DHCP Snooping

A security feature in Cisco switches to protect against attacks taking advantage of DHCP, it filters DHCP messages received on untrusted ports, all ports are untrusted by default (usually uplink (ports pointing towards network devices monitored by admin) ports are configured as trusted, downlink (ports pointing towards endhosts). as untrusted, malicious messages are discarded.

CHAADR (Client Hardware Address) field in DHCP is used for indicating the requesting client's mac address.

DHCP starvation/exhaustion: an attacker uses spoofed MAC addresses to flood DHCP discover messages causing DoS.

DHCP Poisoning: Man in the Middle attack, a spurious DHCP server replies to client's discover messages, assigns them IP addresses and makes them use use it as their default gateway. (Clients usually accept the first offer message they receive and decline the others), the spurious DHCP server then forwards packets to the legitimate default gateway after examining/ modifying them causing the client to feel normal.

DHCP snooping differentiates between server and client messages, server messages received on untrusted ports are always discarded, while client messages are inspected then decided whether to be forwarded or not.

DHCP server messages: OFFER/ACK/NAK(to decline a client's request).

DHCP client messages; DISCOVER-REQUEST-RELEASE-DECLINE (IP address offered by server).

DISCOVER/REQUEST messages: check if frame's MAC address matches the DHCP CHADDR else discarded.

RELEASE/DECLINE messages: check if the packet's source IP address and receiving interface match the entry in DHCP Snooping Binding table. (when a client successfully leases an IP address, it creates a new entry in the DHCP Snooping Binding table).

Command: ip dhcp snooping. To enable globally **Command: ip dhcp snooping vlan <number>.** To enable on a specific vlan.

Command: no ip dhcp snooping information option.

Command: ip dhcp snooping trust. Command: show ip dhcp snooping binding.

DHCP snooping can limit the rate at which DHCP messages are allowed to enter an inetrface, if rate exceeded the configured limit, the interface is err-disabled.

Command: ip dhcp snooping limit rate <number of packets/second>.

Command: errdisable recovery cause dhcp-rate-limit.

Option 82 known as DHCP relay agent information option, provides additional info about which relay agent received the client's message on which interface, in which vlan, by default Cisco switches will add option 82 to DHCP messages they receive from clients, even if the switch itself is not acting as a DHCP relay agent, by default Cisco switches will drop DHCP messages with option 82 received on untrusted ports.

A router will drop a DHCP message having option 82 and not sent by a relay agent.

Command: banner login $<banner>$.