Study of DHCP Snooping

1. Configure DHCP snooping on a L3 switch and configure the trusted port to the DHCP server

In this example, the L3 switch connects to the DHCP server via fa0/4 :

```
SW-3560(config)#ip dhcp snooping
SW-3560(config)#int fa0/4
SW-3560(config-if)#ip dhcp snooping trust
```

The DHCP client connects to fa0/1 :

```
SW-3560(config-if)#int fa0/1
SW-3560(config-if)#switchport mode access
SW-3560(config-if)#switchport access vlan 1
```

Option 82 is enabled by default. Option 82 adds the port-identifier (fa0/1) to the DHCP request, just like a DHCP relay agent would. The port-identifier is the "gi-addr" or 'gateway address'.

2. The effect of DHCP snooping with option 82

Once a DHCP address has been submitted to a client, DHCP snooping shows:

```
SW-3560#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:  1
DHCP snooping is operational on following VLANs: 1
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 18ef.6326.2880 (MAC)            ->> this is the BASE MAC
Verification of hwaddr field is enabled
Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/4            yes        yes             unlimited
```

The client receives a DHCP address on fa0/1:

```
SW-3560#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
10:DD:B1:33:AA:00   192.168.3.105    2591997     dhcp-snooping   1     FastEthernet0/1

Total number of bindings: 1
```

3. Now see how IP Source Guard prevents an IP spoof

Configure IP Source Guard on the Fa0/1 and 0/5 port:

```
SW-3560(config-if)#ip verify source
SW-3560#sh ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
```

```
---------  -----------  -----------  ---------------  -----------------  ----
Fa0/1      ip           active       192.168.3.105                         1
Fa0/4      ip           inactive-trust-port
```

Now we will provide the client with a “false” / different MAC address while maintaining the same DHCP IP address:

```
$ ifconfig en0 ether 10:dd:b1:99:c1:00
```

On the same Switch interface fa0/1, nothing happens despite that the MAC address has changed.

Now connect this client with the altered MAC address to **fa0/5** where IP Source Guard is configured as well**:**

```
SW-3560# sh ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Fa0/1      ip           inactive-no-snooping-vlan
Fa0/4      ip           inactive-trust-port
Fa0/5      ip           active       192.168.3.105                        1
```

The interface is unable to communicate over Fa0/5 because as the output shows, fa0/5 is Filtered due to the dhcp snoop – binding.. The interface remains up however; IP Source Guard works.