
Cấu hình Switch Layer 3 - NOVAON-sw

Cấu hình hiện tại

---

1. Cấu hình Hệ thống và Quản trị (System & Management)

Đây là các thiết lập cơ bản để đảm bảo switch hoạt động ổn định và an toàn trong việc quản trị.

- **Định danh:**
  - **Hostname:** NOVAON-sw.
  - **Domain Name:** novaon.local.
- **Bảo mật Truy cập Quản trị:**
  - **Mật khẩu enable:** Đã được mã hóa (enable secret).
  - **Tài khoản người dùng cục bộ:** Hai tài khoản giahung và it được tạo với đặc quyền cao nhất (privilege 15) và mật khẩu được mã hóa.
  - **Mật khẩu:** Novaon@#$2025
  - **Giao thức truy cập:** Chỉ cho phép truy cập quản trị từ xa thông qua **SSH (transport input ssh)**, vô hiệu hóa Telnet không an toàn.
- **Dịch vụ Hệ thống:**
  - **NTP (Network Time Protocol):** Không được cấu hình, nhưng múi giờ được đặt là ICT 7 0 để đảm bảo log hệ thống có dấu thời gian chính xác.
  - **DNS:** Được cấu hình với domain **novaon.local.**
- **Định tuyến IP (IP Routing):**
  - **Lệnh:** ip routing.
    + 18.9.6.0/24 via 192.168.11.251 (Để OpenVPN SSH được Switch)
    + 192.168.4.0/24 via 192.168.11.251 (Để Site to Site giao tiếp Switch

---

2. Uplink to Firewall

Đây là kết nối quan trọng nhất của switch, nơi toàn bộ lưu lượng của mạng nội bộ sẽ đi qua để đến tường lửa và ra Internet.

- **Port-channel 1 (Link Aggregation):**
  - **Cấu hình:** Hai cổng vật lý GigabitEthernet1/0/23 và GigabitEthernet1/0/24 được gộp lại thành một giao diện logic Port-channel1 bằng giao thức **LACP (chế độ active)**.
  - **Mục đích:** Tạo một liên kết gộp 2Gbps đến giao diện lagg0 trên pfSense.
  - **Chế độ hoạt động:** Cấu hình ở chế độ switchport mode trunk.
  - **VLANs cho phép:** Chỉ cho phép các VLAN từ 11 đến 16 đi qua (switchport trunk allowed vlan 11-16), khớp chính xác với cấu hình trên pfSense.
  - **Lợi ích:** Tăng băng thông và cung cấp khả năng dự phòng cho kết nối trọng yếu giữa switch lõi và tường lửa.

---

3. Cấu hình Mạng Nội bộ và Phân đoạn VLAN

Switch này là nơi các VLAN được tạo ra và quản lý.

- **Định tuyến giữa các VLAN (Inter-VLAN Routing):**
    - **Cấu hình:** Mỗi VLAN (11-16) được gán một giao diện ảo (Switched Virtual Interface - SVI) có tên interface VlanXX và được đặt một địa chỉ IP. Ví dụ:
        - interface Vlan11: ip address 192.168.11.254 255.255.255.0
        - interface Vlan12: ip address 192.168.12.254 255.255.255.0
        - ... và tương tự cho các VLAN khác.
    - **Vai trò:** Các địa chỉ IP này (.254) đóng vai trò là **Default Gateway** cho tất cả các thiết bị trong VLAN tương ứng. Khi một thiết bị ở VLAN 11 muốn nói chuyện với một thiết bị ở VLAN 12, nó sẽ gửi gói tin đến gateway 192.168.11.254. Switch sẽ nhận gói tin này và định tuyến nó sang VLAN 12.
- **DHCP Relay (ip helper-address):**
    - **Cấu hình:** Trên mỗi giao diện SVI của VLAN, có lệnh ip helper-address trỏ đến địa chỉ IP của pfSense trong cùng VLAN đó. Ví dụ:
        - Trên interface Vlan11: ip helper-address 192.168.11.251
        - Trên interface Vlan12: ip helper-address 192.168.12.251
    - **Mục đích:** Vì các máy khách và máy chủ DHCP (pfSense) nằm ở các VLAN khác nhau (broadcast domain khác nhau), các yêu cầu DHCP (là các gói tin broadcast) sẽ không thể tự đi qua router. Lệnh ip helper-address ra lệnh cho switch "bắt" các gói tin broadcast DHCP này, chuyển đổi chúng thành gói tin unicast và chuyển tiếp (relay) đến địa chỉ của máy chủ DHCP được chỉ định (pfSense).

- **Định tuyến đến Internet và các Mạng Khác (Static Route):**
    - **Cấu hình:** Switch không có default route. Thay vào đó, nó có các route tĩnh cụ thể.
        - ip route 18.9.6.0 255.255.255.0 192.168.11.251
        - ip route 192.168.4.0 255.255.255.0 192.168.11.251
    - **Giải thích:**
        - Lệnh đầu tiên chỉ cho switch biết rằng để đi đến mạng của **OpenVPN clients** (18.9.6.0/24), hãy gửi gói tin đến pfSense (192.168.11.251).
        - Lệnh thứ hai chỉ cho switch biết rằng để đi đến mạng của **văn phòng từ xa** (qua IPsec VPN - 192.168.4.0/24), cũng hãy gửi gói tin đến pfSense.
        - **Thiếu Default Route:** Cấu hình này có vẻ **thiếu một default route** (ip route 0.0.0.0 0.0.0.0 192.168.11.251). Nếu không có default route, các thiết bị trong mạng nội bộ **sẽ không thể đi ra Internet** thông qua switch này. Rất có thể việc định tuyến ra Internet được xử lý hoàn toàn bởi pfSense, và các thiết bị người dùng đang trỏ gateway trực tiếp về pfSense (.251) thay vì switch (.254). Cần kiểm tra lại cấu hình gateway trên các máy khách.

---

4. Access Ports & Security

Đây là các cấu hình áp dụng cho các cổng nơi người dùng cuối cắm vào.

- **Phân chia Cổng theo VLAN:**
    - **Cấu hình:** Mỗi cổng từ GigabitEthernet1/0/1 đến 1/0/22 được gán vào một VLAN cụ thể ở chế độ access. Ví dụ:
        - Cổng g1/0/1 đến g1/0/4 thuộc Vlan 11.
        - Cổng g1/0/5 đến g1/0/8 thuộc Vlan 12.
    - **Mục đích:** Đảm bảo rằng thiết bị cắm vào một cổng sẽ tự động thuộc về đúng phòng ban và nhận IP từ đúng dải DHCP.
- **Bảo mật Lớp Truy cập (Access Layer Security):**
    - **PortFast:**
        - **Lệnh:** spanning-tree portfast.
        - **Mục đích:** Được bật trên tất cả các cổng access. Lệnh này cho phép cổng ngay lập tức chuyển sang trạng thái forwarding khi có thiết bị cắm vào, bỏ qua các bước lắng nghe và học hỏi của Spanning Tree, giúp máy tính nhận IP và vào mạng nhanh hơn.
        - **Lưu ý:** Chỉ nên dùng trên các cổng cắm vào thiết bị đầu cuối (PC, máy in), không dùng trên cổng nối với switch khác.
    - **BPDU Guard:**
        - **Lệnh:** spanning-tree bpduguard enable.
        - **Mục đích:** Được bật trên hầu hết các cổng access. Đây là một tính năng an ninh quan trọng. Nếu cổng này nhận được một gói tin BPDU (thường chỉ được gửi bởi các switch khác), nó sẽ ngay lập tức bị đưa vào trạng thái err-disable (tắt). Điều này giúp ngăn chặn việc người dùng tự ý cắm một switch không được quản lý vào mạng, có thể gây ra vòng lặp (loop) và làm sập toàn bộ hệ thống.
