First Hop Security

This chapter contains the following sections:

About First Hop Security

First-Hop Security (FHS) features enable a better IPv4 and IPv6 link security and management over the layer 2 links. In a service provider environment, these features closely control address assignment and derived operations, such as Duplicate Address Detection (DAD) and Address Resolution (AR).

The following supported FHS features secure the protocols and help build a secure endpoint database on the fabric leaf switches, that are used to mitigate security threats such as MIM attacks and IP thefts:

- ARP Inspection—allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings.
- ND Inspection—learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables.
- DHCP Inspection—validates DHCP messages received from untrusted sources and filters out invalid messages.
- RA Guard—allows the network administrator to block or reject unwanted or rogue router advertisement (RA) guard messages.
- IPv4 and IPv6 Source Guard—blocks any data traffic from an unknown source.
- Trust Control—a trusted source is a device that is under your administrative control. These devices include the switches, routers, and servers in the Fabric. Any device beyond the firewall or outside the network is an untrusted source. Generally, host ports are treated as untrusted sources.

FHS features provide the following security measures:

- **Role Enforcement**—Prevents untrusted hosts from sending messages that are out the scope of their role.
- **Binding Enforcement**—Prevents address theft.
- **DoS Attack Mitigations**—Prevents malicious end-points to grow the end-point database to the point where the database could stop providing operation services.
- **Proxy Services**—Provides some proxy-services to increase the efficiency of address resolution.

FHS features are enabled on a per tenant bridge domain (BD) basis. As the bridge domain, may be deployed on a single or across multiple leaf switches, the FHS threat control and mitigation mechanisms cater to a single switch and multiple switch scenarios.

Beginning with Cisco APIC release 6.0(2), FHS is supported on the VMware DVS VMM domain. If you need to implement FHS within an EPG, enable intra EPG isolation. If intra EPG isolation is not enabled, then, the endpoints within the same VMware ESX port-group can bypass FHS. If you do not enable intra EPG isolation, FHS features still take effect for endpoints that are in different port-groups, for instance, FHS can prevent a compromised VM from poisoning the ARP table of another VM in a different port-group.

ACI FHS Deployment

Most FHS features are configured in a two-step fashion: firstly you define a policy which describes the behavior of the feature, secondly you apply this policy to a "domain" (being the Tenant Bridge Domain or the Tenant Endpoint Group). Different policies that define different behaviors can be applied to different intersecting domains. The decision to use a specific policy is taken by the most specific domain to which the policy is applied.

The policy options can be defined from the Cisco APIC GUI found under the Tenant_*name*>Networking>Protocol Policies>First Hop Security tab.

Guidelines and Limitations

Follow these guidelines and limitations:

- Any secured endpoint entry in the FHS Binding Table Database in **DOWN** state will get cleared after **18 Hours** of timeout. The entry moves to **DOWN** state when the front panel port where the entry is learned is link down. During this window of **18 Hours**, if the endpoint is moved to a different location and is seen on a different port, the entry will be gracefully moved out of **DOWN** state to **REACHABLE/STALE** as long as the endpoint is reachable from the other port it is moved from.
- When IP Source Guard is enabled, the IPv6 traffic that is sourced using IPv6 Link Local address as IP source address is not subject to the IP Source Guard enforcement (i.e. Enforcement of Source Mac <=> Source IP Bindings secured by IP Inspect Feature). This traffic is permitted by default irrespective of binding check failures.
- FHS is not supported on L3Out interfaces.
- FHS is not supported N9K-M12PQ based TORs.
- FHS in ACI Multi-Site is a site local capability therefore it can only be enabled in a site from the APIC cluster. Also, FHS in ACI Multi-Site only works when the BD and EPG is site local and not stretched across sites. FHS security cannot be enabled for stretched BD or EPGs.

- FHS is not supported on a Layer 2 only bridge domain.
- Enabling FHS feature can disrupt traffic for 50 seconds because the EP in the BD are flushed and EP Learning in the BD is disabled for 50 seconds.
- FHS is not supported on uSeg EPGs that match an ESG by using EPG selectors. If FHS is required for endpoints that need to move to an ESG from a uSeg EPG, classify those endpoints to an ESG by using other selectors, such as an IP subnet or tag selector, and remove matching criteria from the uSeg EPG. Then, configure FHS on the base EPG.
- When EPGs are matched to an ESG by using EPG selectors, the FHS binding table and corresponding endpoints are flushed. Traffic will not work until the binding table is refreshed using ARP, DHCP, and so on.

Guidelines and Limitations for FHS support on VMM Domains

Follow these guidelines and limitations:

- EPG attached to a VMM domain must be deployed with resolution immediacy set to immediate/ pre-provision.
- ARP flooding must be enabled on the bridge domain.

Configuring FHS Using the APIC GUI

Before you begin

- The tenant and Bridge Domain configured.

Procedure

Step 1 On the menu bar, click **Tenants** > **Tenant_name**. In the **Navigation** pane, click **Policies** > **Protocol** > **First Hop Security**. Right click on **First Hop Security** to open **Create Feature Policy** and perform the following actions:

a) In the **Name** field, enter a name for the First Hop Security policy.
b) Verify that the **IP Inspection**, **Source Guard**, and **Router Advertisement** fields are enabled and click **Submit**.

Step 2 In the **Navigation** pane, expand **First Hop Security** and right click on **Trust Control Policies** to open **Create Trust Control Policy** and perform the following actions:

a) In the **Name** field, enter a name for the Trust Control policy.
b) Select the desired features to be allowed on the policy and click **Submit**.

Step 3 (Optional) To apply the Trust Control policy to an EPG, in the **Navigation** pane, expand **Application Profiles** > **Application Profile_*name*** > **Application EPGs** and click on **Application EPG_*name*** and perform the following actions:

a) In the **Work** pane, click on the **General** tab.
b) Click on the down-arrow for **FHS Trust Control Policy** and select the policy you previously created and click **Submit**.

Step 4 In the **Navigation** pane, expand **Bridge Domains** > **Bridge Domain_name** and click on the **Advanced/Troubleshooting** tab and perform the following action:

a) In the **First Hop Security Policy** field, select the policy you just created and click **Submit**. This completes FHS configuration.

Configuring FHS Using the NX-OS CLI

Before you begin

- The tenant and Bridge Domain configured.

Procedure

Step 1 **configure**

Enters configuration mode.

Example:

```
apic1# configure
```

Step 2 Configure FHS policy.

Example:

```
apic1(config)# tenant coke
apic1(config-tenant)# first-hop-security
apic1(config-tenant-fhs)# security-policy pol1
apic1(config-tenant-fhs-secpol)#
apic1(config-tenant-fhs-secpol)# ip-inspection-admin-status enabled-both
apic1(config-tenant-fhs-secpol)# source-guard-admin-status enabled-both
apic1(config-tenant-fhs-secpol)# router-advertisement-guard-admin-status enabled
apic1(config-tenant-fhs-secpol)# router-advertisement-guard
apic1(config-tenant-fhs-raguard)#
apic1(config-tenant-fhs-raguard)# managed-config-check
apic1(config-tenant-fhs-raguard)# managed-config-flag
apic1(config-tenant-fhs-raguard)# other-config-check
apic1(config-tenant-fhs-raguard)# other-config-flag
apic1(config-tenant-fhs-raguard)# maximum-router-preference low
apic1(config-tenant-fhs-raguard)# minimum-hop-limit 10
apic1(config-tenant-fhs-raguard)# maximum-hop-limit 100
apic1(config-tenant-fhs-raguard)# exit
apic1(config-tenant-fhs-secpol)# exit
apic1(config-tenant-fhs)# trust-control tcpol1
pic1(config-tenant-fhs-trustctrl)# arp
apic1(config-tenant-fhs-trustctrl)# dhcpv4-server
apic1(config-tenant-fhs-trustctrl)# dhcpv6-server
apic1(config-tenant-fhs-trustctrl)# ipv6-router
apic1(config-tenant-fhs-trustctrl)#  router-advertisement
apic1(config-tenant-fhs-trustctrl)# neighbor-discovery
apic1(config-tenant-fhs-trustctrl)# exit
apic1(config-tenant-fhs)# exit
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# first-hop-security security-policy pol1
apic1(config-tenant-bd)# exit
apic1(config-tenant)# application ap1
```

```
apic1(config-tenant-app)# epg epg1
apic1(config-tenant-app-epg)# first-hop-security trust-control tcpol1
```

Step 3 Show FHS configuration example:

Example:

```
leaf4# show fhs bt all

Legend:
    TR       : trusted-access                       UNRES : unresolved              Age   : Age since
 creation
    UNTR     : untrusted-access                      UNDTR : undetermined-trust      CRTNG : creating

    UNKNW    : unknown                               TENTV : tentative               INV   : invalid

    NDP      : Neighbor Discovery Protocol          STA   : static-authenticated    REACH : reachable

    INCMP    : incomplete                           VERFY : verify                  INTF  : Interface

    TimeLeft : Remaining time since last refresh    LM    : lla-mac-match           DHCP  :
dhcp-assigned

EPG-Mode:
    U : unknown    M : mac    V : vlan    I : ip

BD-VNID             BD-Vlan             BD-Name
15630220            3                   t0:bd200

-------------------------------------------------------------------------------------------------------------------
| Origin | IP              | MAC               | INTF   | EPG(sclass)(mode) | Trust-lvl | State |
Age      | TimeLeft |
-------------------------------------------------------------------------------------------------------------------
| ARP    | 192.0.200.12    | D0:72:DC:A0:3D:4F | eth1/1 | epg300(49154)(V)  | LM,TR     | STALE |
00:04:49 | 18:08:13 |
| ARP    | 172.29.205.232  | D0:72:DC:A0:3D:4F | eth1/1 | epg300(49154)(V)  | LM,TR     | STALE |
00:03:55 | 18:08:21 |
| ARP    | 192.0.200.21    | D0:72:DC:A0:3D:4F | eth1/1 | epg300(49154)(V)  | LM,TR     | REACH |
00:03:36 | 00:00:02 |
| LOCAL  | 192.0.200.1     | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       | REACH |
04:49:41 | N/A      |
| LOCAL  | fe80::200       | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       | REACH |
04:49:40 | N/A      |
| LOCAL  | 2001:0:0:200::1 | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       | REACH |
04:49:39 | N/A      |
-------------------------------------------------------------------------------------------------------------------
```

The trust levels are:

- **TR**— Trusted. Displayed when the endpoint is learned from an EPG where the trust configuration is enabled.
- **UNTR**— Untrusted. Displayed when the endpoint is learned from an EPG where the trust configuration is not enabled.
- **UNDTR**— Undetermined. Displayed in the case of a DHCP relay topology where the DHCP server bridge domain (BD) is on a remote leaf and the DHCP clients are on a local leaf. In this situation, the local leaf will not know whether the DHCP server BD has trust DHCP enabled.

Step 4 Show violations with the different types and reasons example:

Example:

```
leaf4# show fhs violations all
```

```
Violation-Type:
    POL  : policy      THR : address-theft-remote
    ROLE : role        TH  : address-theft
    INT  : internal

Violation-Reason:
    IP-MAC-TH   : ip-mac-theft                    OCFG_CHK  : ra-other-cfg-check-fail     ANC-COL
   : anchor-collision
    PRF-LVL-CHK : ra-rtr-pref-level-check-fail    INT-ERR   : internal-error              TRUST-CHK
   : trust-check-fail
    SRV-ROL-CHK : srv-role-check-fail             ST-EP-COL : static-ep-collision         LCL-EP-COL
  : local-ep-collision
    MAC-TH      : mac-theft                       EP-LIM    : ep-limit-reached            MCFG-CHK
   : ra-managed-cfg-check-fail
    HOP-LMT-CHK : ra-hoplimit-check-fail         MOV-COL   : competing-move-collision    RTR-ROL-CHK
 : rtr-role-check-fail
    IP-TH       : ip-theft

EPG-Mode:
    U : unknown    M : mac    V : vlan    I : ip

BD-VNID             BD-Vlan             BD-Name
15630220            3                   t0:bd200
-------------------------------------------------------------------------------------------------------
| Type | Last-Reason | Proto | IP           | MAC               | Port    | EPG(sclass)(mode) | Count
 |
-------------------------------------------------------------------------------------------------------
| THR  | IP-TH       | ARP   | 192.0.200.21 | D0:72:DC:A0:3D:4F | tunnel5 | epg300(49154)(V)  | 21
   |
-------------------------------------------------------------------------------------------------------
Table Count: 1
```

Step 5 Show FHS configuration:

Example:

```
swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security binding-table

Pod/Node  Type    Family  IP Address            MAC Address        Interface     Level
State
--------  ------  ------  --------------------  -----------------  ------------  ---------------
-----
1/102     local   ipv4    192.0.200.1           00:22:BD:F8:19:FF  vlan3         static-
reach
                                                                                 authenticated
able
1/102     local   ipv6    fe80::200             00:22:BD:F8:19:FF  vlan3         static-
reach
                                                                                 authenticated
able
1/102     local   ipv6    2001:0:0:200::1       00:22:BD:F8:19:FF  vlan3         static-
reach
                                                                                 authenticated
able
1/101     arp     ipv4    192.0.200.23          D0:72:DC:A0:02:61  eth1/2        lla-mac-match
stale
                                                                                 ,untrusted-
                                                                                 access
1/101     local   ipv4    192.0.200.1           00:22:BD:F8:19:FF  vlan3         static-
reach
                                                                                 authenticated
able
1/101     nd      ipv6    fe80::d272:dcff:fea0  D0:72:DC:A0:02:61  eth1/2        lla-mac-match
reach
                           :261                                                  ,untrusted-
```

```
able
                                                                                access
1/101     nd      ipv6    2001:0:0:200::20      D0:72:DC:A0:02:61  eth1/2        lla-mac-match
stale
                                                                                ,untrusted-
                                                                                access
1/101     nd      ipv6    2001::200:d272:dcff:  D0:72:DC:A0:02:61  eth1/2        lla-mac-match
stale
                           fea0:261                                             ,untrusted-
                                                                                access
1/101     local   ipv6    fe80::200             00:22:BD:F8:19:FF  vlan3         static-
reach
                                                                                authenticated
able
1/101     local   ipv6    2001:0:0:200::1       00:22:BD:F8:19:FF  vlan3         static-
reach
                                                                                authenticated
able
1/103     local   ipv4    192.0.200.1           00:22:BD:F8:19:FF  vlan4         static-
reach
                                                                                authenticated
able
1/103     local   ipv6    fe80::200             00:22:BD:F8:19:FF  vlan4         static-
reach
                                                                                authenticated
able
1/103     local   ipv6    2001:0:0:200::1       00:22:BD:F8:19:FF  vlan4         static-
reach
                                                                                authenticated
able
1/104     arp     ipv4    192.0.200.10          F8:72:EA:AD:C4:7C  eth1/1        lla-mac-match
stale
                                                                                ,trusted-access
1/104     arp     ipv4    172.29.207.222        D0:72:DC:A0:3D:4C  eth1/1        lla-mac-match
stale
                                                                                ,trusted-access
1/104     local   ipv4    192.0.200.1           00:22:BD:F8:19:FF  vlan4         static-
reach
                                                                                authenticated
able
1/104     nd      ipv6    fe80::fa72:eaff:fead  F8:72:EA:AD:C4:7C  eth1/1        lla-mac-match
stale
                           :c47c                                                ,trusted-access
1/104     nd      ipv6    2001:0:0:200::10      F8:72:EA:AD:C4:7C  eth1/1        lla-mac-match
stale
                                                                                ,trusted-access
1/104     local   ipv6    fe80::200             00:22:BD:F8:19:FF  vlan4         static-
reach
                                                                                authenticated
able
1/104     local   ipv6    2001:0:0:200::1       00:22:BD:F8:19:FF  vlan4         static-
reach
                                                                                authenticated
able
```

```
Pod/Node  Type    IP Address            Creation TS                    Last Refresh TS
   Lease Period
--------  ------  --------------------  -----------------------------  -----------------------------
  ------------
1/102     local   192.0.200.1           2017-07-20T04:22:38.000+00:00  2017-07-20T04:22:38.000+00:00
1/102     local   fe80::200             2017-07-20T04:22:56.000+00:00  2017-07-20T04:22:56.000+00:00
1/102     local   2001:0:0:200::1       2017-07-20T04:22:57.000+00:00  2017-07-20T04:22:57.000+00:00
1/101     arp     192.0.200.23          2017-07-27T10:55:20.000+00:00  2017-07-27T16:07:24.000+00:00
```

```
1/101     local   192.0.200.1           2017-07-27T10:48:09.000+00:00  2017-07-27T10:48:09.000+00:00
1/101     nd      fe80::d272:dcff:fea0  2017-07-27T10:52:16.000+00:00  2017-07-27T16:04:29.000+00:00

                   :261
1/101     nd      2001:0:0:200::20      2017-07-27T10:57:32.000+00:00  2017-07-27T16:07:24.000+00:00
1/101     nd      2001::200:d272:dcff:  2017-07-27T11:21:45.000+00:00  2017-07-27T16:07:24.000+00:00

                   fea0:261
1/101     local   fe80::200             2017-07-27T10:48:10.000+00:00  2017-07-27T10:48:10.000+00:00
1/101     local   2001:0:0:200::1       2017-07-27T10:48:11.000+00:00  2017-07-27T10:48:11.000+00:00
1/103     local   192.0.200.1           2017-07-26T22:03:56.000+00:00  2017-07-26T22:03:56.000+00:00
1/103     local   fe80::200             2017-07-26T22:03:57.000+00:00  2017-07-26T22:03:57.000+00:00
1/103     local   2001:0:0:200::1       2017-07-26T22:03:58.000+00:00  2017-07-26T22:03:58.000+00:00
1/104     arp     192.0.200.10          2017-07-27T11:21:13.000+00:00  2017-07-27T16:05:48.000+00:00
1/104     arp     172.29.207.222        2017-07-27T11:54:48.000+00:00  2017-07-27T16:06:38.000+00:00
1/104     local   192.0.200.1           2017-07-27T10:49:13.000+00:00  2017-07-27T10:49:13.000+00:00
1/104     nd      fe80::fa72:eaff:fead  2017-07-27T11:21:13.000+00:00  2017-07-27T16:06:43.000+00:00

                   :c47c
1/104     nd      2001:0:0:200::10      2017-07-27T11:21:13.000+00:00  2017-07-27T16:06:19.000+00:00
1/104     local   fe80::200             2017-07-27T10:49:14.000+00:00  2017-07-27T10:49:14.000+00:00
1/104     local   2001:0:0:200::1       2017-07-27T10:49:15.000+00:00  2017-07-27T10:49:15.000+00:00


swtb23-ifc1#

swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security statistics arp
Pod/Node         : 1/101
Request Received : 4
Request Switched : 2
Request Dropped  : 2
Reply Received   : 257
Reply Switched   : 257
Reply Dropped    : 0

Pod/Node         : 1/104
Request Received : 6
Request Switched : 6
Request Dropped  : 0
Reply Received   : 954
Reply Switched   : 954
Reply Dropped    : 0


swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security statistics dhcpv4
Pod/Node                    : 1/102
Discovery Received          : 5
Discovery Switched          : 5
Discovery Dropped           : 0
Offer Received              : 0
Offer Switched              : 0
Offer Dropped               : 0
Request Received            : 0
Request Switched            : 0
Request Dropped             : 0
Ack Received                : 0
Ack Switched                : 0
Ack Dropped                 : 0
Nack Received               : 0
Nack Switched               : 0
Nack Dropped                : 0
Decline Received            : 0
Decline Switched            : 0
Decline Dropped             : 0
```

```
Release Received            : 0
Release Switched            : 0
Release Dropped             : 0
Information Received        : 0
Information Switched        : 0
Information Dropped         : 0
Lease Query Received        : 0
Lease Query Switched        : 0
Lease Query Dropped         : 0
Lease Active Received       : 0
Lease Active Switched       : 0
Lease Active Dropped        : 0
Lease Unassignment Received : 0
Lease Unassignment Switched : 0
Lease Unassignment Dropped  : 0
Lease Unknown Received      : 0
Lease Unknown Switched      : 0
Lease Unknown Dropped       : 0

swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security statistics neighbor-discovery
Pod/Node                        : 1/101
Neighbor Solicitation Received  : 125
Neighbor Solicitation Switched  : 121
Neighbor Solicitation Dropped   : 4
Neighbor Advertisement Received : 519
Neighbor Advertisement Switched : 519
Neighbor Advertisement Drop     : 0
Router Solicitation Received    : 4
Router Solicitation Switched    : 4
Router Solicitation Dropped     : 0
Router Adv Received             : 0
Router Adv Switched             : 0
Router Adv Dropped              : 0
Redirect Received               : 0
Redirect Switched               : 0
Redirect Dropped                : 0

Pod/Node                        : 1/104
Neighbor Solicitation Received  : 123
Neighbor Solicitation Switched  : 47
Neighbor Solicitation Dropped   : 76
Neighbor Advertisement Received : 252
Neighbor Advertisement Switched : 228
Neighbor Advertisement Drop     : 24
Router Solicitation Received    : 0
Router Solicitation Switched    : 0
Router Solicitation Dropped     : 0
Router Adv Received             : 53
Router Adv Switched             : 6
Router Adv Dropped              : 47
Redirect Received               : 0
Redirect Switched               : 0
Redirect Dropped                : 0
```

FHS Switch iBASH Commands

Procedure

Step 1 Show command to display the FHS feature configuration on the BD and the Trust control policy configuration on the EPG:

Example:

```
leaf4# show fhs features all

BD-VNID             BD-Vlan             BD-Name
15630220            4                   t0:bd200
    Feature Policy:
        Feature      Family    Protocol    Operational-State    Options
        ipinspect    IPV4      ARP         UP                   stalelifetime: 180s
        ipinspect    IPV4      DHCP        UP                   -
        ipinspect    IPV4      LOCAL       UP                   -
        ipinspect    IPV4      STATIC      UP                   -
        ipinspect    IPV6      ND          UP                   stalelifetime: 180s
        ipinspect    IPV6      DHCP        UP                   -
        ipinspect    IPV6      LOCAL       UP                   -
        ipinspect    IPV6      STATIC      UP                   -
        raguard      IPV6      -           UP                   ManagedCfgFlag: on
                                                                  OtherCfgFlag: on
                                                                  maxHopLimit: 15
                                                                  minHopLimit: 3
                                                                  routerPref: medium
    ------------------------------------------------------------------------------
    Trust Policy:
    Epg-id              Epg-type            Epg-name
    49154               Ckt-Vlan            epg300
        Trust-Attribute    Operational-State
        PROTO-ARP          UP
        PROTO-ND           UP
        DHCPV4-SERVER      UP
        DHCPV6-SERVER      UP
        ROUTER             UP
```

Step 2 Show commands to display the FHS secured endpoint database:

Example:

```
leaf1# show fhs bt
all       data      dhcpv4    local     static
arp       detailed  dhcpv6    nd        summary

leaf1# show fhs bt all

Legend:
    DHCP     : dhcp-assigned                      TR    : trusted-access          UNRES : unresolved

    Age      : Age since creation                 CRTNG : creating                TENTV : tentative

    VERFY    : verify                              UNDTR : undetermined-trust      INV   : invalid

    NDP      : Neighbor Discovery Protocol        STA   : static-authenticated    REACH : reachable

    LM       : lla-mac-match                      UNKNW : unknown                 INTF  : Interface
```

```
    TimeLeft : Remaining time since last refresh    INCMP : incomplete              UNTR  :
untrusted-access

EPG-Mode:
    U : unknown    M : mac    V : vlan    I : ip

BD-VNID             BD-Vlan             BD-Name
15630220            3                   t0:bd200

------------------------------------------------------------------------------------------------------------------------
| Origin | IP                        | MAC               | INTF   | EPG(sclass)(mode) | Trust-lvl |
State | Age      | TimeLeft |
------------------------------------------------------------------------------------------------------------------------
| ARP    | 192.0.200.23              | D0:72:DC:A0:02:61 | eth1/2 | epg200(32770)(V)  | LM,UNTR   |
STALE | 00:07:47 | 00:01:33 |
| LOCAL  | 192.0.200.1               | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       |
REACH | 00:14:58 | N/A      |
| NDP    | fe80::d272:dcff:fea0:261 | D0:72:DC:A0:02:61 | eth1/2 | epg200(32770)(V)  | LM,UNTR   |
STALE | 00:10:51 | 00:00:47 |
| NDP    | 2001:0:0:200::20          | D0:72:DC:A0:02:61 | eth1/2 | epg200(32770)(V)  | LM,UNTR   |
STALE | 00:05:35 | 00:00:42 |
| LOCAL  | fe80::200                 | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       |
REACH | 00:14:58 | N/A      |
| LOCAL  | 2001:0:0:200::1           | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       |
REACH | 00:14:57 | N/A      |
------------------------------------------------------------------------------------------------------------------------


leaf1# show fhs bt summary all

-------------------------------------------------------------------------
                        FHS Binding Table Summary
-------------------------------------------------------------------------
BD-Vlan: 3        BD-Name: t0:bd200
    Total number of ARP entries       : 1
    Total number of DHCPv4 entries    : 0
    Total number of ND entries        : 2
    Total number of DHCPv6 entries    : 0
    Total number of Data entries      : 0
    Total number of Static entries    : 0
    Total number of Local entries     : 3
    Total number of entries           : 6
-------------------------------------------------------------------------
Total entries across all BDs matching given filters
    Total number of ARP entries       : 1
    Total number of DHCPv4 entries    : 0
    Total number of ND entries        : 2
    Total number of DHCPv6 entries    : 0
    Total number of Data entries      : 0
    Total number of Static entries    : 0
    Total number of Local entries     : 3
    Total number of entries           : 6
-------------------------------------------------------------------------
```

Step 3 Show command to display FHS endpoint violations:

Example:

```
leaf1# show fhs violations all

Violation-Type:
    POL  : policy      THR : address-theft-remote
    ROLE : role        TH  : address-theft
    INT  : internal
```

```
Violation-Reason:
    IP-MAC-TH   : ip-mac-theft                    OCFG_CHK  : ra-other-cfg-check-fail     ANC-COL
   : anchor-collision
    PRF-LVL-CHK : ra-rtr-pref-level-check-fail    INT-ERR   : internal-error              TRUST-CHK
   : trust-check-fail
    SRV-ROL-CHK : srv-role-check-fail             ST-EP-COL : static-ep-collision         LCL-EP-COL
  : local-ep-collision
    MAC-TH      : mac-theft                       EP-LIM    : ep-limit-reached            MCFG-CHK
   : ra-managed-cfg-check-fail
    HOP-LMT-CHK : ra-hoplimit-check-fail          MOV-COL   : competing-move-collision    RTR-ROL-CHK
 : rtr-role-check-fail
    IP-TH       : ip-theft

Trust-Level:
    TR   : trusted-access    UNTR : untrusted-access        UNDTR : undetermined-trust
    INV  : invalid           STA  : static-authenticated    LM    : lla-mac-match
    DHCP : dhcp-assigned

EPG-Mode:
    U : unknown    M : mac    V : vlan    I : ip

BD-VNID             BD-Vlan             BD-Name
15630220            4                   t0:bd200
-------------------------------------------------------------------------------------------------------------------
| Type | Last-Reason | Proto | IP                          | MAC               | Port    |
EPG(sclass)(mode) | Trust-lvl | Count |
-------------------------------------------------------------------------------------------------------------------
| TH   | IP-TH      | ND    | 2001:0:0:200::20         | D0:72:DC:A0:3D:4F | eth1/1 | epg300(49154)(V)
  | LM,UNTR   | 2     |
| POL  | HOP-LMT-CHK | RD    | fe80::fa72:eaff:fead:c47c | F8:72:EA:AD:C4:7C | eth1/1 | epg300(49154)(V)
  | LM,TR     | 2     |
-------------------------------------------------------------------------------------------------------------------
Table Count: 2
```

Step 4 Show command to display FHS control packet forwarding counters:

Example:

```
leaf1# show fhs counters
all     arp     dhcpv4  dhcpv6  nd
leaf4# show fhs counters all

BD-VNID             BD-Vlan             BD-Name
15630220            4                   t0:bd200
 ------------------------------------------------------------------------------------------
| Counter Type           |            Received |            Switched |             Dropped |
|------------------------------------------------------------------------------------------|
| Arp Request            |                   6 |                   6 |                   0 |
| Arp Reply              |                  94 |                  94 |                   0 |
-------------------------------------------------------------------------------------------
| Dhcpv4 Ack             |                   0 |                   0 |                   0 |
| Dhcpv4 Decline         |                   0 |                   0 |                   0 |
| Dhcpv4 Discover        |                   0 |                   0 |                   0 |
| Dhcpv4 Inform          |                   0 |                   0 |                   0 |
| Dhcpv4 Leaseactive     |                   0 |                   0 |                   0 |
| Dhcpv4 Leasequery      |                   0 |                   0 |                   0 |
| Dhcpv4 Leaseunassigned |                   0 |                   0 |                   0 |
| Dhcpv4 Leaseunknown    |                   0 |                   0 |                   0 |
| Dhcpv4 Nack            |                   0 |                   0 |                   0 |
| Dhcpv4 Offer           |                   0 |                   0 |                   0 |
| Dhcpv4 Release         |                   0 |                   0 |                   0 |
| Dhcpv4 Request         |                   0 |                   0 |                   0 |
-------------------------------------------------------------------------------------------
| Dhcpv6 Advertise       |                   0 |                   0 |                   0 |
```

```
| Dhcpv6 Confirm         |                  0 |                  0 |                  0 |
| Dhcpv6 Decline         |                  0 |                  0 |                  0 |
| Dhcpv6 Informationreq  |                  0 |                  0 |                  0 |
| Dhcpv6 Rebind          |                  0 |                  0 |                  0 |
| Dhcpv6 Reconfigure     |                  0 |                  0 |                  0 |
| Dhcpv6 Relayforw       |                  0 |                  0 |                  0 |
| Dhcpv6 Relayreply      |                  0 |                  0 |                  0 |
| Dhcpv6 Release         |                  0 |                  0 |                  0 |
| Dhcpv6 Renew           |                  0 |                  0 |                  0 |
| Dhcpv6 Reply           |                  0 |                  0 |                  0 |
| Dhcpv6 Request         |                  0 |                  0 |                  0 |
| Dhcpv6 Solicit         |                  0 |                  0 |                  0 |
-------------------------------------------------------------------------------------------
| Nd Na                  |                 18 |                 18 |                  0 |
| Nd Ns                  |                 26 |                 22 |                  4 |
| Nd Ra                  |                 11 |                  6 |                  5 |
| Nd Redirect            |                  0 |                  0 |                  0 |
| Nd Rs                  |                  0 |                  0 |                  0 |
-------------------------------------------------------------------------------------------
```

Step 5 Display FHS secured endpoint database from the NxOS memory:

Example:

```
leaf1# vsh -c 'show system internal fhs bt'

Binding Table has 7 entries, 4 dynamic

Codes:
L - Local         S - Static        ND - Neighbor Discovery   ARP - Address Resolution Protocol
DH4 - IPv4 DHCP   DH6 - IPv6 DHCP   PKT - Other Packet        API - API created

Preflevel flags (prlvl):
0001: MAC and LLA match     0002: Orig trunk            0004: Orig access
0008: Orig trusted trunk    0010: Orig trusted access   0020: DHCP assigned
0040: Cga authenticated     0080: Cert authenticated    0100: Statically assigned

EPG types:
V - Vlan Based EPG      M - MAC Based EPG       I - IP Based EPG

-------------------------------------------------------------------------------------------------------------------------------
| Code | Network Layer Address                    | Link Layer Address | Interface      | Vlan | Epg
                | prlvl | Age        | State      | Time left       |
-------------------------------------------------------------------------------------------------------------------------------
| ARP  | 172.29.207.222                           | d0:72:dc:a0:3d:4c  | Eth1/1         |    4 |
0x40000c002 (V)    | 0011  | 29 s       | STALE      | 157 s           |
| L    | 192.0.200.1                              | 00:22:bd:f8:19:ff  | Vlan4          |    4 |
0x400004003 (I)    | 0100  | 55 mn      | REACHABLE  |                 |
| ARP  | 192.0.200.10                             | f8:72:ea:ad:c4:7c  | Eth1/1         |    4 |
0x40000c002 (V)    | 0011  | 156 s      | STALE      | 30 s            |
| L    | 2001:0:0:200::1                          | 00:22:bd:f8:19:ff  | Vlan4          |    4 |
0x400004003 (I)    | 0100  | 55 mn      | REACHABLE  |                 |
| ND   | 2001:0:0:200::10                         | f8:72:ea:ad:c4:7c  | Eth1/1         |    4 |
0x40000c002 (V)    | 0011  | 143 s      | STALE      | 47 s            |
| L    | fe80::200                                | 00:22:bd:f8:19:ff  | Vlan4          |    4 |
0x400004003 (I)    | 0100  | 55 mn      | REACHABLE  |                 |
| ND   | fe80::fa72:eaff:fead:c47c                | f8:72:ea:ad:c4:7c  | Eth1/1         |    4 |
0x40000c002 (V)    | 0011  | 176 s      | STALE      | 11 s            |
-------------------------------------------------------------------------------------------------------------------------------
```

Step 6 Display FHS feature configuration from the NX-OS FHS process internal memory:

Example:

```
leaf4# vsh -c 'show system internal fhs pol'

Target           Type  Policy           Feature       Target-Range Sub-Feature
epg 0x40000c002  EPG   epg 0x40000c002  Trustctrl      vlan 4      Device-Roles: DHCPv4-Server,
DHCPv6-Server, Router
                                                                    Protocols: ARP ND
vlan 4          VLAN  vlan 4          IP inspect     vlan all    Protocols: ARP, DHCPv4, ND, DHCPv6,
vlan 4           VLAN  vlan 4           RA guard       vlan all    Min-HL:3, Max-HL:15,
M-Config-flag:Enable,On
                                                                    O-Config-flag:Enable,On,
Router-Pref:medium
```

Step 7 Display FHS secured endpoint database from the NX-OS shared database:

Example:

```
leaf1# vsh -c 'show system internal fhs sdb bt'

Preflevel flags (preflvl):
0001: MAC and LLA match     0002: Orig trunk            0004: Orig access
0008: Orig trusted trunk    0010: Orig trusted access   0020: DHCP assigned
0040: Cga authenticated     0080: Cert authenticated    0100: Statically assigned

Origin      Zone ID     L3 Address                                 MAC Address         VLAN ID  EPG ID
              If-name         Preflvl  State
----------  ----------  ---------------------------------------  ------------------  -------
------------------  --------------  -------  ---------
ARP         0x4         172.29.207.222                           d0:72:dc:a0:3d:4c   4
0x40000c002         Eth1/1          0011     STALE
L           0x4         192.0.200.1                              00:22:bd:f8:19:ff   4
0x400004003         Vlan4           0100     REACHABLE
ARP         0x4         192.0.200.10                             f8:72:ea:ad:c4:7c   4
0x40000c002         Eth1/1          0011     REACHABLE
L           0x4         2001:0:0:200::1                          00:22:bd:f8:19:ff   4
0x400004003         Vlan4           0100     REACHABLE
ND          0x4         2001:0:0:200::10                         f8:72:ea:ad:c4:7c   4
0x40000c002         Eth1/1          0011     STALE
L           0x80000004  fe80::200                                00:22:bd:f8:19:ff   4
0x400004003         Vlan4           0100     REACHABLE
ND          0x80000004  fe80::fa72:eaff:fead:c47c                 f8:72:ea:ad:c4:7c   4
0x40000c002         Eth1/1          0011     STALE
```

Step 8 Display FHS feature configurations from the NxOS shared database:

Example:

```
leaf1# vsh -c 'show system internal fhs sdb pol'
Policies:

IP inspect      Vlan 4                  Protocols:ARP DHCPv4 ND DHCPv6
RA guard        Vlan 4                  Min-HL:3 Max-HL:15 M-Config-Flag:enable,on
O-Config-Flag:enable,on Router-Pref:medium
Trustctrl       Epg 0x40000c002         Vlan:4
                                        Device-Roles:DHCPv4-Server DHCPv6-Server Router
                                        Protocols:ARP ND
```

Step 9 Show command to clear a secured database endpoint entry:

Example:

```
leaf1# vsh -c 'clear system internal fhs bt ipv4 172.29.207.222'
```

Configuring FHS in APIC Using REST API

Before you begin

- The tenant and bridge domain must be configured.

Procedure

Configure the FHS and Trust Control policies.

Example:

```
<polUni>
    <fvTenant name="Coke">
        <fhsBDPol name="bdpol5" ipInspectAdminSt="enabled-ipv6" srcGuardAdminSt="enabled-both"
raGuardAdminSt="enabled" status="">
            <fhsRaGuardPol name="raguard5" managedConfigCheck="true" managedConfigFlag="true"
otherConfigCheck="true" otherConfigFlag="true" maxRouterPref="medium" minHopLimit="3" maxHopLimit="15"
 status=""/>
        </fhsBDPol>
        <fvBD name="bd3">
            <fvRsBDToFhs tnFhsBDPolName="bdpol5" status=""/>
        </fvBD>
    </fvTenant>
</polUni>

<polUni>
<fvTenant name="Coke">
        <fhsTrustCtrlPol name="trustctrl5" hasDhcpv4Server="true" hasDhcpv6Server="true"
hasIpv6Router="true" trustRa="true" trustArp="true" trustNd="true" />
        <fvAp name="wwwCokecom3">
           <fvAEPg name="test966">
           <fvRsTrustCtrl tnFhsTrustCtrlPolName="trustctrl5" status=""/>
        </fvAEPg>
        </fvAp>
</fvTenant>
</polUni>
```