How DHCP snooping works under DWS-4026

DHCP Snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP server to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are considered authorized. The network administrator enables DHCP snooping globally and on specific VLANs, and configures ports within the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports. DHCP snooping enforces the following security rules:

DHCP packets from a DHCP server (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped if received on an untrusted port.

DHCPRELEASE and DHCPDECLINE messages are dropped if for a MAC address in the snooping database, but the binding's interface is other than the interface where the message was received.

On untrusted interfaces, the switch drops DHCP packets whose source MAC address does not match the client hardware address. This feature is a configurable option.

Below two cases just a simple setup, so user can easily understand the usage. This feature better work with Dynamic Arp Inspection & IP Source Guard, for a better protection. I have attached the cpature for those two cases under L7_capture1.txt.

platform: DWS 4026

code: 1.0.0.10

repro case1: dynamic binding, verify a foul PC or malicious SW won't interfere the DHCP message

1. connect a hub to a port (Ex: 0/2), plug in PC1 to hub and get ip address from DWS4K.

2. Verify the binding status by "show ip dhcp snooping binding"

3. From PC1, do release IP

4. Verify the binding status by "show ip dhcp snooping binding"

Expect: binding entry disappear

5. PC1 then renew IP

Expect: PC get same IP

6. Plug in PC2 to same hub, set PC2 to the same ip as PC1 with diff MAC, do release IP

Expect: binding entry won't disappear, statistics display the error message

repro case2: static binding, verify a PC can't get DHCP IP from different port, and DHCP message will get drop

1. connect 1 PC to port 2 and set ip address

2. Verify the binding status by "show ip dhcp snooping binding"

3. config the static binding for this PC

4. Verify the binding status & statistics log by "show ip dhcp snooping statistics"

5. Move the PC from port 2 to port 4, From PC, chnage NIC to DHCP, then renew IP

Verify the DHCP request get drop by "show logging buffered"

6. Move the PC back to port 2, From PC, DHCP renew IP

Verify the DHCP request get drop by "show logging buffered"