# Configuring First Hop Security

This chapter contains the following sections:



# DHCP Snooping in VXLAN BGP EVPN Overview

First Hop Security (FHS) is an access security feature that provides security to the network at the access (where the host attaches to the first switch in the network). The Dot1x, port-security and DHCP Snooping are examples of access security features. Together, these security features authorize and authenticate the host and thereby protect the network by ensuring that only legitimate hosts are allowed to use the network.

# DHCP Snooping on VXLAN Topology

In a VXLAN fabric, the host can be attached to an interface on one VTEP, while the DHCP server can be attached to an interface on a different VTEP.

As shown in the figure, the host H1 is attached to VTEP1, while the DHCP server is attached to VTEP3.

The host and the DHCP server exchange a set of messages as part of this host IP assignment procedure. These are popularly known as Discover-Offer-Request-Ack (DORA) exchange messages.

The DORA exchange, for a particular host (H1), must now be sent over the VXLAN fabric to reach remote DHCP servers (VTEP3).

VTEP3 checks that the “Offer” and “Ack” messages (that are part of a DORA sequence) and coming from the DHCP server, are received on a Trusted Interface on VTEP3.

Upon completion of the DORA exchange, the VTEP1 creates a “DHCP snooping DB” entry. This DB contains the MAC-address of the host, the IP-address assigned to the host by the DHCP server, VLAN, and other details like the “lease time”. The major driving part of this feature is that the snooping DB entry created on VTEP1 for host (H1) as a "Local snooping DB entry" is also propagated to remote VTEPs using BGP-EVPN

and will be seen as "Remote snooping DB entry" for host (H1). Thus this DHCP snooping DB will be seen as a "Distributed DB" across the VTEPs and the snooping entries will be in sync with all VTEPs.

For use-cases where the IP address assignment to the host is predefined, the snooping DB entry can be configured using the **ip source binding** *ip address* **vlan** *vlan-id* **interface** *interface* command. Snooping entries added through this command are referred as static entries and even these are also distributed across all VTEPs.

The Distributed DHCP Snooping DB is used as follows:

- To validate ARPs/GARPs sent from the host using DAI - This ensures that any spoofing of the ARP/GARP using different host credentials, and consequent malicious-ARP-storm in the network, is prevented.

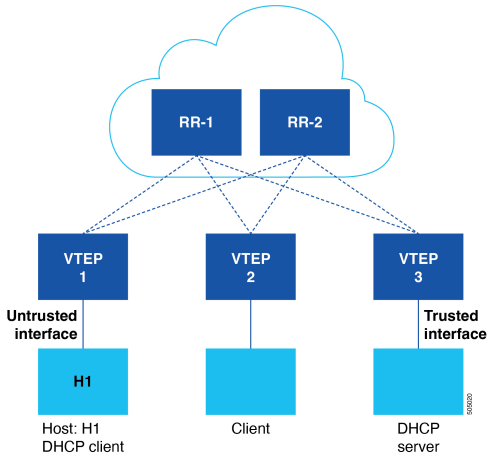
  In a VXLAN environment, we must account for host-move. Since the DHCP Snooping DB is replicated across the fabric, DAI can now work across the fabric after the host-move also. Thus, the control plane is protected in a VXLAN environment.

**Note** If there is no matching entry in the DB, the ARP/GARP will be dropped.

- To validate the data-plane traffic from the host using IPSG. This validates the data-traffic and prevents malicious hosts from sending data traffic to the network.

  The DHCP snooping entry is replicated across the fabric. Only local DHCP clients for that VTEP are programmed in the IPSG. The local DHCP clients are identified with anchor flag set to true in the DHCP snooping table. If a host moves to a different VTEP and settles down, IPSG has to reprogram the client behind the new VTEP to validate the data-traffic. On the old VTEP, IPSG has to remove this DHCP client. The anchor flag will change accordingly. The host move is triggered by the receipt of an ARP request from the host which is received on the new VTEP that the host moved to.

***Figure 1: DHCP Snooping on VXLAN***




# Guidelines and Limitations for DHCP Snooping on VXLAN

DHCP Snooping on VXLAN feature has the following configuration guidelines and limitations:

- Beginning with Cisco NX-OS Release 10.4(1)F, DHCP snooping and associated features such as Dynamic ARP Inspection (DAI) and IP Source Guard (IPSG) support is extended to VXLAN fabric on Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2 platform switches and Cisco Nexus 9500 switches with 9700-EX/FX/GX line cards.

  Beginning with Cisco NX-OS Release 10.4(2)F, First Hop Security feature is supported on Cisco Nexus 9332D-H2R, and 93400LD-H1 switches.

  Beginning with Cisco NX-OS Release 10.4(3)F, First Hop Security feature is supported on Cisco Nexus 9364C-H1 switches.

- Beginning with Cisco NX-OS Release 10.5(2)F, First Hop Security feature is supported on Cisco Nexus 9500 Series switches with N9K-X9736C-FX3 line card.

- Ensure that the DHCP snooping, DAI and IPSG together are enabled on all VTEPs.

**Note** DAI and IPSG depend on DHCP snooping. DHCP snooping creates the snooping DB and this DB is used by DAI and IPSG.

- Only IPv4 multicast underlay is supported. However, IPv4 ingress replication underlay, IPv6 ingress replication underlay and IPv6 multicast underlay are not supported.
- Only IPv4 DHCP hosts is supported.
- The host-move is indicated by ARP/GARP/RARP receipt. In case of RARP (which contains MAC info alone), VTEPs start ARP Refreshes for the IPs learned against MAC. Hence, essentially, ARP-GARP is the trigger for host-move and not any other data packet.
- For vPC VTEPs, only physical MCT is supported.
- This feature cannot coexist with FabricPath to VXLAN migration feature and counter ACL (CNT ACL) feature.
- In the ingress SUP region, the TCAM must be carved out to 768 entries instead of the default 512 entries to set up the ingress ACLs using the **hardware access-list tcam region ing-sup** command. Reload of a switch is required for the TCAM carving changes to reflect.
- If an I/O module lacks the resources required for an atomic update, you can disable atomic updates by using the **no hardware access-list update atomic** command; however, during the brief time required for the device to remove the preexisting ACL and implement the updated ACL, traffic that the ACL applies to is dropped by default.
- If you want to permit all traffic that an ACL applies to while it receives a nonatomic update, use the **hardware access-list update default-result permit** command.
- In case of multisite and with vPC BGW, if DHCP snooping is enabled on the vPC BGW, ensure that DHCP clients and DHCP servers are on same sites.

**Note**

- DHCP snooping needs to be enabled (on a VTEP) for the VLAN belonging to the DHCP host that must avail the DHCP service.
- All the VLANs serviced by the DHCP server in the fabric should be enabled with DHCP snooping on all the VTEPs of the fabric.

- The DHCP server cannot be deployed behind the EoR.
- On vPC nodes, static DHCP snooping is supported only with vPC port-channel ports and not with orphan ports.

# Prerequisites for DHCP Snooping

DHCP has the following prerequisites:

- You should be familiar with DHCP before you configure DHCP snooping or the DHCP relay agent.
- Make sure that the DHCP Snooping, DAI and IPSG features are enabled together on a leaf VTEP.

# Enabling DHCP Snooping on VXLAN

You can enable or disable DHCP snooping on a single-box feature or enable this feature for a VLAN for the entire fabric. By default, DHCP snooping is disabled on all VLANs.

### Before you begin

- Make sure that the DHCP feature is enabled.
- Make sure that the **nv overlay evpn** command is configured.
- Make sure that the DHCP Snooping, DAI and IPSG features are enabled. For more information see Prerequisites for DHCP Snooping, on page 4 section.
- Make sure that DHCP snooping and DAI are enabled on all the VXLAN nodes. For more information on configuration, see **Configuring DHCP Snooping** section of Cisco Nexus 9000 Series NX-OS Security Configuration Guide.
- Make sure that DHCP snooping trust and ARP inspection trust are enabled on interfaces connected to the DHCP server nodes. For more information on configuration, see **Configuring DHCP Snooping** section of Cisco Nexus 9000 Series NX-OS Security Configuration Guide.
- Make sure that IP Source Guard is enabled on the interfaces connected to the DHCP client nodes. For more information on configuration, see **Configuring DHCP Snooping** section of Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

### SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ip dhcp snooping vlan** *vlan-list* **evpn**
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

### DETAILED STEPS

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | [**no**] **ip dhcp snooping vlan** *vlan-list* **evpn**<br>**Example:**<br>`switch(config)# ip dhcp snooping vlan 100,200,250-252 evpn` | Enables DHCP snooping on the VLANs specified by *vlan-list*.<br>Beginning with Cisco NX-OS Release 10.4(1)F, the **evpn** option is provided to support host move to other interfaces on the same VTEP or other VTEPs<br>**Note**<br>• When we enable this feature with the **evpn** option, the **nve** will be implicitly added as a trusted interface.<br>• We can have one vlan-list-1 with **evpn** keyword and another vlan-list-2 with no evpn keyword.<br>The **no** form of this command disables DHCP snooping on the VLANs specified. |
| **Step 3** | (Optional) **show running-config dhcp**<br>**Example:**<br>`switch(config)# show running-config dhcp` | Displays the DHCP configuration. |
| **Step 4** | (Optional) **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | Copies the running configuration to the startup configuration. |

# Clearing the Duplicate Host After Permanent Freeze

The mobility and duplicate detection logic for DHCP clients in FHS enabled VTEPs is same as BGP EVPN mobility and duplicate detection logic. However duplicate detection may happen in any of the VTEPs in non-FHS deployments. In the FHS deployments, the host duplicate will be detected always on a VTEP where DHCP binding entry is remote.

For more information on mobility and duplicate detection, see Duplicate Detection for IP and MAC Addresses section.

Once the MAC or MAC-IP is permanently frozen, there is no auto recovery mechanism to re-initiate mobility or duplicate check sequences. To clear MAC and MAC-IP permanent freeze state, use the following commands:

- For MAC:

**clear l2route evpn mac** [*mac-address*] [**topo**] **permanently-frozen-list**

- For MAC-IP:

  **clear fabric forwarding dup-host** [{ **ip**|**ipv6** *address* }] [**vrf** {*vrf-name* | *vrf-known-name* | **all**}]

# Verifying DHCP Snooping Bindings

To display DHCP snooping bindings information, enter the following commands:

| Command | Purpose |
|---|---|
| **show ip dhcp snooping binding evpn** | Displays all entries from the DHCP snooping binding database. |
| **show l2route fhs** [**topology** *topology id* \| **all**] | Displays all entries from the L2RIB database. |

The following example shows sample output for the **show ip dhcp snooping binding evpn** command:

```
switch(config)# show ip dhcp snooping binding evpn
MacAddress          IpAddress        Lease(Sec)  Type      BD    Interface       anchor
  Freeze
------------------ -------------- ----------- ---------- ---- ----------------- ----------
---------
00:10:00:10:00:10  10.10.10.10      infinite  static      2001  Ethernet1/48         YES
     NONE
00:15:06:00:00:01  100.1.150.156    86282     dhcp-snoop  2001  Ethernet1/31         YES
     NONE
00:17:06:00:00:01  100.1.150.155    86265     dhcp-snoop  2001  nve1(peer-id: 1)     NO
     NONE
```

The following example shows sample output for the **show l2route fhs** command:

```
switch(config)# show l2route fhs all
Flags - (Stt):Static (Dyn):Dynamic (R):Remote
Topo ID  Mac Address     Host IP             Prod          Flags      Seq No     Next-Hops
---- -- ---- ----------- ------------------ ---------- ----------- ------------ -------------
2001     0015.0600.0001  100.1.150.156      DHCP_DYNAMIC  Dyn,       0          Eth1/31
2001     0017.0600.0001  100.1.150.155      BGP           Dyn,R,     0          1.13.13.13
 (Label: 0)
switch(config)#
```

The following example shows DHCP configurations for a VTEP with DHCP clients:

```
feature dhcp
service dhcp
ip dhcp snooping
ip dhcp snooping vlan 2001-2002 evpn
ip arp inspection vlan 2001-2002

interface Ethernet1/31
ip verify source dhcp-snooping-vlan
```

The following example shows DHCP configurations for a VTEP with DHCP server:

```
feature dhcp
service dhcp
ip dhcp snooping
ip dhcp snooping vlan 2001-2002 evpn
ip arp inspection vlan 2001-2002
```

```
interface Ethernet1/47
ip dhcp snooping trust
ip arp inspection trust
```