

Lab Guide & Module

Cisco Certified Network Associate 200-301 V.1.1



2. Port-Security

Seringkali kita perlu melakukan konfigurasi basic security pada switch agar interface yang digunakan hanya dapat dikoneksikan dari MAC Address yang sudah terdaftar. Jika fitur ini tidak diaktifkan, maka koneksi antara Switch dengan Host (PC/Server) dapat dengan mudah ditukar dengan Host lain yang berpotensi menjadi celah keamanan pada jaringan switching.

Port-security dapat menjadi solusi untuk permasalahan tersebut. Mekanisme dari port-security cukup simpel, kita cukup mendaftarkan MAC Address dari Host (PC/Server) yang ingin kita allow access nya ke switch.

Terdapat dua metode pendaftaran MAC Address, Dynamic (sticky) atau mode Manual. Kita dapat memilih sesuai preferensi masing-masing. Dalam lab kali ini, kita akan coba mengamankan akses host dengan mendaftarkan MAC Address dengan metode dynamic sticky.

Jika terdapat pelanggaran akses dari MAC Address yang tidak terdaftar, maka kita bisa menentukan action violation apa yang akan dilakukan. Ada 3 violation yang bisa dipilih ketika suatu port pada switch digunakan oleh MAC Address yang tidak terdaftar:

- Protect: Data yang diterima tersebut tidak akan diteruskan ke tujuan (discard).
- Restrict: Sama seperti protect dan mengirimkan notifikasi log message SNMP.
- Shutdown: Default violation, port dalam keadaan err-disable (port mati).

Masih menggunakan Lab InterVLAN MLS, kita akan mengaktifkan fitur Port-security ke beberapa port yang terhubung ke host-device. Sebagai pengujian kita dapat mengubah MAC Address PC menjadi MAC address yang lain.

Langkah Pengerjaan:

Konfigurasikan port-security berikut di MLS0:

MLS0

```
MLS0(config)#int range fa0/1-2
```

```
MLS0(config-if-range)#switchport port-security
```

```
MLS0(config-if-range)#switchport port-security mac sticky
```

```
MLS0(config-if-range)#switchport port-security violation shutdown
MLS0(config-if-range)#
MLS0(config-if-range)#int range fa0/3-4
MLS0(config-if-range)#switchport port-security
MLS0(config-if-range)#switchport port-security mac sticky
MLS0(config-if-range)#switchport port-security violation restrict
MLS0(config-if-range)#
MLS0(config-if-range)#int fa0/5
MLS0(config-if)#switchport port-security
MLS0(config-if)#switchport port-security mac sticky
MLS0(config-if)#switchport port-security violation protect
```

Selanjutnya coba lakukan ping dari setiap perangkat, ke arah MLSO. Lalu coba cek perintah

berikut:

```
MLS0
MLS0#show port-security
```

Pada bagian Current Address kita sudah melihat masing-masing interface memiliki 1 MAC address terdaftar. Jika salah satu interface Current Address terisi 0, maka kemungkinan port tersebut belum menerima traffic dari host device.

Selain perintah diatas, kita juga bisa melihat konfigurasi port-security secara detail via perintah berikut:

```
MLS0
MLS0#show port-security address
MLS0#show port-security interface fa0/1
```