NETWORK SWITCHING FEATURES

DHCP SNOOPING

Document ID: SW-DHCPSNOOP -002
Revision ID: 01 | Revision Date: 11-09-2024

Table of Contents

Glossary

The following terms are frequently used in this document.

Term	Definition
DHCP	Dynamic Host Configuration Protocol
VLAN	Virtual Local Area Network
MAC	Media Access Control
IP	Internet Protocol
ARP	Address Resolution Protocol

Functional Description

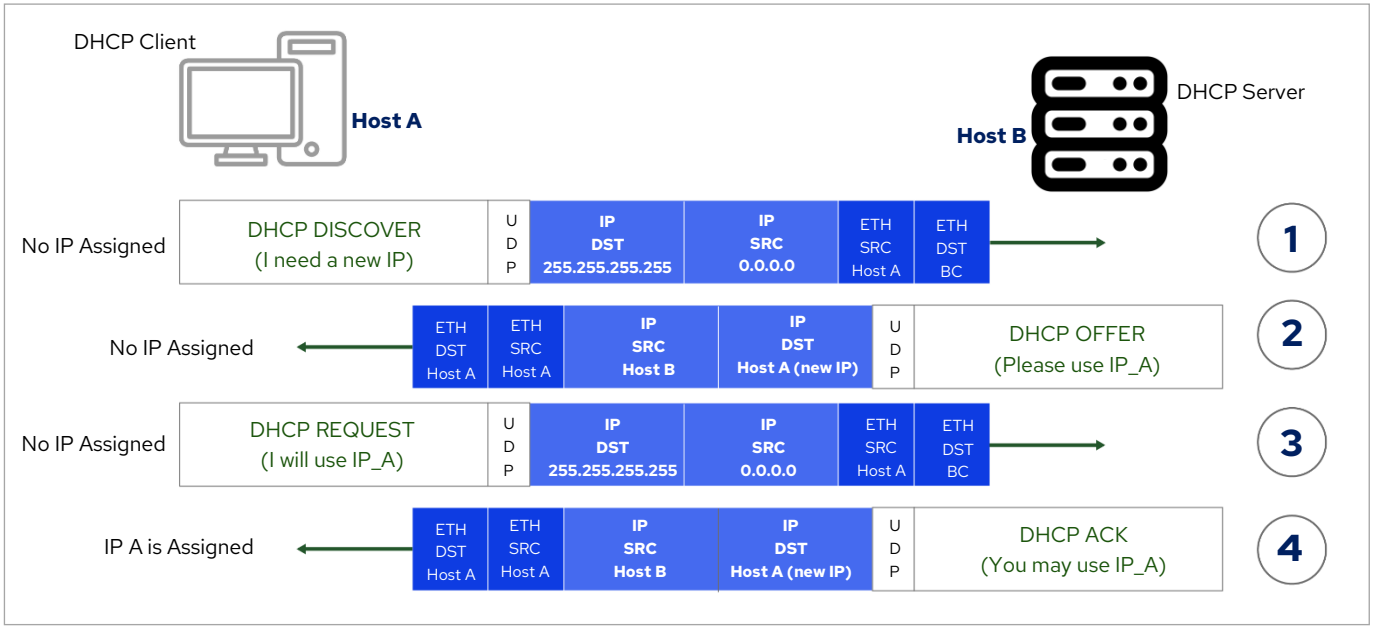
DHCP snooping in the switch secures your network by blocking unauthorized DHCP servers (rogue devices) and malicious traffic. It acts like a firewall between untrusted devices and the legitimate DHCP servers.

The Dynamic Host Configuration Protocol (DHCP) snooping function allows a device to snoop DHCP packets exchanged between clients and a server to record and monitor the IP address usage and filter out invalid DHCP packets, including request packets from the clients and response packets from the server. User data entries generated from DHCP Snooping records may serve security applications such as IP Source Guard.

- The DHCP snooping feature performs tasks to ensure network security and proper functioning.
- It verifies the integrity of messages received from sources and filters out any invalid messages.
- It controls traffic flow from both untrusted sources to prevent congestion or potential attacks.
- It maintains a binding table that stores information about clients that have obtained an IP address from a trusted server.
- It utilizes the data in the binding table to enforce security measures like IP source guard and dynamic ARP inspection, which protect against IP and ARP spoofing attacks.

DHCP

To understand how DHCP snooping operates, it is essential to understand the DHCP process. The diagram below illustrates an exchange between a client and a server:



The DORA process in DHCP involves four steps:

DISCOVER

The client sends a Limited Broadcasts (255.255.255.255) with a DHCP DISCOVER message, and shows so that he needs an IPv4 configuration.

OFFER

The DHCP Server responds with an Unicast message which contains a proposal for the new IPv4 address and the DHCP OFFER also may provide additional information like subnet mask, Default Gateway, DNS server and NTP server. The additional information depends on how the DHCP server is configured.

REQUEST

The client answers the proposal with a DHCP REQUEST again as a Limited Broadcast. With this DHCP REQUEST he also shows other DHCP servers which DHCP server the client has selected.

ACK

The server acknowledges the DHCP REQUEST with an Unicast DHCP ACK message.

Trusted / Untrusted source

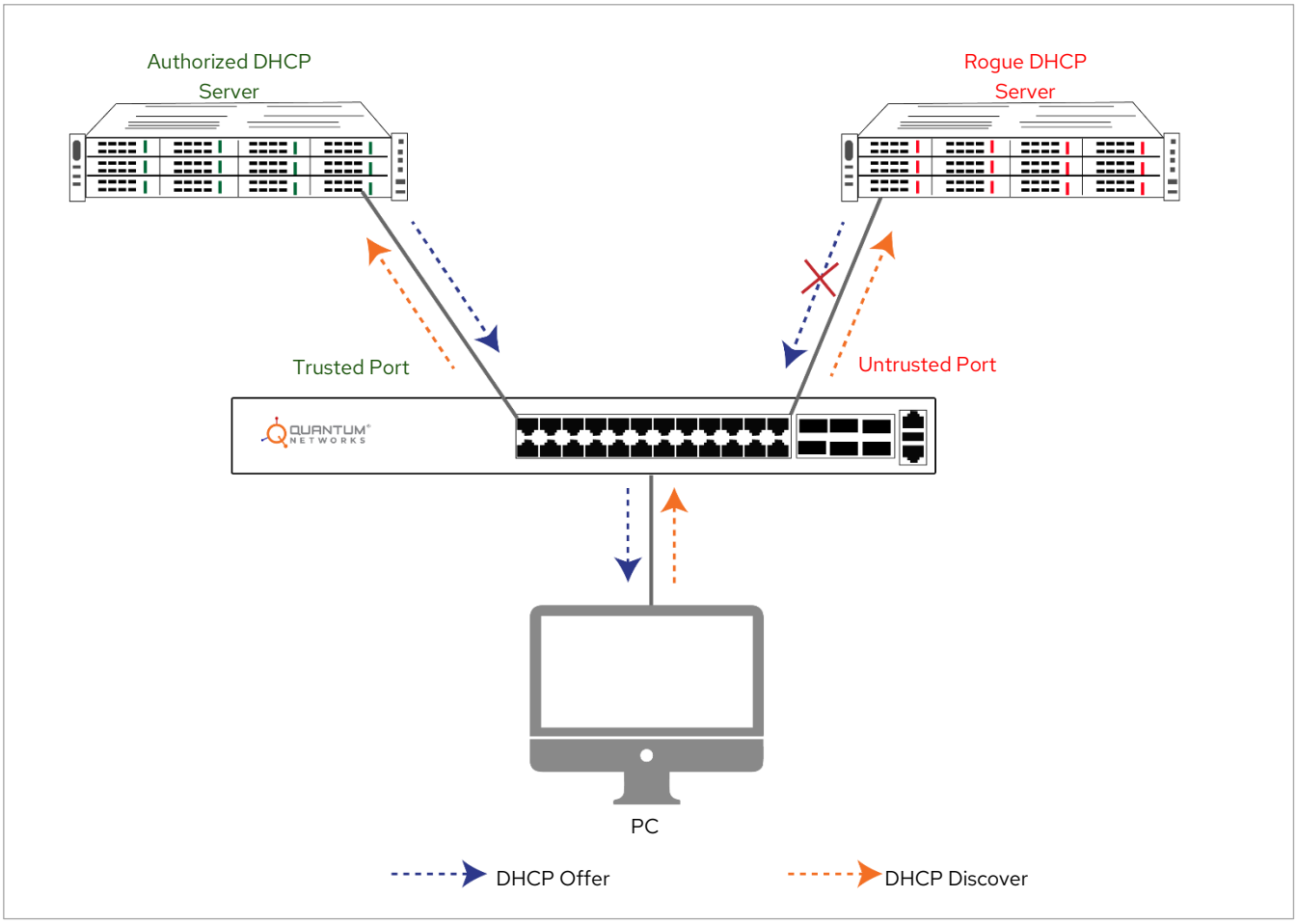


Fig 1

DHCP Snooping prevents unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.

In DHCP, trusted ports are ports that are connected to a DHCP server and can assign DHCP addresses. Untrusted ports are ports that cannot assign DHCP addresses. By default, all ports are considered untrusted unless you declare them trusted.

Purpose of DHCP Snooping

DHCP Snooping blocks unauthorized (rogue) DHCP servers from assigning IP addresses to clients. This feature works by validating DHCP messages from untrusted sources and filtering out any invalid messages.

- **Prevent unauthorized DHCP servers:** Ensures only legitimate DHCP servers assign IP addresses.
- **IP address management:** Maintains proper IP address allocation and prevents conflicts.
- **Network security:** Protects against IP address spoofing and other attacks.
- **Network stability:** Prevents disruptions caused by conflicting IP addresses.
- **Compliance:** Helps meet compliance requirements for network security.

DHCP Snooping in QN switches

Commands Outline

Use the ip dhcp snooping Global Configuration mode command to enable Dynamic Host Configuration Protocol (DHCP) snooping globally. Use the no form of this command to restore the default configuration.

switch(config)# ip dhcp snooping

Use the ip dhcp snooping VLAN Global Configuration mode command to enable DHCP snooping on a VLAN. Use the no form of this command to disable DHCP Snooping on a VLAN.

switch(config)# ip dhcp snooping vlan 21

Use the ip dhcp snooping trust Interface Configuration (Ethernet, Port-channel) mode command to configure a port as trusted for DHCP snooping purposes. Use the no form of this command to restore the default configuration.

switch(config)# interface te1/0/4

switch(config-if)# ip dhcp snooping trust

Use the ip dhcp snooping information option allow-untrusted Global Configuration mode command to allow a device to accept DHCP packets with option-82 information from an untrusted port. Use the no form of this command to drop these packets from an untrusted port.

switch(config-if)#ip dhcp snooping information option allow-untrusted

Use the ip dhcp snooping verify Global Configuration mode command to configure a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address. Use the no form of this command to disable MAC address verification in a DHCP packet received on an untrusted port.

switch(config)# ip dhcp snooping verify

Use the ip dhcp snooping database Global Configuration mode command to enable the DHCP snooping binding database file. Use the no form of this command to delete the DHCP Snooping binding database file.

switch(config)# ip dhcp snooping database

Use the ip dhcp snooping binding Privileged EXEC mode commands to configure the DHCP snooping binding database and add dynamic binding entries to the database. Use the no form of this command to delete entries from the binding database.

switch# ip dhcp snooping binding 0060.704C.73FF 23 176.10.1.1

te1/0/4 expiry 900

Use The Clear ip dhcp snooping database Privileged EXEC mode command to clear the DHCP snooping binding database.

switch# clear ip dhcp snooping database

Use the show ip dhcp snooping EXEC mode command to display the DHCP snooping configuration for all interfaces or for a specific interface.

switch# show ip dhcp snooping

DHCP snooping is Enabled

DHCP snooping is configured on following VLANs: 21

DHCP snooping database is Enabled

Relay agent Information option 82 is Enabled

Option 82 on untrusted port is allowed

Verification of hwaddr field is Enabled

DHCP snooping file update frequency is configured to: 6666 seconds

Interface Trusted

---------- ----------

te1/0/1 Yes

te1/0/2 Yes

Use the show ip dhcp snooping binding User EXEC mode command to display the DHCP Snooping binding database and configuration information for all interfaces or for a specific interface.

switch# show ip dhcp snooping binding

Update frequency: 1200

Total number of binding: 2

Mac Address	*Ip address*	*lease (Sec)*	*Type*	*VLAN*	*Interface*
0060.704C.73FF	*10.1.8.1*	*7983*	*snooping*	*3*	*te1/0/1*
0060.704C.7BC1	*10.1.8.2*	*92332*	*snooping*	*3*	*te1/0/2*

Configuration Steps

Let's consider that we are applying DHCP Snooping on SW1 to prevent users from having dynamic IP addresses to ensure that every user obtains IP address from Legit DHCP server.

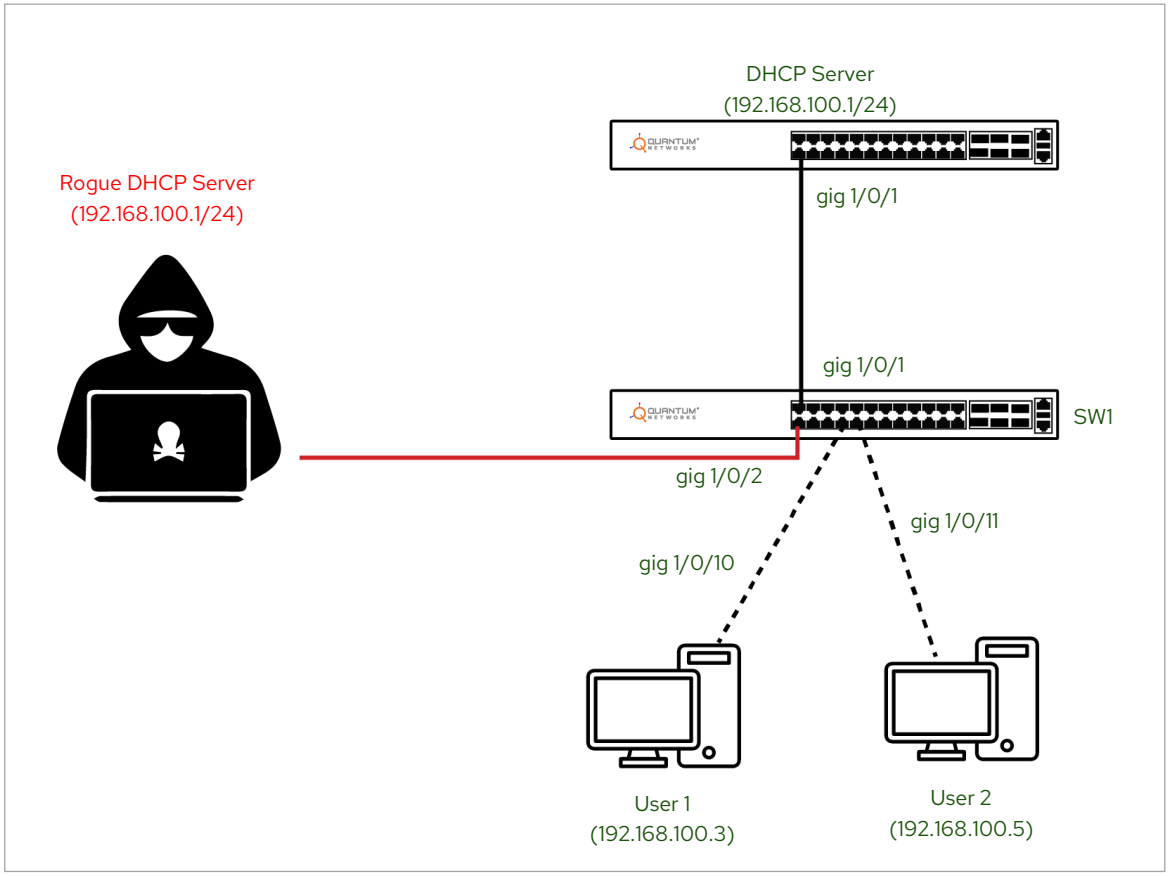


Fig 2

To enable DHCP snooping globally on the switch, below command must be executed to activate DHCP snooping features.

console(config)#ip dhcp snooping

To configure the switch to store DHCP snooping binding information. This helps to protect the network from DHCP spoofing attacks by maintaining a record of which IP addresses are assigned to which devices. The database allows the switch to enforce DHCP policies and validate DHCP messages more effectively.

console(config)#ip dhcp snooping database

<optional command>

To allow DHCP snooping information to be accepted from untrusted ports, which helps to preserve DHCP option data in scenarios where DHCP servers are connected to these ports.

console(config)#ip dhcp snooping information option allowed-untrusted <optional command>

To configure a device, to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address.

console(config)#ip dhcp snooping verify <optional command>

Navigate to the interface, for defining dhcp snooping trust.

console(config)#interface GigabitEthernet1/0/1

Enable dhcp snooping trust, to ensure that legitimate DHCP servers and trusted devices can send DHCP offers and acknowledgments. Without setting specific interfaces as trusted, DHCP Snooping would block all DHCP traffic on those interfaces, potentially disrupting network services. By marking certain interfaces as trusted, ARP Inspection can correctly validate ARP packets and prevent spoofing while allowing legitimate DHCP communications to occur.

console(config-if)#ip dhcp snooping trust

Navigate to the interface vlan, for defining dhcp snooping trust.

console(config)# ip dhcp snooping vlan 1

<optional command>

Verifying the configuration

console#show ip dhcp snooping

DHCP snooping is Enabled

DHCP snooping is configured on following VLANs:

DHCP snooping database is Disabled

Relay agent Information option 82 is Disabled

Option 82 on untrusted port is forbidden

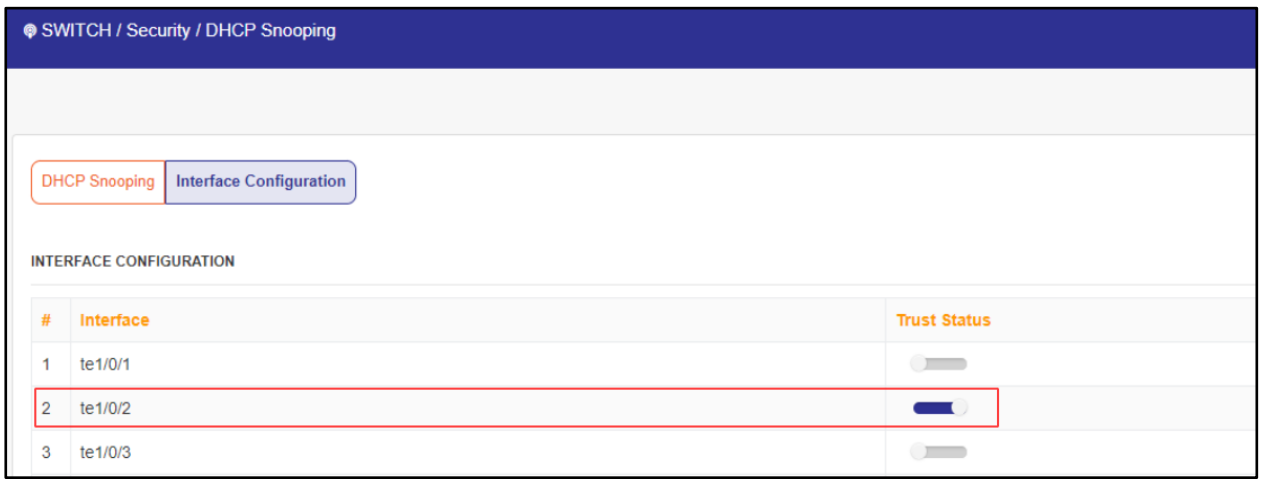
Verification of hwaddr field is Enabled

Interface Trusted

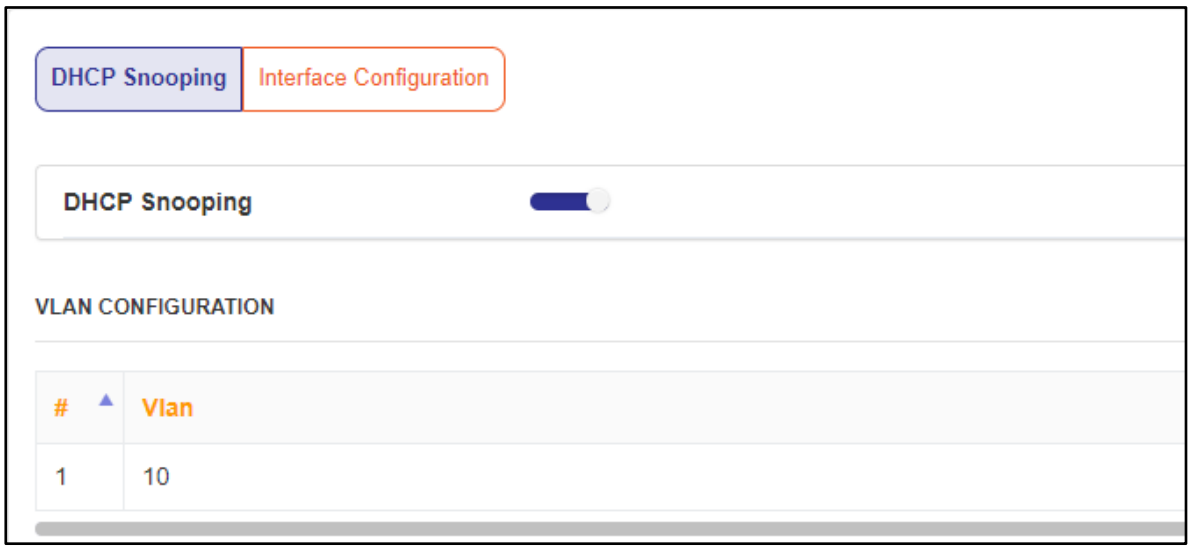
```
----------  ------
gi1/0/1          Yes

console# show ip dhcp snooping  binding
Update frequency: 1200
Total number of binding: 2
Mac Address          Ip address      lease      Type      VLAN      Interface
.....
0060.704C.73FF  192.168.100.3   7983     snooping    1          gi1/0/10
0060.704C.7BC1  192.168.100.4   92332    snooping    1          gi1/0/11
```

DHCP Snooping in GUI

To enable DHCP Snooping in GUI Go to Switch > Security > DHCP Snooping. DHCP Snooping can only be enabled if the trust port is enabled.



DHCP Snooping can be enabled globally and on a particular VLAN by adding a VLAN.



Notes & Limitations

- DHCP snooping can consume CPU and memory resources on network devices, especially when DHCP traffic is high or the binding database is large.
- When DHCP snooping is disabled for a VLAN, the bindings that were collected for that VLAN are removed.
- DHCP snooping will drop DHCP messages from a DHCP server that is not trusted.
- DHCP snooping can drop packets under certain conditions, such as when a broadcast packet has a MAC address in the DHCP binding database but the port does not match the port on which the packet is received.