https://community.fs.com/blog/what-is-dhcp-snooping-and-how-it-works.html

What Is DHCP Snooping and How It Works?

"Why can't I access the network even if my laptop has acquired the IP address dynamically?" Have you encountered this issue in your daily life? Have you suspected the genuineness of the IP address? Whether it is from the authorized DHCP server? If not, how to prevent this from happening? In this post, a term DHCP Snooping will be introduced to help users to avoid illegal IP addresses.

What Is DHCP Snooping?

DHCP Snooping is a layer 2 security technology incorporated into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. DHCP Snooping prevents unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. The DHCP Snooping feature performs the following activities:

Validates DHCP messages from untrusted sources and filters out invalid messages.

Builds and maintains the DHCP Snooping binding database, which contains information about untrusted hosts with leased IP addresses.

Utilizes the DHCP Snooping binding database to validate subsequent requests from untrusted hosts.

How DHCP Snooping Works?

To figure out how DHCP Snooping works, we must catch on the working mechanism of DHCP which stands for dynamic host configuration protocol. With DHCP enabled, a network device without IP address will "interact" with the DHCP server through 4 stages as follows.

DHCP Snooping generally classifies interfaces on the switch into two categories: trusted and untrusted ports as shown in Figure 2. A trusted port is a port or source whose DHCP server messages are trusted. An untrusted port is a port from which DHCP server messages are not trusted. If the DHCP Snooping is initiated, the DHCP offer message can only be sent through the trusted port. Otherwise, it will be dropped.

In the acknowledgment stage, a DHCP binding table will be created according to the DHCP ACK message. It writes down the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host, as is shown in Figure 3. If the subsequent DHCP packet received from untrusted hosts fails to match with the information, it will be dropped.

Common Attacks Prevented by DHCP Snooping

DHCP Spoofing Attack

DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list itself (spoof) as the default gateway or DNS server, hence, initiating a man in the middle attack. With that, it is possible that they can intercept traffic from users before forwarding to the real gateway or perform DoS by flooding the real DHCP server with requests to choke IP address resources.

DHCP Starvation Attack

DHCP starvation attack commonly targets network DHCP servers, in a bid to flood the authorized DHCP server with DHCP REQUEST messages using spoofed source MAC addresses. The DHCP server will respond to all requests, not knowing this is a DHCP starvation attack, by assigning available IP addresses, resulting in the depletion of DHCP pool.

How to Enable DHCP snooping?

DHCP Snooping is only applicable to wired users. As an access layer security feature, it is mostly enabled on any switch containing access ports in a VLAN serviced by DHCP. When deploying DHCP Snooping, you need to set up the trusted ports (the ports through which legitimate DHCP server messages will flow) before enabling DHCP Snooping on the VLAN you wish to protect. This can be realized in both the CLI interface and also the Web GUI. The CLI commands are showcased in DHCP Snooping Configuration on FS S3900 Series Switches.

Conclusion

Though DHCP simplifies the IP addressing, it raises security concerns at the same time. To address the concerns, DHCP Snooping, one of the protection mechanisms can prevent the invalid DHCP addresses from the rogue DHCP server and can ward off the resource-exhausting attack that attempts to use up all existing DHCP addresses. FS S3900 series gigabit stackable managed switches can give full play to this feature to protect your network.