DHCP SNOOPING

Dynamic Host Configuration Protocol (DHCP) snooping provides security to the network by preventing DHCP spoofing. DHCP spoofing refers to an attacker's ability to respond to DHCP requests with false IP information. DHCP snooping acts like a firewall between untrusted hosts and the DHCP servers, so that DHCP spoofing cannot occur. There are 2 types of ports in DHCP snooping, **trusted** and **untrusted**. The network will only allow DHCP responses from trusted ports – usually uplinks as opposed to allowing DHCP responses from untrusted ports – usually edge switch ports.
Example, if someone brings a Linksys router into the office and connects the LAN side to your network the Linksys router will start handing out 192.168.1.x IP DHCP addresses which will likely cause some chaos. DHCP Snooping will prevent those DHCP responses from poisoning your network. I'm happy to admit that this is happened to me on more than one occasion, usually at our remote finance office where auditors think their second job could be in Information Technology.

DHCP Option 82 – With DHCP Option 82 the switch will append additional information to the DHCP request which can be stored in your IPAM (IP Address Management) solution to help identify the switch and port from which the request was initiated. This can provide diagnostic and troubleshooting information which can all be stored directly in your IPAM if it supports DHCP Option 82. Infoblox supports DHCP Option 82.
The latest software releases support the ability to copy the DHCP binding table up to a TFTP server. This prevents the switch from throwing away all the previously learned DHCP transactions between reboots or restarts of the switch.

In this example our uplinks are 1/24 and 2/24, all interfaces are untrusted by default.

```
ip dhcp-snooping vlan 10

ip dhcp-snooping vlan 11

ip dhcp-snooping enable
```

```
interface fa 1/24,2/24

 ip dhcp-snooping trusted

exit
```

If you want to enable DHCP Option 82 support;

```
ip dhcp-relay option82

interface vlan 10

 ip dhcp-relay option82

interface vlan 11

 ip dhcp-relay option82
```

You can also edit the text string the switch will append per port with the following;

```
interface FastEthernet 1

 ip dhcp-relay option82-subscriber-id
```

Issues with DHCP Snooping

While you need to properly identify trusted and untrusted ports there are very few draw backs to utilizing DHCP snooping. It only prevents DHCP replies from untrusted ports essentially preventing DHCP spoofing in the network. DHCP Snooping can be enabled in most networks with a few configuration changes and very little danger (impact).

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