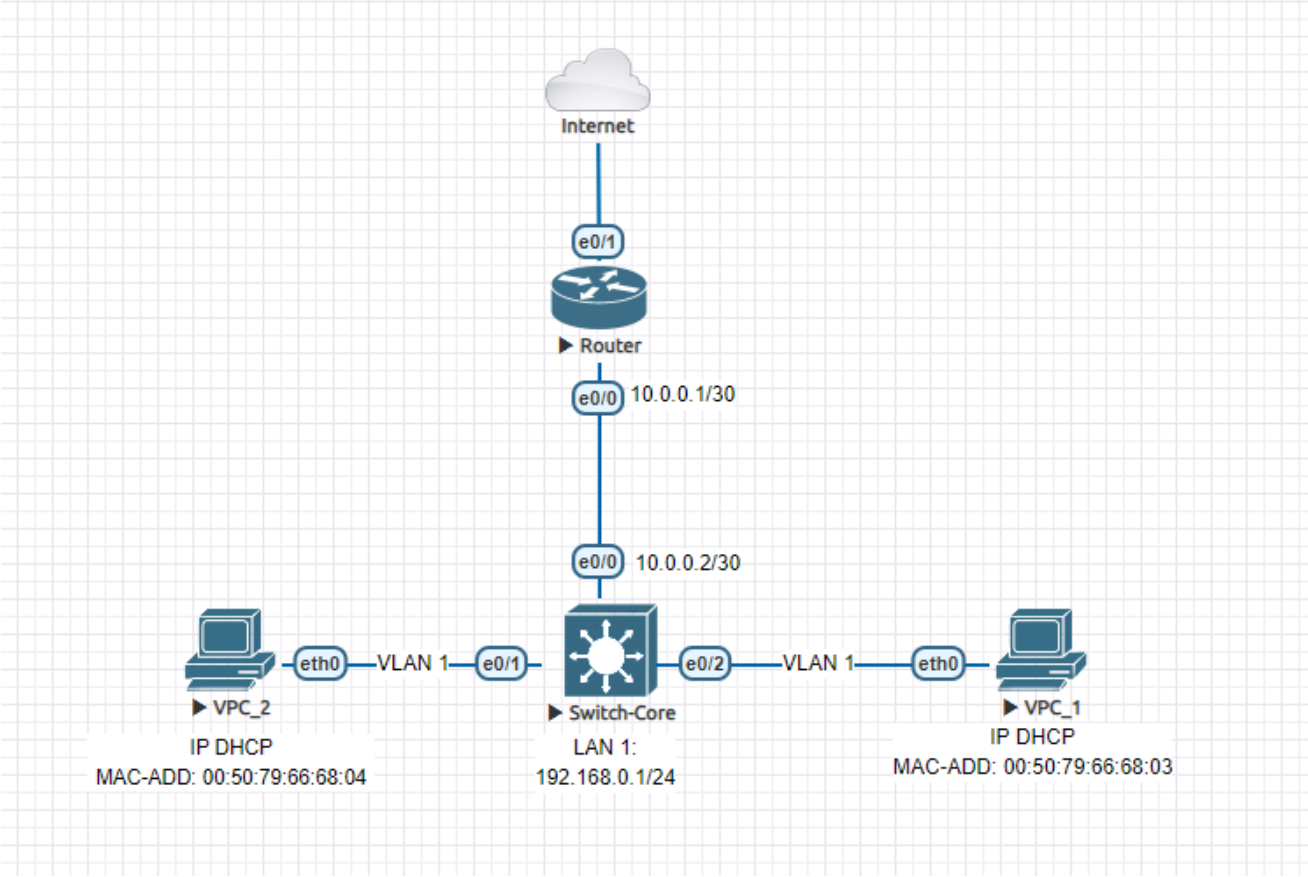
VLAN FILTER

MAC-ADDRESS

01/04/2023

Mô hình:



Trong mô hình ta có 1 Router đảm nhiệm vai trò Gateway Internet. Router này kết nối đến Switch Core thông qua Network ID 10.0.0.0/30, trong đó bản thân Router là 10.0.0.1/30 và Switch-Core 10.0.0.2/30.

Bây giờ, mục tiêu là sẽ sử dụng kỹ thuật để lọc các địa chỉ MAC-ADDR cho phép tại Switch-Core, chặn các địa chỉ MAC-ADDR lạ. Trong kịch bản này sẽ dùng VLAN 1 để thực hiện kỹ thuật này.

Thực Hiện Cấu Hình:

Sử dụng giao diện Console hoặc SSH | Telnet để thực hiện cấu hình

Cấu hình IP Address và Routing cơ bản

Switch-Core

```
!
enable
config t
```

```
ip routing
interface Vlan1
 Description LAN
 ip address 192.168.0.1 255.255.255.0
 no shutdown
exit
!
interface Ethernet0/0
 no switchport
 Description To Gateway Internet Router
 ip address 10.0.0.2 255.255.255.252
 duplex auto
exit
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
!
ip dhcp pool lan
 Description DHCP Server for LAN
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 dns-server 8.8.8.8
!
```

Router

```
!
enable
config t
interface Ethernet0/0
 Description LAN
 ip address 10.0.0.1 255.255.255.252
 ip nat inside
exit
!
interface Ethernet0/1
 Description WAN
```

```
 ip address dhcp
 ip nat outside
exit
!
ip route 192.168.0.0 255.255.255.0 10.0.0.2
!
ip nat inside source list 1 interface Ethernet0/1 overload
!
access-list 1 permit any
!
```

Giả sử VLAN 1 là giành cho Wi-Fi sẽ cho phép MAC-ADDR **00:50:79:66:68:03** cũng là địa chỉ của VPC_1 được phép truy cập vào hệ thống bao gồm Internet và các LAN Network, nhưng chặn **00:50:79:66:68:04** VPC_2 **#**

`` ! enable config t mac access-list extended Permit permit host 0050.7966.6803 any permit host aabb.cc80.2000 any ! ip access-list extended IP permit ip any any ! ```	● Tạo Access-list mac với thông số cho phép địa chỉ MAC đuôi **00:50:79:66:68:03** được phép đi any ● Đồng thời cho phép địa chỉ MAC đuôi 2000 là địa chỉ MAC của Interface VLAN 1 chính Switch Core để được phép truy cập any (Bắt buột), để lấy thông tin địa chỉ này dùng câu lệnh show int vlan 1 tại mode enable ● Tiếp tục, tạo một Access-list Filter IP Address cho phép đi any any để cho phép các Users nhận được địa chỉ DHCP và truy cập các IP address khác
`` ! vlan access-map MAC 5 match ip address IP action forward vlan access-map MAC 10 match mac address Permit action forward ! vlan filter MAC vlan-list 1 ! ```	● Tạo vlan access-map để thực thi các hành động và thực hiện các Access-list vừa tạo phía trên, chúng ta cần tạo 2 profile khác nhau với priority là 5 và 10 tên profile là MAC đặt tùy ý, sau đó gán profile này áp dụng cho các VLAN mình cần filter.