IPV6 FIRST HOP SECURITY - RA GUARD

I. Mô tả

Tính năng RA guard sẽ giúp lọc những router advertisement message đến từ nguồn không xác thực (Rouge RA). Tính năng này cấu hình trên thiết bị switch ở một số ios nhất định (không hỗ trợ lệnh trên 1 số dòng switch).

II. Cấu hình

Cấu hình căn bản cho router R1:

```
R1(config)#ipv6 unicast-routing
R1(config)#int e0/0
R1(config-if)#no ip add
R1(config-if)#ipv6 add FE80::1 link-local
R1(config-if)#ipv6 add 2001::1/64
```

Cấu hình căn bản trên switch: với việc tạo vlan 5 và gán port nối với router vào vlan 5.

```
SW1(config)#vlan 5
SW1(config-vlan)#name RA
SW1(config)#int e0/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 5
```

Tiến hành đặt địa chỉ ip link local cho int vlan 5 và cấu hình địa chỉ global ipv6 là

```
SW1(config)#int vlan 5
SW1(config-if)#ipv6 address FE80::2 link-local
SW1(config-if)#ipv6 address autoconfig
```

autoconfig (xem như một dạng dhcp client trong ipv6).

Cấu hình tính năng neigbor binding theo vlan 5 và subnet 2001::/64

```
SW1(config)#ipv6 neighbor binding vlan 5 2001::/64 int e0/0
SW1(config)#ipv6 neighbor binding max-entries 200
```

Kiểm tra cấu hình neigbor binding

```
SW1#show ipv6 neighbor binding
Binding Table has 1 entries, 0 dynamic (limit 200)
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other Packet, API -
API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    IPv6 address         Link-Layer addr Interface        vlan prlvl  age   state    Time left
S   2001::/64            any             Et0/0             5  0100   24s  REACHABLE
```

Chúng ta bắt đầu cấu hình tính năng RA Guard

```
SW1(config)#ipv6 nd raguard policy RAGUARD
SW1(config-nd-raguard)#device-role host
SW1(config-nd-raguard)#exit
SW1(config)#int e0/0
SW1(config-if)#ipv6 raguard attach-policy RAGUARD
```

Kiểm tra lại cấu hình RAGuard vừa thực hiện với lệnh show ipv6 raguard policy <Tên policy>

```
SW1#show ipv6 nd raguard policy RAGUARD
Policy RAGUARD configuration:
  device-role host
Policy RAGUARD is applied on the following targets:
Target               Type  Policy               Feature        Target range
Et0/0                PORT  RAGUARD              RA guard       vlan all
```

Thử lệnh xem thông tin ipv6 trên cổng vlan 5 với lệnh **show ipv6 int vlan 5.**

```
SW1#show ipv6 int vlan 5
Vlan5 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::2
  No Virtual link-local address(es):
  Stateless address autoconfig enabled
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
```

```
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

Lúc này có thể thấy được rằng trước khi cấu hình tính năng RAGuard trên switch 1, thì cổng int vlan 5 sẽ có địa chỉ ip global chẳng hạn 2001::2/64 với default router là ip global cổng e0/0 của R1. Nhưng sau khi bật tính năng RAGuard, các thông tin này sẽ bị chặn lại, thông điệp message Router Advertisement sẽ bị drop bỏ, do vậy cổng int vlan 5 chỉ nhận ip link local như đã đặt, còn ip global xin từ R1 sẽ không nhận được.

(optional: Có thể sử dụng câu lệnh trên thiết bị thật **show ipv6 snooping counters int <name>** để xem các gói bị drop bỏ (lưu ý thiết bị ảo lệnh nào có thể không quan sát được gì)).