MAC LIMITING

E' una funzionalità di protezione layer 2 switching, applicata a livello di porta di accesso, contro attacchi che usano MAC addresses quali MAC flooding e MAC spoofing (DoS attack).

MAC Limiting utilizza due metodi:

- *MAC limit:* permette di specificare il numero massimo di MAC addresses che possono essere appresi attraverso una singola porta di accesso; una volta che lo switch raggiunge il numero limite di MAC, tutto il traffico sorgente da nuovi MAC address sono droppati, sulla base della azioni previste in configurazione

- *MAC allowed:* permette di definire MAC addresses per una specifica porta di accesso; qualsiasi MAC addresses che non è specificato nella lista per quella determinata porta non sarà preso in considerazione e pertanto negato.

Il primo metodo (*MAC address limit*) è efficace contro attacchi flooding; il secondo metodo (*MAC statically binding*) contro attacchi spoofing.

Un terzo metodo è quello di usare la funzionalità di *MAC move limit* che limita il valore temporale per cui un indirizzo MAC può "spostarsi" verso una nuova interfaccia layer 2; questo metodo è efficace a prevenire MAC spoofing ed eventuali loops (questo metodo si può configurare anche per-vlan).

MAC LIMITING ACTIONS:

Le azioni che si possono configurare sulla base di questa funzionalità sono:

- none
- syslog
- drop and syslog
- shutdown della porta and error-log

N.B. di default l'azione è quella di Drop (switch Juniper)

Quindi per tutti i MAC addresses che eccedono le funzionalità indicate in configurazione (su base interface oppure per-vlan) vengono intraprese le azioni suddette

Di seguito aspetti di configurazione (junos)

Esempio di configurazione ***MAC limiting options***

```
edit ethernet-switching-option secure-access-port
!
set interface ge-0/0/2.0 allowed-mac [00:20:77:02:84:34 00:20:77:02:84:35]
set interface ge-0/0/3.0 mac-limit 2 action log
set interface ge-0/0/4.0 mac-limit 2 action drop
set interface all mac-limit 1 action shutdown
!
set vlan pippo mac-move-limit 1 action shutdown
```

L'opzione **none** viene usata in caso si voglia escludere una determinata porta o vlan, quando si usa in configurazione lo statements " interface all" oppure "vlan all", dalle azioni di MAC limiting presenti.

Es:

```
edit ethernet-switching-option secure-access-port
!
set interface ge-0/0/4.0 mac-limit 1 action none
set interface all mac-limit 1 action shutdown
!
set vlan all mac-move-limit 1 action shutdown
set vlan pippo mac-move-limit 1 action none
```