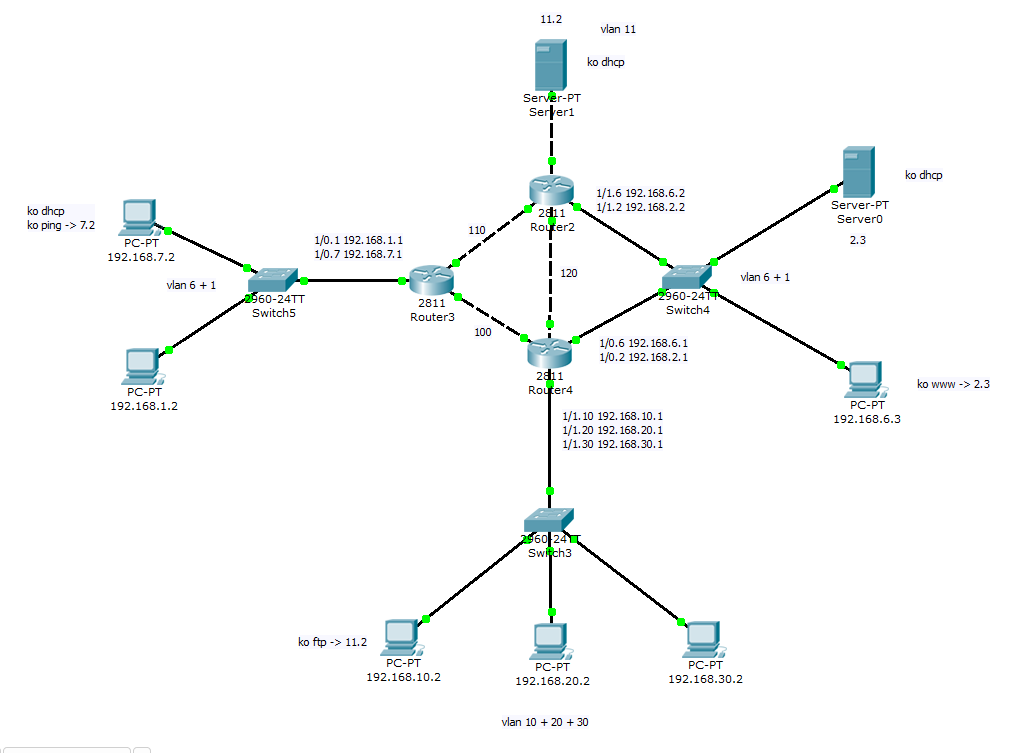
Lab 5 ACL

ACL: bộ lọc các gói dữ liệu trên router, thực hiện qua câu lệnh trên router

**Thực hành:**

Mạch + vlan như trên hình vẽ



1. Thiết lập vlan trên các inteface của switch

Config t

Int fa0/1

Switchport access vlan 1

Làm tương tự cho các interface khác

1. Thiết lập vlan trên các interface và sub interface của router

Cho sub interface:

Int fa0/0

No sh

Ex

Int fa0/0.1

Encapsulation dot1q 1

Ip address 192.168.1.1 255.255.255.0

Cho interface:

Config t

Int fa0/0

Ip address 192.168.10.1 255.255.255.0

Làm tương tự cho các interface và sub interface khác

Nhớ thêm vlan vào vlan database cho tất cả các switch và router, đổi mode của dây nối swtich-switch, switch-router -> trunk

1. Nhập Ip cho các thiết bị ko sử dụng DHCP
2. Thiết lập DHCP

Chuyển mode ip trên thiết bị về DHCP

Thực hiện DHCP trên router

Config t

Ip dhcp excluded 192.168.1.1 (192.168.1.10) - loại bỏ 1.1 (loại bỏ 1.1 -> 1,10)

* Loại bỏ các ip đã được dùng hoặc ko muốn được dùng bởi các thiết bị sử dụng DHCP
* Nếu trên 1 router cung cấp DHCP cho nhiểu vlan cần lặp lại lệnh excludedd nhiều lần cho các vlan khác nhau

Ip dhcp pool vlan1 (vlan1 là tên của pool dhcp, tên nào cũng dc)

Network 192.168.1.0 255.255.255.0 (mạng và mask của mạng nhận ip từ DHCP)

default-router 192.168.1.1 (ip interface/sub interface router của vlan đó – default gateway)

dns-server 8.8.4.4 (dns ko quan trọng, chọn số nào cũng dc, có thể ko cần làm)

làm tương tự cho các thiết bị cần cấp ip DHCP, thiết bị thuộc subnet nào thì làm DHCP trên router gắn trực tiếp với subnet đấy, nếu có nhiều hơn 1 router gắn với subnet đó -> trọn 1 router để làm DHCP

1. Làm routing trên các router

Chọn 1 loại routing RIP/OSPF để làm trên các router

Làm tương tự như trong lab routing

Xong bước này, kiểm tra mạch bằng cách ping giữa các thiết bị, tất cả các thiết bị phải ping dc đến nhau bth.

1. Thiết lập ACL trên các router

Ở đây chỉ sử dụng ACL extended

Config t

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Access-list | Số ACL | Permit /  Deny | Protocol mạng  (icmp, tcp, ...) | Địa chỉ gửi gói tin | Địa chỉ nhận gói tin | Eq port  echo  ... |

- Số ACL chọn theo normal (1-99/1300-1999) hoặc extended (100-199/2000-2699)

- protocol là icmp, arp, tcp, ...

- địa chỉ gửi/ nhận:

+ nếu là 1 mạng: 192.168.1.0 0.0.0.255

+ nếu là 1 địa chỉ cụ thể: host 192.168.1.1

+ nếu là địa chỉ nào cũng dc: any

- port sẽ tương ứng với các protocol sử dụng port: eq 21/ eq ftp – đây là port nhận

VD: access-list 100 deny ftp host 192.168.1.3 192.168.10.0 0.0.0.255 eq 110 (eq pop3)

* Tất cả các tin nhắn sử dụng giao thức pop3 đến mạng 10/24 từ ip 1.3 sẽ bị chặn ở router

Int fa0/0

Ip access-group 100 in/out

* Sau khi viết xong acl cần áp dụng acl đó cho 1 interface/sub interface cụ thể để acl hoạt động được. Int/ subint đấy chính là default gateway của mạng gửi gói tin
* In/out là inbound/outbound: in lọc gói tin khi nó cần đi vào trong int/subint, out lọc gói tin khi nó cần đi ra ngoài int/subint

Lưu ý: mỗi acl gồm 2 phần:

I. ACL thực hiện yêu cầu được giao

II. ACL cho phép các protocol khác ko liên quan đến yêu cầu hoạt động bth

Phần II **LUÔN PHẢI VIẾT SAU PHẦN** I

VD: access-list 100 deny ftp host 192.168.1.3 192.168.10.0 0.0.0.255 eq 110

Access-list 100 permit ip any any => nếu ko có thì ACL chặn toàn bộ các giao thức khác vì ko có trong acl

Sau khi đã hoàn thành các acl, kiểm tra bằng cách gửi gói tin sử dụng giao thức tương ứng với ACL xem Acl đã hoạt đông bth chưa.

access-list 100 deny tcp host 192.168.10.11 host 192.168.11.5 eq ftp

access-list 100 permit ip any any

access-list 100 deny tcp host 192.168.10.11 host 192.168.11.5 eq 20

access-list 101 deny tcp host 192.168.30.8 host 192.168.11.5 eq telnet

access-list 101 deny tcp 192.168.30.12 0.0.0.3 host 192.168.11.5 eq telnet

access-list 101 deny tcp 192.168.30.16 0.0.0.15 host 192.168.11.5 eq telnet

access-list 101 deny tcp 192.168.30.32 0.0.0.15 host 192.168.11.5 eq telnet

access-list 101 deny tcp 192.168.30.48 0.0.0.7 host 192.168.11.5 eq telnet

access-list 101 deny tcp 192.168.30.56 0.0.0.1 host 192.168.11.5 eq telnet

access-list 101 permit ip any any

access-list 102 deny tcp 192.168.30.60 0.0.0.2 host 192.168.11.5 eq www

access-list 102 deny tcp 192.168.30.64 0.0.0.14 host 192.168.11.5 eq www

access-list 102 deny tcp 192.168.30.80 0.0.0.14 host 192.168.11.5 eq www

access-list 102 deny tcp 192.168.30.96 0.0.0.14 host 192.168.11.5 eq www

access-list 102 deny tcp host 192.168.30.112 host 192.168.11.5 eq www

access-list 102 permit ip any any

interface FastEthernet0/0

ip address 192.168.5.1 255.255.255.0

duplex auto

speed auto

!

interface FastEthernet0/1

ip address 192.168.4.2 255.255.255.0

duplex auto

speed auto

!

interface FastEthernet1/0

no ip address

duplex auto

speed auto

!

interface FastEthernet1/0.2

encapsulation dot1Q 2

ip address 192.168.2.2 255.255.255.0

interface FastEthernet1/0.6

encapsulation dot1Q 6

ip address 192.168.6.2 255.255.255.0

interface FastEthernet1/1

no ip address

ip access-group 102 in

duplex auto

speed auto

interface FastEthernet1/1.1

no ip address

ip access-group 100 in

interface FastEthernet1/1.10

encapsulation dot1Q 10

ip address 192.168.10.1 255.255.255.0

ip access-group 100 in

interface FastEthernet1/1.20

encapsulation dot1Q 20

ip address 192.168.20.1 255.255.255.0

interface FastEthernet1/1.30

encapsulation dot1Q 30

ip address 192.168.30.1 255.255.255.0

ip access-group 101 out