**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HỒ CHÍ MINH**

**KHOA ĐÀO TẠO CHẤT LƯỢNG CAO**

-----oOo-----



**BÁO CÁO ĐỒ ÁN CÔNG NGHỆ THÔNG TIN**

**ĐỀ TÀI: THIẾT KẾ HỆ THỐNG MẠNG LAN CHO DOANH NGHIỆP VỪA VÀ NHỎ**

Sinh viên thực hiện:

* Trần Quang Hiệp – 18110108
* Cao Thị Mai Trâm – 181102

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HỒ CHÍ MINH**

**KHOA ĐÀO TẠO CHẤT LƯỢNG CAO**

-----oOo-----

**BÁO CÁO ĐỒ ÁN CÔNG NGHỆ THÔNG TIN**

**ĐỀ TÀI: THIẾT KẾ HỆ THỐNG MẠNG LAN CHO DOANH NGHIỆP VỪA VÀ NHỎ**

Sinh viên thực hiện:

* Trần Quang Hiệp – 18110108
* Cao Thị Mai Trâm – 18110218

MỤC LỤC

[MỤC LỤC 2](#_Toc58840495)

[DANH MỤC HÌNH 4](#_Toc58840496)

[DANH MỤC BẢNG 5](#_Toc58840497)

[DANH MỤC CÁC TỪ VIẾT TẮT 6](#_Toc58840498)

[LỜI MỞ ĐẦU 8](#_Toc58840499)

[MÔ TẢ ĐỀ TÀI 9](#_Toc58840500)

[THIẾT KẾ 11](#_Toc58840501)

[1. Thiết kế lớp địa chỉ IP 11](#_Toc58840502)

[1.1. ISP 11](#_Toc58840503)

[1.2. RBD1 12](#_Toc58840504)

[1.3. RBD2 12](#_Toc58840505)

[2. Thiết kế dịch vụ 12](#_Toc58840506)

[2.1. DHCP 12](#_Toc58840507)

[2.2. WEB 14](#_Toc58840508)

[2.3. MAIL 15](#_Toc58840509)

[2.4. DNS 17](#_Toc58840510)

[3. Danh mục thiết bị, kinh phí dự kiến 18](#_Toc58840511)

[4. Cài đặt và cấu hình 18](#_Toc58840512)

[4.1. Route 18](#_Toc58840513)

[4.2. OSPF 21](#_Toc58840514)

[4.3. DHCP 22](#_Toc58840517)

[4.4. NAT 24](#_Toc58840518)

[4.5. GRE VPN 26](#_Toc58840519)

[4.6. Trunking 28](#_Toc58840520)

[4.7. VTP 29](#_Toc58840521)

[4.8. SSH 32](#_Toc58840522)

[4.9. ACL 32](#_Toc58840523)

[MÔ TẢ PHÂN CÔNG CÔNG VIỆC 34](#_Toc58840524)

[TÀI LIỆU THAM KHẢO 35](#_Toc58840525)

DANH MỤC HÌNH

[Hình 1.DHCP service 13](#_Toc58676078)

[Hình 2.WEB service 14](#_Toc58676079)

[Hình 3.MAIL service 15](#_Toc58676080)

[Hình 4.Config mail trên PC 16](#_Toc58676081)

[Hình 5. DNS service 17](#_Toc58676082)

[Hình 6. Bảng định tuyến ISP 18](#_Toc58676083)

[Hình 7. Bảng đinh tuyến của RBD1 19](#_Toc58676084)

[Hình 8. Bảng định tuyến của RBD2 19](#_Toc58676085)

[Hình 9. Bảng định tuyến OSPF của RBD1 21](#_Toc58676086)

[Hình 10. Bảng định tuyến OSPF của SWBD1 21](#_Toc58676087)

[Hình 11. Cấu hình DHCP trên BDB2 22](#_Toc58676088)

[Hình 12. Kết quả cấp phát DHCP của RBD2 23](#_Toc58676089)

[Hình 13. VTP server 28](#_Toc58676090)

[Hình 14. VTP client 29](#_Toc58676091)

DANH MỤC BẢNG

[Bảng 1. Bảng qui hoạch IP 11](#_Toc58840483)

[Bảng 2.Bảng danh mục thiết bị và kinh phí dự kiến 18](#_Toc58840484)

[Bảng 3. Bảng phân công công việc 34](#_Toc58840485)

DANH MỤC CÁC TỪ VIẾT TẮT

**VLAN (Virtual Local Area Network)**: VLAN là một kỹ thuật cho phép tạo lập các mạng LAN độc lập một cách logic trên cùng một kiến trúc hạ tầng vật lý

**IP (Internet Protocol):** là một địa chỉ đơn nhất mà những thiết bị điện tử hiện nay đang sử dụng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet.

**ISP (Internet Service Provider):** Nhà cung cấp dịch vụ Internet hay Nhà cung cấp dịch vụ nối mạng chuyên cung cấp các giải pháp kết nối mạng toàn cầu (Internet) cho các đơn vị tổ chức hay các cá nhân người dùng.

**OSPF (Open Shortest Path First):** Là một giao thức định tuyến Link – state điển hình.

**NAT (Network Address Translation):** Giúp địa chỉ mạng cục bộ (Private) truy cập được đến mạng công cộng (Internet)

**ACL (Access Control List):** Danh sách điều khiển truy cập

**DHCP (Dynamic Host Configuration Protocol):** Giao thức cấu hình tự động địa chỉ ip

**LSA (Link state Advertisement)**

**DR (Designated Router)**

**BDR (Backup Designated Router)**

**GRE (Generic Routing Encapsulation):** Là giao thức được phát triển bởi Cisco, với mục đích tạo ra kênh truyền ảo (tunnel) để mang các giao thức lớp thứ 3 thông qua mạng ip

**VPN (Virtual Private Network):** cho phép người dùng thiết lập mạng riêng ảo với một mạng khác trên Internet

**VTP (VLAN Trunking Protocol)**: Duy trì cấu hình VLAN thông qua admin domain của mạng.. VTP là một giao thức lớp 2 sử dụng các Trunk frame để quản lí việc them, bớt, xóa, sửa VLAN trên một domain.

**HTTP (HyperText Transfer Protocol):** là một giao thức lớp ứng dụng cho các hệ thống thông tin siêu phương tiện phân tán, cộng tác.

**HTTPS (HyperText Transfer Protocol Secure)**: Là một sự kết hợp giữa giao thứ HTTP và giao thức bảo mật SSL hay TLS cho phép treo đổi thông tin một cách bảo math trên Internet.

**DNS (Domain Name System)**: Là một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên Internet

**SMTP (Simple Mail Transfer Protocol):** Là một chuẩn truyền tải thư điện tử qua mạng Internet.

**POP3 (Post Offic Protocol version 3)**: được sử dụng để kết nối tới server email và tải email xuống máy tính cá nhân thông qua một ứng dụng email

**SSL (Secure Sockets Layer)**:.Đây là một tiêu chuẩn an ninh công nghệ toàn cầu tạo ra một liên kết giữa máy chủ web và trình duyệt.

**TSL (Transport Layer Security)**: là giao thức mật mã được thiết kế để cung cấp truyền thông an toàn qua một mạng máy tính.

**SSH (Secure Shell):** là một giao thức mạng dùng để thiết lập kết nối mạng một cách bảo mật.

LỜI MỞ ĐẦU

Ngày nay, Công nghệ thông tin đã trở nên phổ biến và hầu như phủ sóng trên mọi lĩnh vực. Với sự phát triển chống mặt của Công nghệ thông tin thì Mạng máy tính cũng đã len lỏi vào cuộc sống của con người.

Ở Việt Nam, các công ty, doanh nghiệp, tôt chức mọc lên ngày càng nhiều với nhiều loại hình qui mô, đòi hỏi ngày càng nhiều về trình độ cũng như cở hạ tầng, cơ sở vật chất hiện đại. Từ hệ thống quản lí đặc biệt giúp con người đơn giản hóa công việc, làm việc một cách nhanh chóng và hiệu quả hơn. Việc ứng dụng Công nghệ thông tin vào các công ty, doanh nghiệp, tổ chức là một điều thiết yếu, là một yếu tố quan trọng để giúp thúc đẩy sự phát triển của các công ty, doanh nghiệp. Đất nước ngày càng phát triển cùng với sự chuyển biến của của Thế giới, công nghệ thông tin là xu thế tất yếu để hội nhập với các nền công nghệ mới. Có thể nói Công nghệ thông tin đóng vai trò như chiếc cầu nối giúp Việt Nam tiếp cận với Thế giới nhanh hơn. Để đảm bảo nguồn thông tin luôn sẵn sàng và kịp thời đáp ứng nhu cầu truy xuất, quản lí dữ liệu thì công cụ giúp con người thực hiện chúng một cách tốt nhất không gì khác ngoài máy tính. Và để có thể giải quyết được nhiều vấn đề trong một lúc thì ta phải có một mô hình nhiều máy tính để làm việc hiệu quả hơn. Và đó là Mạng máy tính. Mô hình mạng cho công ty, doanh nghiệp đã không còn quá xa lạ. Một công ty bất kể lớn hay nhỏ, thì vẫn cần phải có hệ thống mạng máy tính. Việc sử dụng mô hình mạng máy tính mang lại nhiều lợi ích thiết thực và tiết kiệm thời gian. Tính bảo mật cao, quản lí thông tin tập tin, khi có sự cố khắc phục nhanh chóng.

Vì những lý do đó nên nhóm chúng em chọn đề tài “ Xây dựng hệ thống mạng LAN cho doanh nghiệp vừa và nhỏ”. Đề tài này là những bước cụ thể để xây dựng một hệ thống mạng cho doanh nghiệp.

Nhóm sinh viên thực hiện:

* Trần Quang Hiệp – MSSV: 18110108
* Cao Thị Mai Trâm – MSSV: 18110218

MÔ TẢ ĐỀ TÀI

* Tên đề tài: **Xây dựng hệ thống mạng LAN cho doanh nghiệp vừa và nhỏ**
* Hiện trạng hệ thống mạng của doanh nghiệp: **Xây dựng mới hoàn toàn**
* Thiết bị mạng: Cisco
* Mô tả hệ thống:

Công ty bao gồm 2 cơ sở.

Cở sở 1 bao gồm:

+ RBD1: Đây là router chính của cơ sở 1, có 2 nhiệm vụ chính là để giúp các thiết bị bên trong có thể NAT ra ngoài Internet cùng với đó là tạo 1 đường hầm VPN tunnel để 2 cơ sở có thể giao tiếp được với nhau. Ở đây ta đã tạo ra 1 ACL gồm 5 dãy mạng nội bộ và tất cả địa chỉ này đều ra ngoài bằng 1 địa chỉ IP là 10.0.0.1/8. Với VPN tunnel thì ở Router này ta có địa chỉ ip là 172.16.2.1/24 đây là địa chỉ IP tượng trưng cho Router ở cơ sở 1, cùng với đó ta sử dụng định tuyến tĩnh Static để giúp các máy ở cơ sở 1 liên kết với cơ sở 2.

+ SWBD1: Đây là SW layer 3 và cũng là Switch chính của cả Building 1. Nhiệm vụ của Switch này là để định tuyến giữa các Vlan trong hệ thống mạng LAN của ta, và định tuyến tới router để ra ngoài Internet, cùng với đó đây là VTP server để có thể kiểm soát được các Switch khác.

+ SWSERVER: Đây là Switch của phòng Server. Ta đã cấu hình để các thiết bị được kiểm soát bằng Server này đều thuộc Vlan 12 và đây là VTP client.

+ SW1: Phòng Giám đốc. Các thiết bị ở phòng Giám đốc thuộc Vlan 10, ở đây ta còn cấu hình thêm 1 ACL để chỉ cho các thiết bị ở phồng này ping thấy nhau còn các thiết bị phòng khác không thể ping thấy được, nhưng ở chiều ngược lại các máy ở phòng này vẫn có thể ping ra ngoài được.

+ SW2: Phòng Nhân sự. Các thiết bị ở phòng Nhân sự thuộc Vlan 20

+ SW3: Phòng Kế toán. Các thiết bị ở phòng Kế toán thuộc Vlan 30

+ SW4: Phòng Marketing. Các thiết bị ở phòng Marketing thuộc Vlan 40

Cơ sở 2 bao gồm:

+ RBD2: Đây là router chính của cơ sở 2, ở đây có 3 nhiệm vụ chính 2 nhiệm vụ tương tự như ở RBD2 là NAT (ra ngoài Internet bằng ip 20.0.0.1/8) và VPN (địa chỉ ip là 172.16.2.2/24) ngoài ra còn được cấc hình DHCP server để cung cấp địa chỉ ip cho các máy tính ở trong cơ sở 2 trong dãy mạng 192.168.1.0/24.

+ SW5: Đây là Switch chính của cơ sở 2. SW này chỉ được cấu hình để mọi thiết bị văn phòng thuộc Vlan 1.

THIẾT KẾ

1. Thiết kế lớp địa chỉ IP

IP có nghĩa là địa chỉ giao thức của internet, nó tương tự như địa chỉ nhà hay địa chỉ doanh nghiệp vậy. Các thiết bị phần cứng trong mạng muốn kết nối và giao tiếp với nhau được đều phải có địa chỉ IP.

Chúng ta tiến hành đặt IP cho các thiết bị theo bảng qui hoạch IP sau:

|  |  |  |
| --- | --- | --- |
| **Thiết bị** | **Cổng** | **Địa chỉ ip** |
| ISP | F0/0 | 10.0.0.2/8 |
| F0/1 | 20.0.0.2/8 |
| RBD1 | F0/0 | 172.16.1.2/24 |
| F0/1 | 10.0.0.1/8 |
| SWBD1 | Vlan 1 | 172.16.1.1/24 |
| Vlan 10 | 192.168.10.1/24 |
| Vlan 12 | 172.16.12.1/24 |
| Vlan 20 | 192.168.20.1/24 |
| Vlan 30 | 192.168.30.1/24 |
| Vlan 40 | 192.168.40.1/24 |
| RBD2 | F0/0 | 20.0.0.1/8 |
| F0/1 | 192.168.1.1/24 |

Bảng 1. Bảng qui hoạch IP

* 1. ISP

ISP(config)#int f0/0

ISP(config-if)#ip add 10.0.0.2 255.0.0.0

ISP(config)#int f0/1

ISP(config-if)#ip add 20.0.0.2 255.0.0.0

* 1. RBD1

RBD1(config)#int f0/0

RBD1 (config-if)#ip add 172.16.1.2 255.255.255.0

RBD1 (config)#int f0/1

RBD1 (config-if)#ip add 10.0.0.1 255.0.0.0

* 1. RBD2

RBD2(config)#int f0/0

RBD2 (config-if)#ip add 20.0.0.1 255.0.0.0

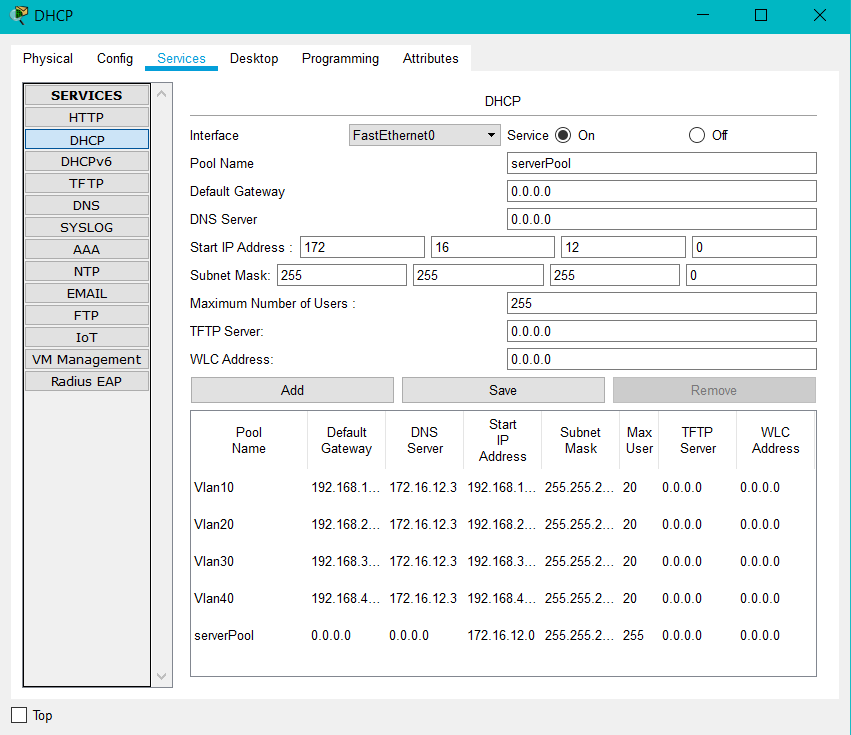
RBD2 (config)#int f0/1

RBD2 (config-if)#ip add 192.168.1.1 255.255.255.0

1. Thiết kế dịch vụ
   1. DHCP

Cấu hình DHCP server cấp phát địa chỉ IP cho các host ở cơ sở 1:

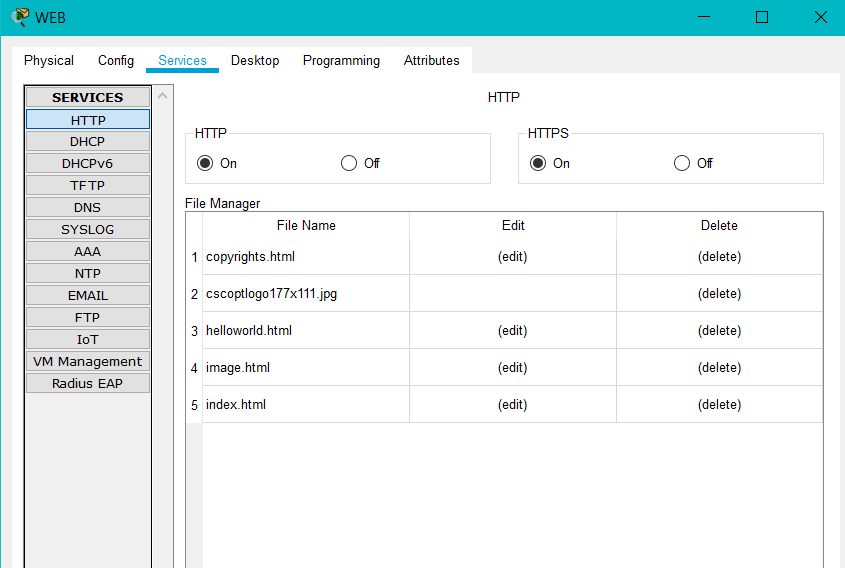
* Các host thuộc VLan10 (Phòng Giám đốc) sẽ nhận được IP:
* Bắt đầu từ: 192.168.10.10
* Subnet mask: 255.255.255.0
* Default gateway: 192.168.10.1
* DNS server: 172.16.12.3
* Các host thuộc VLan20 (Phòng Nhân sự) sẽ nhận được IP:
* Bắt đầu từ: 192.168.20.10
* Subnet mask: 255.255.255.0
* Default gateway: 192.168.20.1
* DNS server: 172.16.12.3
* Các host thuộc VLan30 (Phòng Kế toán) sẽ nhận được IP:
* Bắt đầu từ: 192.168.30.10
* Subnet mask: 255.255.255.0
* Default gateway: 192.168.30.1
* DNS server: 172.16.12.3
* Các host thuộc VLan40 (Phòng Marketing) sẽ nhận được IP:
* Bắt đầu từ: 192.168.40.10
* Subnet mask: 255.255.255.0
* Default gateway: 192.168.40.1
* DNS server: 172.16.12.3



Hình 1.DHCP service

* 1. WEB

Bật chế độ On cho cả HTTP VÀ HTTPS

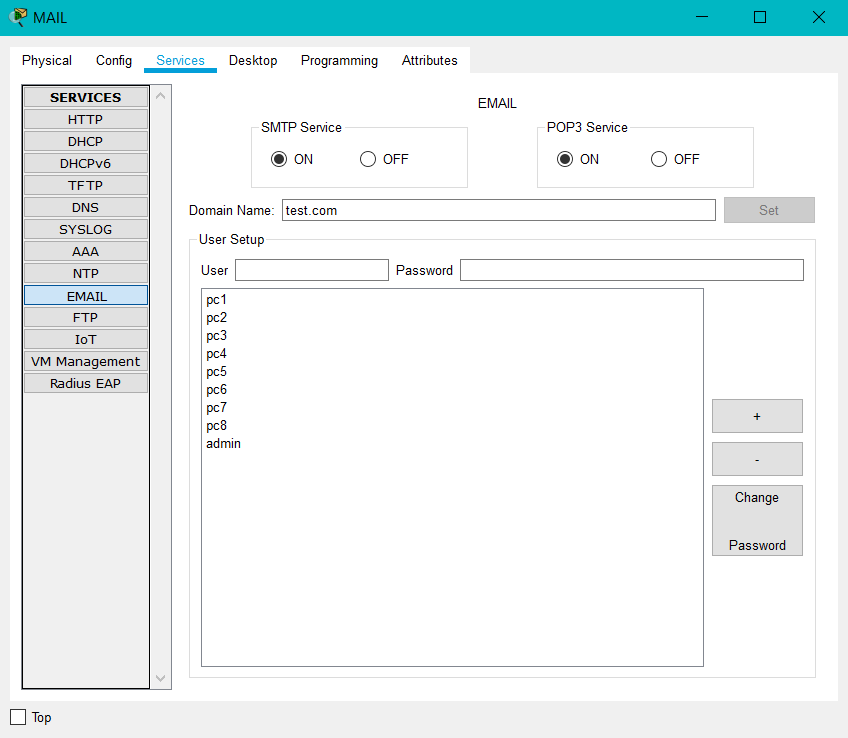


Hình 2.WEB service

* 1. MAIL

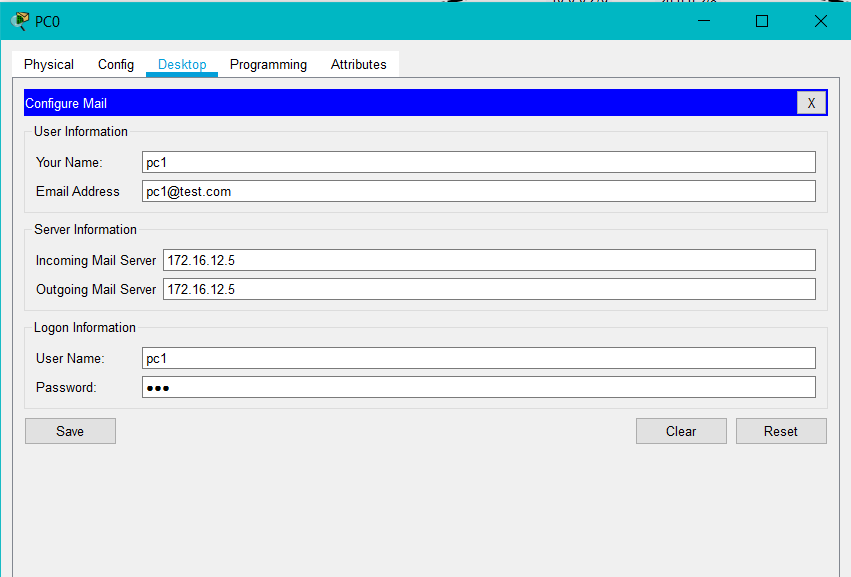
Bật chế độ ON cho SMTP (gởi mail) và POP3 (nhận mail).

Tiến hành Add user và password



Hình 3.MAIL service

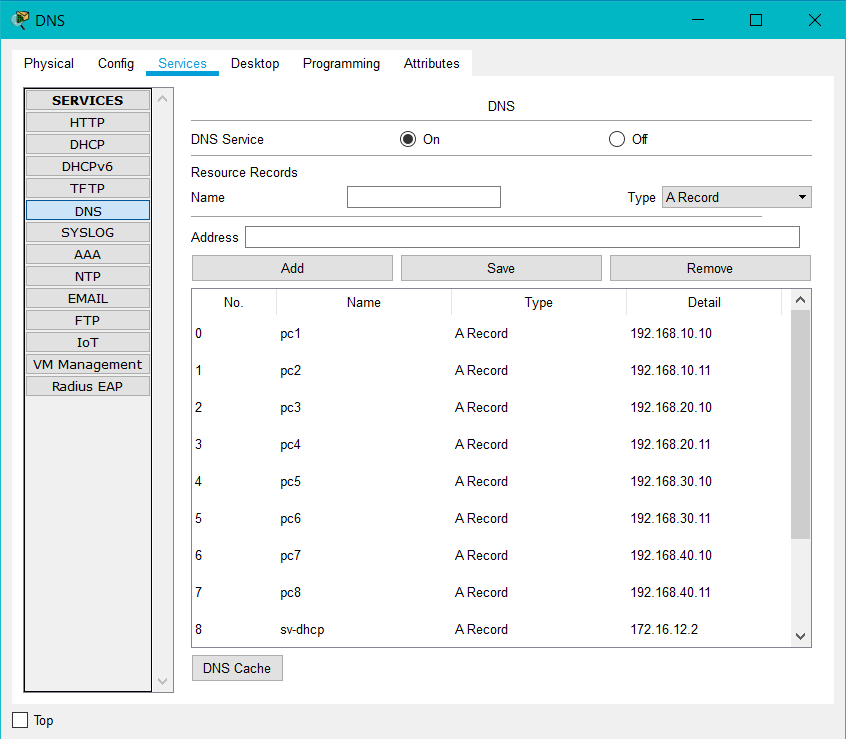
Sau đó tiến hành cấu hình Mail Config trên PC. Với user và password là những account chúng ta đã tạo trên Mail Server



Hình 4.Config mail trên PC

* 1. DNS

Bật chế đọ ON cho DNS service



Hình 5. DNS service

1. Danh mục thiết bị, kinh phí dự kiến

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Thiết bị | Số lượng | Đơn giá | Thành tiền |
| 1 | Router Cisco 2811 | 2 | 16.000.000 VNĐ | 32.000.000 VNĐ |
| 2 | Switch Cisco 2960 24 port | 6 | 14.500.000 VNĐ | 87.000.000 VNĐ |
| 3 | Swith Cisco 3560 24 port | 1 | 25.600.000 VNĐ | 25.600.000 VNĐ |
| 4 | Thùng dây cáp cat6 305m | 3 | 500.000 VNĐ | 1.500.000 VNĐ |
| 5 | Hộp đầu chụp mạng RJ45 cat6 (100cái/hộp) | 2 | 100.000 VNĐ | 200.000 VNĐ |
| 6 | Hộp đầu RJ45 (100 đầu/hộp) | 2 | 60.000 VNĐ | 120.000 VNĐ |
| **TỔNG KINH PHÍ DỰ KIẾN** | | | | 143.420.000 VNĐ |

Bảng 2.Bảng danh mục thiết bị và kinh phí dự kiến

1. Cài đặt và cấu hình
   1. Route

Routing chỉ ra hướng, sự di chuyển của các gói (dữ liệu) được đánh địa chỉ từ mạng nguồn của chúng, hướng đến đích cuối thông qua các node trung gian.

Tiến trình định tuyến thường chỉ hướng đi dựa vào bảng định tuyến, đó là bảng chứa những lộ trình tốt nhất đến các đích khác nhau trên mạng. Vì vậy việc xây dựng bảng định tuyến, được tổ chức trong bộ nhớ của router, trở nên vô cùng quan trọng cho việc định tuyến hiệu quả.

Trong hệ thống của chúng ta có 3 loại route:

+ C: Các lớp mạng Connected được kết nối trực tiếp với Router

+ O: Được hình thành thông qua OSPF

+ S: Được cấu hình định tuyến tĩnh trên Router

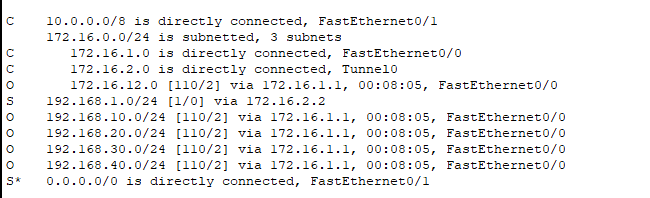
+ S\*: Đây là đường dẫn default route được truyền từ router để giúp các thiết bị ra ngoài mạng Wan

* + 1. ISP



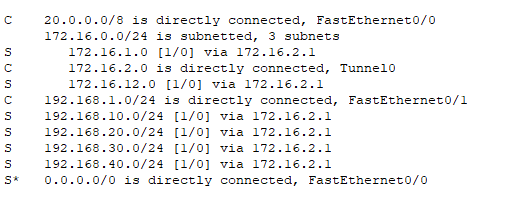
Hình 6. Bảng định tuyến ISP

* Lớp mạng 10.0.0.0/8 và 20.0.0.0/8 được kết nối trực tiếp thông qua cổng f0/0 và f0/1.
  + 1. RBD1



Hình 7. Bảng đinh tuyến của RBD1

* Các lớp mạng 10.0.0.0/8, 172.16.1.0/24, 172.16.2.0/24 được kết nối trực tiếp lần lượt thông qua các cổng f0/1, f0/0 và tunnel0.
* Các lớp mạng 192.168.12.0/24, 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, 192.168.40.0/24 được định tuyến thông qua OSPF.
* Các lớp ngoài lớp mạng LAN được định tuyến qua cổng F0/1.
  + 1. RBD2



Hình 8. Bảng định tuyến của RBD2

* Lớp mạng 20.0.0.0/8 được kết nối qua cổng f0/0, lớp mạng 172.16.2.0/24 được kết nối trực tiếp qua tunnel0, lớp mạng 192.168.1.0/24 được kết nối qua cổng f0/1
* Các lớp mạng 172.16.1.0/24, 172.16.12.0/24, 192.16.10.0/24, 192.16.20.0/24, 192.16.30.0/24, 192.16.40.0/24 được cấu hình định tuyến thông qua 172.16.2.1
* Các lớp ngoài lớp mạng LAN được định tuyến qua cổng F0/0.

Câu lệnh cấu hình định tuyến tĩnh:

RBD1(config)# ip route 192.168.1.0 255.255.255.0 192.168.2.2

RBD1(config)# ip route 192.168.1.0 255.255.255.0 192.168.2.2

RBD2(config)# ip route 192.168.10.0 255.255.255.0 172.16.2.1

RBD2(config)# ip route 192.168.20.0 255.255.255.0 172.16.2.1

RBD2(config)# ip route 192.168.30.0 255.255.255.0 172.16.2.1

RBD2(config)# ip route 192.168.40.0 255.255.255.0 172.16.2.1

RBD2(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.1

RBD2(config)# ip route 172.16.12.0 255.255.255.0 172.16.2.1

* 1. OSPF

OSPF là một giao thức link – state điển hình. Mỗi Router khi chạy giao thức này sẽ gởi các bản tin trạng thái link LSA của nó cho tất cả các Router trong vùng (area). Sau một thời gian trao đổi, các Router sẽ đồng thống nhất được bảng cơ sở dữ liệu trạng thái đường link với nhau, mỗi router đều có được “bản đồ mạng” của cả vùng. Từ đó các Router sẽ chạy thuật toán Dijasktra tính toán ra một cây đường đi ngắn nhất và dựa vào đó để thiết lập bảng định tuyến.

* + 1. RBD1

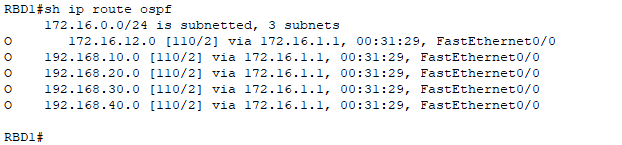
RBD1 sẽ đóng vai trò là DR. Có nghĩa là RBD1 sẽ đóng vai trò như đầu mối. Các Router không trao đổi trực tiếp với nhau mà sẽ tiến hành trao đổi thông tin qua một Router khác

Câu lệnh cấu hình:

RBD1(config)#ip ospf 100

RBD1(config-router)#network 172.16.1.0 0.0.0.255 area 0

RBD1(config-router)#exit



Hình 9. Bảng định tuyến OSPF của RBD1

* + 1. SWBD1

Câu lệnh cấu hình:

SWBD1(config)#ip ospf 100

SWBD1(config-router)#network 192.168.12.0 0.0.0.255 area 0

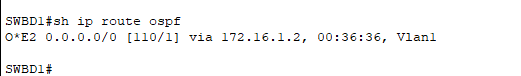
SWBD1(config-router)#network 192.168.10.0 0.0.0.255 area 0

SWBD1(config-router)#network 192.168.20.0 0.0.0.255 area 0

SWBD1(config-router)#network 192.168.30.0 0.0.0.255 area 0

SWBD1(config-router)#network 192.168.40.0 0.0.0.255 area 0

SWBD1(config-router)#exit



Hình 10. Bảng định tuyến OSPF của SWBD1

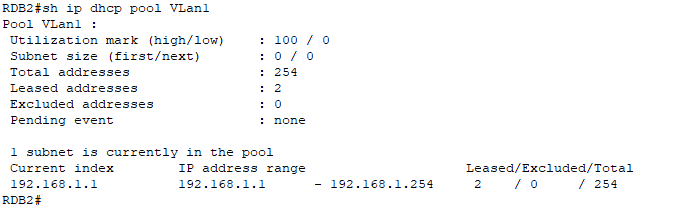
* 1. DHCP

DHCP là một giao thức cho phép cấp phát tự động cấu hình IP cho các host trên một mạng Ethernet LAN. DHCP hoạt động thoe mô hình client – server: các host xin cấp phát IP đóng vai trò là các DHCP client và thiết bị thực hiện cấp phát IP cho các host đóng vai trò là DHCP server. DHCP server có thể là một server chuyện dụng trên nền tảng Linux hoặc Window hoặc một thiết bị mạng Router, Switch hay Firewall.

* + 1. Cấu hình DHCP

Cấu hình RBD2 thành DHCP server thõa các yêu cầu sau:

* DHCP server cấp phát địa chỉ IP cho các host thuộc Vlan 1 của SW5 (Switch 5)
* Dãy IP được cấp phát thuộc lớp mạng 192.168.1.0/24
* DHCP server cũng cấp phát cho các host thuộc Vlan 1 của SW5 địa chỉ default – getway là 192.168.1.1 và DNS server là 172.16.12.3.



Hình 11. Cấu hình DHCP trên BDB2

**Câu lệnh cấu hình**

RBD2(config)#ip dhcp pool VLan1

RBD2(dhcp-config)#network 192.168.1.0 255.255.255.0

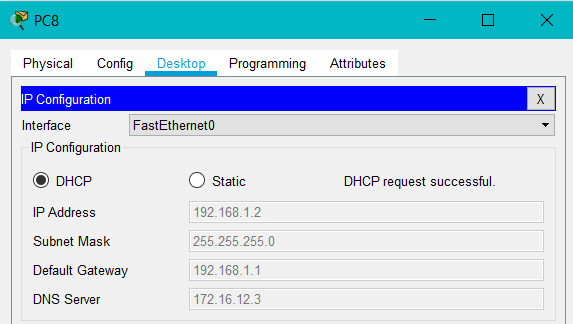
RBD2(dhcp-config)#default-router 192.168.1.1

RBD2(dhcp-config)#dns-server 172.16.12.3

RBD2(dhcp-config)#exit

Khi chúng ta dùng câu lệnh “network” trong pool, toàn bộ subnet được khai báo trong câu lệnh sẽ được lần lượt cấp xuống cho các host. Câu lệnh “default-router” sẽ khai báo default gateway cho các host thuộc subnet trên, còn DNS server sẽ được cấp phát thông qua câu lệnh “dns-server”

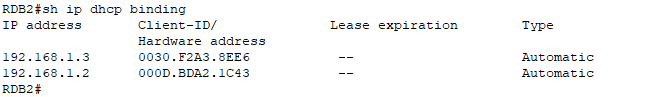
Sau khi cấu hình xong, chúng ta thực hiện kiểm tra. Ta tiến hành xin IP mới.



Hình 12. Kết quả cấp phát DHCP cảu RBD2

Ta thấy PC đã nhận được IP từ DHCP server đúng như yêu cầu.

Ta kiểm tra trên DHCP server RBD2 để thấy rằng địa chỉ IP trong pool đã được cấp.



Hình 4.3.3.Bảng IP đã cấp ở DHCP server

* 1. NAT

Không gian IP được chia thành 2 loại: Private và Public. Các địa chỉ IP Private được sử dụng trong nội bộ mạng doanh nghiệp, không sử dụng trên môi trường Internet, dùng cho các host trên Internet. Các địa chỉ IP Public được sử dụng trên qui mô Internet, dùng cho các host trên Internet. Một địa chỉ IP Private có thể được sử dụng lại từ nội bộ này sang nội bộ khác nhưng địa chỉ IP Public phải mang tính duy nhất trên Thế giới.

Nhưng IP Private không được định tuyến trên môi trường Internet toàn cầu nhưng các host được gán IP Private trong các mạng nội bộ vẫn có nhu cầu sử dụng Internet. Để giải quyết vấn đề đó thì kỹ thuật NAT đã được sử dụng.

NAT sẽ thực hiện chuyển đổi địa chỉ IP của gói tin xuấ phát từ vùng Private thành địa chỉ IP Public khi gói tin này đi từ mạng nội bộ ra môi trường Internet bên ngoài và thực hiện chuyển ngược lại các IP Public thành Private khi gói tin được trả về từ Internet vào trong mạng nội bộ.

Đối với hệ thống này chúng ta tiến hành NAT overload. NAT overload cho phép NAT cùng một lúc nhiều địa chỉ private bên trong thành một địa chỉ public bên ngoài. Tiến hành NAT trên cả 2 cơ sở.

Các bước cấu hình:

* Cở sở 1:

Bước 1: Xác định inside và outside

RBD1(config)# int f0/0

RBD1(config-if)#ip nat inside

RBD1(config)#exit

RBD1(config)# int f0/1

RBD1(config-if)#ip nat outside

RBD1(config)#exit

Bước 2: Viết ACL mô tả danh sác các địa chỉ Priavate sẽ được NAT

RBD1(config)# access-list 1 permit 192.168.10.0 0.0.0.255

RBD1(config)# access-list 1 permit 192.168.20.0 0.0.0.255

RBD1(config)# access-list 1 permit 192.168.30.0 0.0.0.255

RBD1(config)# access-list 1 permit 192.168.40.0 0.0.0.255

RBD1(config)# access-list 1 permit 172.16.12.0 0.0.0.255

Bước 3: Cấu hình NAT toàn bộ NAT toàn bộ các địa chỉ trong ACL 1 thành một địa chỉ public trên cổng f0/1 của RBD1

RBD1(config)#ip nat inside source list 1 interface f0/0 overload

* Cơ sở 2:

Bước 1: Xác định inside và outside

RBD2(config)# int f0/1

RBD2(config-if)#ip nat inside

RBD2(config)#exit

RBD2(config)# int f0/0

RBD2(config-if)#ip nat outside

RBD2(config)#exit

Bước 2: Viết ACL mô tả danh sác các địa chỉ Priavate sẽ được NAT

RBD2(config)# access-list 1 permit 192.168.1.0 0.0.0.255

Bước 3: Cấu hình NAT toàn bộ NAT toàn bộ các địa chỉ trong ACL 1 thành một địa chỉ public trên cổng f0/0 của RBD2

RBD2(config)#ip nat inside source list 1 interface f0/1 overload

* 1. GRE VPN

GRE là một kỹ thuật đường hầm ở lớp thứ 3 cho phép đóng gói dữ liệu của nhiều loại giao thức khác nhau như IP, IPX, các giao thức định tuyến,… để truyền tải qua một mạng IP.

Điểm nổi bật của GRE là hỗ trợ truyền tải thông tin của các giao thứ định tuyến

Khi cả 2 chi nhánh đều đã được kết nối Internet, chúng ta sẽ thiết lập một đường GRE VPN để nối 2 đầu chi nhánh này qua môi trường Internet.

Cấu hình GRE:

* Cơ sở 1:

RBD1(config)#interface Tunnel0

RBD1(config-if)#tunnel source FastEthernet0/1

RBD1(config-if)#tunnel destination 20.0.0.1

RBD1(config-if)#ip address 172.16.2.1 255.255.255.0

RBD1(config-if)#exit

Cơ sở 2:

RBD2(config)# interface Tunnel0

RBD2(config)# tunnel source FastEthernet0/0

RBD2(config)# tunnel destination 10.0.0.1

RBD2(config)# ip address 172.16.2.2 255.255.255.0

RBD2(config)#exit

* 1. Trunking

Việc sử dụng quá nhiều đường nối để đấu nối các VLAN trên nhiều Switch là không hợp lý. Một giải pháp được đưa ra để chỉ cần sử dụng một đường đấu nối giữa 2 Switch mà vẫn đảm bảo thông suốt. Đường nối như vậy được gọi là đường Trunk.

Cấu hình Trunk trên các Switch

* SW1:

SW1(config)# int f0/1

SW1(config-if)#switchport trunk encapsulation dot1q

SW1(config-if)#switchport mode trunk

* SW2:

SW2(config)# int f0/1

SW2(config-if)#switchport trunk encapsulation dot1q

SW2(config-if)#switchport mode trunk

* SW3:

SW3(config)# int f0/1

SW3(config-if)#switchport trunk encapsulation dot1q

SW3(config-if)#switchport mode trunk

* SW4:

SW4(config)# int f0/1

SW4(config-if)#switchport trunk encapsulation dot1q

SW4(config-if)#switchport mode trunk

* SWSERVER:

SWSERVER (config)# int f0/1

SWSERVER (config-if)#switchport trunk encapsulation dot1q

SWSERVER (config-if)#switchport mode trunk

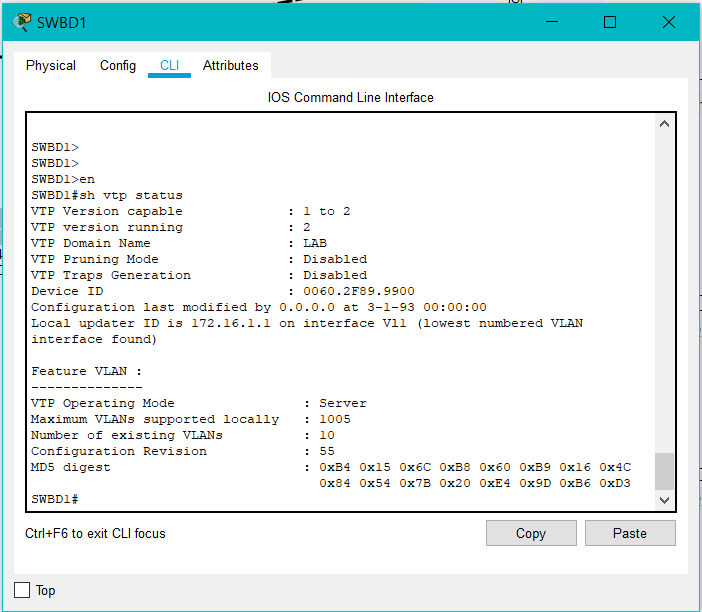
* 1. VTP

Một yêu cầu đặt ra trên hệ thống chuyển mạch Ethernet là các Switch phải thống nhất với nhau về cấu hình VLAN. Khi số lượng VLAN trên hệ thống đủ lớn, việc kiểm tra và duy trì tính đồng bộ cấu hình VLAN giữa các Switch trở nên khó khan. Cisco đưa ra một gai thức chạy trên các Switch cho phép các Switch tự động đồng bộ cấu hình VLAN mà không cần sự can thiệp của người quản trị. Dịch vụ đó gọi là VTP.

VTP sử dụng các đường trunk layer 2 để trao đổi thông tin. Do đó ta phải thiết lập đường trunk giữa các Switch.

* + 1. VTP server

Switch ở mode server sẽ có toàn quyền thao tác trên cấu hình VLAN. Trogn hệ thống này SWBD1 sẽ đóng vai trò là VTP server.



Hình 13. VTP server

Câu lệnh cấu hình:

SWBD1(config)#vtp mode server

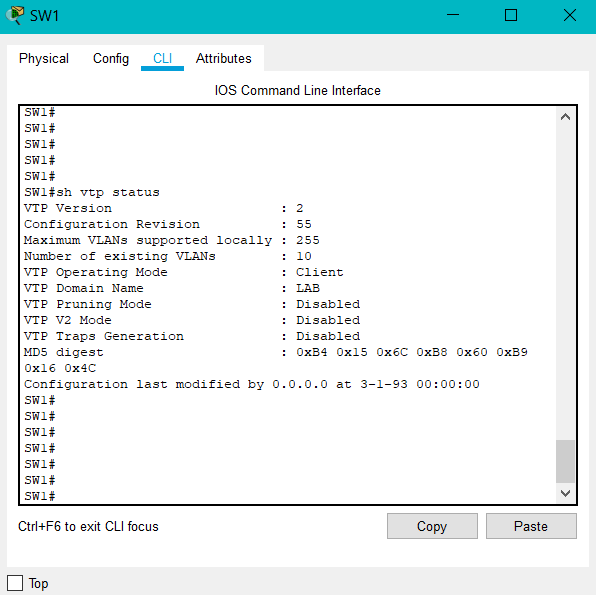
SWBD1(config)#vtp domain LAB

SWBD1(config)#vtp password cisco

* + 1. VTP client

Ngược lại với mode server, các Switch ở mode client không được phép thay đổi cấu hình VLAN của mình. Các hành động mà một Switch ở mode này có thể làm là:

* Đồng bộ cấu hình từ Switch khác
* Forward thông tin VLAN



Hình 14. VTP client

Câu lệnh cấu hình:

* SW1:

SW1(config)#vtp mode client

SW1(config)#vtp domain LAB

SW1(config)#vtp password cisco

* SW2:

SW2(config)#vtp mode client

SW2(config)#vtp domain LAB

SW2(config)#vtp password cisco

* SW3:

SW3(config)#vtp mode client

SW3(config)#vtp domain LAB

SW3(config)#vtp password cisco

* SW4

SW4(config)#vtp mode client

SW4(config)#vtp domain LAB

SW4(config)#vtp password cisco

* SWSERVER

SWSERVER(config)#vtp mode client

SWSERVER(config)#vtp domain LAB

SWSERVER(config)#vtp password cisco

* 1. SSH

Một yêu cầu được đề ra là điều khiển các thiết bị từ xa, thông qua mạng LAN. Vì khi có vấn đề không quá lớn ta có thể trực tiếp sửa chữa mà không cần đi tới vị trí từng thiết bị. Cisco đã đưa ra giải pháp đó là SSH.

Ở các thiết bị SWBD1,RBD1,RBD2 ta cấu hình để các thiết bị này đều sử dụng được SSH và có tài khoản là admin và password là cisco:

Câu lệnh cấu hình:

RBD2(config)#ip domain-name LAB.com

RBD2(config)#crypto key generate rsa

RBD2(config)#line vty 0 4

RBD2(config-line)#login local

RBD2(config-line)#transport input ssh

RBD2(config)#username admin privilege 15 secret cisco

Các thiết bị còn lại cấu hình tương tự.

Ở đây ta cung cấp quyền của account admin là 15 nghĩa là đây là quyền cao nhất có thể làm mọi thứ.

* 1. ACL

Đôi khi ta cần lọc một vài gói tin để tránh trường hợp người dùng đó sử dụng những chức năng không đúng với chức vụ. Do đó ACL là một lựa chọn tốt để ta tránh được trường hợp này. ACL có 2 loại là Standard và Extended.

Standarad đây là loại ACL đơn giản dùng để chặn hoặc cho phép 1 dựa theo địa chỉ ip.

Cách cấu hình Standarad:

RBD1(config)#access-list 2 permit 192.168.10.0 0.0.0.255

RBD1(config)#access-list 2 deny any

RBD1(config)#line vty 0 4

RBD1(config-line)#access-class 2 in

Ở đây ta tạo ra 1 ACL 2 cho phép các gói tin từ dãy mạng 192.168.10.0/24 đi qua còn tất cả dãy mạng khác đều chặn lại. Và ta add ACL 2 này vào line vty 0 4 để chỉ cho duy nhất dãy mạng 192.168.10.0/24 có thể SSH vào thiết bị RBD1.

Cách cấu hình Extended:

RBD1(config)# access-list 101 permit icmp any 192.168.10.0 0.0.0.255 echo-reply

RBD1(config)# access-list 101 deny icmp 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255

RBD1(config)# access-list 101 permit ip any any

RBD1(config)#interface vlan 10

RBD1(config-if)#ip access-group 101 out

Ở đây ta tạo ra ACL 101 cho phép dãy mạng 192.168.10.0/24 có thể ping ra ngoài nhưng không địa chỉ ip nào có thể ping tới dãy mạng đó được. Và ta gắn ACL 101 này vào Vlan 10.

MÔ TẢ PHÂN CÔNG CÔNG VIỆC

|  |  |  |
| --- | --- | --- |
| **Tên SV** | **Đánh giá chung phần trăm đóng góp** | **Mô tả khái quát mảng công việc SV thực hiện trong đồ án.** |
| Trần Quang Hiệp | Đáp ứng đủ mục tiêu đề ra, hơi trễ hơn thời hạn đặt ra 1 ngày. Đóng góp 60%. | Thiết kế mô hình mạng, cấu hình VPN, DHCP, NAT, ACL, thiết kế danh mục thiết bị, chi phí, viết báo cáo. |
| Cao Thị Mai Trâm | Đáp ứng đủ mục tiêu và thời gian đặt ra. Đóng góp 40%. | Cấu hình bảng IP, Route, OSPF, Trunking, VTP, SSH, viết báo cáo. |

Bảng 3. Bảng phân công công việc

TÀI LIỆU THAM KHẢO

1. Hướng dẫn học CCNA Routing & Switching (Trung tâm tin học VnPro, Nhà xuất bản Thông tin và Truyền thông, Tái bản lần 3)