TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN CUỐI KÌ MÔN MẠNG MÁY TÍNH NÂNG CAO**

**TRIỂN KHAI XÂY DỰNG MỘT HỆ THỐNG MẠNG MÁY TÍNH AN TOÀN CHO KÝ TÚC XÁ TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

*Người hướng dẫn*: **Thầy TRƯƠNG ĐÌNH TÚ**

*Người thực hiện*: **TRẦN VŨ CÔNG KHANH-51900804**

**LÊ HUYỀN ĐỨC-51900789**

Lớp **: 19050401 - 19050402**

Khoá  **: 23**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN CUỐI KÌ MÔN MẠNG MÁY TÍNH NÂNG CAO**

**TRIỂN KHAI XÂY DỰNG MỘT HỆ THỐNG MẠNG MÁY TÍNH AN TOÀN CHO KÝ TÚC XÁ TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

*Người hướng dẫn*: **Thầy TRƯƠNG ĐÌNH TÚ**

*Người thực hiện*: **TRẦN VŨ CÔNG KHANH-51900804**

**LÊ HUYỀN ĐỨC-51900789**

Lớp **: 19050401 - 19050402**

Khoá  **: 23**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

LỜI CẢM ƠN

Nhóm em xin gửi lời cảm ơn chân thành tới thầy Trương Đình Tú, người đã đứng lớp cả lý thuyết lẫn thực hành cho chúng em. Qua các tiết học cũng như những giờ nghiên cứu cùng thầy, chúng em đã hiểu cũng như nắm bắt được nhiều kiến thức bổ ích có thể áp dụng vào công việc cũng như nâng cao kĩ năng chuyên môn của chúng em. Trong các giờ giảng dạy, thầy luôn luôn nhiệt tình và chu đáo, cũng như sẵn sàng bỏ hết thời gian ra để giải đáp thắc mắc và chỉ ra các lỗi sai trong các đề tài và bài tập nghiên cứu của tụi em. Trong giờ học, thầy cũng đồng thời truyền được nhiệt trong học tập và khơi gợi lên sự tò mò của lớp khi bàn về một vấn đề chuyên môn và từ đó mở rộng kiến thức cùng với kinh nghiệm của thầy đã giúp cho chúng em mở mang thêm kiến thức và nhiều điều mới mẻ trong môn học này.

Lời cảm ơn thứ hai là dành tới cho những người bạn học cùng và cũng như anh chị tham gia môn học này chung với chúng em, nhờ các bạn và anh chị mà những giờ ngoài giờ lên lớp, chúng em đã có thể hỏi, tranh luận và trao đổi các kiến thức cho nhau để cùng nhau hiểu sâu sắc và nắm rõ hơn các chi tiết, nội dung mà trong lúc nghiên cứu đã nảy sinh. Nhờ những thời gian quý báu như vậy đã giúp nhóm chúng em có thể vạch ra được một kế hoạch cũng như một bản chi tiết dự án để mà có thể thiết kế và lắp đặt một cách chính xác trong bài báo cáo này.

Tuy bài báo cáo có thể vẫn còn nhiều thiếu sót nhưng dù vậy, nhóm em vẫn luôn biết ơn và chân thành gửi lời cảm ơn sâu sắc nhất tới thầy Trương Đình Tú và các bạn, anh, chị đã cùng chúng em đi qua một khoảng thời gian dài trong môn học này, từ những sai sót và sai lầm cũng như sự thiếu hụt kiến thức trong bài báo cáo này sẽ được rút ra và biến thành kinh nghiệm quý giá để chúng em có thể hoàn thiện bản thân trong tương lai.

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

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

*TP. Hồ Chí Minh, ngày 24 tháng 11 năm 2022*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Trần Vũ Công Khanh*

*Lê Huyền Đức*

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

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

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

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

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

TÓM TẮT

Vẽ và thiết kế hệ thống mạng bằng Cisco Packet Tracer.

Có cấu hình VLAN, inter-VLAN phù hợp.

Có sử dụng kỹ thuật VLSM để chia các subnet cho hệ thống mạng.

Có cấu hình song song IPv4 và IPv6 cho các thiết bị.

Thiết kế mạng có tính dự phòng, và có sử dụng STP để chống LOOP.

Có cấu hình định tuyến động dùng OSPF.

Có cấu hình bảo mật dùng ACLs, VPN, IPSec.

Có cấu hình kết nối WAN, WLAN.

Trong hệ thống có cài đặt và cấu hình đầy đủ các dịch vụ mạng như: DHCP,

DNS Server, Web Server, FTP server và Mail server. Ngoài ra còn có các server khác như NTP Server, Syslog Server và Radius Server A/B/C.

Trên DNS server đặt tên Domain lần lượt là khuA.tdtu.edu.vn, khuB.tdtu.edu.vn, khuC.tdtu.edu.vn và tdtu.edu.vn.

Trên Mail Server tạo một domain name là tdtu.edu.vn với các tài khoản lần lượt là [sinhvien1@tdtu.edu.vn](mailto:sinhvien1@tdtu.edu.vn), [sinhvien2@tdtu.edu.vn](mailto:sinhvien2@tdtu.edu.vn), [quanly1@tdtu.edu.vn](mailto:quanly1@tdtu.edu.vn), [quanly2@tdtu.edu.vn](mailto:quanly2@tdtu.edu.vn), [giangvien1@tdtu.edu.vn](mailto:giangvien1@tdtu.edu.vn) và [giangvien2@tdtu.edu.vn](mailto:giangvien2@tdtu.edu.vn). Các user đều gửi mail được với nhau. Password chung là: 123.

Các client có thể sử dụng dịch vụ FTP để download/upload file từ/đến server. Có 2 user có toàn quyền là student1 và student2 với password chung là 123.

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc120191389)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc120191390)

[TÓM TẮT iv](#_Toc120191391)

[MỤC LỤC 1](#_Toc120191392)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 2](#_Toc120191393)

[I. SƠ ĐỒ LẮP ĐẶT TỦ RACK: 3](#_Toc120191394)

[II. MÔ HÌNH HỆ THỐNG: 4](#_Toc120191395)

[a. Mô hình kết nối luận lý: 4](#_Toc120191396)

[b. Mô hình kết nối vật lý: 4](#_Toc120191397)

[III. THÔNG TIN CÀI ĐẶT CẤU HÌNH HỆ THỐNG: 5](#_Toc120191398)

[a. Thông tin kết nối port trong hệ thống: 5](#_Toc120191399)

[b. Thông tin vlan, interface vlan trong hệ thống: 9](#_Toc120191400)

[c. Bảng địa chỉ IP: 13](#_Toc120191401)

[d. Bảng Mode VLAN của các Switch: 17](#_Toc120191402)

[IV. Cấu hình hạ tầng: 18](#_Toc120191403)

[TÀI LIỆU THAM KHẢO 34](#_Toc120191404)

[Tiếng Việt 34](#_Toc120191405)

[Tiếng Anh 34](#_Toc120191406)

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

[Hình 1.1: Sơ đồ lắp đặt tủ rack. 3](#_Toc120191407)

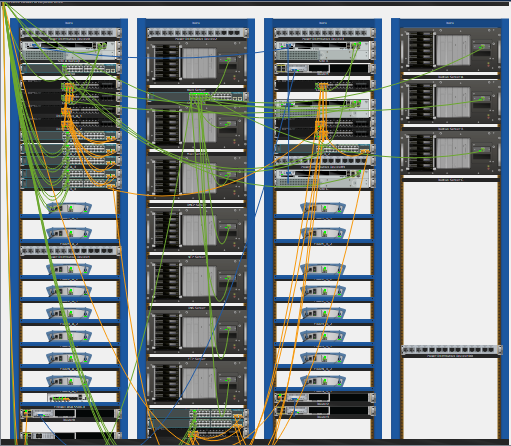
[Hình 2.1: Mô hình kết nối luận lý. 4](#_Toc120191408)

[Hình 2.2: Mô hình kết nối vật lý. 4](#_Toc120191409)

[Hình 4.1: Bảng ACL trên Router Site C. 32](#_Toc120191410)

[Hình 4.2: Bảng ACL trên Router Servers. 33](#_Toc120191411)

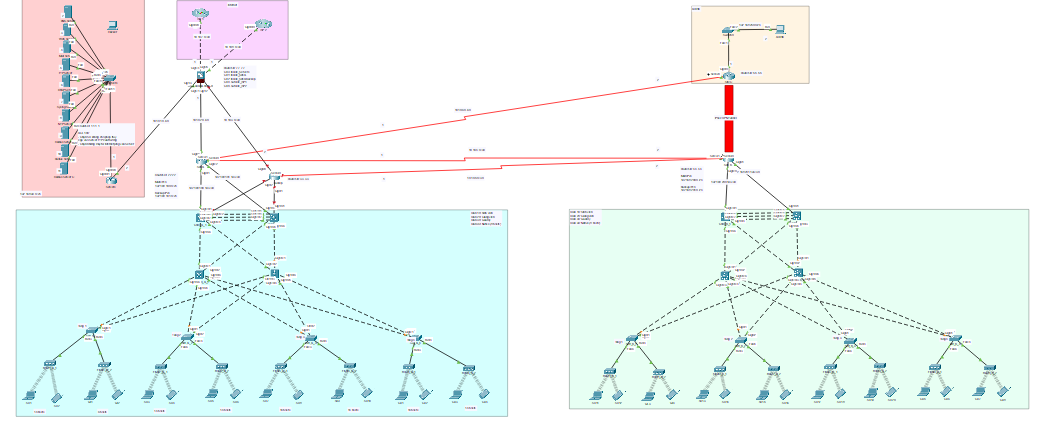
I. SƠ ĐỒ LẮP ĐẶT TỦ RACK:



Hình 1.1: Sơ đồ lắp đặt tủ rack.

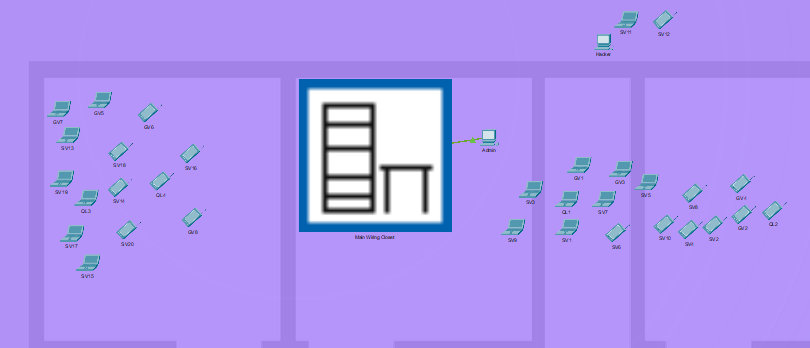
II. MÔ HÌNH HỆ THỐNG:

a. Mô hình kết nối luận lý:

****

Hình 2.1: Mô hình kết nối luận lý.

b. Mô hình kết nối vật lý:

****

Hình 2.2: Mô hình kết nối vật lý.

III. THÔNG TIN CÀI ĐẶT CẤU HÌNH HỆ THỐNG:

a. Thông tin kết nối port trong hệ thống:

|  |  |  |  |
| --- | --- | --- | --- |
| **Source to Destination Device** | **Source interface** | **Destination interface** | **VLAN / TRUNKING** |
| Site A to ASA 5506-X | G0/0 | G1/1 | N/A |
| Site A to Core\_A\_1 | G0/1 | G1/0/1 | TRUNKING NATIVE VLAN 99 |
| Site A to Core\_A\_2 | G0/2 | G1/0/1 | TRUNKING NATIVE VLAN 99 |
| Site A to Site B | Se0/3/0 | Se0/3/0 | N/A |
| Site A to Site C | Se0/3/1 | Se0/3/0 | N/A |
| Site A BackUp to ASA 5506-X | G0/0 | G1/2 | N/A |
| Site A BackUp to Core\_A\_1 | G0/1 | G1/0/1 | TRUNKING NATIVE VLAN 99 |
| Site A BackUp to Core\_A\_2 | G0/2 | G1/0/1 | TRUNKING NATIVE VLAN 99 |
| Site A BackUp to Site B | Se0/3/0 | Se0/3/1 | N/A |
| Servers to ASA 5506-X | G0/0/0 | G1/3 | N/A |
| Core\_A\_1 to Distribution\_A\_1 | G1/0/3 | G1/0/1 | TRUNKING NATIVE VLAN 99 |
| Core\_A\_1 to Distribution\_A\_2 | G1/0/4 | G1/0/2 | TRUNKING NATIVE VLAN 99 |
| Core\_A\_2 to Distribution\_A\_1 | G1/0/3 | G1/0/1 | TRUNKING NATIVE VLAN 99 |
| Core\_A\_2 to Distribution\_A\_2 | G1/0/4 | G1/0/2 | TRUNKING NATIVE VLAN 99 |
| Distribution A\_1 to SW\_A\_1,  SW\_A\_2,  SW\_A\_3,  SW\_A\_4 | G1/0/5-6 | G0/1 | TRUNKING NATIVE VLAN 99 |
| Distribution A\_2 to SW\_A\_1,  SW\_A\_2,  SW\_A\_3,  SW\_A\_4 | G1/0/5-6 | G0/2 | TRUNKING NATIVE VLAN 99 |
| SW\_A\_1 to Floor1\_A\_1, Floor1\_A\_2 | Fa0/3-4 | Port0 | VLAN 10, VLAN 30 |
| SW\_A\_2 to Floor2\_A\_1, Floor2\_A\_2 | Fa0/3-4 | Port0 | VLAN 10 |
| SW\_A\_3 to Floor3\_A\_1, Floor3\_A\_2 | Fa0/3-4 | Port0 | VLAN 10 |
| SW\_A\_4 to Floor4\_A\_1, Floor4\_A\_2 | Fa0/3-4 | Port0 | VLAN 30 |
| Servers to SW\_Servers | G0/0/1 | Fa0/1 | N/A |
| SW\_Servers to All Servers | Fa0/2-11 | Fa0 | N/A |
| ASA 5506-X to ISP1 | G1/4 | G/0/0/0 | N/A |
| ASA 5506-X to ISP2 | G1/5 | G/0/0/0 | N/A |
| Site B to Core\_B\_1 | G0/0 | G1/0/1 | TRUNKING NATIVE VLAN 99 |
| Site B to Core\_B\_2 | G0/1 | G1/0/1 | TRUNKING NATIVE VLAN 99 |
| Core\_B\_1 to Distribution\_B\_1 | G1/0/3 | G1/0/1 | TRUNKING NATIVE VLAN 99 |
| Core\_B\_1 to Distribution\_B\_2 | G1/0/4 | G1/0/2 | TRUNKING NATIVE VLAN 99 |
| Core\_B\_2 to Distribution\_B\_1 | G1/0/3 | G1/0/1 | TRUNKING NATIVE VLAN 99 |
| Core\_B\_2 to Distribution\_B\_2 | G1/0/4 | G1/0/2 | TRUNKING NATIVE VLAN 99 |
| Distribution B\_1 to SW\_B\_1,  SW\_B\_2,  SW\_B\_3,  SW\_B\_4 | G1/0/5-6 | G0/1 | TRUNKING NATIVE VLAN 99 |
| Distribution B\_2 to SW\_B\_1,  SW\_B\_2,  SW\_B\_3,  SW\_B\_4 | G1/0/5-6 | G0/2 | TRUNKING NATIVE VLAN 99 |
| SW\_B\_1 to Floor1\_B\_1, Floor1\_B\_2 | Fa0/3-4 | Port0 | VLAN 10, VLAN 30 |
| SW\_B\_2 to Floor2\_B\_1, Floor2\_B\_2 | Fa0/3-4 | Port0 | VLAN 10 |
| SW\_B\_3 to Floor3\_B\_1, Floor3\_B\_2 | Fa0/3-4 | Port0 | VLAN 10 |
| SW\_B\_4 to Floor4\_B\_1, Floor4\_B\_2 | Fa0/3-4 | Port0 | VLAN 30 |
| Core\_A\_1 to Core\_A\_2 | G1/0/5-7 | G1/0/5-7 | TRUNKING NATIVE VLAN 99/EtherGroup1 |
| Core\_B\_1 to Core\_B\_2 | G1/0/5-7 | G1/0/5-7 | TRUNKING NATIVE VLAN 99/EtherGroup1 |
| Site C to Switch0 | G0/0 | Fa0/1 | N/A |
| Switch0 to Admin | Fa0/2 | Fa0 | N/A |

b. Thông tin vlan, interface vlan trong hệ thống:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Bảng địa mạng cho các VLAN/Router trong các KTX A** | | | | | | | |
| **VLAN Id** | **VLAN Name** | **Number**  **(118 host)** | **Network** | **Subnet** | **Usable Range** | **Broadcast** | **Wildcard** |
| VLAN 10 | SinhVien | 72 | 192.168.100.0 | 255.255.255.128  (/25) | 192.168.100.1 - 192.168.100.126 | 192.168.100.127 | 0.0.0.127 |
| 192.168.101.0 | 255.255.255.128  (/25) | 192.168.101.1 - 192.168.101.126 | 192.168.101.127 | 0.0.0.127 |
| VLAN 20 | GiangVien | 30 | 192.168.100.128 | 255.255.255.224  (/27) | 192.168.100.129 - 192.168.100.158 | 192.168.100.159 | 0.0.0.31 |
| 192.168.101.128 | 255.255.255.224  (/27) | 192.168.101.129 - 192.168.101.158 | 192.168.101.159 | 0.0.0.31 |
| VLAN 30 | QuanLy | 8 | 192.168.100.176 | 255.255.255.240  (/28) | 192.168.100.177 - 192.168.100.190 | 192.168.100.191 | 0.0.0.15 |
| 192.168.101.176 | 255.255.255.240  (/28) | 192.168.101.177 - 192.168.101.190 | 192.168.101.191 | 0.0.0.15 |
| VLAN 99 | Native | 10 | 192.168.100.160 | 255.255.255.240  (/28) | 192.168.100.161 - 192.168.100.174 | 192.168.100.175 | 0.0.0.15 |
| 192.168.101.160 | 255.255.255.240  (/28) | 192.168.101.161 - 192.168.101.174 | 192.168.101.175 | 0.0.0.15 |
| Router | Router | 2 | 192.168.100.192 | 255.255.255.252  (/30) | 192.168.100.193 - 192.168.100.194 | 192.168.100.195 | 0.0.0.3 |
| 192.168.101.192 | 255.255.255.252  (/30) | 192.168.101.193 - 192.168.101.194 | 192.168.101.195 | 0.0.0.3 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Bảng địa mạng cho các VLAN/Router trong các KTX B** | | | | | | | |
| **VLAN Id** | **VLAN Name** | **Number**  **(118 host)** | **Network** | **Subnet** | **Usable Range** | **Broadcast** | **Wildcard** |
| VLAN 10 | SinhVien | 72 | 192.168.200.0 | 255.255.255.128  (/25) | 192.168.200.1 - 192.168.200.126 | 192.168.200.127 | 0.0.0.127 |
| 192.168.201.0 | 255.255.255.128  (/25) | 192.168.201.1 - 192.168.201.126 | 192.168.201.127 | 0.0.0.127 |
| VLAN 20 | GiangVien | 30 | 192.168.200.128 | 255.255.255.224  (/27) | 192.168.200.129 - 192.168.200.158 | 192.168.200.159 | 0.0.0.31 |
| 192.168.201.128 | 255.255.255.224  (/27) | 192.168.201.129 - 192.168.201.158 | 192.168.201.159 | 0.0.0.31 |
| VLAN 30 | QuanLy | 8 | 192.168.200.176 | 255.255.255.240  (/28) | 192.168.200.177 - 192.168.200.190 | 192.168.200.191 | 0.0.0.15 |
| 192.168.201.176 | 255.255.255.240  (/28) | 192.168.201.177 - 192.168.201.190 | 192.168.201.191 | 0.0.0.15 |
| VLAN 99 | Native | 10 | 192.168.200.160 | 255.255.255.240  (/28) | 192.168.200.161 - 192.168.200.174 | 192.168.200.175 | 0.0.0.15 |
| 192.168.201.160 | 255.255.255.240  (/28) | 192.168.201.161 - 192.168.201.174 | 192.168.201.175 | 0.0.0.15 |
| Router | Router | 2 | 192.168.200.192 | 255.255.255.252  (/30) | 192.168.200.193 - 192.168.200.194 | 192.168.200.195 | 0.0.0.3 |
| 192.168.201.192 | 255.255.255.252  (/30) | 192.168.201.193 - 192.168.201.194 | 192.168.201.195 | 0.0.0.3 |

c. Bảng địa chỉ IP:

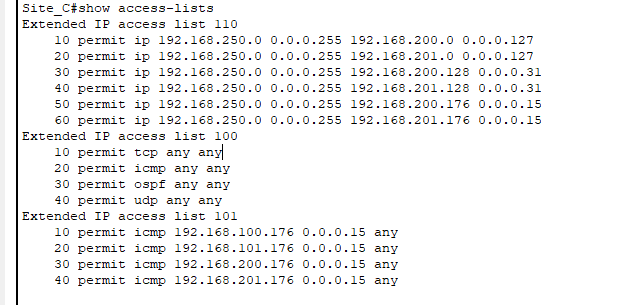
|  |  |  |  |
| --- | --- | --- | --- |
| **Servers** | **Port** | **Ipv4/Subnet Mask** | **Ipv6** |
| DNS | Fa0 | 192.168.99.2 /24 | 2001:C0A8:99::2 |
| WEB | Fa0 | 192.168.99.3 /24 | 2001:C0A8:99::3 |
| MAIL | Fa0 | 192.168.99.4 /24 | 2001:C0A8:99::4 |
| FTP | Fa0 | 192.168.99.5 /24 | 2001:C0A8:99::5 |
| DHCP | Fa0 | 192.168.99.6 /24 | 2001:C0A8:99::6 |
| SYSLOG | Fa0 | 192.168.99.7 /24 | 2001:C0A8:99::7 |
| NTP | Fa0 | 192.168.99.8 /24 | 2001:C0A8:99::8 |
| Radius Server A | Fa0 | 192.168.99.9 /24 | 2001:C0A8:99::9 |
| Radius Server B | Fa0 | 192.168.99.10 /24 | 2001:C0A8:99::10 |
| Radius Server C | Fa0 | 192.168.99.11 /24 | 2001:C0A8:99::11 |
| **Router** | **Port** | **Ipv4/Subnet Mask** | **Ipv6** |
| Site A | G0/0 | 10.10.2.2 /30 | 2001:C0A8:2::2  FE80::2 |
| G0/1 | 192.168.100.193 /30 | 2001:C0A8:100::1  FE80::2 |
| G0/1.10 | 192.168.100.1 /25 | 2001:C0A8:110::1  FE80::2 |
| G0/1.20 | 192.168.100.129 /27 | 2001:C0A8:120::1  FE80::2 |
| G0/1.30 | 192.168.100.177 /28 | 2001:C0A8:130::1  FE80::2 |
| G0/2 | 192.168.101.193 /30 | 2001:C0A8:101::1  FE80::2 |
| G0/2.10 | 192.168.101.1 /25 | 2001:C0A8:111::1  FE80::2 |
| G0/2.20 | 192.168.101.129 /27 | 2001:C0A8:121::1  FE80::2 |
| G0/2.30 | 192.168.101.177 /28 | 2001:C0A8:131::1  FE80::2 |
| Se0/3/0 | 10.10.4.1 /30 | 2001:C0A8:4::2  FE80::2 |
| Se0/3/1 | 10.10.6.1 /30 | N/A |
| Site A\_BackUp | G0/0 | 10.10.3.2 /30 | 2001:C0A8:3::2  FE80::3 |
| G0/1 | 192.168.100.193 /30 | 2001:C0A8:100::1  FE80::3 |
| G0/1.10 | 192.168.100.1 /25 | 2001:C0A8:110::1  FE80::3 |
| G0/1.20 | 192.168.100.129 /27 | 2001:C0A8:120::1  FE80::3 |
| G0/1.30 | 192.168.100.177 /28 | 2001:C0A8:130::1  FE80::3 |
| G0/2 | 192.168.101.193 /30 | 2001:C0A8:101::1  FE80::3 |
| G0/2.10 | 192.168.101.1 /25 | 2001:C0A8:111::1  FE80::3 |
| G0/2.20 | 192.168.101.129 /27 | 2001:C0A8:121::1  FE80::3 |
| G0/2.30 | 192.168.101.177 /28 | 2001:C0A8:131::1  FE80::3 |
| Se0/3/0 | 10.10.5.1 /30 | 2001:C0A8:5::2  FE80::2 |
| Se0/3/1 | N/A | N/A |
| Site B | G0/0 | 192.168.200.193 /30 | 2001:C0A8:200::1  FE80::4 |
| G0/1 | 192.168.201.193 /30 | 2001:C0A8:201::1  FE80::4 |
| G0/0.10 | 192.168.200.1 /25 | 2001:C0A8:210::1  FE80::4 |
| G0/0.20 | 192.168.200.129 /27 | 2001:C0A8:220::1  FE80::4 |
| G0/0.30 | 192.168.200.177 /28 | 2001:C0A8:230::1  FE80::4 |
| G0/2 | N/A | N/A |
| G0/1.10 | 192.168.201.1 /25 | 2001:C0A8:211::1  FE80::4 |
| G0/1.20 | 192.168.201.129 /27 | 2001:C0A8:221::1  FE80::4 |
| G0/1.30 | 192.168.201.177 /28 | 2001:C0A8:231::1  FE80::4 |
| Se0/3/0 | 10.10.4.2 /30 | 2001:C0A8:4::1  FE80::4 |
| Se0/3/1 | 10.10.5.2 /30 | 2001:C0A8:5::1  FE80::4 |
| Site C | Se0/3/0 | 10.10.6.2 /30 | N/A |
| G0/0 | 192.168.250.1 /24 | N/A |
| Admin | Fa0 | 192.168.250.2 /24 | N/A |
| Server | Gig0/0/0 | 10.10.1.2 /30 | 2001:C0A8:1::2  FE80::1 |
| Gig0/0/1 | 192.168.99.1 /24 | 2001:C0A8:99::1  FE80::1 |
| ASA 5506-X | Gig1/1 | 10.10.2.1 /30 | 2001:C0A8:2::1  FE80::8 |
| Gig1/2 | 10.10.3.1 /30 | 2001:C0A8:3::1  FE80::9 |
| Gig1/3 | 10.10.1.1 /30 | 2001:C0A8:1::1  FE80::7 |
| Gig1/4 | 10.10.7.1 /30 | N/A |
| G1/5 | 10.10.8.1 /30 | N/A |
| Router0 | G0/0/0 | 10.10.7.2 /30 | N/A |
| Router2 | G0/0/0 | 10.10.7.2 /30 | N/A |

d. Bảng Mode VLAN của các Switch:

|  |  |  |  |
| --- | --- | --- | --- |
| **Switch** | **Port** | **Mode** | **VLAN** |
| Core\_A\_1  Core\_B\_1 | Fa0/1-4 | Trunking Native Vlan 99 | N/A |
| G1/0/5-7 | Etherchannel group 1 PAgP  Trunking Native Vlan 99 | N/A |
| Core\_A\_2  Core\_B\_2 | Fa0/1-4 | Trunking Native Vlan 99 | N/A |
| G1/0/5-7 | Etherchannel group 1 PAgP  Trunking Native Vlan 99 | N/A |
| Distribution\_A\_1  Distribution\_B\_1 | Fa0/1-6 | Trunking Native Vlan 99 | N/A |
| Distribution\_A\_2  Distribution\_B\_2 | Fa0/1-6 | Trunking Native Vlan 99 | N/A |
| SW\_A\_1  SW\_B\_1 | Fa0/3 | Access | 10 |
| Fa0/4 | Access | 30 |
| Fa0/1-2 | Trunking Native Vlan 99 | N/A |
| SW\_A\_2  SW\_B\_2 | Fa0/3-4 | Access | 10 |
| Fa0/1-2 | Trunking Native Vlan 99 | N/A |
| SW\_A\_3  SW\_B\_3 | Fa0/3-4 | Access | 10 |
| Fa0/1-2 | Trunking Native Vlan 99 | N/A |
| SW\_A\_4  SW\_B\_4 | Fa0/3-4 | Access | 20 |
| Fa0/1-2 | Trunking Native Vlan 99 | N/A |

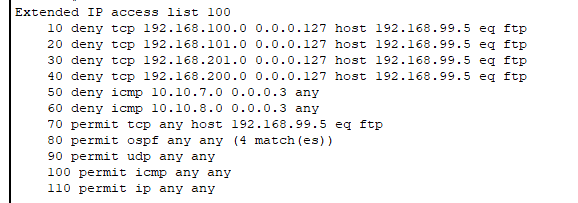
IV. Cấu hình hạ tầng:

* OSPF giữa các router:
  + Show ip protocols
  + *Router Site A:*
    - Router-id: 2.2.2.2
    - ospf 1
    - network 192.168.100.0 0.0.0.255 area 0
    - network 192.168.101.0 0.0.0.255 area 0
    - network 10.10.2.0 0.0.0.3 area 0
    - network 10.10.4.0 0.0.0.3 area 0
  + *Router Site A\_BackUp:*
    - Router-id: 3.3.3.3
    - ospf 1
    - network 192.168.100.0 0.0.0.255 area 0
    - network 192.168.101.0 0.0.0.255 area 0
    - network 10.10.3.0 0.0.0.3 area 0
    - network 10.10.5.0 0.0.0.3 area 0
  + *Router Site B:*
    - Router-id: 4.4.4.4
    - ospf 1
    - network 192.168.200.0 0.0.0.255 area 0
    - network 192.168.201.0 0.0.0.255 area 0
    - network 10.10.4.0 0.0.0.3 area 0
    - network 10.10.5.0 0.0.0.3 area 0
  + *Router Servers:*
    - Router-id: 1.1.1.1
    - ospf 1
    - network 192.168.99.0 0.0.0.255 area 0
    - network 10.10.1.0 0.0.0.3 area 0
  + *Router Site A\_BackUp:*
    - Router-id: 3.3.3.3
    - ospf 1
    - network 10.10.3.0 0.0.0.3 area 0
  + *ASA 5506-X:*
    - Router-id: 7.7.7.7
    - ospf 1
    - network 10.10.1.0 255.255.255.252 area 0
    - network 10.10.2.0 255.255.255.252 area 0
    - network 10.10.3.0 255.255.255.252 area 0
    - network 10.10.7.0 255.255.255.252 area 0
    - network 10.10.8.0 255.255.255.252 area 0
* Cấu hình ip trên ASA 5506-X:
  + *Gig 1/3:*
    - namif inside\_Servers
    - security-level 100
    - ip address 10.10.1.1 255.255.255.252
    - no shutdown
  + *Gig 1/1:*
    - namif inside\_SiteA
    - security-level 100
    - ip address 10.10.2.1 255.255.255.252
    - no shutdown
  + *Gig 1/2:*
    - namif inside\_SiteABackUp
    - security-level 100
    - ip address 10.10.3.1 255.255.255.252
    - no shutdown
* Thiết lập trên Mail server:
  + domain name: tdtu.edu.vn
    - User: student1
      * Password: 123
    - User: student2
      * Password: 123
* Thiết lập trên FTP server:
  + User: student1
    - Password: 123
  + User: student2
    - Password: 123
* Thiết lập trên các Access Point:
  + *Floor1\_A\_1*
    - SSID: Floor1\_A\_1
    - Password: 12345678
  + *Floor2\_A\_1*
    - SSID: Floor2\_A\_1
    - Password: 12345678
  + *Floor3\_A\_1*
    - SSID: Floor3\_A\_1
    - Password: 12345678
  + *Floor4\_A\_1*
    - SSID: Floor4\_A\_1
    - Password: 12345678
  + *Floor1\_A\_2*
    - SSID: Floor1\_A\_2
    - Password: 12345678
  + *Floor2\_A\_2*
    - SSID: Floor2\_A\_2
    - Password: 12345678
  + *Floor3\_A\_2*
    - SSID: Floor3\_A\_2
    - Password: 12345678
  + *Floor4\_A\_2*
    - SSID: Floor4\_A\_2
    - Password: 12345678
* Sub-interface cho VLAN 10 trên Router Site A:
  + interface g0/1.10
  + encapsulation dot1q 10
  + ip address 192.168.100.1 255.255.255.128
  + no shutdown
  + Làm tương tự cho các VLAN khác tương ứng với các interface .20, .30 cùng với địa chỉ VLAN tương ứng đã chia ở trên.
* Lấy địa chỉ ip từ DHCP Server trên các cổng sub-interface trên Router Site A:
  + interface g0/1.10
  + ip helper-address 192.168.99.6
  + Làm tương tự các sub-interface còn lại
* Thiết lập spanning-tree vlan 1, 10, 20, 30, 99 root primary trên Core\_A\_1 và Core\_B\_1
* Thiết lập port-security trên switch nối các server.
  + show port-security
* Thiết lập dhcp snooping với các cổng từ các switch nối các thiết bị host, switch và router. (limit rate là 20: giới hạn các packet truyền nhận mỗi giây để ngăn server quá tải).
  + show ip dhcp snooping
* ACL Extended 100
  + Chặn các SV trong ktx xài ftp
  + Đặt lên các subinterface của SV theo chiều in.
* Tạo dhcpv6 pool cho Router Site\_A:
  + ipv6 dhcp pool vlan\_10:
    - address prefix 2001:C0A8:110::/64
    - dns-server 2001:C0A8:99::3
  + Trên cổng interface gig 0/1.10:
    - ipv6 address FE80::2 link-local
    - ipv6 nd managed-config-flag
    - ipv6 dhcp server vlan\_10
  + Làm tương tự cho các vlan và các cổng còn lại.
* Thiết lập ntp server trên toàn bộ thiết bị trừ các host.
  + ntp server 192.168.99.8
* Thiết lập syslog server trên router servers.
  + logging 192.168.99.7
* Xây dựng ipsec giữa site B và site C
  + show crypto ipsec sa
  + Xây dựng site C với địa chỉ ipv4 là 192.168.250.0 /24
    - Router G0/0: 192.168.250.1 /24
    - PC: 192.168.250.2 /24
    - Router Serial 0/3/0: 10.10.6.2 /30
    - Router Site A Serial 0/3/1: 10.10.6.1 /30
    - Định tuyến ospf 1 với area 0 với router id là 5.5.5.5 bao gồm các mạng 192.168.250.0 và 10.10.6.0
    - Bên Router Site A cũng định tuyến ospf 1 với area 0 với ip 10.10.6.0
  + Trên router site B:
    - license boot module c1900 technology-package securityk9
    - save config và reload lại router
    - Tạo access-list 110 cho phép toàn bộ SV, GV và QL qua bên mạng của site C
    - crypto isakmp policy 10
    - encryption aes 256
    - authentication pre-share
    - group 5
    - exit
    - crypto isakmp key vpnpa55 address 10.10.6.2
    - crypto map VPN-MAP 10 ipsec-isakmp
    - description VPN connection to site C
    - set peer 10.10.6.2
    - set transform-set VPN-SET
    - match address 110
    - exit
    - interface s0/3/0
    - crypto map VPN-MAP
  + Trên router site C:
    - license boot module c1900 technology-package securityk9
    - save config và reload lại router
    - Tạo access-list 110 cho phép mạng từ site C qua các mạng SV, GV, QL
    - crypto isakmp policy 10
    - encryption aes 256
    - authentication pre-share
    - group 5
    - exit
    - crypto isakmp key vpnpa55 address 10.10.4.2
    - crypto map VPN-MAP 10 ipsec-isakmp
    - description VPN connection to site C
    - set peer 10.10.4.2
    - set transform-set VPN-SET
    - match address 110
    - exit
    - interface s0/3/0
    - crypto map VPN-MAP
* Thiết lập portfast và bpguard trên các cổng của switch nối với các host.
* Thiết lập Etherchannel cho các Switch Core với phạm vi là 3 port.
  + interface range gig1/0/5-7
    - channel-protocol pagp (giao thức của cisco)
    - channel-group 1 mode desirable (để gửi lời yêu cầu thiết lập ethernet channel với thiết bị còn lại)
    - exit
  + interface port-channel 1
    - switchport mode trunk
    - switchport trunk native vlan 99
  + Làm tương tự các bước trên với thiết bị còn lại nhưng thiết lập channel-group 1 với mode auto (không cần phải khởi tạo yêu cầu nữa).
  + show etherchannel summary
* Thiết lập cân bằng tải cho các Etherchannel:
  + port-channel load-balance src-dst-mac
  + show etherchannel load-balance
* Cấu hình cho các Radius Server tương ứng:
  + Mục AAA On:
    - Client Name:
      * RouterSiteA – 10.10.2.2 – SiteA
      * RouterSiteBackUp – 10.10.3.2 – SiteABackUp
    - Username: AdminSiteA – Password: AdminSiteA123
  + Làm tương tự cho các Radius Server B và C, sửa lại các địa chỉ IP và username với password cho phù hợp.
* Áp Radius Server vào các Router:
  + Router Site A:
    - aaa new-model
    - username AdminA secret AdminA123
    - aaa authentication login default group radius local
    - aaa authentication enable default group radius local
    - aaa authorization exec default group radius local
    - radius-server host 192.168.99.9 key SiteA
    - ip domain-name SiteA.com
    - ip ssh version 2
    - crypto key generate rsa
    - 1024
    - line vty 0 4
    - transport input ssh
    - login authentication default
    - line console 0
    - login authentication default
  + Làm tương tự cho các Router còn lại với user, pass và radius server phù hợp. (AdminB – AdminB123 | AdminC – AdminC123)
* Cấu hình PAT trên các Router:
  + show ip nat translations
  + Router Site A:
    - interface gigabitEthernet 0/1.10
    - ip nat inside
    - interface gigabitEthernet 0/1.20
    - ip nat inside
    - interface gigabitEthernet 0/1.30
    - ip nat inside
    - interface gigabitEthernet 0/2.10
    - ip nat inside
    - interface gigabitEthernet 0/2.10
    - ip nat inside
    - interface gigabitEthernet 0/2.10
    - ip nat inside
    - interface gigabitEthernet 0/0
    - ip nat outside
    - access-list 102 permit ip 192.168.100.1 0.0.0.127 any
    - access-list 102 permit ip 192.168.101.1 0.0.0.127 any
    - access-list 102 permit ip 192.168.100.129 0.0.0.31 any
    - access-list 102 permit ip 192.168.101.129 0.0.0.31 any
    - access-list 102 permit ip 192.168.100.177 0.0.0.15 any
    - access-list 102 permit ip 192.168.101.177 0.0.0.15 any
    - ip nat inside source list 102 interface gigabitEthernet 0/0 overload
* Cấu hình zone-pair trên router Servers.
  + **Tạo zone security**
    - Zone security Server
    - Zone security Outside
  + **Tạo class-map**
    - Class-map type inspect FTP
    - Match access-group 100
  + **Tạo policy-map và gắn class-map tương ứng**
    - Policy-map type inspect Server-To-Outside
    - Class type inspect 100
    - Inspect
    - Policy-map type inspect Outside-To-Server
    - Class type inspect 100
    - Inspect
  + **Tạo zone-pair và gắn policy-map tương ứng**
    - Zone-pair security Server-To-Outside source Server destination Outside
    - Service-policy type inspect Server-To-Outside
    - Zone-pair security Outside-To-Server source Outside destination Server
    - Service-policy type inspect Outside-To-Server
  + **Gán zone cho port cổng (interface) tương ứng**
    - Interface g0/0/1
    - Zone-member security Server
    - Interface g0/0/0
    - Zone-member security Outside
  + show policy-map type inspect zone-pair sessions
* ssh tới Router Site A:
  + ssh -l AdminSiteA 192.168.100.193
  + AdminSiteA123
* Thiết lập lại policy-map global-policy trên ASA 5506-X để cho phép các máy ICMP tới Internet.
  + no policy-map global\_policy
  + no class-map inspection\_default
  + class-map inspection\_default
  + match default-inspection-traffic
  + exit
  + policy-map global\_policy
  + class inspection\_default
  + inspect icmp
  + inspect dns preset\_dns\_map
  + inspect ftp
  + inspect tftp
  + exit
  + no service-policy global\_policy global
  + service-policy global\_policy global
  + exit
  + write memory
  + class-map inspection\_ICMP
  + match default-inspection-traffic
  + exit
  + policy-map ICMP\_policy
  + class inspection\_ICMP
  + inspect icmp
  + exit
  + service-policy ICMP\_policy in interface outside\_ISP1/outside\_ISP2
  + exit
* PAT/NAT từ router site A ra tường lửa:
  + Trên cổng inside\_SiteA ra cổng outside\_ISP1:
    - object network inside\_SiteA\_outside\_ISP1
    - subnet 10.10.2.0 255.255.255.252
    - nat (inside\_SiteA,outside\_ISP1) dynamic interface
* Bảo mật trên ASA 5560-X:
  + Username: Admin – Password: Admin
  + enable password Admin
* Bảo mật trên Router Servers
  + Username: AdminServer – Password: AdminServer123
  + enable secret AdminServer123
  + ip domain-name Servers.com
  + crypto key generate rsa general-keys modulus 1024
  + line console 0
  + login local
  + exec-timeout 5 0
  + logging synchronous
  + exit
  + line vty 0 4
  + login local
  + transport input ssh
  + exec-timeout 5 0
  + exit
  + service password-encryption
* Cấu hình ACL trên router SiteC:



Hình 4.1: Bảng ACL trên Router Site C.

* Cấu hình ACL trên router Servers:



Hình 4.2: Bảng ACL trên Router Servers.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. *Giới thiệu về Inter-VLAN - Đại học Không Giấy*. (n.d.). <https://www.daihockhonggiay.com/blogs/post/gioi-thieu-ve-inter-vlan>
2. *Tìm hiểu và cấu hình RIPng và OSPFv3 trong IPv6*. (n.d.-b). <https://thegioimang.vn/dien-dan/threads/t%C3%ACm-hi%E1%BB%83u-v%C3%A0-c%E1%BA%A5u-h%C3%ACnh-ripng-v%C3%A0-ospfv3-trong-ipv6.2242/>
3. *EtherChannel - Gộp link kết nối giữa 2 switch Cisco*. (n.d.-b). VnExperts Networks. <https://vnexperts.vn/etherchannel.html>
4. *Tìm hiểu Cisco ASA 5506-X, hướng dẫn cấu hình Firewall Cisco ASA 5506-X với 2 mô hình thực tế*. (n.d.-d). <https://thegioimang.vn/dien-dan/threads/t%C3%ACm-hi%E1%BB%83u-cisco-asa-5506-x-h%C6%B0%E1%BB%9Bng-d%E1%BA%ABn-c%E1%BA%A5u-h%C3%ACnh-firewall-cisco-asa-5506-x-v%E1%BB%9Bi-2-m%C3%B4-h%C3%ACnh-th%E1%BB%B1c-t%E1%BA%BF.910/>
5. *TÍNH NĂNG BPDU GUARD -*. (n.d.-b). <https://vnpro.vn/thu-vien/tinh-nang-bpdu-guard-3181.html>

Tiếng Anh

1. Trương, Đ. T. (2022). *Side bài giảng trong lớp và các bài lab thực hành môn mạng máy tính nâng cao*. trường Đại học Tôn Đức Thắng, thành phố Hồ Chí Minh.
2. samelington (2021), Community Cisco, 5506-X in packet tracer can’t configure global policy/policy map, <https://community.cisco.com/t5/network-management/5506-x-in-packet-tracer-can-t-configure-global-policy-policy-map/td-p/4442553>
3. GD Networking Newbie (2020), AAA Local and Server based Authentication Configuration in Packet Tracer, <https://www.youtube.com/watch?v=04sYhU32S0k>