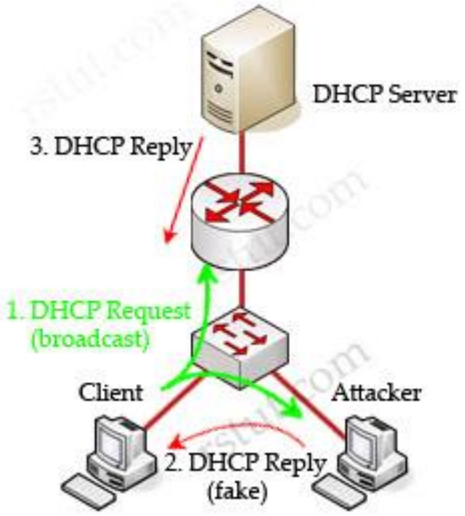
DHCP snooping

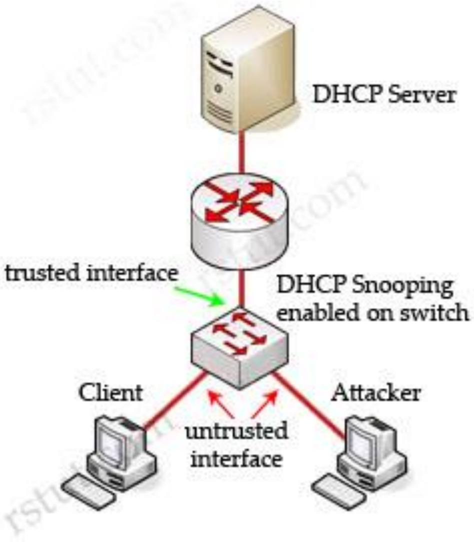
DHCP snooping is a feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. DHCP snooping allows all DHCP messages on trusted ports, but it filters DHCP messages on untrusted ports.

Let’s see an example without DHCP snooping.



In this example, a client is trying to get a valid IP address from the DHCP Server. It sends out a DHCP Request (broadcast) message so both the DHCP Server and the Attacker can hear it. The attacker pretends to be a DHCP Server and replies to the request with a valid IP address but using its own IP address as the default gateway. If its reply can arrive before the real DHCP reply, it will be considered the default gateway. From now, the client will send packets to the attacker as it believes the attacker is the default gateway. The attacker captures these packets and sends a copy to the desired default gateway -> it becomes a “man in the middle”.



Cisco switches can use DHCP snooping feature to mitigate this type of attack. When DHCP snooping is enabled, switch ports are classified as trusted or untrusted. Trusted ports are allowed to send all types of DHCP messages while untrusted ports can send only DHCP requests. If a DHCP reply is seen on an untrusted port, the port is shut down.

By default, if you enable IP source guard without any DHCP snooping bindings on the port, a default port access-list (PACL) that denies all IP traffic expect the DHCP Request (DHCP Discover) is installed on the port. Therefore the DHCP Server can hear the DHCP Request from the Client but its reply is filtered by the switch and the client can’t obtain an IP address.

Some useful information about DHCP snooping & IP Source Guard:

When enabled along with DHCP snooping, IP Source Guard checks both the source IP and source MAC addresses against the DHCP snooping binding database (or a static IP source entry). If the entries do not match, the frame is filtered. For example, assume that the **show ip dhcp snooping binding** command displays the following binding table entry:

MacAddress	IpAddress	LeaseSec	Type	VLAN	Interface
01:23:4A:5B:6C:88	10.1.2.30	6943	dhcp-snooping	10	FastEthernet0/10

If the switch receives an IP packet with an IP address of 10.1.2.30, IP Source Guard forwards the packet only if the MAC address of the packet is 01:23:4A:5B:6C:88.