IP SOURCE GUARD

IP Source Guard provides security to the network by filtering clients with invalid or spoofed IP addresses. IP Source Guard is a Layer 2 (L2), port-to-port feature that works closely with information in the Dynamic Host Control Protocol (DHCP) snooping binding table. When you enable IP Source Guard on an untrusted port with DHCP snooping enabled, an IP filter entry is created or deleted for that port automatically, based on IP information stored in the corresponding DHCP binding table entry. When a connecting client receives a valid IP address from the DHCP server, a filter is installed on the port to allow traffic only from the assigned IP address. A maximum of 10 IP addresses are allowed on each IP Source Guard-enabled port. When this number is reached, no more filters are set up and traffic is dropped.

While Dynamic ARP Inspection blocks only ARP packets, IP Source Guard blocks all IP packets.

```
interface fa 1/1-23,2/1-23


 ip verify source


exit
```

Issues with IP Source Guard

IP Source Guard utilizes the information stored in the DHCP binding table (from DHCP Snooping) to validate the IP traffic. Any device whether it be statically configured or dynamically configured would need to appear in the DHCP binding table. Statically

configured devices would need to be manually placed in the DHCP binding table. If someone changed out a device the MAC address would most likely need to be updated in the DHCP binding table. If the DHCP binding table was accidentally cleared the switch would block IP traffic until the DHCP binding table was re-built either manually or from DHCP transactions.

This feature will likely create some significant administrative overhead based on the number of devices configured with a static IP address over the number of DHCP configured devices.

Source : http://blog.michaelfmcnamara.com/2013/01/dhcp-snooping-arp-inspection-ip-source-guard/