IPv6 First-Hop Security Features

This chapter describes how to configure the IPv6 First-Hop Security (FHS) features.

This chapter includes the following sections:

Understanding IPv6 First-Hop Security features

IPv6 FHS features enable a better 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).

These are the features supported on the c7600 platform:

- IPv6 Snooping
- IPv6 Router Advertisement Guard
- IPv6 - Destination Guard
- Binding Table Recovery
- DHCPv6 Guard
- IPv6 Source Guard
- IPv6 Prefix Guard
- Data Gleaning

IPv6 Snooping

IPv6 snooping captures the IPv6 traffic and helps in populating the binding table. It gathers addresses in control messages such as Neighbor Discovery Protocol (NDP) or Dynamic Host Configuration Protocol (DHCP) packets. Depending on the security level, it blocks unwanted messages such as Router Advertisements (RA) or DHCP replies. This feature is a pre-requisite to the remaining security features mentioned here.

IPv6 Router Advertisement Guard

IPv6 RA Guard validates the content of the RAs and redirect messages, and blocks or rejects unwanted RA. Depending on the configuration options, RA guard validates various parameters such as the IPv6 source address of the packet, flags in the RA, prefixes advertised by the router, hop-count limit advertised, and the default router preference advertised.

On the c7600, the ports can be configured to allow or disallow RA messages. If the port is configured to disallow the RA and router-redirect packets, the RA guard blocks them. The RA guard can be configured on the VLAN, including all the ports on the VLAN.

IPv6 - Destination Guard

The Destination Guard feature helps in minimizing denial-of-service (DoS) attacks. It performs address resolutions only for those addresses that are active on the link, and requires the FHS binding table to be populated with the help of the IPv6 snooping feature.

The feature enables the filtering of IPv6 traffic based on the destination address, and blocks the NDP resolution for destination addresses that are not found in the binding table. By default, the policy drops traffic coming for an unknown destination.

Binding Table Recovery

This feature helps in recovering the missing binding table entries when the resolution for a destination address fails in the destination guard. It does so by querying the DHCP server or the destination host, depending on the configuration.

DHCPv6 Guard

The DHCPv6 Guard blocks DHCP replies or advertisements not originating from a DHCP server or relay. It decides whether or not to switch or block the DHCP replies based on the device-role configuration. It also verifies the information found in the message.

The DHCPv6 Guard classifies the information into one of the three DHCP type messages (client message, server message, and relay message), and takes action depending on the device role. All client messages are switched regardless of the device role, and the DHCP server messages are only processed further if the device role is set to server.

IPv6 Source Guard

IPv6 Source Guard (SG) is a security feature that filters the IPv6 traffic on Layer 2 ports that are not trusted. SG helps a switch or router deny access to traffic from an address that is not stored in the binding table of the IPv6 Snooping feature. SG drops those data packets whose IPv6 source addresses are unavailable in the binding table. The binding table has entries for the link local addresses of hosts.

An entry is installed in the binding table when one of the following conditions is satisfied:

- An IPv6 binding is learnt through DHCP.
- An IPv6 address or prefix is learnt through NDP.
- A static binding is configured by the user.

A corresponding entry is also installed in Network Processor Ternary Content-Addressable Memory (NP TCAM) of the line card. A data packet that does not match any NP TCAM entry is dropped.

SG installs a “deny-all” Access Control Entry (ACE) on targets, except control packets, where the feature is configured. SG also installs an IPv6, MAC address, Port, or VLAN ID filter to validate the binding table entries learnt from the targets.

Table 41-1 lists the filters that SG applies to incoming network traffic.

Table 41-1 Filters for IPv6 Source Guard

Filter	What It Means
IPv6 address	IPv6 address of the host
MAC address	MAC address of the host
VLAN ID	VLAN ID of the port associated with the host
Port	Number of the port associated with the host

SG is an ingress feature and filters incoming data packets alone. If SG is enabled, every ingress packet on a switch port or Layer 2 VLAN is checked against entries in the IPv6 binding table. Initially, SG blocks all IPv6 traffic on the target except for Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP) packets that are used for IPv6 Snooping processes.

SG works in the policy mode. SG and snooping policies are configured in the global configuration mode. The policies are applied to switch ports and VLANs. Validate Address, which inspects IPv6 addresses, is enabled by default in the IPv6 Source Guard policy. The configurations only apply to the ports of ES 40 cards. Enabling IPv6 SG causes the attachment of ICMPv6 policies and DHCPv6 Snooping policies on NP TCAM for the interface.

The configuration of IPv6 Snooping is a prerequisite for SG. SG requires the configuration of IPv6 Snooping on one of the following:

- Layer 2 access or trunk ports
- Layer 2 VLANs

IPv6 Prefix Guard

IPv6 Prefix Guard (PG) is an ingress, security feature. PG helps a switch or router deny access to traffic from sources with addresses that are correct, but are topologically incorrect.

PG works in the policy mode. The policy for PG includes both IPv6 addresses and their prefixes.

The following are prerequisites for PG:

- Enablement of Prefix-glean under the IPv6 Snooping policy options
- Enablement of Validate Prefix under the Source Guard policy

Prefix Guard can be used in the following kinds of deployment:

- Service Provider (SP) deployment
- Enterprise deployment

PG in Service Provider Deployment

PG in an SP deployment involves the delegation of prefixes to routers that are connected to a switch. Prefixes are gleaned in DHCP Prefix Delegation messages to create entries in the binding table. A binding entry binds the prefix to the port and MAC address, and indicates the router to which the prefix is delegated. PG verifies if the traffic received from that router matches the binding entry.

Note Prefixes that are snooped from a DHCP REQUEST/REPLY sequence or a manual configuration are bound to the MAC address or port. Only incoming traffic with snooped prefixes from that MAC address or port is given network access.

PG in Enterprise Deployment

PG in an enterprise deployment involves the gleaning of prefixes in Router Advertisements (RA). PG blocks traffic that originates from nodes with a source outside any known prefix.

Note Ensure that you attach the RA guard policy and a snooping policy to the ports of the switch on which you learn bindings.

Note A prefix that is learnt from a multicast RA applies to an entire VLAN, and not to a specific port or MAC address.

Data Gleaning

If a network receives valid data packets with binding information that is either lost or incorrectly set, the process of data gleaning populates the binding table with binding information extracted from the data packets.The process of punting or gleaning data packets from unknown hosts to get new bindings is called data gleaning.

When an unknown host sends a data packet with IPv6 and MAC addresses along with its VLAN ID to the network, the network processor checks if IPv6 SG is enabled for the port or VLAN. If the host is trusted, and data gleaning is configured on the VLAN or port, new bindings are extracted from the data packets.

Data gleaning is commonly used in conjunction with IPv6 Source and Prefix Guard. Data gleaning works the same way as IPv6 SG works with the snooping feature configured. Data gleaning is a configuration in the snooping policy.

When you use data gleaning, run the following command to limit the rate of data that is redirected to the Route Processor (RP):

hw-module *slot number* **rate-limit punt_rate**

Restrictions for IPv6 FHS features

Following restrictions apply to the IPv6 FHS features:

- The c7600 only supports port and VLAN as the targets.

- The Ternary Content-Addressable Memory (TCAM) stores around 16,000 IPv6 ACL entries and 2000 masks. Therefore, an approximate number of 8000 IPv6 prefixes are supported for the FHS features.
- The c7600 does not support per-port and VLAN Access Control List (PVACL).
- The c7600 does not support the IPv6 address if it is not compressed. Use the **mls ipv6 acl compress address unicast** command to compress the IPv6 address.
- The c7600 supports a maximum of 16 broadcast groups.
- The IPv6 FHS features are SSO compliant.
- The c7600 internally creates a Switch Virtual Interface (SVI) of the layer 2 VLAN for the access port. But for the trunk ports, you need to create a SVI of the layer 2 VLAN to prevent traffic from dropping.
- All the FHS configurations are supported only in the ingress direction.
- The FHS configurations are supported on the trunk-port only in the port prefer mode.
- The Destination Guard is applicable only on the VLAN mode.

Restrictions for IPv6 Source and Prefix Guards

The following restrictions apply to Source Guard and Prefix Guard usage:

- SG and PG are used only for ES 40 cards, and the configurations are applied to the ports of ES 40 cards.
- SG and PG are layer 2 features that are supported only on access or trunk ports, and L2 VLAN configurations.
- To configure SG or PG on a trunk port, you must first configure ‘port prefer mode’ on the trunk port using ‘access-group mode prefer port’ under the interface configurations.
- For SG and PG to operate properly, when you enable SG or PG on a switch port, ensure that you attach IPv6 Snooping to the interface. All data traffic from this port is blocked unless bindings are available.
- The hardware resources on the line card limit not only the number of ACLs learnt through SG and PG, but also the ACEs that you can configure for SG and PG. The different features that are configured on the line card share the TCAM resources that are available.
- SG and PG are ingress traffic only features.
- SG and PG do not support the software forwarding of data packets.
- During an LC Online Insertion and Removal (OIR) event, all the relevant IPV6 snooping bindings are distributed to the line card and programmed into TCAM. A large number of bindings may need more time for processing.
- Support is available only for 4096 SG or PG entries per network processor (NP).
- For IPv6 Prefix Guard and RA Guard to work on the system in the PFC3CXL mode, ensure that you globally configure ‘No mld ipv6 snooping’.
- Not all incoming data traffic is sent to the Route Processor (RP) to learn binding for data gleaning. The rate of data that is redirected to RP is limited.
- SG and PG are not supported on Port Channels.
- PG that is attached to a VLAN configuration will apply to the entire VLAN. It is recommended that PG be configured either at the VLAN or port level.

Note For more information on network processors, see Network Processors: Programmable Technology for Building Network Systems.

Configuring IPv6 FHS Features

- For information on IPv6 Router Advertisement (RA) Guard configurations, see: http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_fhsec/configuration/15-2s/ip6-ra-guard.html
- For information on IPv6 - Destination Guard configurations, see: http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ipv6-dest-guard.html
- For information on Binding Table Recovery configurations, see: http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-fhs-bind-table.html
- For information on DHCP - DHCPv6 Guard configurations, see: http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-2s/ip6-dhcpv6-guard.html
- For information on IPv6 Source Guard configurations, see:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_fhsec/configuration/15-2s/ipv6-sg-guard.html
- For information on IPv6 Prefix Guard configurations, see:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_fhsec/configuration/15-2s/ipv6-pg-guard.html

Verifying IPv6 FHS Configuration

Use these commands to verify the configuration of IPv6 FHS features on c7600:

- The **show ipv6 snooping policy trusted** command displays the IPv6 snooping policy configuration, and the interfaces where the policy is applied.

```
Router# show ipv6 snooping policy trusted

   Policy trusted configuration:
     trusted-port
     device-role node
   Policy applied on the following interfaces:
      Et0/0    vlan all
      Et1/0    vlan all
   Policy applied on the following vlans:
      vlan 1-100,200,300-400
```

- The **show ipv6 snooping messages** command displays the latest messages that were processed by ipv6 snooping.

```
Router# show ipv6 snooping messages

   On VLAN 100, From Et0/0 NDP::NS,  FE80::A8BB:CCFF:FE01:F500,
    On VLAN 100, From Et1/0 MAC AABB.CC01.F500: NDP::NA,  FE80::A8BB:CCFF:FE01:F500, Drop
   reason=Message unauthorized on port
    On VLAN 100, From Et0/0 MAC AABB.CC01.F500: NDP::NA,  FE80::A8BB:CCFF:FE01:F500,
    On VLAN 100, From Et0/0 NDP::NS,  FE80::A8BB:CCFF:FE01:F500,
    On VLAN 100, From Et1/0 MAC AABB.CC01.F500: NDP::NA,  FE80::A8BB:CCFF:FE01:F500,
```

- The **show ipv6 snooping messages detailed *N*** command displays a defined number of messages as specified.

```
Router# show ipv6 snooping messages detailed 8


    On VLAN 100, From Et0/0 seclvl [guard], unparsed message.

     On VLAN 100, From Et0/0 seclvl [guard], NDP::NS,
     1 addresses advertised:
            IPv6 addr: FE80::A8BB:CCFF:FE01:F500,

     On VLAN 100, From Et0/0 seclvl [glean], NDP::NS,
     1 addresses advertised:
            IPv6 addr: FE80::A8BB:CCFF:FE01:F500,

     On VLAN 100, From Et0/0 seclvl [glean], MAC AABB.C901.6601: DHCPv6::SOL, no IPv6
    target. packet ignored.

     On VLAN 100, From Et0/0 seclvl [glean], DHCPv6::REP,
     1 addresses advertised:
            IPv6 addr: 3000:901:1::14, protocol lifetime: 0xE10==3600, packet ignored.

     On VLAN 100, From Et0/0 seclvl [glean], DHCPv6::REP,
     1 addresses advertised:
            IPv6 addr: 3000:901:1::14, protocol lifetime: 0xFFFFFFFF==4294967295, packet
    ignored.

     On VLAN 100, From Et0/0 seclvl [glean], MAC AABB.CC01.F500: DHCPv6::REN, no IPv6
    target. packet ignored.

     On VLAN 100, From Et1/0 seclvl [glean], about Et0/0, MAC AABB.CC01.F500: DHCPv6::REP,
     3 addresses advertised:
            IPv6 addr: 2001:600::60AF:3195:BC06:EAFB, protocol lifetime: 0x5==5,
            IPv6 addr: 2001:400::A1C9:9B4F:2D34:C621, protocol lifetime: 0x5==5,
            IPv6 addr: 2001:500::2, protocol lifetime: 0x5==5,
```

- The **show ipv6 snooping counters** ***target*** command displays the drop counters statistics. Whenever any feature drops a received packet, the counters are incremented.

```
Router# show ipv6 snooping counters vlan 100
    Received messages on vlan 100 :
    Protocol        Protocol message
    NDP             RA[58] NS[23] NA[14]
    DHCPv6      SOL[7] ADV[6] REQ[1] REN[6] REP[7]


    Bridged messages from vlan 100 :
    Protocol       Protocol message
    NDP             RA[47] NS[22] NA[14]
    DHCPv6      SOL[7] ADV[1] REQ[1] REN[6] REP[7]


    Dropped messages on vlan 100 :
    ND Suppress    NS[1] reason ND multicast suppressed[1]
    Gleaner         RA[11] reason Packet is not authorized on the received port[11]
                    ADV[5] reason Packet is not authorized on the received port[5]

    On the port:
    SWITCH#show ipv6 snooping counters int e 1/0
    Received messages on Et1/0:
    Protocol        Protocol message
    NDP             RA[63] NA[13]
    DHCPv6      ADV[1] REP[10]
```

```
Bridged messages from Et1/0:
Protocol        Protocol message
NDP              RA[63] NA[13]
DHCPv6         DV[1] REP[10]
```

- The **show ipv6 destination-guard** command displays the destination guard policy configuration, and all the interfaces where the policy is applied.

```
Router# show ipv6 destination-guard
   ? Shows the policy configuration as well as all the interfaces where the policy is
   applied:

   Policy default configuration:
   Policy applied on the following vlans:
     vlan 1-100,200,300-400
```

- The **show ipv6 neighbors binding** command displays the binding table entries populated by the snooping policy.

```
Router# show ipv6 neighbors binding

   Binding Table has 1 entries, 1 dynamic
   Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - 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:HCP assigned
   0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


      IPv6 address                            Link-Layer addr Interface vlan prlvl  age
   state    Time left
   ND  1000::2                                  0000.0AA3.FB6A  Gi3/3       30  0005
   13mn STALE      88671 s
```

- The **show ipv6 nd raguard policy** command displays the RA guard policy configuration, and all the interfaces where the policy is applied.

```
Router# show ipv6 nd raguard policy

   Policy raguard configuration:
     device-role host
   Policy raguard is applied on the following targets:
   Target              Type  Policy              Feature        Target range
   Gi3/7               PORT  raguard             RA guard       vlan all
```

- The **show ipv6 dhcp guard policy** command displays the DHCP guard policy configuration, and all the interfaces where the policy is applied.

```
Router# show ipv6 dhcp guard

   Dhcp guard policy: dhcp
   Device Role: dhcp client
   Target: Gi3/7
```

- The **show tcam interface** command displays the following output when the IPv6 snooping is configured on an interface.

```
Router# show tcam interface gigabitEthernet 3/3 acl in ipv6

   * Global Defaults shared

   ------------------------------------------------------
   ICMP Neighbor Discovery Packet Types:
   na - neighbor advertisement  ra - router advertisement
   ns - neighbor solicit        rs - router solicit
   r  - redirect
```

```
IPV6 Address Types:
full - IPv6 Full             eui - IPv6 EUI
eipv4 - IPv6 embeded IPv4
------------------------------------------------------
   redirect     icmp(nd-ns) any(eui) any
   redirect     icmp(nd-na) any(eui) any
   redirect     icmp(nd-rs) any(eui) any
   redirect     icmp(nd-ra) any(eui) any
   redirect     icmp(nd-r) any(eui) any
   redirect     icmp(nd-ns) any(full) any
   redirect     icmp(nd-na) any(full) any
   redirect     icmp(nd-rs) any(full) any
   redirect     icmp(nd-ra) any(full) any
   redirect     icmp(nd-r) any(full) any
   redirect     udp any(eui) eq 547 any(eui) eq 546
   redirect     udp any(eui) eq 546 any(eui) eq 547
   permit       ipv6 any(eipv4) any
   permit       ipv6 any(eui) any
   permit       ipv6 any(full) any
```

Troubleshooting Tips

Table 41-2 Troubleshooting Tips

Problem	Solution
The IPv6 snooping feature is not working.	• Use the **debug ipv6 snooping** command to check if the TCAM is programmed in the hardware.
Packets are not switching as expected during router reboot.	• Use the **show ipv6 neighbors binding** and **debug ipv6 neighbor discovery** commands to check the configuration.
The Switch Integrated Security Features (SISF) does not work as expected.	• Use the **debug fm sisf** command to print the debugs for the feature manager.