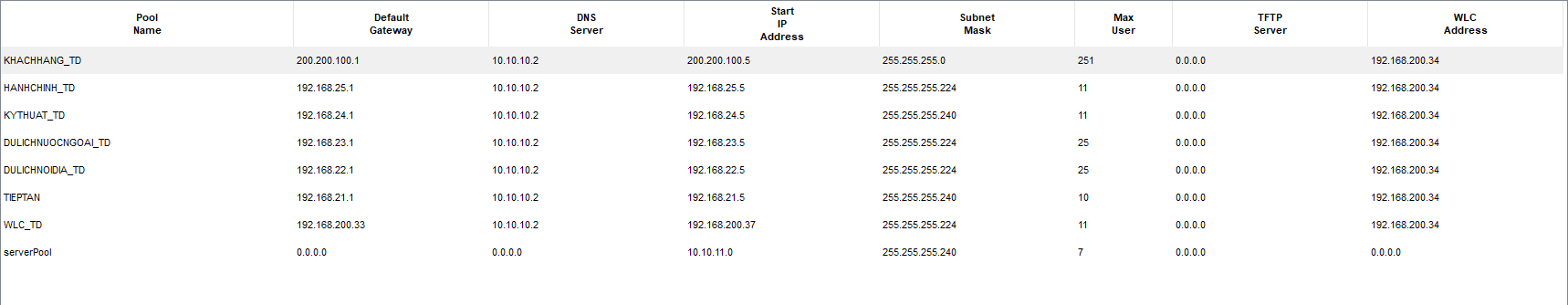
*ip add 192.168.200.2 255.255.255.224*

*ipv6 add 2001:db8:acad:110::2/64*

*ip help 10.10.10.4*

### *Khu vực* Đà Nẵng

#### Tạo các pool DHCP cho các VLAN tương tự khu vực quận 7



#### Hình 4.33 Tạo các Pool DHCP trên Server

#### Sau khi tạo pool trên Server, cấu hình inter-vlan trên hai switch Distribution như

**Switch Distribution 1**

*int vlan 19*

*ip add 192.168.19.3 255.255.255.240*

*ipv6 add 2001:db8:acad:19::3/64*

*ip help 10.10.11.3*

*int vlan 20*

*ip add 192.168.20.3 255.255.255.224*

*ipv6 add 2001:db8:acad:20::3/64*

*ip help 10.10.11.3*

*int vlan 21*

*ip add 192.168.21.3 255.255.255.192*

*ipv6 add 2001:db8:acad:21::3/64*

*ip help 10.10.11.3*

*int vlan 22*

*ip add 192.168.22.3 255.255.255.240*

*ipv6 add 2001:db8:acad:22::3/64*

*ip help 10.10.11.3*

*int vlan 150*

*ip add 200.200.150.3 255.255.255.0*

*ipv6 add 2001:db8:acad:150::3/64*

*ip help 10.10.11.3*

*int vlan 111*

*ip add 192.168.200.36 255.255.255.224*

*ipv6 add 2001:db8:acad:111::3/64*

*ip help 10.10.11.3*

**Switch Distribution 2**

*int vlan 19*

*ip add 192.168.19.2 255.255.255.240*

*ipv6 add 2001:db8:acad:19::2/64*

*ip help 10.10.11.3*

*int vlan 20*

*ip add 192.168.20.2 255.255.255.224*

*ipv6 add 2001:db8:acad:20::2/64*

*ip help 10.10.11.3*

*int vlan 21*

*ip add 192.168.21.2 255.255.255.192*

*ipv6 add 2001:db8:acad:21::2/64*

*ip help 10.10.11.3*

*int vlan 22*

*ip add 192.168.22.2 255.255.255.240*

*ipv6 add 2001:db8:acad:22::2/64*

*ip help 10.10.11.3*

*int vlan 150*

*ip add 200.200.150.2 255.255.255.0*

*ipv6 add 2001:db8:acad:150::2/64*

*ip help 10.10.11.3*

*int vlan 111*

*ip add 192.168.200.35 255.255.255.224*

*ipv6 add 2001:db8:acad:111::2/64*

*ip help 10.10.11.3*

***4.6.3 Khu vực Hà Nội***

***Switch Distribution 1***

*int vlan 23*

*ip add 192.168.23.3 255.255.255.240*

*ipv6 add 2001:db8:acad:23::3/64*

*ip help 10.10.12.3*

*int vlan 24*

*ip add 192.168.24.3 255.255.255.224*

*ipv6 add 2001:db8:acad:24::3/64*

*ip help 10.10.12.3*

*int vlan 25*

*ip add 192.168.25.3 255.255.255.192*

*ipv6 add 2001:db8:acad:25::3/64*

*ip help 10.10.12.3*

*int vlan 26*

*ip add 192.168.26.3 255.255.255.240*

*ipv6 add 2001:db8:acad:26::3/64*

*ip help 10.10.12.3*

*int vlan 200*

*ip add 200.200.200.3 255.255.255.0*

*ipv6 add 2001:db8:acad:200::3/64*

*ip help 10.10.12.3*

*int vlan 112*

*ip add 192.168.200.68 255.255.255.224*

*ipv6 add 2001:db8:acad:112::3/64*

*ip help 10.10.12.3*

***Switch Distribution 2***

*int vlan 23*

*ip add 192.168.23.2 255.255.255.240*

*end*

*copy running-config startup-config*

*ipv6 add 2001:db8:acad:23::2/64*

*ip help 10.10.12.3*

*int vlan 24*

*ip add 192.168.24.2 255.255.255.224*

*ipv6 add 2001:db8:acad:24::2/64*

*ip help 10.10.12.3*

*int vlan 25*

*ip add 192.168.25.2 255.255.255.192*

*ipv6 add 2001:db8:acad:25::2/64*

*ip help 10.10.12.3*

*int vlan 26*

*ip add 192.168.26.2 255.255.255.240*

*ipv6 add 2001:db8:acad:26::2/64*

*ip help 10.10.12.3*

*int vlan 200*

*ip add 200.200.200.2 255.255.255.0*

*ipv6 add 2001:db8:acad:200::2/64*

*ip help 10.10.12.3*

*int vlan 112*

*ip add 192.168.200.67 255.255.255.224*

*ipv6 add 2001:db8:acad:112::2/64*

*ip help 10.10.12.3*

## Cấu hình DHCP Snooping

TPHCM

Acc Tiếp tân, Nhân sự, kế toán, kinh doanh, marketing

no ip dhcp snooping information option

ip dhcp snooping vlan 10

ip dhcp snooping vlan 11

ip dhcp snooping vlan 12

ip dhcp snooping vlan 13

ip dhcp snooping vlan 14

ip dhcp snooping vlan 15

ip dhcp snooping vlan 16

ip dhcp snooping vlan 17

ip dhcp snooping vlan 18

ip dhcp snooping vlan 110

ip dhcp snooping vlan 100

inter range g0/1-2

ip dhcp snooping trust

inter range f0/1-2

ip dhcp snooping limit rate 30

end

copy running-config startup-config

Acc Kỹ thuật và phòng ban

no ip dhcp snooping information option

ip dhcp snooping vlan 10

ip dhcp snooping vlan 11

ip dhcp snooping vlan 12

ip dhcp snooping vlan 13

ip dhcp snooping vlan 14

ip dhcp snooping vlan 15

ip dhcp snooping vlan 16

ip dhcp snooping vlan 17

ip dhcp snooping vlan 18

ip dhcp snooping vlan 110

ip dhcp snooping vlan 100

inter range g0/1-2

ip dhcp snooping trust

inter range f0/1-4

ip dhcp snooping limit rate 30

end

copy running-config startup-config

## Cấu hình Ethernet-Channel

#### EtherChannel là một kỹ thuật nhóm hai hay nhiều đường kết nối truyền tải dữ liệu vật lý thành một đường ảo duy nhất có Port ảo thậm chí cả MAC ảo nhằm mục đích tăng tốc độ truyền dữ liệu và tăng khả năng dự phòng cho hệ thống. Nếu một trong các link thuộc EtherChannel bị down thì traffic sẽ tự động được chuyển sang link khác trong channel chỉ trong vòng vài miliseconds. Khi link up trở lại thì traffic được phân bố lại như cũ.

### *Khu vực* TPHCM

* + - 1. **Switch Core 1**

*interface range g1/0/19-20*

*no sw*

*no shutdown*

*channel-group 1 mode on*

*interface port-channel 1*

*ip address 172.16.0.65 255.255.255.252*

*ipv6 add 2001:db8:acad:185::1/64*

*no shutdown*

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.21 255.255.255.252*

*ipv6 add 2001:db8:acad:182::1/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.17 255.255.255.252*

*ipv6 add 2001:db8:acad:181::1/64*

*no shutdown*

* + - 1. **Switch Core 2**

*interface range g1/0/19-20*

*no sw*

*no shutdown*

*channel-group 1 mode on*

*interface port-channel 1*

*ip address 172.16.0.66 255.255.255.252*

*ipv6 add 2001:db8:acad:185::2/64*

*no shutdown*

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.25 255.255.255.252*

*ipv6 add 2001:db8:acad:183::1/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.29 255.255.255.252*

*ipv6 add 2001:db8:acad:184::1/64*

*no shutdown*

* + - 1. **Switch Distribution 1**

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.26 255.255.255.252*

*ipv6 add 2001:db8:acad:183::2/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.18 255.255.255.252*

*ipv6 add 2001:db8:acad:181::2/64*

*no shutdown*

* + - 1. **Switch Distribution 2**

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.22 255.255.255.252*

*ipv6 add 2001:db8:acad:182::2/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.30 255.255.255.252*

*ipv6 add 2001:db8:acad:184::2/64*

*no shutdown*

### *Khu vực* Đà Nẵng

* + - 1. **Switch Core 1**

*interface range g1/0/19-20*

*no sw*

*no shutdown*

*channel-group 1 mode on*

*interface port-channel 1*

*ip address 172.16.0.69 255.255.255.252*

*ipv6 add 2001:db8:acad:194::1/64*

*no shutdown*

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.53 255.255.255.252*

*ipv6 add 2001:db8:acad:191::1/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.49 255.255.255.252*

*ipv6 add 2001:db8:acad:190::1/64*

*no shutdown*

* + - 1. **Switch Core 2**

*interface range g1/0/19-20*

*no sw*

*no shutdown*

*channel-group 1 mode on*

*interface port-channel 1*

*ip address 172.16.0.70 255.255.255.252*

*ipv6 add 2001:db8:acad:194::2/64*

*no shutdown*

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.57 255.255.255.252*

*ipv6 add 2001:db8:acad:192::1/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.61 255.255.255.252*

*ipv6 add 2001:db8:acad:193::1/64*

*no shutdown*

* + - 1. **Switch Distribution 1**

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.58 255.255.255.252*

*ipv6 add 2001:db8:acad:192::2/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.50 255.255.255.252*

*ipv6 add 2001:db8:acad:190::2/64*

*no shutdown*

* + - 1. **Switch Distribution 2**

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.54 255.255.255.252*

*ipv6 add 2001:db8:acad:191::2/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.62 255.255.255.252*

*ipv6 add 2001:db8:acad:193::2/64*

*no shutdown*

### Khu vực Hà Nội

* + - 1. **Switch Core 1**

*interface range g1/0/19-20*

*no sw*

*no shutdown*

*channel-group 1 mode on*

*interface port-channel 1*

*ip address 172.16.0.109 255.255.255.252*

*ipv6 add 2001:db8:acad:219::1/64*

*no shutdown*

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.117 255.255.255.252*

*ipv6 add 2001:db8:acad:221::1/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.113 255.255.255.252*

*ipv6 add 2001:db8:acad:220::1/64*

*no shutdown*

* + - 1. **Switch Core 2**

*interface range g1/0/19-20*

*no sw*

*no shutdown*

*channel-group 1 mode on*

*interface port-channel 1*

*ip address 172.16.0.110 255.255.255.252*

*ipv6 add 2001:db8:acad:219::2/64*

*no shutdown*

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.125 255.255.255.252*

*ipv6 add 2001:db8:acad:224::1/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.121 255.255.255.252*

*ipv6 add 2001:db8:acad:223::1/64*

*no shutdown*

* + - 1. **Switch Distribution 1**

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.126 255.255.255.252*

*ipv6 add 2001:db8:acad:224::2/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.114 255.255.255.252*

*ipv6 add 2001:db8:acad:220::2/64*

*no shutdown*

* + - 1. **Switch Distribution 2**

*interface range g1/0/21-22*

*no sw*

*no shutdown*

*channel-group 3 mode on*

*interface port-channel 3*

*ip address 172.16.0.118 255.255.255.252*

*ipv6 add 2001:db8:acad:221::2/64*

*no shutdown*

*interface range g1/0/23-24*

*no sw*

*no shutdown*

*channel-group 2 mode on*

*interface port-channel 2*

*ip address 172.16.0.122 255.255.255.252*

*ipv6 add 2001:db8:acad:223::2/64*

*no shutdown*

## Cấu hình Spanning Tree

### *Khu vực* Hồ Chí Minh

#### Cấu hình Spanning tree của các vlan trên switch Distribution 1 là primary và Distribution 2 là secondary

**Distribution 1**

*spanning-tree mode rapid-pvst*

*spanning-tree vlan 10 root primary*

*spanning-tree vlan 11 root primary*

*spanning-tree vlan 12 root primary*

*spanning-tree vlan 13 root primary*

*spanning-tree vlan 14 root primary*

*spanning-tree vlan 15 root primary*

*spanning-tree vlan 16 root primary*

*spanning-tree vlan 17 root primary*

*spanning-tree vlan 18 root primary*

*spanning-tree vlan 100 root primary*

*spanning-tree vlan 110 root primary*

**Distribution 2**

*spanning-tree mode rapid-pvst*

*spanning-tree vlan 10 root secondary*

*spanning-tree vlan 11 root secondary*

*spanning-tree vlan 12 root secondary*

*spanning-tree vlan 13 root secondary*

*spanning-tree vlan 14 root secondary*

*spanning-tree vlan 15 root secondary*

*spanning-tree vlan 16 root secondary*

*spanning-tree vlan 17 root secondary*

*spanning-tree vlan 18 root secondary*

*spanning-tree vlan 100 root secondary*

*spanning-tree vlan 110 root secondary* **Các Switch Access**

*spanning-tree mode rapid-pvst*

***int range G0/1-2***

*sw mode trunk*

### *Khu vực* Đà Nẵng

#### Cấu hình tương tự như khu vực Hồ Chí Minh

**Distribution 1**

*spanning-tree mode rapid-pvst*

*panning-tree vlan 19 root primary*

*spanning-tree vlan 20 root primary*

*spanning-tree vlan 21 root primary*

*spanning-tree vlan 22 root primary*

*spanning-tree vlan 150 root primary*

*spanning-tree vlan 111 root primary*

**Distribution 2**

*spanning-tree mode rapid-pvst*

*spanning-tree vlan 19 root secondary*

*spanning-tree vlan 20 root secondary*

*spanning-tree vlan 21 root secondary*

*spanning-tree vlan 22 root secondary*

*spanning-tree vlan 150 root secondary*

*spanning-tree vlan 111 root secondary*

**Các Switch Access**

*spanning-tree mode rapid-pvst*

***int range g0/1-2***

*sw mode trunk*

### Khu vực Hà Nội

**Distribution 1**

*spanning-tree mode rapid-pvst*

*spanning-tree vlan 23 root primary*

*spanning-tree vlan 24 root primary*

*spanning-tree vlan 25 root primary*

*spanning-tree vlan 26 root primary*

*spanning-tree vlan 200 root primary*

*spanning-tree vlan 112 root primary*

***Distribution 2***

*spanning-tree mode rapid-pvst*

*spanning-tree vlan 23 root secondary*

*spanning-tree vlan 24 root secondary*

*spanning-tree vlan 25 root secondary*

*spanning-tree vlan 26 root secondary*

*spanning-tree vlan 200 root secondary*

*spanning-tree vlan 112 root secondary*

**Các Switch Access**

*spanning-tree mode rapid-pvst*

***int range g0/1-2***

*sw mode trunk*

*end*

*copy running-config startup-config*

## HSRP

*hspace\*{1cm}Chúng ta sẽ tạo các standby ở các VLAN trên các Distribution Switch, mục đích là để khi một con Switch bị hỏng, Switch còn lại sẽ đứng lên thay thế Switch chính.*

*\hspace\*{1cm}Đặt standby ở Switch Distribution với priority là 110, đóng vai trò active và priority ở Switch Distribution 2 là 90, đóng vai trò dự phòng*

*\hspace\*{1cm}\textbf{Switch Distribution 1}*

*\textit{*

*TPHCM*

*int vlan 10*

*standby 10 ip 192.168.10.1*

*standby 10 prio 110*

*standby 10 preempt*

*int vlan 11*

*standby 11 ip 192.168.11.1*

*standby 11 prio 110*

*standby 11 preempt*

*int vlan 12*

*standby 12 ip 192.168.12.1*

*standby 12 prio 110*

*standby 12 preempt*

*int vlan 13*

*standby 13 ip 192.168.13.1*

*standby 13 prio 110*

*standby 13 preempt*

*int vlan 14*

*standby 14 ip 192.168.14.1*

*standby 14 prio 110*

*standby 14 preempt*

*int vlan 15*

*standby 15 ip 192.168.15.1*

*standby 15 prio 110*

*standby 15 preempt*

*int vlan 16*

*standby 16 ip 192.168.16.1*

*standby 16 prio 110*

*standby 16 preempt*

*int vlan 17*

*standby 17 ip 192.168.17.1*

*standby 17 prio 110*

*standby 17 preempt*

*int vlan 18*

*standby 18 ip 192.168.18.1*

*standby 18 prio 110*

*standby 18 preempt*

*int vlan 100*

*standby 100 ip 200.200.100.1*

*standby 100 prio 110*

*standby 100 preempt*

*int vlan 110*

*standby 110 ip 192.168.200.1*

*standby 110 prio 110*

*standby 110 preempt*

*Switch Distribution 2*

*int vlan 10*

*standby 10 ip 192.168.10.1*

*standby 10 prio 90*

*int vlan 11*

*standby 11 ip 192.168.11.1*

*standby 11 prio 90*

*int vlan 12*

*standby 12 ip 192.168.12.1*

*standby 12 prio 90*

*int vlan 13*

*standby 13 ip 192.168.13.1*

*standby 13 prio 90*

*int vlan 14*

*standby 14 ip 192.168.14.1*

*standby 14 prio 90*

*int vlan 15*

*standby 15 ip 192.168.15.1*

*standby 15 prio 90*

*int vlan 16*

*standby 16 ip 192.168.16.1*

*standby 16 prio 90*

*int vlan 17*

*standby 17 ip 192.168.17.1*

*standby 17 prio 90*

*int vlan 18*

*standby 18 ip 192.168.18.1*

*standby 18 prio 90*

*standby 10 prio 90*

*int vlan 100*

*standby 100 ip 200.200.100.1*

*standby 100 prio 90*

*int vlan 110*

*standby 110 ip 192.168.200.1*

*standby 110 prio 90*

*Đà Nẵng*

*Switch Distribute 1*

*int vlan 19*

*standby 19 ip 192.168.19.1*

*standby 19 prio 110*

*standby 19 preempt*

*int vlan 20*

*standby 20 ip 192.168.20.1*

*standby 20 prio 110*

*standby 20 preempt*

*int vlan 21*

*standby 21 ip 192.168.21.1*

*standby 21 prio 110*

*standby 21 preempt*

*int vlan 22*

*standby 22 ip 192.168.22.1*

*standby 22 prio 110*

*standby 22 preempt*

*int vlan 150*

*standby 150 ip 200.200.150.1*

*standby 150 prio 110*

*standby 150 preempt*

*int vlan 111*

*standby 111 ip 192.168.200.33*

*standby 111 prio 110*

*standby 111 preempt*

*Switch Distribution 2*

*int vlan 19*

*standby 19 ip 192.168.19.1*

*standby 19 prio 90*

*int vlan 20*

*standby 20 ip 192.168.20.1*

*standby 20 prio 90*

*int vlan 21*

*standby 21 ip 192.168.21.1*

*standby 21 prio 90*

*int vlan 22*

*standby 22 ip 192.168.22.1*

*standby 22 prio 90*

*int vlan 150*

*standby 150 ip 200.200.150.1*

*standby 150 prio 90*

*int vlan 111*

*standby 111 ip 192.168.200.33*

*standby 111 prio 90*

*end*

*copy running-config startup-config*

## Cấu hình Firewall ASA

### *Khu vực* TPHCM

#### Sau khi cấu hình interface cho thiết bị ASA, chúng ta sẽ tiến hành đặt tên các zone phù hợp với các interface của Firewall ASA, interface g1/4 và g1/5 nối với 2 Router biên, sẽ tương ứng với hai vùng OUTSIDE, interface g1/3 nối với khu vực Server, ta sẽ đặt tên zone là DMZ. Và hai interface còn lại là g1/1 và g1/2 nối với hai Switch Core, sẽ là vùng INSIDE.

access-list 110 permit tcp 200.200.100.0 0.0.0.255 any eq www

access-list 110 permit udp 200.200.100.0 0.0.0.255 any eq domain

access-list 110 permit tcp 192.168.15.0 0.0.0.31 any eq 22

access-list 110 permit tcp 192.168.15.0 0.0.0.31 any eq telnet

access-list 110 permit ip any any

access-list 10 permit 192.168.15.0 0.0.0.31

end

copy running-config startup-config

**ASA 1 và 2**

*interface G1/4*

*nameif OUTSIDE1*

*security-level 20*

*interface G1/5*

*nameif OUTSIDE2*

*security-level 20*

*interface G1/3*

*nameif DMZ*

*security-level 60*

*interface G1/1*

*nameif INSIDE1*

*security-level 100*

*interface G1/2*

*nameif INSIDE2*

*security-level 100*

#### Do ASA là một tường lửa vật lý, nên ta cần phải đặt các rule access list để lọc các traffic vào ra phù hợp với chính sách bảo mật của công ty.

**ASA 1**

*object network DMZ*

*subnet 10.10.10.0 255.255.255.240*

*description SERVER NETWORK*

*access-list OUT-IN extended permit udp any host 10.10.10.2 eq domain*

*access-list OUT-IN extended permit tcp any host 10.10.10.2 eq www*

*access-list OUT-IN extended permit ip 192.168.0.0 255.255.0.0 any*

*access-list OUT-IN extended permit ip 192.168.15.0 255.255.255.0 any*

*access-list OUT-IN extended permit ip 10.10.11.0 255.255.255.240 any*

*access-list OUT-IN extended permit ip 10.10.12.0 255.255.255.240 any*

*access-list OUT-IN extended permit icmp any any echo-reply*

*access-list OUT-IN extended permit icmp6 any any*

*access-list OUT-IN extended permit ip host 172.16.0.34 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.38 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.42 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.46 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.50 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.54 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.58 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.62 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.33 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.37 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit udp any host 10.10.10.7*

*access-list OUT-IN extended permit ip host 172.16.0.89 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.77 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.94 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.98 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.102 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.106 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.114 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.118 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.126 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.122 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.93 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.97 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit tcp any host 10.10.10.2 eq domain*

*access-list OUT-IN extended permit udp any host 10.10.10.3 eq domain*

*access-list DMZ-ANY extended permit ip object DMZ any*

*access-list DMZ-ANY extended permit icmp6 any any*

*access-list IN-OUT extended permit ip any object DMZ*

*access-list IN-OUT extended permit ip any 192.168.0.0 255.255.0.0*

*access-list IN-OUT extended permit ip any 10.10.11.0 255.255.255.240*

*access-list IN-OUT extended permit tcp any any eq www*

*access-list IN-OUT extended permit tcp any any eq domain*

*access-list IN-OUT extended permit udp any any eq domain*

*access-list IN-OUT extended permit icmp any any*

*access-list IN-OUT extended permit icmp6 any any*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.33*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.37*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.34*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.38*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.42*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.46*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.50*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.58*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.62*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.54*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.89*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.77*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.94*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.98*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.102*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.106*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.114*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.118*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.126*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.122*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.93*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.97*

*access-group OUT-IN in interface OUTSIDE1*

*access-group OUT-IN in interface OUTSIDE2*

*access-group DMZ-ANY in interface DMZ*

*access-group IN-OUT in interface INSIDE1*

*access-group IN-OUT in interface INSIDE2*

#### IN-DMZ là ACL extended được dùng để cho phép tất cả các gói ip của khu vực DMZ. OUT-DMZ là ACL extended cho phép các đường mạng outside chỉ được sử dụng dịch vụ duyệt web. Sau khi tạo ACL, chúng ta sẽ áp nó vào các zone đã tạo trước đó.

**ASA 2**

*object network DMZ*

*subnet 10.10.10.0 255.255.255.240*

*description SERVER NETWORK*

*access-list OUT-IN extended permit udp any host 10.10.10.2 eq domain*

*access-list OUT-IN extended permit tcp any host 10.10.10.2 eq www*

*access-list OUT-IN extended permit ip 192.168.0.0 255.255.0.0 any*

*access-list OUT-IN extended permit ip 10.10.11.0 255.255.255.240 any*

*access-list OUT-IN extended permit ip 10.10.12.0 255.255.255.240 any*

*access-list OUT-IN extended permit icmp any any echo-reply*

*access-list OUT-IN extended permit icmp6 any any*

*access-list OUT-IN extended permit ip host 172.16.0.34 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.38 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.42 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.46 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.50 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.54 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.58 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.62 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.33 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.37 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit udp any host 10.10.10.7*

*access-list OUT-IN extended permit ip host 172.16.0.89 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.77 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.94 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.98 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.102 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.106 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.114 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.118 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.126 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.122 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.93 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit ip host 172.16.0.97 192.168.15.0 255.255.255.224*

*access-list OUT-IN extended permit tcp any host 10.10.10.2 eq domain*

*access-list OUT-IN extended permit udp any host 10.10.10.3 eq domain*

*access-list DMZ-ANY extended permit ip object DMZ any*

*access-list DMZ-ANY extended permit icmp6 any any*

*access-list IN-OUT extended permit ip any object DMZ*

*access-list IN-OUT extended permit ip any 192.168.0.0 255.255.0.0*

*access-list IN-OUT extended permit ip any 10.10.11.0 255.255.255.240*

*access-list IN-OUT extended permit tcp any any eq www*

*access-list IN-OUT extended permit tcp any any eq domain*

*access-list IN-OUT extended permit udp any any eq domain*

*access-list IN-OUT extended permit icmp any any*

*access-list IN-OUT extended permit icmp6 any any*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.33*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.37*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.34*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.38*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.42*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.46*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.50*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.58*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.62*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.54*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.89*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.77*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.94*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.98*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.102*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.106*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.114*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.118*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.126*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.122*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.93*

*access-list IN-OUT extended permit ip 192.168.15.0 255.255.255.224 host 172.16.0.97*

*access-group OUT-IN in interface OUTSIDE1*

*access-group OUT-IN in interface OUTSIDE2*

*access-group DMZ-ANY in interface DMZ*

*access-group IN-OUT in interface INSIDE1*

*access-group IN-OUT in interface INSIDE2*

### *Khu vực* Đà Nẵng

#### Cấu hình tương tự khu vực TPHCM

*interface G1/3*

*nameif OUTSIDE\_DN1*

*security-level 20*

*interface G1/4*

*nameif OUTSIDE\_DN2*

*security-level 20*

*interface G1/5*

*nameif DMZ\_DN*

*security-level 60*

*interface G1/1*

*nameif INSIDE\_DN1*

*security-level 100*

*interface G1/2*

*nameif INSIDE\_DN2*

*security-level 100*

#### Áp dụng ACL vào ASA

*object network DMZ\_DN*

*subnet 10.10.11.0 255.255.255.240*

*description SERVER NETWORK*

*access-list OUT-IN extended permit udp any host 10.10.10.2 eq domain*

*access-list OUT-IN extended permit tcp any host 10.10.11.2 eq www*

*access-list OUT-IN extended permit ip 192.168.0.0 255.255.0.0 any*

*access-list OUT-IN extended permit ip 10.10.10.0 255.255.255.240 any*

*access-list OUT-IN extended permit ip 10.10.11.0 255.255.255.240 any*

*access-list OUT-IN extended permit icmp6 any any*

*access-list OUT-IN extended permit icmp any any echo-reply*

*access-list OUT-IN extended permit ip 192.168.22.0 255.255.255.224 host 172.16.0.42*

*access-list OUT-IN extended permit ip 192.168.22.0 255.255.255.224 host 172.16.0.46*

*access-list OUT-IN extended permit ip 192.168.22.0 255.255.255.224 host 172.16.0.50*

*access-list OUT-IN extended permit ip 192.168.22.0 255.255.255.224 host 172.16.0.54*

*access-list OUT-IN extended permit ip 192.168.22.0 255.255.255.224 host 172.16.0.58*

*access-list OUT-IN extended permit ip 192.168.22.0 255.255.255.224 host 172.16.0.62*

*access-list OUT-IN extended permit ip host 172.16.0.33 192.168.22.0 255.255.255.240*

*access-list OUT-IN extended permit ip host 172.16.0.37 192.168.22.0 255.255.255.240*

*access-list DMZ-ANY extended permit ip object DMZ\_DN any*

*access-list DMZ-ANY extended permit icmp6 any any*

*access-list IN-OUT extended permit ip any object DMZ\_DN*

*access-list IN-OUT extended permit ip any 192.168.0.0 255.255.0.0*

*access-list IN-OUT extended permit ip any 10.10.10.0 255.255.255.240*

*access-list IN-OUT extended permit ip any 10.10.11.0 255.255.255.240*

*access-list IN-OUT extended permit tcp any any eq www*

*access-list IN-OUT extended permit tcp any any eq domain*

*access-list IN-OUT extended permit udp any any eq domain*

*access-list IN-OUT extended permit icmp any any*

*access-list IN-OUT extended permit icmp6 any any*

*access-list IN-OUT extended permit ip host 172.16.0.42 192.168.22.0 255.255.255.224*

*access-list IN-OUT extended permit ip host 172.16.0.46 192.168.22.0 255.255.255.224*

*access-list IN-OUT extended permit ip host 172.16.0.50 192.168.22.0 255.255.255.224*

*access-list IN-OUT extended permit ip host 172.16.0.54 192.168.22.0 255.255.255.224*

*access-list IN-OUT extended permit ip host 172.16.0.58 192.168.22.0 255.255.255.224*

*access-list IN-OUT extended permit ip host 172.16.0.62 192.168.22.0 255.255.255.224*

*access-list IN-OUT extended permit ip 192.168.22.0 255.255.255.240 host 172.16.0.33*

*access-list IN-OUT extended permit ip 192.168.22.0 255.255.255.240 host 172.16.0.37*

*access-group OUT-IN in interface OUTSIDE\_DN1*

*access-group OUT-IN in interface OUTSIDE\_DN2*

*access-group DMZ-ANY in interface DMZ\_DN*

*access-group IN-OUT in interface INSIDE\_DN1*

*access-group IN-OUT in interface INSIDE\_DN2*

### Khu vực Hà Nội

#### Cấu hình tương tự khu vực TPHCM

*interface G1/3*

*nameif OUTSIDE\_HN1*

*security-level 20*

*interface G1/4*

*nameif OUTSIDE\_HN2*

*security-level 20*

*interface G1/5*

*nameif DMZ\_HN*

*security-level 60*

*interface G1/1*

*nameif INSIDE\_HN1*

*security-level 100*

*interface G1/2*

*nameif INSIDE\_HN2*

*security-level 100*

#### Áp dụng ACL vào ASA

*object network DMZ\_HN*

*subnet 10.10.12.0 255.255.255.240*

*description SERVER NETWORK*

*access-list OUT-IN extended permit udp any host 10.10.12.2 eq domain*

*access-list OUT-IN extended permit tcp any host 10.10.12.2 eq www*

*access-list OUT-IN extended permit ip 192.168.0.0 255.255.0.0 any*

*access-list OUT-IN extended permit ip 10.10.10.0 255.255.255.240 any*

*access-list OUT-IN extended permit ip 10.10.12.0 255.255.255.240 any*

*access-list OUT-IN extended permit icmp6 any any*

*access-list OUT-IN extended permit icmp any any echo-reply*

*access-list OUT-IN extended permit ip 192.168.26.0 255.255.255.224 host 172.16.0.102*

*access-list OUT-IN extended permit ip 192.168.26.0 255.255.255.224 host 172.16.0.106*

*access-list OUT-IN extended permit ip 192.168.26.0 255.255.255.224 host 172.16.0.114*

*access-list OUT-IN extended permit ip 192.168.26.0 255.255.255.224 host 172.16.0.118*

*access-list OUT-IN extended permit ip 192.168.26.0 255.255.255.224 host 172.16.0.126*

*access-list OUT-IN extended permit ip 192.168.26.0 255.255.255.224 host 172.16.0.122*

*access-list OUT-IN extended permit ip host 172.16.0.93 192.168.26.0 255.255.255.240*

*access-list OUT-IN extended permit ip host 172.16.0.97 192.168.26.0 255.255.255.240*

*access-list DMZ-ANY extended permit ip object DMZ\_HN any*

*access-list DMZ-ANY extended permit icmp6 any any*

*access-list IN-OUT extended permit ip any object DMZ\_HN*

*access-list IN-OUT extended permit ip any 192.168.0.0 255.255.0.0*

*access-list IN-OUT extended permit ip any 10.10.10.0 255.255.255.240*

*access-list IN-OUT extended permit ip any 10.10.12.0 255.255.255.240*

*access-list IN-OUT extended permit tcp any any eq www*

*access-list IN-OUT extended permit tcp any any eq domain*

*access-list IN-OUT extended permit udp any any eq domain*

*access-list IN-OUT extended permit icmp any any*

*access-list IN-OUT extended permit icmp6 any any*

*access-list IN-OUT extended permit ip host 172.16.0.102 192.168.26.0 255.255.255.224*

*access-list IN-OUT extended permit ip host 172.16.0.106 192.168.26.0 255.255.255.224*

*access-list IN-OUT extended permit ip host 172.16.0.114 192.168.26.0 255.255.255.224*

*access-list IN-OUT extended permit ip host 172.16.0.118 192.168.26.0 255.255.255.224*

*access-list IN-OUT extended permit ip host 172.16.0.126 192.168.26.0 255.255.255.224*

*access-list IN-OUT extended permit ip host 172.16.0.122 192.168.26.0 255.255.255.224*

*access-list IN-OUT extended permit ip 192.168.26.0 255.255.255.240 host 172.16.0.93*

*access-list IN-OUT extended permit ip 192.168.26.0 255.255.255.240 host 172.16.0.97*

*access-group OUT-IN in interface OUTSIDE\_HN1*

*access-group OUT-IN in interface OUTSIDE\_HN2*

*access-group DMZ-ANY in interface DMZ\_HN*

*access-group IN-OUT in interface INSIDE\_HN1*

*access-group IN-OUT in interface INSIDE\_HN2*

## Cấu hình Access Control List

### *Khu vực* TPHCM

#### Cấu hình Access List cho tất cả switch và Router R1, R2 chỉ cho phép phòng kỹ thuật truy cập Telnet và SSH đến.

*access-list 10 permit 192.168.15.0 0.0.0.31 line vty 0 4*

*access-class 10 in*

**Switch Distribution 1 và 2**

*access-list 1 permit 192.168.15.0 0.0.0.31*

*access-list 110 deny tcp 200.200.100.0 0.0.0.255 10.10.10.0 0.0.0.15 eq ftp access-list 110 deny tcp 200.200.100.0 0.0.0.255 10.10.10.0 0.0.0.15 eq pop3 access-list 110 deny tcp 200.200.100.0 0.0.0.255 10.10.10.0 0.0.0.15 eq smtp*

*access-list 110 deny tcp 200.200.100.0 0.0.0.255 any eq 22*

*access-list 110 deny tcp 200.200.100.0 0.0.0.255 any eq telnet*

*access-list 110 deny udp 200.200.100.0 0.0.0.255 10.10.10.0 0.0.0.15 eq tftp access-list 110 permit tcp 200.200.100.0 0.0.0.255 any eq www*

*access-list 110 permit udp 200.200.100.0 0.0.0.255 any eq domain access-list 110 permit tcp 192.168.15.0 0.0.0.31 any eq 22*

*access-list 110 permit tcp 192.168.15.0 0.0.0.31 any eq telnet access-list 110 permit ip any any*

*inter range g1/0/19-22 ip access-group 110 out inter po 2*

*ip access-group 110 out inter po 3*

*ip access-group 110 out*

### *Khu vực* Đà Nẵng

#### Cấu hình Access List cho tất cả các Switch và Router R3, R4 chỉ cho phép phòng kỹ thuật TPHCM và Đà Nẵng truy cập Telnet và SSH đến

*access-list 10 permit 192.168.17.0 0.0.0.31 access-list 10 permit 192.168.24.0 0.0.0.15 line vty 0 4*

*access-class 10 in*

**Switch Distribution 1 và 2**

*access-list 110 deny tcp 200.200.100.0 0.0.0.255 10.10.11.0 0.0.0.15 eq ftp access-list 110 deny tcp 200.200.100.0 0.0.0.255 10.10.11.0 0.0.0.15 eq pop3 access-list 110 deny tcp 200.200.100.0 0.0.0.255 10.10.11.0 0.0.0.15 eq smtp access-list 110 deny tcp 200.200.100.0 0.0.0.255 any eq 22*

*access-list 110 deny tcp 200.200.100.0 0.0.0.255 any eq telnet*

*access-list 110 deny udp 200.200.100.0 0.0.0.255 10.10.11.0 0.0.0.15 eq tftp access-list 110 permit tcp 200.200.100.0 0.0.0.255 any eq www*

*access-list 110 permit udp 200.200.100.0 0.0.0.255 any eq domain access-list 110 permit tcp 192.168.24.0 0.0.0.15 any eq 22*

*access-list 110 permit tcp 192.168.24.0 0.0.0.15 any eq telnet access-list 110 permit ip any any*

*inter range g1/0/19-22 ip access-group 110 out inter po 2*

*ip access-group 110 out inter po 3*

*ip access-group 110 out*

## Cấu hình Port Security

### *Khu vực Quận 7*

#### Để ngăn chặn người lạ xâm nhập vào hệ thống mạng nội bộ, chúng ta sẽ cấu hình Port Security trên các Switch Access dựa vào địa chỉ MAC của các thiết bị để bảo vệ port, nếu có một thiết bị lạ được gắn vào Switch, port sẽ tự động tắt.

**Switch Access Tiếp Tân**

*inter range f0/3-24*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address sticky*

*switchport port-security violation shutdown*

*shutdown*

*int f0/1*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0007.ECCC.801E*

*end*

*copy running-config startup-config*

**Switch Access Nhân sự** *inter range f0/3-24*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address sticky*

*switchport port-security violation shutdown*

*shutdown*

*int f0/1*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0090.2B18.5472*

*end*

*copy running-config startup-config*

**Switch Access Kế toán**

*inter range f0/3-24*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address sticky*

*switchport port-security violation shutdown*

*shutdown*

*int f0/1*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0090.21DD.9A5B*

**Switch Access Kinh Doanh**

*inter range f0/3-24*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address sticky*

*switchport port-security violation shutdown*

*shutdown*

*int f0/1*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 00D0.BC26.6853*

*end*

*copy running-config startup-config*

**Switch Access Marketing**

*inter range f0/3-24*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address sticky*

*switchport port-security violation shutdown*

*shutdown*

*int f0/1*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0060.3E3C.7559*

*end*

*copy running-config startup-config*

**Switch Access Phòng kỹ thuật**

*inter range f0/5-24*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address sticky*

*switchport port-security violation shutdown*

*shutdown*

*int f0/1*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0001.9752.723E*

*int f0/4*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0001.97A8.1918*

*end*

*copy running-config startup-config*

**Switch Access Phòng ban**

*inter range f0/5-24*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address sticky*

*switchport port-security violation shutdown*

*shutdown*

*int f0/1*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0001.6413.799B*

*int f0/2*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0060.2F9C.CCBB*

*int f0/3*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0010.117D.AE68*

*end*

*copy running-config startup-config*

*inter range f0/5-24 switchport mode access switchport port-security*

*switchport port-security maximum 1 switchport port-security mac-address sticky switchport port-security vio shut*

*shutdown ex*

*int f0/1*

*switchport mode access switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0001.6413.799B int f0/2*

*switchport mode access switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0060.2F9C.CCBB int f0/3*

*switchport mode access switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0010.117D.AE68*

### *Khu vực* Đà Nẵng

**Switch Access Phòng kĩ thuật**

*inter range f0/5-24 switchport mode access*

*switchport port-security*

*switchport port-security maximum 1 switchport port-security mac-address sticky switchport port-security vio shut*

*shutdown ex*

*int f0/1*

*switchport mode access switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 00D0.BC14.7DD6*

*int f0/2*

*switchport mode access switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 000D.BD62.362A*

**Switch Access Phòng kinh doanh**

*inter range f0/3-24 switchport mode access switchport port-security*

*switchport port-security maximum 1 switchport port-security mac-address sticky switchport port-security vio shut*

*shutdown ex*

*int f0/1*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0001.43DB.242D*

**Switch Access Phòng hành chính**

*inter range f0/3-24 switchport mode access switchport port-security*

*switchport port-security maximum 1 switchport port-security mac-address sticky switchport port-security vio shut*

*shutdown ex*

*int f0/1*

*switchport mode access switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 00E0.8FC8.D29B*

**Switch Access Phòng tiếp tân**

*inter range f0/3-24*

*switchport mode access switchport port-security*

*switchport port-security maximum 1 switchport port-security mac-address sticky switchport port-security vio shut*

*shutdown ex*

*int f0/1*

*switchport mode access switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0090.0CAA.478D*

### Khu vực Hà Nội

**Switch Access Phòng kĩ thuật**

*inter range f0/5-24 switchport mode access*

*switchport port-security*

*switchport port-security maximum 1 switchport port-security mac-address sticky switchport port-security vio shut*

*shutdown ex*

*int f0/1*

*switchport mode access switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0007.EC76.2646*

*int f0/2*

*switchport mode access switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 00E0.B087.DD0E*

**Switch Access Phòng kinh doanh**

*inter range f0/3-24 switchport mode access switchport port-security*

*switchport port-security maximum 1 switchport port-security mac-address sticky switchport port-security vio shut*

*shutdown ex*

*int f0/1*

*switchport mode access*

*switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0060.3E97.37A7*

**Switch Access Phòng hành chính**

*inter range f0/3-24 switchport mode access switchport port-security*

*switchport port-security maximum 1 switchport port-security mac-address sticky switchport port-security vio shut*

*shutdown ex*

*int f0/1*

*switchport mode access switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0002.1615.0AA5*

**Switch Access Phòng tiếp tân**

*inter range f0/3-24*

*switchport mode access switchport port-security*

*switchport port-security maximum 1 switchport port-security mac-address sticky switchport port-security vio shut*

*shutdown ex*

*int f0/1*

*switchport mode access switchport port-security*

*switchport port-security maximum 1*

*switchport port-security mac-address 0060.70B6.C388*

## Cấu hình SSH access

#### Trên tất cả các thiết bị Router, Multilayer Switch, chúng ta sẽ cấu hình bảo mật cơ bản, đồng thời chỉ cho phép phòng kỹ thuật được phép truy cập SSH vào.

### *Khu vực Quận 7*

**Cấu hình SSH access Local trên các thiết bị Multilayer Switch và Router**

*line console 0 pass dulichquan7 login*

*exit*

*enable secret level 15 vanphongcongtidulichquan7 banner motd "KHONG PHAN SU MIEN VAO" exit*

*conf t*

*service password-encryption security passwords min-length 10*

*login block-for 180 attempts 4 within 120 ip domain-name dulichquan7.com*

*no ip domain-lookup*

*crypto key generate rsa general-keys modulus 1024 username adminlocalQ7 secret dulichcompanyquan7 ip ssh ver 2*

*aaa new-model*

*aaa authentication login ADMINLOCALQ7 local line vty 0 4*

*exec-timeout 5 30 transport input SSH login local*

*login authentication ADMINLOCALQ7 exit*

*do copy running-config startup-config*

**Cấu hình SSH access Local trên thiết bị Tường lửa**

*username adminlocalQ7 password dulichcompanyquan7 encrypted aaa authentication ssh console local*

*crypto key generate rsa general-keys modulus 1024 yes*

*ssh 192.168.17.0 255.255.255.224 INSIDE ssh 192.168.17.0 255.255.255.224 INSIDE2*

*ssh timeout 20*

**Cấu hình SSH access Central trên các thiết bị Core 1**

*aaa new-model*

*aaa authentication login Central group radius local radius-server host 172.16.0.17*

*radius-server key dulichcompanyquan7*

*username admincentralQ7 password dulichcompanyquan7 line vty 0 4*

*login authentication admincentralQ7 exit*

**Core 2**

*aaa new-model*

*aaa authentication login Central group radius local radius-server host 172.16.0.29*

*radius-server key dulichcompanyquan7*

*username admincentralQ7 password dulichcompanyquan7 line vty 0 4*

*login authentication admincentralQ7 exit*

**Distribution 1**

*aaa new-model*

*aaa authentication login Central group radius local radius-server host 172.16.0.18*

*radius-server key dulichcompanyquan7*

*username admincentralQ7 password dulichcompanyquan7 line vty 0 4*

*login authentication admincentralQ7 exit*

**Distribution 2**

*aaa new-model*

*aaa authentication login Central group radius local radius-server host 172.16.0.30*

*radius-server key dulichcompanyquan7*

*username admincentralQ7 password dulichcompanyquan7 line vty 0 4*

*login authentication admincentralQ7 exit*

### *Khu vực Thủ Đức*

**Cấu hình SSH access Local trên các thiết bị Multilayer Switch và Router**

*line console 0 pass dulichthuduc login*

*exit*

*enable secret level 15 vanphongcongtidulichthuduc banner motd "KHONG PHAN SU MIEN VAO"*

*exit conf t*

*service password-encryption security passwords min-length 10*

*login block-for 180 attempts 4 within 120 ip domain-name dulichthuduc.com*

*no ip domain-lookup*

*crypto key generate rsa general-keys modulus 1024 username adminlocalTD secret dulichcompanythuduc ip ssh ver 2*

*aaa new-model*

*aaa authentication login ADMINLOCALTD local line vty 0 4*

*exec-timeout 5 30 transport input SSH login local*

*login authentication ADMINLOCALTD exit*

*do copy running-config startup-config*

**Cấu hình SSH access Local trên thiết bị Tường lửa**

*username adminlocalTD password dulichcompanythuduc encrypted aaa authentication ssh console local*

*crypto key generate rsa general-keys modulus 1024 YES*

*ssh 192.168.24.0 255.255.255.240 INSIDE\_TD ssh 192.168.24.0 255.255.255.240 INSIDE2\_TD ssh 192.168.17.0 255.255.255.224 OUTSIDE\_TD ssh 192.168.17.0 255.255.255.224 OUTSIDE2\_TD*

*ssh timeout 20*

**Cấu hình SSH access Central trên các thiết bị Core 1**

*aaa new-model*

*aaa authentication login Central group radius local radius-server host 172.16.0.49*

*radius-server key dulichcompanythuduc*

*username admincentralTD password dulichcompanythuduc line vty 0 4*

*login authentication admincentralTD ex*

**Core 2**

*aaa new-model*

*aaa authentication login Central group radius local radius-server host 172.16.0.57*

*radius-server key dulichcompanythuduc*

*username admincentralTD password dulichcompanythuduc line vty 0 4*

*login authentication admincentralTD ex*

**Distribution 1**

*aaa new-model*

*aaa authentication login Central group radius local*

*radius-server host 172.16.0.50*

*radius-server key dulichcompanythuduc*

*username admincentralTD password dulichcompanythuduc line vty 0 4*

*login authentication admincentralTD ex*

**Distribution 2**

*aaa new-model*

*aaa authentication login Central group radius local radius-server host 172.16.0.62*

*radius-server key dulichcompanythuduc*

*username admincentralTD password dulichcompanythuduc line vty 0 4*

*login authentication admincentralTD ex*

## Cấu hình NTP, Syslog

#### Khu vực Quận 7 và Thủ Đức sẽ sử dụng một NTP và Syslog Server là 10.10.10.7.

#### Cấu hình NTP cho tất cả thiết bị ở cả hai chi nhánh với key là 1 và mật khẩu là NTPpa55

*ntp server 10.10.10.7 ntp authenticate*

*ntp trusted-key 1*

*ntp authentication-key 1 md5 NTPpa55 ntp update-calendar*

*exit*

*clock set 20:11:00 Nov 7 2022 logging 10.10.10.7*

*service timestamps log datetime msec*

## Cấu hình VPN-IPSec

#### Để hai chi nhánh có thể kết nối với nhau, chúng ta sẽ sử dụng VPN để tạo một mạng riêng ảo, tất cả các VLAN và mạng trong công ti sẽ gửi tin cho nhau thông qua đường hầm Tunnel.

#### Chúng ta sẽ tạo cấu hình chức năng này trên 4 Router R1, R2, R3, R4. Trong đó,

#### chúng ta sẽ tạo 4 đường hầm từ R1 đến R3, R2 đến R4, R1 đến R4 và R2 đến R3.

**Tạo đường hầm từ R1 đến R3 trên Router R1**

*int Tunnel1*

*ip add 192.168.1.1 255.255.255.252*

*tunnel mode gre ip tunnel source S0/1/0*

*tunnel destination 209.165.100.10 no shut*

*exit*

**Tạo đường hầm từ R3 đến R1 trên Router R3**

*int Tunnel1*

*ip add 192.168.1.2 255.255.255.252*

*tunnel mode gre ip tunnel source S0/1/0*

*tunnel destination 209.165.100.2 no shut*

**Tạo đường hầm từ R2 đến R4 trên Router R2**

*int Tunnel1*

*ip add 192.168.2.1 255.255.255.252*

*tunnel mode gre ip tunnel source S0/1/0*

*tunnel destination 209.165.100.14 no shut*

*exit*

**Tạo đường hầm từ R4 đến R2 trên Router R4**

*int Tunnel1*

*ip add 192.168.2.2 255.255.255.252*

*tunnel mode gre ip tunnel source S0/1/0*

*tunnel destination 209.165.100.6 no shut*

*exit*

#### Tạo các ACL để cho phép mạng VLAN và Server được phép đi vào đường hầm.

#### Các mạng còn lại muốn ra ngoài internet sẽ phải NAT.

**Router R1**

*ip access-list extended VPN*

*permit gre host 209.165.100.2 host 209.165.100.10*

*permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255 permit ip 192.168.0.0 0.0.255.255 10.10.11.0 0.0.0.15 permit ip 10.10.10.0 0.0.0.15 10.10.11.0 0.0.0.15*

*permit ip 10.10.10.0 0.0.0.15 192.168.0.0 0.0.255.255 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.34 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.38 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.42 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.46 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.50 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.58 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.62 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.54 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.33 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.37*

*permit tcp 200.200.200.0 0.0.0.255 host 10.10.11.3 eq www permit tcp 200.200.100.0 0.0.0.255 host 10.10.10.3 eq www*

**Router R2**

*ip access-list extended VPN*

*permit gre host 209.165.100.6 host 209.165.100.14*

*permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255 permit ip 192.168.0.0 0.0.255.255 10.10.11.0 0.0.0.15 permit ip 10.10.10.0 0.0.0.15 10.10.11.0 0.0.0.15*

*permit ip 10.10.10.0 0.0.0.15 192.168.0.0 0.0.255.255 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.34 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.38 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.42 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.46 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.50 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.54 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.58 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.62 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.37 permit ip 192.168.17.0 0.0.0.31 host 172.16.0.33*

*permit tcp 200.200.200.0 0.0.0.255 host 10.10.11.3 eq www permit tcp 200.200.100.0 0.0.0.255 host 10.10.10.3 eq www*

*exit*

**Router R3**

*ip access-list extended VPN*

*permit gre host 209.165.100.10 host 209.165.100.2*

*permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255 permit ip 192.168.0.0 0.0.255.255 10.10.10.0 0.0.0.15 permit ip 10.10.11.0 0.0.0.15 10.10.10.0 0.0.0.15*

*permit ip 10.10.11.0 0.0.0.15 192.168.0.0 0.0.255.255 permit ip host 172.16.0.34 192.168.17.0 0.0.0.31 permit ip host 172.16.0.38 192.168.17.0 0.0.0.31 permit ip host 172.16.0.42 192.168.17.0 0.0.0.31 permit ip host 172.16.0.46 192.168.17.0 0.0.0.31 permit ip host 172.16.0.50 192.168.17.0 0.0.0.31 permit ip host 172.16.0.58 192.168.17.0 0.0.0.31 permit ip host 172.16.0.62 192.168.17.0 0.0.0.31 permit ip host 172.16.0.54 192.168.17.0 0.0.0.31 permit ip host 172.16.0.33 192.168.17.0 0.0.0.31 permit ip host 172.16.0.37 192.168.17.0 0.0.0.31*

*permit tcp host 10.10.11.3 200.200.200.0 0.0.0.255 eq www permit tcp host 10.10.10.3 200.200.100.0 0.0.0.255 eq www exit*

**Router R4**

*ip access-list extended VPN*

*permit gre host 209.165.100.14 host 209.165.100.6*

*permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255 permit ip 192.168.0.0 0.0.255.255 10.10.10.0 0.0.0.15 permit ip 10.10.11.0 0.0.0.15 10.10.10.0 0.0.0.15*

*permit ip 10.10.11.0 0.0.0.15 192.168.0.0 0.0.255.255 permit ip host 172.16.0.34 192.168.17.0 0.0.0.31 permit ip host 172.16.0.38 192.168.17.0 0.0.0.31 permit ip host 172.16.0.42 192.168.17.0 0.0.0.31 permit ip host 172.16.0.46 192.168.17.0 0.0.0.31 permit ip host 172.16.0.50 192.168.17.0 0.0.0.31 permit ip host 172.16.0.58 192.168.17.0 0.0.0.31 permit ip host 172.16.0.62 192.168.17.0 0.0.0.31 permit ip host 172.16.0.54 192.168.17.0 0.0.0.31*

*permit ip host 172.16.0.33 192.168.17.0 0.0.0.31 permit ip host 172.16.0.37 192.168.17.0 0.0.0.31*

*permit tcp host 10.10.11.3 200.200.200.0 0.0.0.255 eq www permit tcp host 10.10.10.3 200.200.100.0 0.0.0.255 eq www*

#### Sau khi đã tạo đường hầm xong, chúng ta sẽ tiến hành cấu hình IPsec trên các Router.

**Router R1**

*crypto isakmp policy 10 encryption aes 256 authentication pre-share group 1*

*exit*

*crypto isakmp key vpncisco123 address 209.165.100.10 crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac crypto map R1-R3 10 ipsec-isakmp*

*description VPN connection to R3 set peer 209.165.100.10*

*set transform-set VPN-SET set pfs*

*match address VPN exit*

*int s0/1/0*

*crypto map R1-R3 exit*

**Router R2**

*conf t*

*crypto isakmp policy 10 encryption aes 256 authentication pre-share group 1*

*exit*

*crypto isakmp key vpncisco123 address 209.165.100.14 crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac crypto map R2-R4 10 ipsec-isakmp*

*description VPN connection to R4 set peer 209.165.100.14*

*set transform-set VPN-SET set pfs*

*match address VPN exit*

*int s0/1/0*

*crypto map R2-R4 exit*

**Router R3**

*crypto isakmp policy 10 encryption aes 256 authentication pre-share group 1*

*exit*

*crypto isakmp key vpncisco123 address 209.165.100.2 crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac crypto map R3-R1 10 ipsec-isakmp*

*description VPN connection to R1 set peer 209.165.100.2*

*set pfs*

*set transform-set VPN-SET match address VPN*

*exit*

*int s0/1/0*

*crypto map R3-R1 exit*

**Router R4**

*crypto isakmp policy 10 encryption aes 256 authentication pre-share group 1*

*exit*

*crypto isakmp key vpncisco123 address 209.165.100.6 crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac crypto map R4-R2 10 ipsec-isakmp*

*description VPN connection to R2 set peer 209.165.100.6*

*set transform-set VPN-SET set pfs*

*match address VPN exit*

*int s0/1/0*

*crypto map R4-R2 exit*

## Cấu hình NAT

#### Ở phần trên, chúng ta đã cấu hình VPN cho các mạng thuộc VLAN để chúng có thể đi qua các đường hầm. Vậy để những mạng khác không thuộc VLAN cần truy cập đến doanh nghiệp ví dụ như website, thì NAT sẽ là giải pháp để các mạng khu vực OUTSIDE có thể truy cập vào website hoặc mạng trong công ti muốn gửi gói tin ra khu vực OUTSIDE. Chúng ta sẽ đặt ACL của NAT với câu lệnh ngược lại với ACL của VPN

**Router R1**

*ip access-list extended NAT*

*deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255 deny ip 192.168.0.0 0.0.255.255 10.10.11.0 0.0.0.15 deny ip 10.10.10.0 0.0.0.15 10.10.11.0 0.0.0.15*

*deny ip 10.10.10.0 0.0.0.15 192.168.0.0 0.0.255.255 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.34 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.38 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.42 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.46 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.50 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.58 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.62 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.54 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.37 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.33*

*deny tcp 200.200.200.0 0.0.0.255 host 10.10.11.3 eq www deny tcp 200.200.100.0 0.0.0.255 host 10.10.10.3 eq www permit ip any any*

*exit*

*int s0/1/0 ip nat out int g0/0/0 ip nat in int g0/0/1 ip nat in exit*

*ip nat inside source list NAT interface Serial0/1/0 overload*

*ip nat inside source static udp 10.10.10.3 53 209.165.100.2 53 ip nat inside source static tcp 10.10.10.3 80 209.165.100.2 80*

**Router R2**

*ip access-list extended NAT*

*deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255 deny ip 192.168.0.0 0.0.255.255 10.10.11.0 0.0.0.15 deny ip 10.10.10.0 0.0.0.15 10.10.11.0 0.0.0.15*

*deny ip 10.10.10.0 0.0.0.15 192.168.0.0 0.0.255.255 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.34 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.38 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.42 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.46 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.50 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.54 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.58 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.62 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.37 deny ip 192.168.17.0 0.0.0.31 host 172.16.0.33*

*deny tcp 200.200.200.0 0.0.0.255 host 10.10.11.3 eq www deny tcp 200.200.100.0 0.0.0.255 host 10.10.10.3 eq www permit ip any any*

*exit*

*int s0/1/0 ip nat out ex*

*int g0/0/0 ip nat in*

*exit*

*int g0/0/1 ip nat in exit*

*ip nat inside source list NAT interface Serial0/1/0 overload*

*ip nat inside source static udp 10.10.10.3 53 209.165.100.6 53 ip nat inside source static tcp 10.10.10.3 80 209.165.100.6 8080*

**Router R3**

*ip access-list extended NAT*

*deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255 deny ip 192.168.0.0 0.0.255.255 10.10.10.0 0.0.0.15 deny ip 10.10.11.0 0.0.0.15 10.10.10.0 0.0.0.15*

*deny ip 10.10.11.0 0.0.0.15 192.168.0.0 0.0.255.255 deny ip host 172.16.0.34 192.168.17.0 0.0.0.31 deny ip host 172.16.0.38 192.168.17.0 0.0.0.31 deny ip host 172.16.0.42 192.168.17.0 0.0.0.31 deny ip host 172.16.0.46 192.168.17.0 0.0.0.31 deny ip host 172.16.0.50 192.168.17.0 0.0.0.31 deny ip host 172.16.0.58 192.168.17.0 0.0.0.31 deny ip host 172.16.0.62 192.168.17.0 0.0.0.31 deny ip host 172.16.0.54 192.168.17.0 0.0.0.31 deny ip host 172.16.0.37 192.168.17.0 0.0.0.31 deny ip host 172.16.0.33 192.168.17.0 0.0.0.31*

*deny tcp host 10.10.11.3 200.200.200.0 0.0.0.255 eq www deny tcp host 10.10.10.3 200.200.100.0 0.0.0.255 eq www permit ip any any*

*exit*

*int s0/1/0 ip nat out ex*

*int g0/0/0 ip nat in exit*

*ip nat inside source list NAT interface Serial0/1/0 overload*

*ip nat inside source static tcp 10.10.11.3 80 209.165.100.10 80*

**Router R4**

*ip access-list extended NAT*

*deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255 deny ip 192.168.0.0 0.0.255.255 10.10.10.0 0.0.0.15 deny ip 10.10.11.0 0.0.0.15 10.10.10.0 0.0.0.15*

*deny ip 10.10.11.0 0.0.0.15 192.168.0.0 0.0.255.255 deny ip host 172.16.0.34 192.168.17.0 0.0.0.31 deny ip host 172.16.0.38 192.168.17.0 0.0.0.31 deny ip host 172.16.0.42 192.168.17.0 0.0.0.31 deny ip host 172.16.0.46 192.168.17.0 0.0.0.31 deny ip host 172.16.0.50 192.168.17.0 0.0.0.31 deny ip host 172.16.0.58 192.168.17.0 0.0.0.31 deny ip host 172.16.0.62 192.168.17.0 0.0.0.31 deny ip host 172.16.0.54 192.168.17.0 0.0.0.31 deny ip host 172.16.0.33 192.168.17.0 0.0.0.31 deny ip host 172.16.0.37 192.168.17.0 0.0.0.31*

*deny tcp host 10.10.11.3 200.200.200.0 0.0.0.255 eq www deny tcp host 10.10.10.3 200.200.100.0 0.0.0.255 eq www permit ip any any*

*exit*

*int s0/1/0 ip nat out ex*

*int g0/0/0 ip nat in ex*

*ip nat inside source list NAT interface Serial0/1/0 overload*

*ip nat inside source static tcp 10.10.11.3 80 209.165.100.14 8080*

## Qos Concept

#### Cấu hình các QoS Concept cho tất cả các switch Distribute ở hai chi nhánh, cài đặt dịch vụ Mail và Web với băng thông 10 Mbit, dịch vụ FTP với 20 Mbit, dịch vụ SSH và Telnet với băng thông là 5 Mbit, dịch vụ ICMP với băng thông 100 Kbit.

*class-map match-any MAIL match protocol pop3*

*match protocol smtp*

*ex*

*class-map match-any WEB match protocol http*

*match protocol https match protocol dns ex*

*class-map match-any FTP match protocol ftp*

*match protocol tftp ex*

*class-map match-any REMOTE match protocol ssh*

*match protocol telnet ex*

*class-map ICMP match protocol icmp ex*

*policy-map QoS class MAIL bandwidth 10000 set ip dscp af11 ex*

*class WEB bandwidth 10000*

*random-detect dscp-based ex*

*class FTP bandwidth 20000 ex*

*class REMOTE bandwidth 5000 ex*

*class ICMP bandwidth 100*

*random-detect dscp-based ex*

*ex*

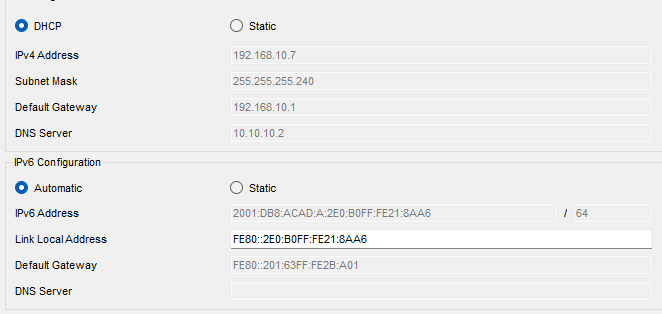
*inter range g1/0/19-22 service-policy output QoS inter po 2*

*service-policy output QoS inter po 3*

*service-policy output QoS*

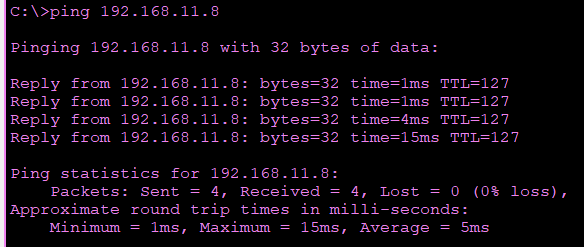
## Chương trình demo

### *Kiểm tra DHCP*

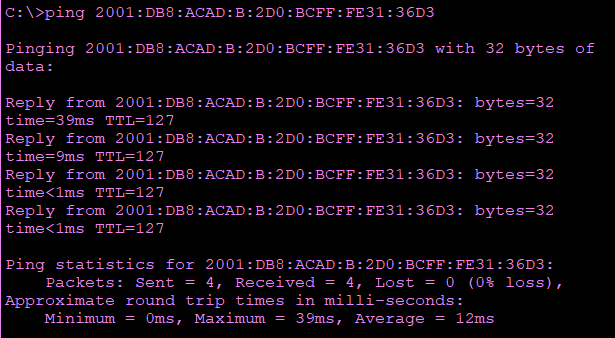


#### Hình 4.34 Các PC lấy DHCPv4 và DHCPv6 thành công

### *Kiểm tra gửi gói tin*

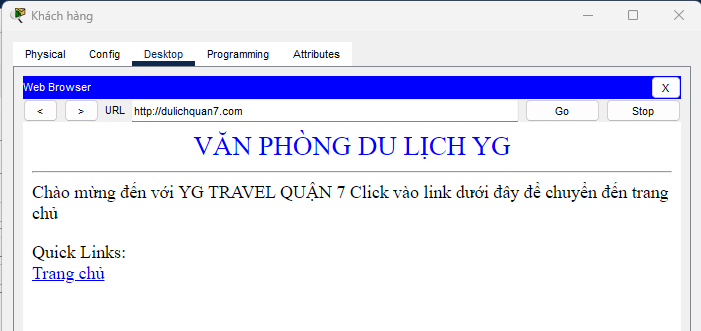


#### Hình 4.35 Các VLAN ping với nhau bằng IPv4 thành công

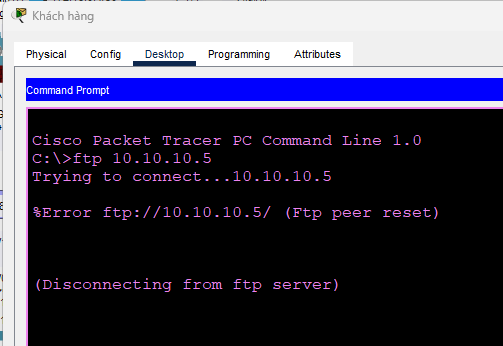


#### Hình 4.36 Các VLAN ping với nhau bằng IPv6 thành công

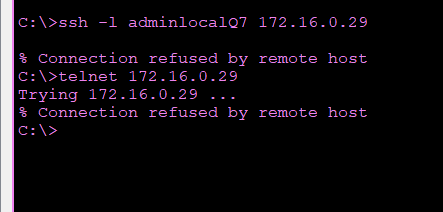
### *Kiểm tra ACL*



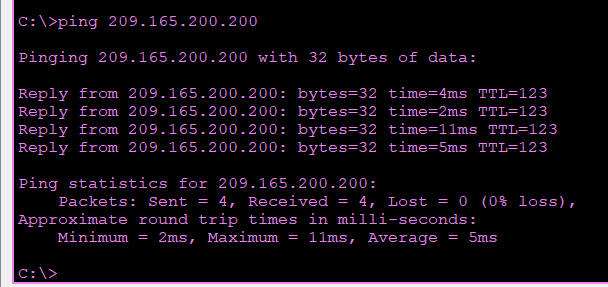
#### Hình 4.37 Khách hàng truy cập được web



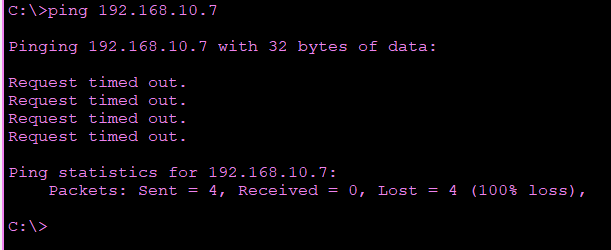
#### Hình 4.38 Khách hàng không truy cập dịch vụ FTP



#### Hình 4.39 Khách hàng không thể Telnet/SSH đến các thiết bị trong công ti

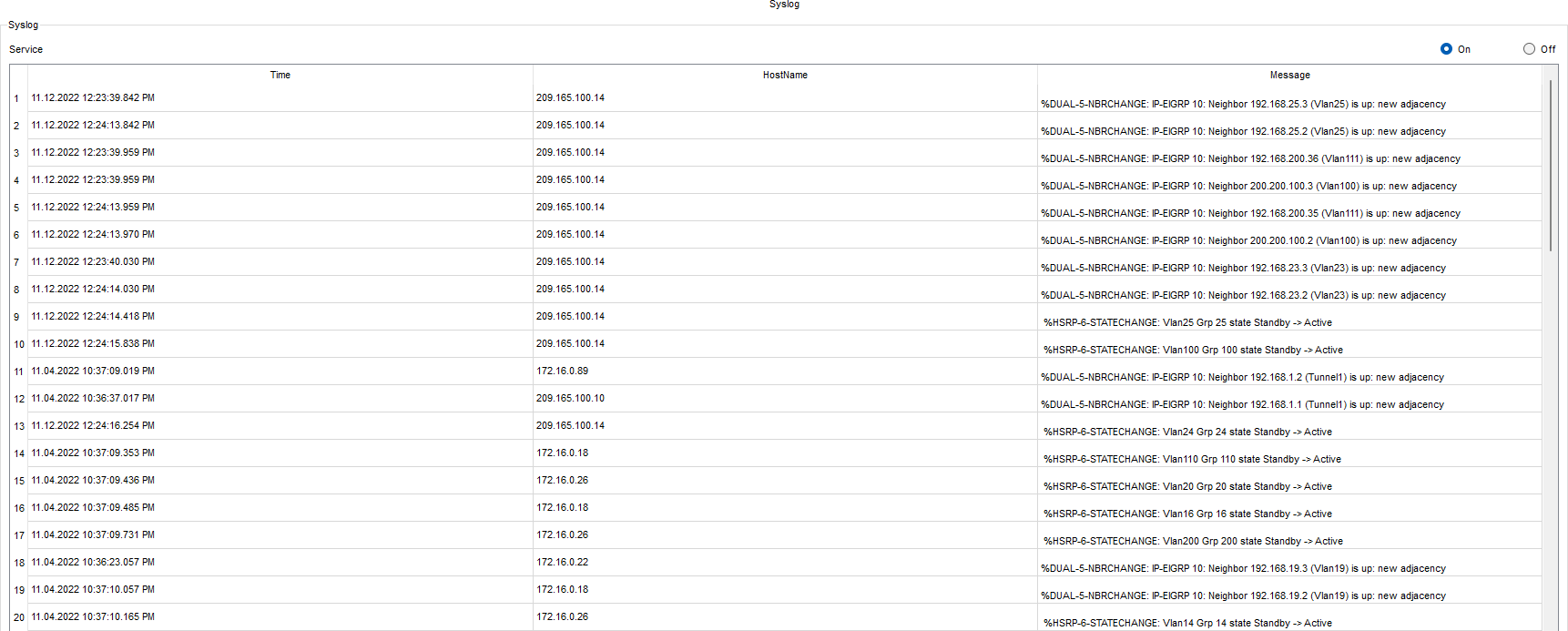


#### Hình 4.40 Khi ping đến OUTSIDE thì cho phép OUTSIDE reply



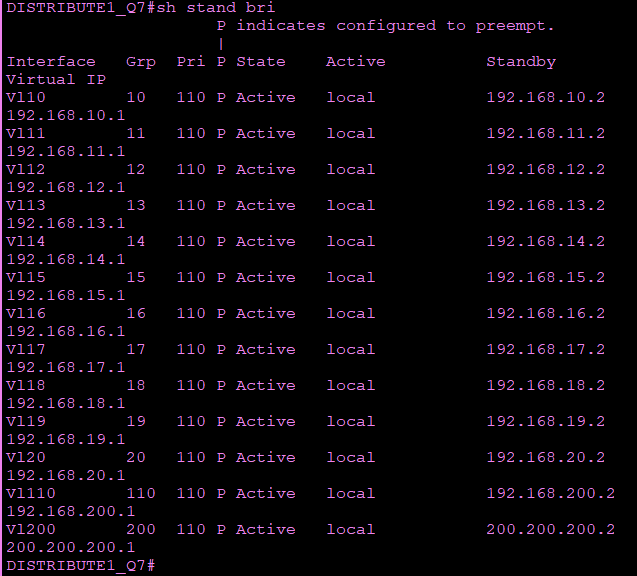
#### Hình 4.41 Nhưng OUTSIDE không thể ping vào trong công ty

### *Kiểm tra dịch vụ NTP và Syslog*

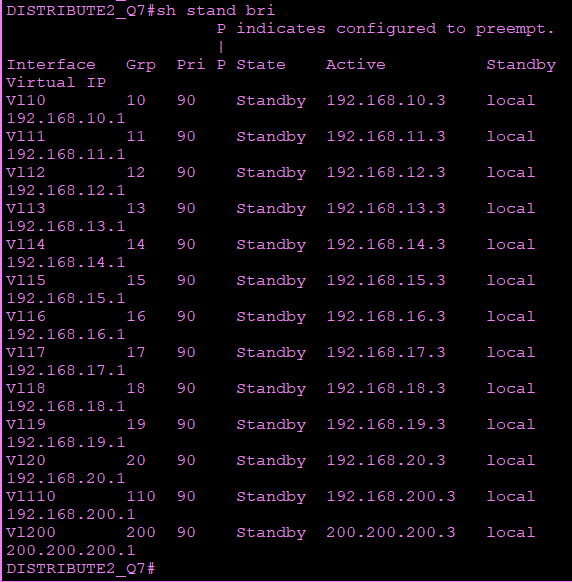


#### Hình 4.42 Syslog Server ghi lại nhật ký đăng nhập vào các thiết bị

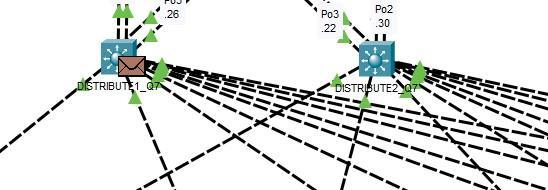
### *Kiểm tra backup*



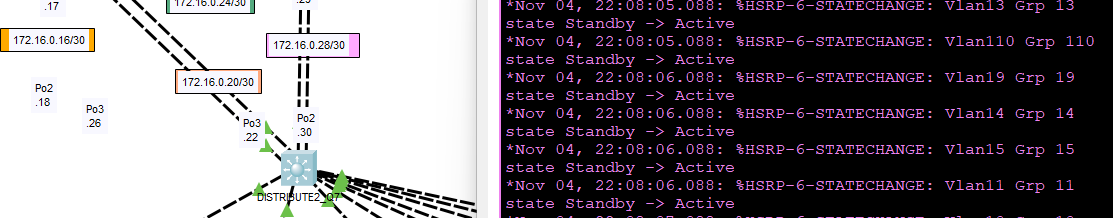
#### Hình 4.43 Cấu hình HSRP trên Distribution 1 ở trạng thái acitve

hsr

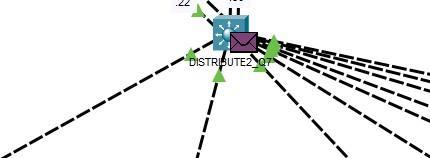
#### Hình 4.44 Cấu hình HSRP trên Distribution 1 ở trạng thái stanby



#### Hình 4.45 Khi Switch Distribution 1 hoạt động bình thường, nó sẽ chiếm quyền gửi gói tin

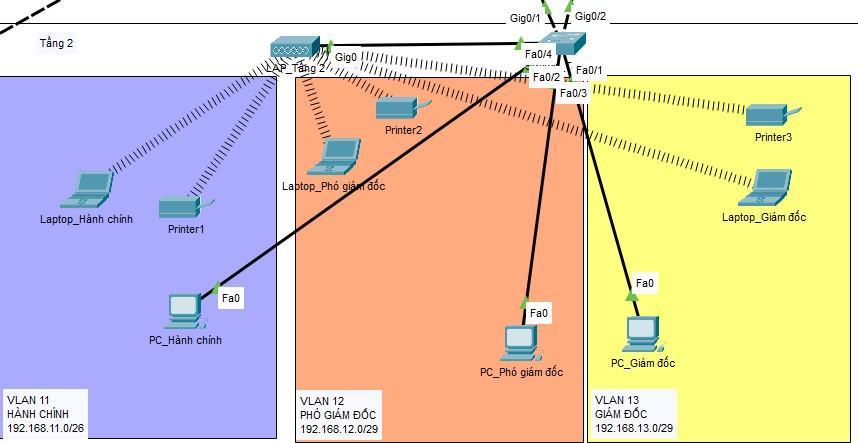


#### Hình 4.46 Khi Distribution 1 bị hư, Distribution 2 sẽ đứng lên chiếm quyền

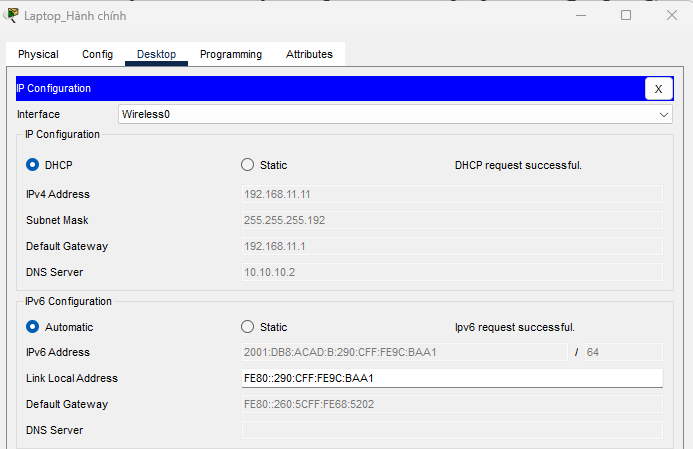


#### Hình 4.47 Khi này các gói tin gửi đi sẽ đi qua Distribution 2

### *Kiểm tra Wifi*

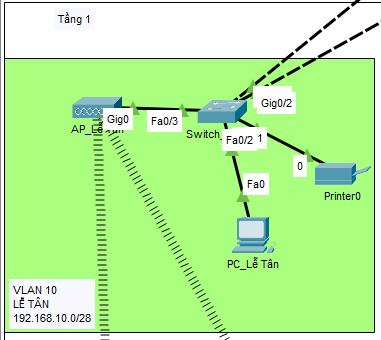


#### Hình 4.48 Các thiết bị không dây kết nối wifi thành công

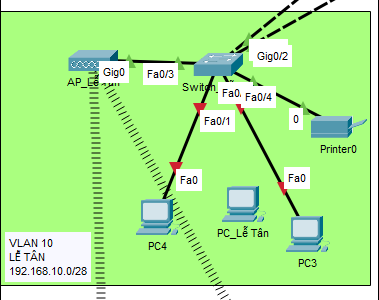


#### Hình 4.49 Thiết bị kết nối với WLAN nào thì sẽ nhận DHCP tương ứng

### *Kiểm tra Port Security*



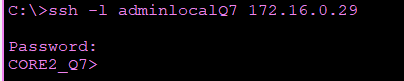
#### Hình 4.50 Port F0/1 mặc định của máy Lễ tân



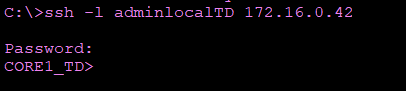
#### Hình 4.51 Port F0/1 khi nối thiết bị khác

### *Kiểm tra SSH Access*

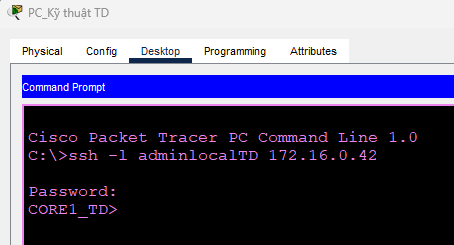
#### Phòng kỹ thuật của trụ sở quận 7 có quyền truy cập SSH vào tất cả các thiết bị ở cả hai chi nhánh. Trong khi đó phòng kỹ thuật ở chi nhánh Thủ Đức chỉ có thể truy cập SSH vào các thiết bị ở Thủ Đức.



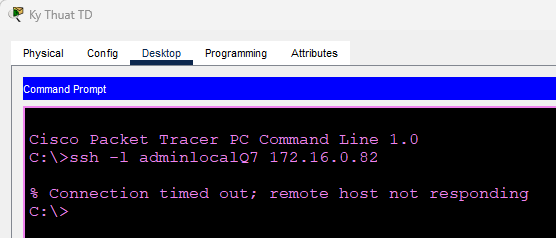
#### Hình 4.52 Phòng Kỹ thuật ở quận 7 có thể truy cập SSH vào các thiết bị ở quận 7



#### Hình 4.53 Phòng Kỹ thuật ở quận 7 có thể truy cập SSH vào các thiết bị ở Thủ Đức

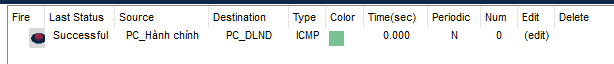


#### Hình 4.54 Phòng Kỹ thuật ở Thủ Đức có thể truy cập SSH vào các thiết bị ở Thủ Đức

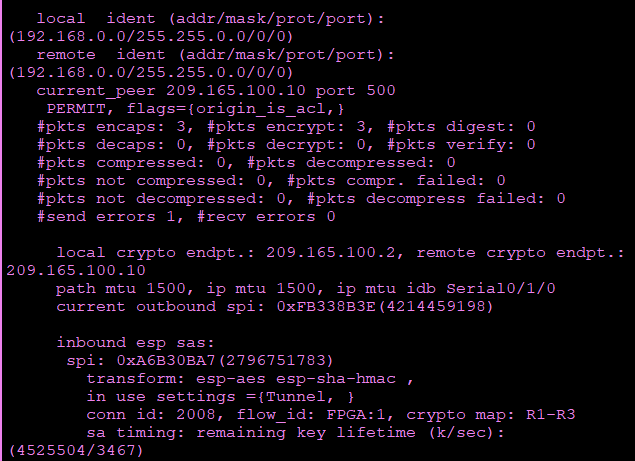


#### Hình 4.55 Phòng Kỹ thuật ở Thủ Đức không thể truy cập SSH vào các thiết bị ở quận 7

### *Kiểm tra VPN-IPsec*



#### Hình 4.56 Hai VLAN hai chi nhánh ping thành công



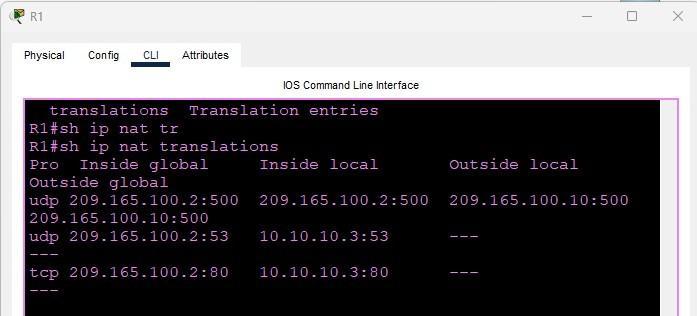
#### Hình 4.57 Mạng VLAN đi qua tunnel

### *Kiểm tra NAT*

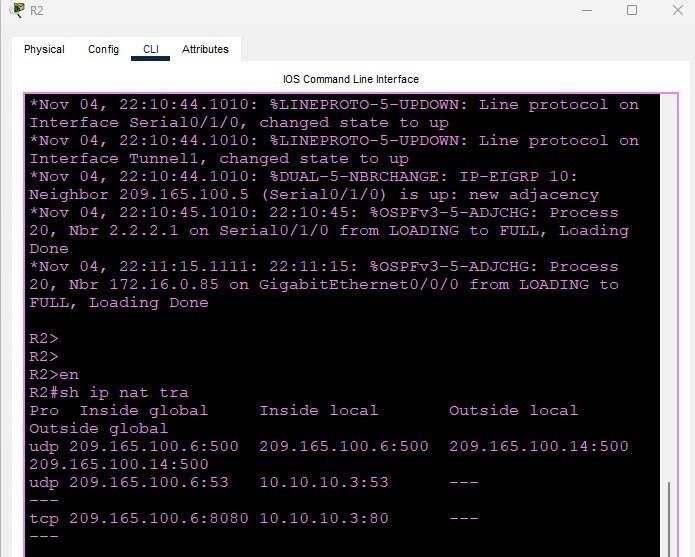
#### Các VLAN kết nối ra outside sẽ được NAT



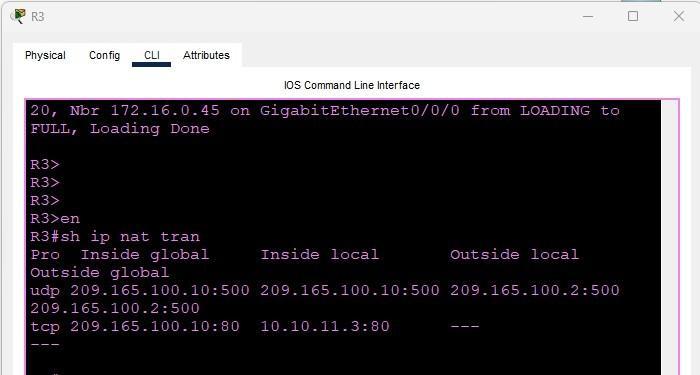
#### Hình 4.58 VLAN đi ra OUTSIDE thành công



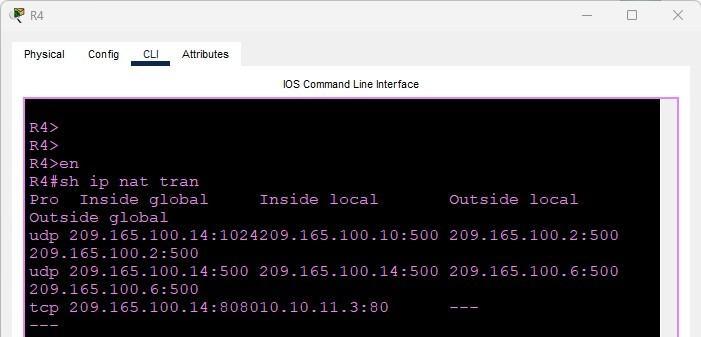
#### Hình 4.59 Kiểm tra NAT trên R1



#### Hình 4.60 Kiểm tra NAT trên R2

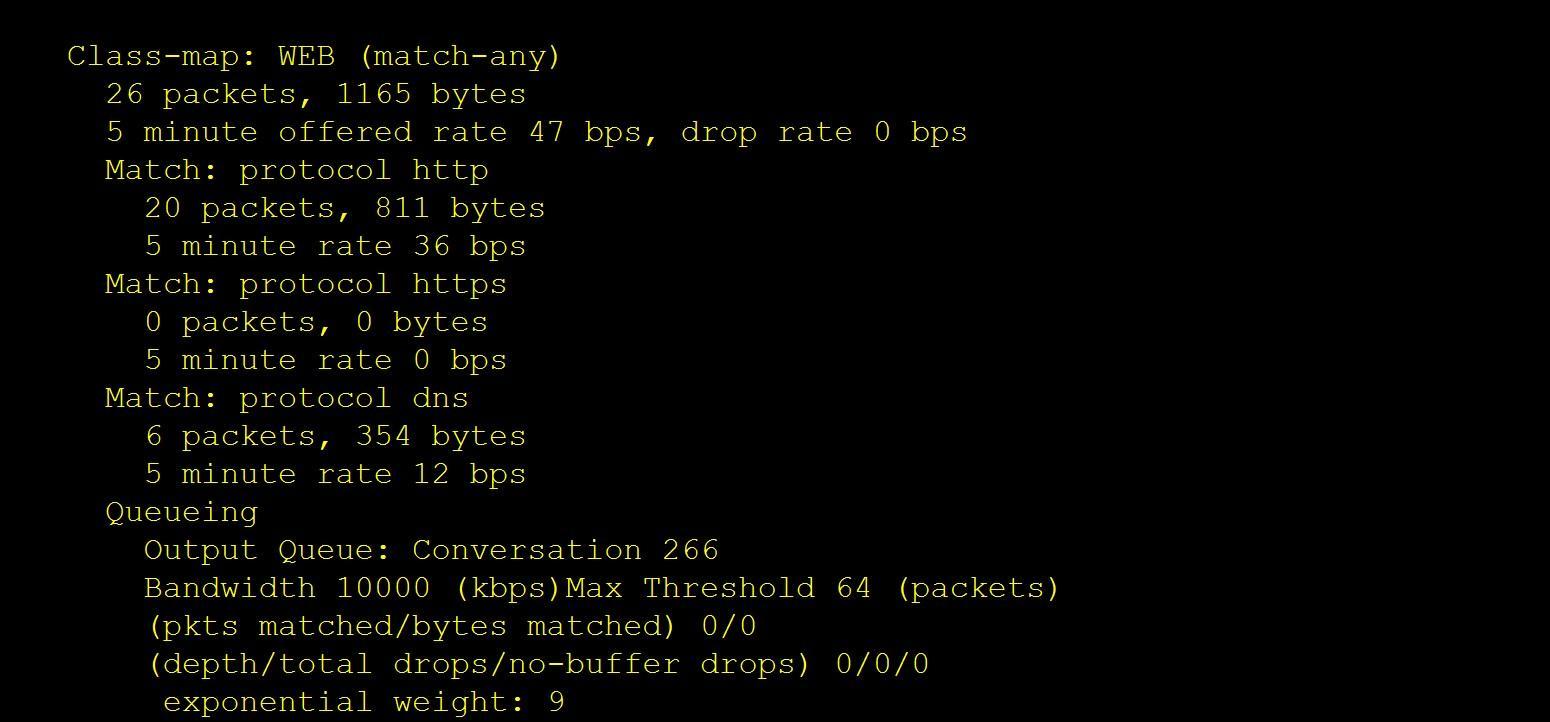


#### Hình 4.61 Kiểm tra NAT trên R3

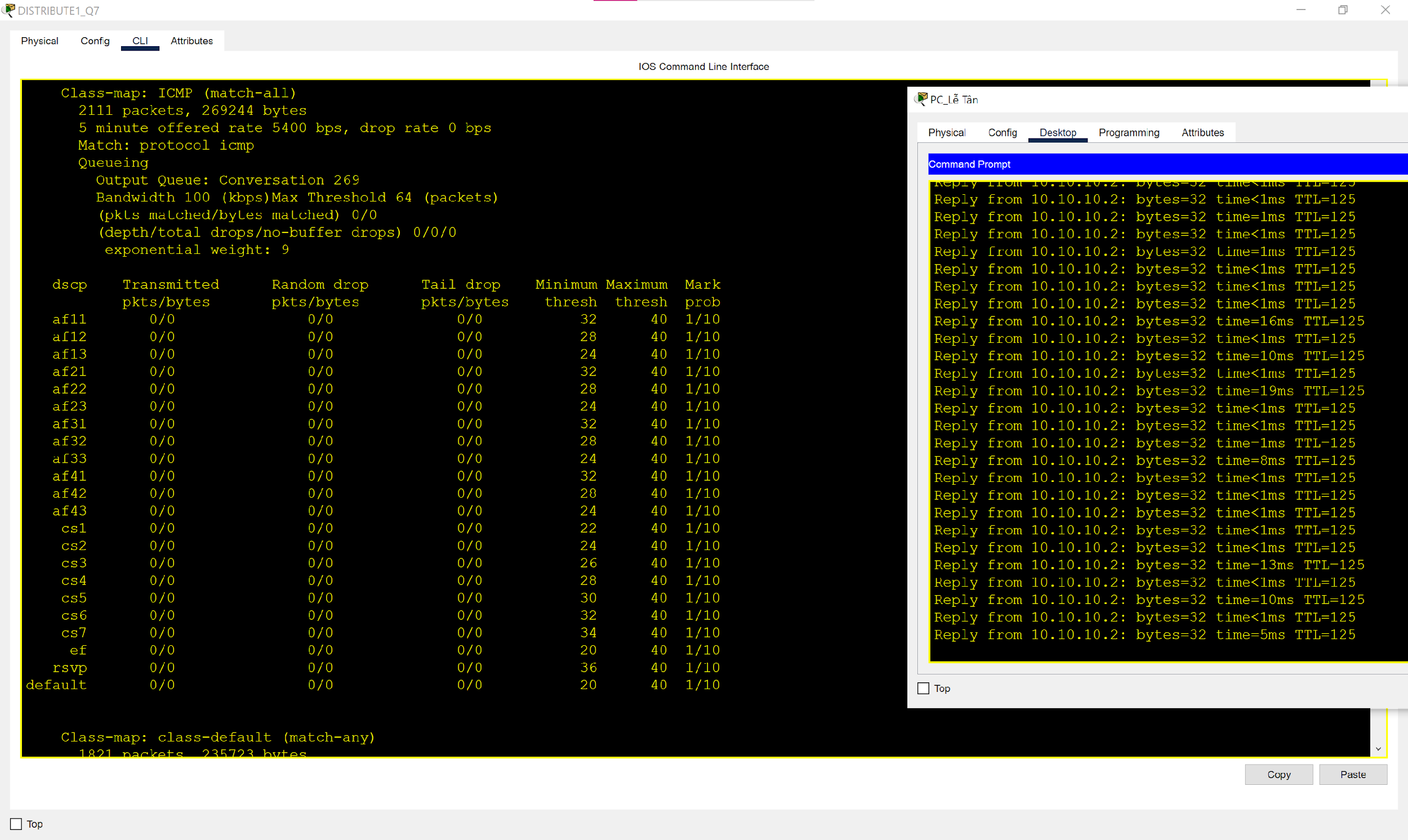


#### Hình 4.62 Kiểm tra NAT trên R4

### *Kiểm tra QoS Concept*



#### Hình 4.63 kiểm tra QoS của các traffic



#### Hình 4.64 kiểm tra QoS của các traffic

# CHƯƠNG 5 - KẾT LUẬN

#### Nhìn chung, mô hình hệ thống mạng cũng đã hoàn thiện. Toàn bộ hệ thống đã được thiết kế và cấu hình trên Cisco Packet Tracer. Mô hình đáp ứng được các yêu cầu mà khách hàng đưa ra như các máy có thể ping được với nhau trong cùng một vlan, có trang web, có thể gửi file, truy cập website thông qua mạng internet, có cấu hình HSRP và STP để dự phòng và chống lặp. Ngoài ra, các phòng chức năng cũng được cấu hình mạng không dây với cấu hình bảo mật WPA2- Enterprise, có cấu hình đầy đủ các chức năng bảo mật như tường lửa, access list, VPN-Ipsec, SSH access, DHCP Snooping và Port security.

#### Để mô hình hệ thống mạng được hoàn thiện hơn trong tương lai thì chúng ta cần phải nâng cấp tính bảo mật của mô hình. Thêm một số tính năng cần thiết như mở rộng thêm nhiều điểm truy cập, mở rộng mô hình thêm nhiều thiết bị hơn

# TÀI LIỆU THAM KHẢO

#### Configuring DHCPv6 (both stateless and stateful) in Packet Tracer. (n.d.). Computernetworking. Retrieved May 27, 2022, from https://computernetworking747640215.wordpress.com/2019/11/05/configuring-dhcpv6- both-stateless-and-stateful-in-packet-tracer/

#### Cấu hình HSRP CISCO. (n.d.). Https://Securityzone.Vn/. Retrieved May 27, 2022, from https://securityzone.vn/t/lab-13-cau-hinh-hsrp-cisco.182/

# PHỤ LỤC

1. **Password console** : dulichquan7
2. **Password console** : dulichthuduc
3. **Password enable** : vanphongcongtidulichquan7
4. **Password enable** : vanphongcongtidulichthuduc
5. **Account truy cập SSH LOCAL** : username : adminlocalQ7 , password : dulichcompanyquan7
6. **Account truy cập SSH LOCAL** : username : adminlocalTD , password : dulichcompanythuduc
7. **Account truy cập SSH CENTRAL**: username : admincentralQ7 , password : dulichcompanyquan7
8. **Account truy cập SSH CENTRAL** : username : admincentralTD , password

#### : dulichcompanythuduc

1. **Domain name** : dulichquan7.com
2. **Domain name** : dulichthuduc.com
3. **Account FTP** : username : admin , password: 123456
4. **Password truy cập vào WLC** :

#### WLC\_Q7 : https://192.168.200.4, user: admin , password: Cisco123 WLC\_TD :https://192.168.200.34, user: admin, password: Cisco123

1. **Password vtp Q7**: dulichquan7
2. **Password vtp TD**: dulichthuduc