IPv6 First-Hop Security Configuration Guide, Cisco IOS Release 15S

First Published: 2012-11-05

Last Modified: 2012-11-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **IPv6 RA Guard** 1

Finding Feature Information 1

Restrictions for IPv6 RA Guard 1

Information About IPv6 RA Guard 2

IPv6 Global Policies 2

IPv6 RA Guard 2

How to Configure IPv6 RA Guard 2

Configuring the IPv6 RA Guard Policy on the Device 2

Configuring IPv6 RA Guard on an Interface 4

Configuration Examples for IPv6 RA Guard 5

Example: IPv6 RA Guard Configuration 5

Example: Configuring IPv6 ND Inspection and RA Guard 6

Additional References 6

Feature Information for IPv6 RA Guard 7

CHAPTER 2 **IPv6 Snooping** 9

Finding Feature Information 9

Restrictions for IPv6 Snooping 9

Information About IPv6 Snooping 10

IPv6 Global Policies 10

IPv6 Neighbor Discovery Inspection 10

IPv6 ND Inspection 10

IPv6 Device Tracking 11

IPv6 Address Glean 11

How to Configure IPv6 Snooping 12

Configuring IPv6 ND Inspection 12

Configuring IPv6 ND Inspection Globally 13
Applying IPv6 ND Inspection on an Interface 14
Verifying and Troubleshooting IPv6 ND Inspection 15
Configuring IPv6 Device Tracking 16
Configuring IPv6 First-Hop Security Binding Table Recovery 16
Configuring IPv6 Device Tracking 21
Configuring IPv6 Prefix Glean 22
Configuration Examples for IPv6 Snooping 22
Example: Configuring IPv6 ND Inspection 22
Example: Configuring IPv6 ND Inspection and RA Guard 23
Example: Configuring IPv6 Binding Table Content 23
Example: Configuring IPv6 First-Hop Security Binding Table Recovery 23
Example: Configuring Address Gleaning and Associating Recovery Protocols with Prefix Lists 24
Example: Verifying IPv6 Device Tracking 24
Additional References for IPv6 Source Guard and Prefix Guard 24
Feature Information for IPv6 Snooping 25

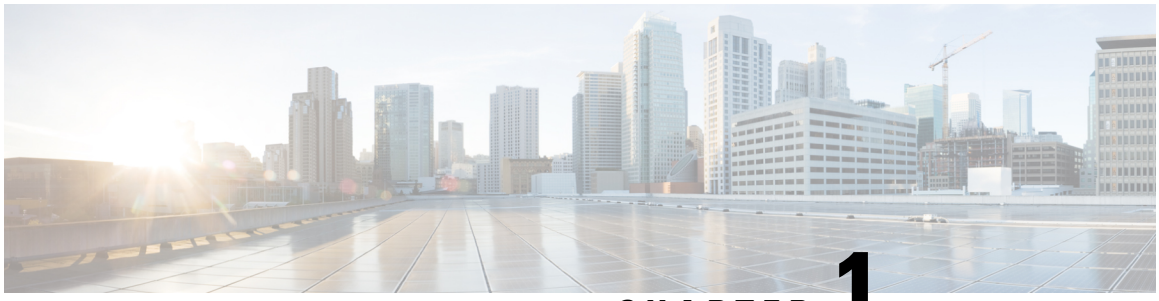
CHAPTER 3 **DHCP—DHCPv6 Guard 27**
Finding Feature Information 27
Restrictions for DHCPv6 Guard 27
Information About DHCPv6 Guard 28
DHCPv6 Guard Overview 28
How to Configure DHCPv6 Guard 28
Configuring DHCP—DHCPv6 Guard 28
Configuration Examples for DHCPv6 Guard 31
Example: Configuring DHCP—DHCPv6 Guard 31
Additional References 31
Feature Information for DHCP—DHCPv6 Guard 32

CHAPTER 4 **IPv6 Source Guard and Prefix Guard 33**
Finding Feature Information 33
Information about IPv6 Source Guard and Prefix Guard 33
IPv6 Source Guard Overview 33
IPv6 Prefix Guard Overview 34

How to Configure IPv6 Source Guard and Prefix Guard 35
Configuring IPv6 Source Guard 35
Configuring IPv6 Source Guard on an Interface 37
Configuring IPv6 Prefix Guard 38
Configuration Examples for IPv6 Source Guard and Prefix Guard 39
Example: Configuring IPv6 Source Guard and Prefix Guard 39
Additional References for IPv6 Source Guard and Prefix Guard 39
Feature Information for IPv6 Source Guard and Prefix Guard 40

CHAPTER 5 **IPv6 Destination Guard 41**
Finding Feature Information 41
Prerequisites for IPv6 Destination Guard 41
Information About IPv6 Destination Guard 42
IPv6 Destination Guard Overview 42
How to Configure the IPv6 Destination Guard 42
Configuring IPv6 Destination Guard 42
Configuration Examples for IPv6 Destination Guard 43
Example: Configuring an IPv6 Destination Guard Policy 43
Additional References 44
Feature Information for IPv6 Destination Guard 44

CHAPTER 6 **IPv6 RFCs 47**



CHAPTER 1

IPv6 RA Guard

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement (RA) guard messages that arrive at the network device platform.

- Finding Feature Information, on page 1
- Restrictions for IPv6 RA Guard, on page 1
- Information About IPv6 RA Guard, on page 2
- How to Configure IPv6 RA Guard, on page 2
- Configuration Examples for IPv6 RA Guard, on page 5
- Additional References, on page 6
- Feature Information for IPv6 RA Guard, on page 7

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IPv6 RA Guard

- The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
- This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
- This feature can be configured on a switch port interface in the ingress direction.
- This feature supports host mode and router mode.
- This feature is supported only in the ingress direction; it is not supported in the egress direction.
- This feature is not supported on EtherChannel and EtherChannel port members.
- This feature is not supported on trunk ports with merge mode.

- This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of PVLANs, primary VLAN features are inherited and merged with port features.
- Packets dropped by the IPv6 RA Guard feature can be spanned.
- If the **platform ipv6 acl icmp optimize neighbor-discovery command** is configured, the IPv6 RA Guard feature cannot be configured and an error message will be displayed. This command adds default global Internet Control Message Protocol (ICMP) entries that will override the RA guard ICMP entries.

Information About IPv6 RA Guard

IPv6 Global Policies

IPv6 global policies provide storage and access policy database services. IPv6 ND inspection and IPv6 RA guard are IPv6 global policies features. Every time an ND inspection or RA guard is configured globally, the policy attributes are stored in the software policy database. The policy is then applied to an interface, and the software policy database entry is updated to include this interface to which the policy is applied.

IPv6 RA Guard

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform. RAs are used by devices to announce themselves on the link. The IPv6 RA Guard feature analyzes these RAs and filters out RAs that are sent by unauthorized devices. In host mode, all RA and router redirect messages are disallowed on the port. The RA guard feature compares configuration information on the Layer 2 (L2) device with the information found in the received RA frame. Once the L2 device has validated the content of the RA frame and router redirect frame against the configuration, it forwards the RA to its unicast or multicast destination. If the RA frame content is not validated, the RA is dropped.

In the wireless deployment RAs coming on wireless ports are dropped as routers cannot reside on these interfaces.

How to Configure IPv6 RA Guard

Configuring the IPv6 RA Guard Policy on the Device

Note When the **ipv6 nd raguard** command is configured on ports, router solicitation messages are not replicated to these ports. To replicate router solicitation messages, all ports that face routers must be set to the router role.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **ipv6 nd raguard policy** *policy-name*
4. **device-role** {**host** | **router**}
5. **hop-limit** {**maximum** | **minimum** *limit*}
6. **managed-config-flag** {**on** | **off**}
7. **match ipv6 access-list** *ipv6-access-list-name*
8. **match ra prefix-list** *ipv6-prefix-list-name*
9. **other-config-flag** {**on** | **off**}
10. **router-preference maximum** {**high** | **low** | **medium**}
11. **trusted-port**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 nd raguard policy** *policy-name* **Example:** `Device(config)# ipv6 nd raguard policy policy1`	Defines the RA guard policy name and enters RA guard policy configuration mode.
Step 4	**device-role** {**host**	**router**} **Example:** `Device(config-ra-guard)# device-role router`	Specifies the role of the device attached to the port.
Step 5	**hop-limit** {**maximum**	**minimum** *limit*} **Example:** `Device(config-ra-guard)# hop-limit minimum 3`	(Optional) Enables verification of the advertised hop count limit. • If not configured, this check will be bypassed.
Step 6	**managed-config-flag** {**on**	**off**} **Example:** `Device(config-ra-guard)# managed-config-flag on`	(Optional) Enables verification that the advertised managed address configuration flag is on. • If not configured, this check will be bypassed.

	Command or Action	Purpose
Step 7	**match ipv6 access-list** *ipv6-access-list-name* **Example:** `Device(config-ra-guard)# match ipv6 access-list list1`	(Optional) Enables verification of the sender's IPv6 address in inspected messages from the configured authorized device source access list. • If not configured, this check will be bypassed.
Step 8	**match ra prefix-list** *ipv6-prefix-list-name* **Example:** `Device(config-ra-guard)# match ra prefix-list listname1`	(Optional) Enables verification of the advertised prefixes in inspected messages from the configured authorized prefix list. • If not configured, this check will be bypassed.
Step 9	**other-config-flag** {**on** | **off**} **Example:** `Device(config-ra-guard)# other-config-flag on`	(Optional) Enables verification of the advertised "other" configuration parameter.
Step 10	**router-preference maximum** {**high** | **low** | **medium**} **Example:** `Device(config-ra-guard)# router-preference maximum high`	(Optional) Enables verification that the advertised default router preference parameter value is lower than or equal to a specified limit.
Step 11	**trusted-port** **Example:** `Device(config-ra-guard)# trusted-port`	(Optional) Specifies that this policy is being applied to trusted ports. • All RA guard policing will be disabled.
Step 12	**exit** **Example:** `Device(config-ra-guard)# exit`	Exits RA guard policy configuration mode and returns to global configuration mode.

Configuring IPv6 RA Guard on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd raguard attach-policy** [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]
5. **exit**
6. **show ipv6 nd raguard policy** [*policy-name*]
7. **debug ipv6 snooping raguard** [*filter* | *interface* | *vlanid*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface fastethernet 3/13`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**ipv6 nd raguard attach-policy** [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]] **Example:** `Device(config-if)# ipv6 nd raguard attach-policy`	Applies the IPv6 RA Guard feature to a specified interface.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 6	**show ipv6 nd raguard policy** [*policy-name*] **Example:** `Device# show ipv6 nd raguard policy raguard1`	Displays the RA guard policy on all interfaces configured with the RA guard.
Step 7	**debug ipv6 snooping raguard** [*filter* | *interface* | *vlanid*] **Example:** `Device# debug ipv6 snooping raguard`	Enables debugging for IPv6 RA guard snooping information.

Configuration Examples for IPv6 RA Guard

Example: IPv6 RA Guard Configuration

```
Device(config)# interface fastethernet 3/13

Device(config-if)# ipv6 nd raguard attach-policy
```

```
Device# show running-config interface fastethernet 3/13

Building configuration...
Current configuration : 129 bytes
!
interface FastEthernet3/13
 switchport
 switchport access vlan 222
 switchport mode access
 access-group mode prefer port
 ipv6 nd raguard
end
```

Example: Configuring IPv6 ND Inspection and RA Guard

This example provides information about an interface on which both the Neighbor Discovery Inspection and RA Guard features are configured:

```
Device# show ipv6 snooping capture-policy interface ethernet 0/0

Hardware policy registered on Ethernet 0/0
Protocol     Protocol value   Message   Value     Action    Feature
ICMP         58               RS        85        punt      RA Guard
                                                  punt      ND Inspection
ICMP         58               RA        86        drop      RA guard
                                                  punt      ND Inspection
ICMP         58               NS        87        punt      ND Inspection
ICM          58               NA        88        punt      ND Inspection
ICMP         58               REDIR     89        drop      RA Guard
                                                  punt      ND Inspection
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

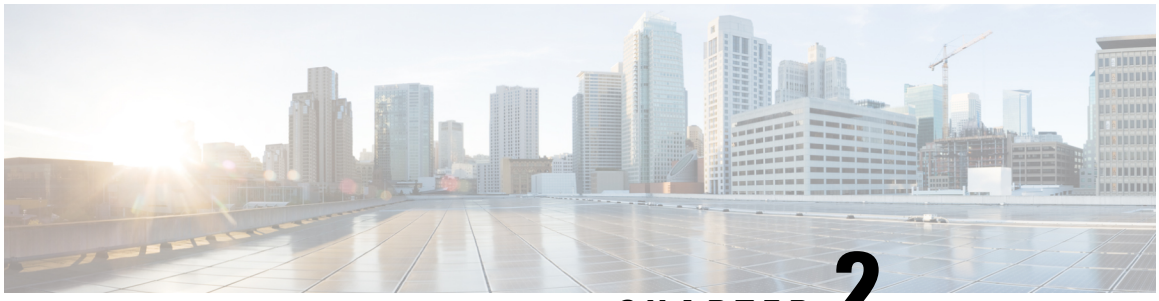
Feature Information for IPv6 RA Guard

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for IPv6 RA Guard

Feature Name	Releases	Feature Information
IPv6 RA Guard	12.2(33)SXI4 12.2(50)SY 12.2(54)SG 15.0(2)SE 15.0(2)SG Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.2SE Cisco IOS XE Release 3.2SG	The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement (RA) guard messages that arrive at the network device platform. The following commands were introduced or modified: **debug ipv6 snooping raguard**, **device-role**, **hop-limit**, **ipv6 nd raguard attach-policy**, **ipv6 nd raguard policy**, **managed-config-flag**, **match ipv6 access-list**, **match ra prefix-list**, **other-config-flag**, **router-preference maximum**, **show ipv6 nd raguard policy**.



CHAPTER 2

IPv6 Snooping

The IPv6 Snooping feature bundles several Layer 2 IPv6 first-hop security features, including IPv6 neighbor discovery inspection, IPv6 device tracking, IPv6 address glean, and IPv6 binding table recovery, to provide security and scalability. IPv6 ND inspection operates at Layer 2, or between Layer 2 and Layer 3, to provide IPv6 functions with security and scalability.

- Finding Feature Information, on page 9
- Restrictions for IPv6 Snooping, on page 9
- Information About IPv6 Snooping, on page 10
- How to Configure IPv6 Snooping, on page 12
- Configuration Examples for IPv6 Snooping, on page 22
- Additional References for IPv6 Source Guard and Prefix Guard, on page 24
- Feature Information for IPv6 Snooping, on page 25

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IPv6 Snooping

The IPv6 snooping feature is not supported on Etherchannel ports.

Information About IPv6 Snooping

IPv6 Global Policies

IPv6 global policies provide storage and access policy database services. IPv6 ND inspection and IPv6 RA guard are IPv6 global policies features. Every time an ND inspection or RA guard is configured globally, the policy attributes are stored in the software policy database. The policy is then applied to an interface, and the software policy database entry is updated to include this interface to which the policy is applied.

IPv6 Neighbor Discovery Inspection

The IPv6 Neighbor Discovery Inspection, or IPv6 "snooping," feature bundles several Layer 2 IPv6 first-hop security features, including IPv6 Address Glean and IPv6 Device Tracking. IPv6 neighbor discovery (ND) inspection operates at Layer 2, or between Layer 2 and Layer 3, and provides IPv6 features with security and scalability. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables and analyzes ND messages in order to build a trusted binding table. IPv6 ND messages that do not have valid bindings are dropped. An ND message is considered trustworthy if its IPv6-to-MAC mapping is verifiable. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

When IPv6 ND inspection is configured on a target (which varies depending on platform target support and may include device ports, switch ports, Layer 2 interfaces, Layer 3 interfaces, and VLANs), capture instructions are downloaded to the hardware to redirect the ND protocol and Dynamic Host Configuration Protocol (DHCP) for IPv6 traffic up to the switch integrated security features (SISF) infrastructure in the routing device. For ND traffic, messages such as NS, NA, RS, RA, and REDIRECT are directed to SISF. For DHCP, UDP messages sourced from port 546 or 547 are redirected.

IPv6 ND inspection registers its "capture rules" to the classifier, which aggregates all rules from all features on a given target and installs the corresponding ACL down into the platform-dependent modules. Upon receiving redirected traffic, the classifier calls all entry points from any registered feature (for the target on which the traffic is being received), including the IPv6 ND inspection entry point. This entry point is the last to be called, so any decision (such as drop) made by another feature supersedes the IPv6 ND inspection decision.

IPv6 ND Inspection

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery messages that do not have valid bindings are dropped. A neighbor discovery message is considered trustworthy if its IPv6-to-MAC mapping is verifiable.

This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 Device Tracking

IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

IPv6 First-Hop Security Binding Table

The IPv6 First-Hop Security Binding Table recovery mechanism feature enables the binding table to recover in the event of a device reboot. A database table of IPv6 neighbors connected to the device is created from information sources such as ND snooping. This database, or binding, table is used by various IPv6 guard features to validate the link-layer address (LLA), the IPv4 or IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.

This mechanism enables the binding table to recover in the event of a device reboot. The recovery mechanism will block any data traffic sourced from an unknown source; that is, a source not already specified in the binding table and previously learned through ND or DHCP gleaning. This feature recovers the missing binding table entries when the resolution for a destination address fails in the destination guard. When a failure occurs, a binding table entry is recovered by querying the DHCP server or the destination host, depending on the configuration.

Recovery Protocols and Prefix Lists

The IPv6 First-Hop Security Binding Table Recovery Mechanism feature introduces the capability to provide a prefix list that is matched before the recovery is attempted for both DHCP and NDP.

If an address does not match the prefix list associated with the protocol, then the recovery of the binding table entry will not be attempted with that protocol. The prefix list should correspond to the prefixes that are valid for address assignment in the Layer 2 domain using the protocol. The default is that there is no prefix list, in which case the recovery is attempted for all addresses. The command to associate a prefix list to a protocol is **protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*].

IPv6 Device Tracking

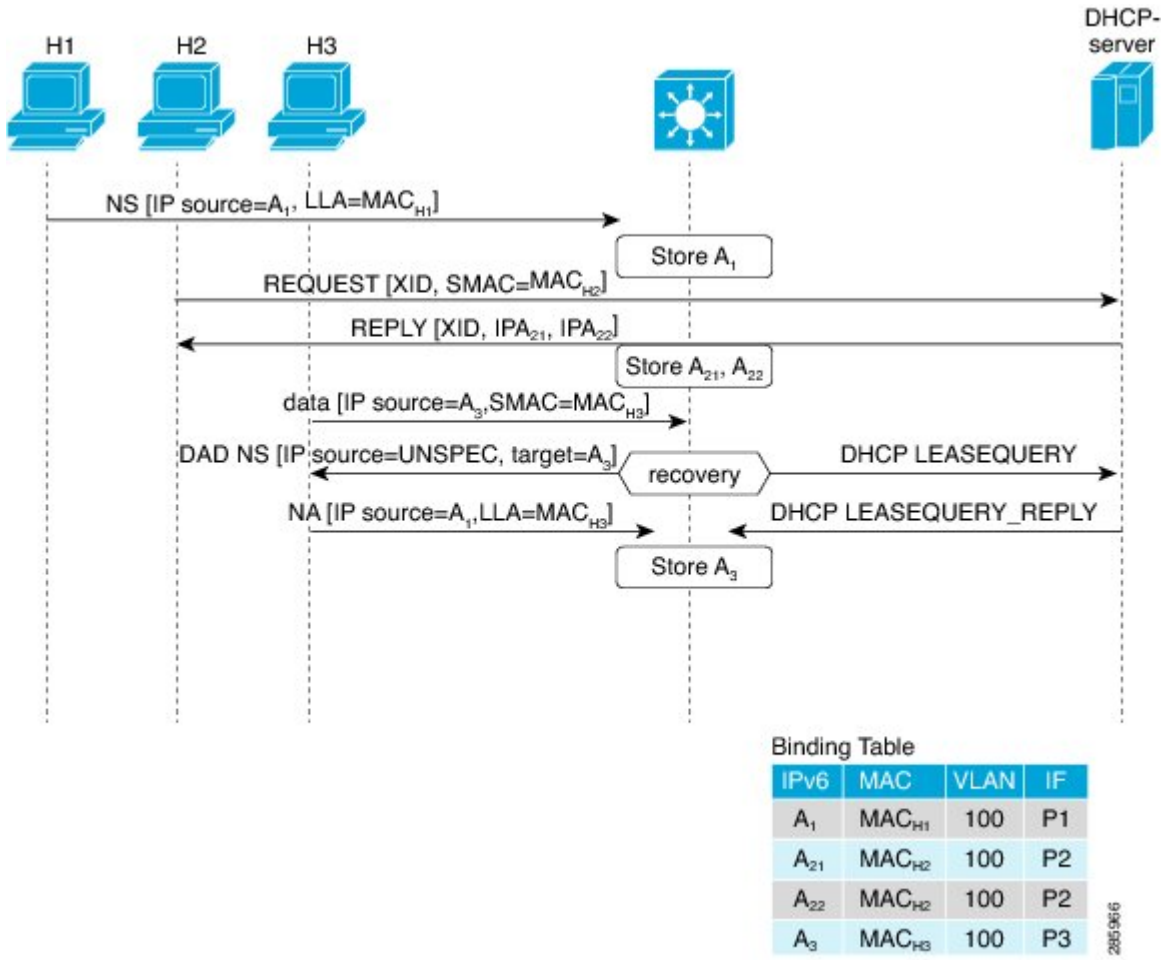
IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

IPv6 Address Glean

IPv6 address glean is the foundation for many other IPv6 features that depend on an accurate binding table. It inspects ND and DHCP messages on a link to glean addresses, and then populates the binding table with these addresses. This feature also enforces address ownership and limits the number of addresses any given node is allowed to claim.

The following figure shows how IPv6 address glean works.

Figure 1: IPv6 Address Glean



How to Configure IPv6 Snooping

Configuring IPv6 ND Inspection

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *snooping-policy*
4. **ipv6 snooping attach-policy** *snooping-policy*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 snooping policy** *snooping-policy* **Example:** `Device(config)# ipv6 snooping policy policy1`	Configures an IPv6 snooping policy and enters IPv6 snooping configuration mode.
Step 4	**ipv6 snooping attach-policy** *snooping-policy* **Example:** `Device(config-ipv6-snooping)# ipv6 snooping attach-policy policy1`	Attaches the IPv6 snooping policy to a target.

Configuring IPv6 ND Inspection Globally

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 nd inspection policy** *policy-name*
4. **drop-unsecure**
5. **sec-level minimum** *value*
6. **device-role** {**host** | **monitor** | **router**}
7. **tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}
8. **trusted-port**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ipv6 nd inspection policy** *policy-name* **Example:** `Device(config)# ipv6 nd inspection policy policy1`	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
Step 4	**drop-unsecure** **Example:** `Device(config-nd-inspection)# drop-unsecure`	Drops messages with no options, invalid options, or an invalid signature.
Step 5	**sec-level minimum** *value* **Example:** `Device(config-nd-inspection)# sec-level minimum 2`	Specifies the minimum security level parameter value when cryptographically generated address (CGA) options are used.
Step 6	**device-role** {**host** | **monitor** | **router**} **Example:** `Device(config-nd-inspection)# device-role monitor`	Specifies the role of the device attached to the port.
Step 7	**tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]} **Example:** `Device(config-nd-inspection)# tracking disable stale-lifetime infinite`	Overrides the default tracking policy on a port.
Step 8	**trusted-port** **Example:** `Device(config-nd-inspection)# trusted-port`	Configures a port to become a trusted port.

Applying IPv6 ND Inspection on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd inspection** [**attach-policy** [**policy** *policy-name*] | **vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/0`	Specifies an interface type and number and enters interface configuration mode.
Step 4	**ipv6 nd inspection** [**attach-policy** [**policy** *policy-name*] | **vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]] **Example:** `Device(config-if)# ipv6 nd inspection`	Applies the ND Inspection feature on the interface.

Verifying and Troubleshooting IPv6 ND Inspection

SUMMARY STEPS

1. **enable**
2. **show ipv6 snooping capture-policy** [**interface** *type number*]
3. **show ipv6 snooping counter** [**interface** *type number*]
4. **show ipv6 snooping features**
5. **show ipv6 snooping policies** [**interface** *type number*]
6. **debug ipv6 snooping**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ipv6 snooping capture-policy** [**interface** *type number*] **Example:**	Displays snooping ND message capture policies.

	Command or Action	Purpose
	`Device# show ipv6 snooping capture-policy interface ethernet 0/0`	
Step 3	**show ipv6 snooping counter** [**interface** *type number*] **Example:** `Device# show ipv6 snooping counter interface FastEthernet 4/12`	Displays information about the packets counted by the interface counter.
Step 4	**show ipv6 snooping features** **Example:** `Device# show ipv6 snooping features`	Displays information about snooping features configured on the device.
Step 5	**show ipv6 snooping policies** [**interface** *type number*] **Example:** `Device# show ipv6 snooping policies`	Displays information about the configured policies and the interfaces to which they are attached.
Step 6	**debug ipv6 snooping** **Example:** `Device# debug ipv6 snooping`	Enables debugging for snooping information in IPv6.

Configuring IPv6 Device Tracking

Configuring IPv6 First-Hop Security Binding Table Recovery

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 neighbor binding vlan** *vlan-id* {**interface** *type number* | *ipv6-address* | *mac-address*} [**tracking** [**disable** | **enable** | **retry-interval** *value*] | **reachable-lifetime** *value*]
4. **ipv6 neighbor binding max-entries** *entries* [**vlan-limit** *number* | **interface-limit** *number* | **mac-limit** *number*]
5. **ipv6 neighbor binding logging**
6. **exit**
7. **show ipv6 neighbor binding** [**vlan** *vlan-id* | **interface** *type number* | **ipv6** *ipv6-address* | **mac** *mac-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 neighbor binding vlan** *vlan-id* {**interface** *type number* | *ipv6-address* | *mac-address*} [**tracking** [**disable** | **enable** | **retry-interval** *value*] | **reachable-lifetime** *value*] **Example:** `Device(config)# ipv6 neighbor binding vlan 100 interface Ethernet 0/0 reachable-lifetime 100`	Adds a static entry to the binding table database.
Step 4	**ipv6 neighbor binding max-entries** *entries* [**vlan-limit** *number* | **interface-limit** *number* | **mac-limit** *number*] **Example:** `Device(config)# ipv6 neighbor binding max-entries 100`	Specifies the maximum number of entries that are allowed to be inserted in the binding table cache.
Step 5	**ipv6 neighbor binding logging** **Example:** `Device(config)# ipv6 neighbor binding logging`	Enables the logging of binding table main events.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 7	**show ipv6 neighbor binding** [**vlan** *vlan-id* | **interface** *type number* | **ipv6** *ipv6-address* | **mac** *mac-address*] **Example:** `Device# show ipv6 neighbor binding`	Displays the contents of a binding table.

Configuring the IPv6 First-Hop Security Binding Table Recovery Mechanism

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 neighbor binding vlan** *vlan-id ipv6-address* **interface** *type number*
4. **ipv6 prefix-list** *list-name* **permit** *ipv6-prefix/prefix-length* **ge** *ge-value*

5. **ipv6 snooping policy** *snooping-policy-id*
6. **destination-glean** {**recovery** | **log-only**} [**dhcp**]
7. **protocol dhcp** [**prefix-list** *prefix-list-name*]
8. **exit**
9. **ipv6 destination-guard policy** *policy-name*
10. **enforcement** {**always** | **stressed**}
11. **exit**
12. **ipv6 dhcp guard policy** *policy-name*
13. **device-role server**
14. **exit**
15. **vlan configuration** *vlan-list-id*
16. **ipv6 snooping attach-policy** *policy-name*
17. **ipv6 destination-guard attach-policy** *policy-name*
18. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 neighbor binding vlan** *vlan-id ipv6-address* **interface** *type number* **Example:** `Device(config)# ipv6 neighbor binding vlan 100 2001:db8::1 interface ethernet3/0`	Adds a static entry to the binding table database.
Step 4	**ipv6 prefix-list** *list-name* **permit** *ipv6-prefix/prefix-length* **ge** *ge-value* **Example:** `Device(config)# ipv6 prefix-list abc permit 2001:DB8::/64 ge 128`	Creates an entry in an IPv6 prefix list.
Step 5	**ipv6 snooping policy** *snooping-policy-id* **Example:** `Device(config)# ipv6 snooping policy xyz`	Enters IPv6 snooping configuration mode and allows you to modify the configuration of the snooping policy specified.

	Command or Action	Purpose
Step 6	**destination-glean** {**recovery** | **log-only**} [**dhcp**] **Example:** `Device(config-ipv6-snooping)# destination-glean recovery dhcp`	Specifies that destination addresses should be recovered from DHCP. **Note** If logging (without recovery) is required, use the **destination-glean log-only** command.
Step 7	**protocol dhcp** [**prefix-list** *prefix-list-name*] **Example:** `Device(config-ipv6-snooping)# protocol dhcp prefix-list abc`	(Optional) Specifies that addresses should be gleaned with DHCP and associates the protocol with a specific IPv6 prefix list.
Step 8	**exit** **Example:** `Device(config-ipv6-snooping)# exit`	Exits IPv6 snooping configuration mode and returns to global configuration mode.
Step 9	**ipv6 destination-guard policy** *policy-name* **Example:** `Device(config)# ipv6 destination-guard policy xyz`	(Optional) Enters destination guard configuration mode and allows you to modify the configuration of the specified destination guard policy.
Step 10	**enforcement** {**always** | **stressed**} **Example:** `Device(config-destguard)# enforcement stressed`	Sets the enforcement level of the policy to be either enforced under all conditions or only when the system is under stress.
Step 11	**exit** **Example:** `Device(config-destguard)# exit`	Exits destination guard configuration mode and returns to global configuration mode.
Step 12	**ipv6 dhcp guard policy** *policy-name* **Example:** `Device(config)# ipv6 dhcp guard policy server_side`	Enters DHCP guard configuration mode and allows you to modify the configuration of the specified DHCP guard policy.
Step 13	**device-role server** **Example:** `Device(config-dhcp-guard)# device-role server`	Sets the role of the device that is attached to the server.
Step 14	**exit** **Example:** `Device(config-destguard)# exit`	Exits DHCP guard configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 15	**vlan configuration** *vlan-list-id* **Example:** `Device(config)# vlan configuration 100`	Enters VLAN configuration mode and allows you to modify the configuration of the specified VLAN.
Step 16	**ipv6 snooping attach-policy** *policy-name* **Example:** `Device(config-vlan-config)# ipv6 snooping attach-policy xyz`	Attaches the IPv6 snooping policy to a VLAN.
Step 17	**ipv6 destination-guard attach-policy** *policy-name* **Example:** `Device(config-vlan-config)# ipv6 destination-guard attach-policy xyz`	Attaches the destination guard policy to the specified VLAN. **Note** For information about how to configure an IPv6 destination guard policy, see the "IPv6 Destination Guard" module.
Step 18	**end** **Example:** `Device(config-vlan-config)# end`	Exits VLAN configuration mode and returns to privileged EXEC mode.

Configuring Address Gleaning and Associating Recovery Protocols with Prefix Lists

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *snooping-policy-id*
4. **protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ipv6 snooping policy** *snooping-policy-id* **Example:** `Device(config)# ipv6 snooping policy 200`	Enters IPv6 snooping configuration mode and allows you to modify the configuration of the snooping policy specified.
Step 4	**protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*] **Example:** `Device(config-ipv6-snooping)# protocol dhcp prefix-list dhcp_prefix_list`	Specifies that address should be gleaned with dynamic Host Configuration Protocol (DHCP) and associates a recovery protocol (DHCP) with the prefix list.
Step 5	**end** **Example:** `Device(config-ipv6-snooping)# end`	Exits IPv6 snooping configuration mode and returns to privileged EXEC mode.

Configuring IPv6 Device Tracking

Perform this task to provide fine tuning for the life cycle of an entry in the binding table for the IPv6 Device Tracking feature. For IPv6 device tracking to work, the binding table needs to be populated.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 neighbor tracking** [**retry-interval** *value*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 neighbor tracking** [**retry-interval** *value*] **Example:** `Device(config)# ipv6 neighbor tracking`	Tracks entries in the binding table.

Configuring IPv6 Prefix Glean

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *snooping-policy*
4. **prefix-glean** [**only**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 snooping policy** *snooping-policy* **Example:** `Device(config)# ipv6 snooping policy policy1`	Configures an IPv6 snooping policy and enters IPv6 snooping policy configuration mode.
Step 4	**prefix-glean** [**only**] **Example:** `Device(config-ipv6-snooping)# prefix-glean`	Enables the device to glean prefixes from IPv6 RAs or DHCPv6 traffic.

Configuration Examples for IPv6 Snooping

Example: Configuring IPv6 ND Inspection

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# ipv6 snooping attach-policy policy1
Device(config-ipv6-snooping)# exit
.
.
.
Device# show ipv6 snooping policies policy1
Policy policy1 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
```

Example: Configuring IPv6 ND Inspection and RA Guard

This example provides information about an interface on which both the Neighbor Discovery Inspection and RA Guard features are configured:

```
Device# show ipv6 snooping capture-policy interface ethernet 0/0

Hardware policy registered on Ethernet 0/0
Protocol     Protocol value   Message   Value     Action    Feature
ICMP         58               RS        85        punt      RA Guard
                                                  punt      ND Inspection
ICMP         58               RA        86        drop      RA guard
                                                  punt      ND Inspection
ICMP         58               NS        87        punt      ND Inspection
ICM          58               NA        88        punt      ND Inspection
ICMP         58               REDIR     89        drop      RA Guard
                                                  punt      ND Inspection
```

Example: Configuring IPv6 Binding Table Content

```
ipv6 neighbor binding vlan 100 ethernet 0/0 reachable-entries 100
 ipv6 neighbor binding max-entries 100
 ipv6 neighbor binding logging
 exit
```

Example: Configuring IPv6 First-Hop Security Binding Table Recovery

```
ipv6 dhcp-client leasequery server 2001:db8::1 vlan 100
ipv6 neighbor binding vlan 100 2001:db8::1 interface ethernet3/0

ipv6 prefix-list abc permit 2001:DB8::/64 ge 128
ipv6 snooping policy xyz
destination-glean recovery dhcp
protocol dhcp prefix-list abc
 ipv6 destination-guard policy xyz
 exit

ipv6 dhcp guard policy server_side
 device-role server

vlan configuration 100
 ipv6 snooping attach-policy xyz
 ipv6 destination-guard attach-policy xyz

interface ethernet3/0
 switchport
 switchport access vlan 100
 switchport mode access
 duplex auto
 ipv6 dhcp guard attach-policy server_side
```

```
interface vlan100
 no ip address
 ipv6 address 2001:DB8::100/64
```

Example: Configuring Address Gleaning and Associating Recovery Protocols with Prefix Lists

The following example shows that NDP will be used for the recovery for all addresses and that DHCP will be used to recover addresses that match the prefix list called dhcp_prefix_list:

```
Device(config-ipv6-snooping)# protocol ndp
Device(config-ipv6-snooping)# protocol dhcp prefix-list dhcp_prefix_list
```

Example: Verifying IPv6 Device Tracking

```
Device# show ipv6 neighbor

    IPv6 address               Link-Layer addr Interface vlan prlvl age   state      Time
left
ND  FE80::A8BB:CCFF:FE01:F500  AABB.CC01.F500  Et0/0     100  0002    0   REACHABLE  8850
L   FE80::21D:71FF:FE99:4900   001D.7199.4900  Vl100     100  0080 7203   DOWN       N/A
ND  2001:600::1                AABB.CC01.F500  Et0/0     100  0003    0   REACHABLE  3181
ND  2001:300::1                AABB.CC01.F500  Et0/0     100  0007    0   REACHABLE  9559
L   2001:400::1                001D.7199.4900  Vl100     100  0080 7188   DOWN       N/A
```

Additional References for IPv6 Source Guard and Prefix Guard

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
IPv4 addressing	*IP Addressing: IPv4 Addressing Configuration Guide*
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

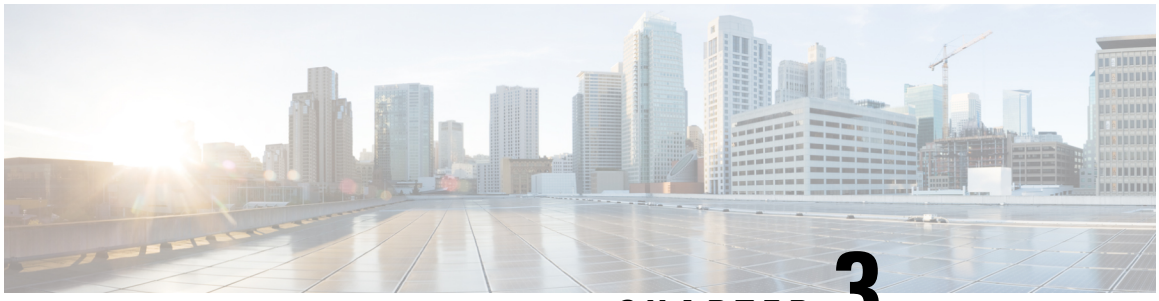
Feature Information for IPv6 Snooping

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for IPv6 Snooping

Feature Name	Releases	Feature Information
IPv6 Snooping	12.2(50)SY 15.0(1)SY 15.0(2)SE 15.1(2)SG 15.3(1)S Cisco IOS XE Release 3.2SE Cisco IOS XE Release 3.8S Cisco IOS Release 15.2(1)E	IPv6 snooping bundles several Layer 2 IPv6 first-hop security features, including IPv6 ND inspection, IPv6 device tracking, IPv6 address glean, and IPv6 first-hop security binding table recovery, to provide security and scalability. IPv6 snooping operates at Layer 2, or between Layer 2 and Layer 3, to provide IPv6 functions with security and scalability. The following commands were introduced or modified: **data-glean**, **debug ipv6 snooping**, **destination-glean**, **device-role**, **drop-unsecure**, **ipv6 nd inspection**, **ipv6 nd inspection policy**, **ipv6 neighbor binding logging**, **ipv6 neighbor binding max-entries**, **ipv6 neighbor binding vlan**, **ipv6 neighbor tracking**, **ipv6 snooping attach-policy**, **ipv6 snooping policy**, **prefix-glean**, **protocol (IPv6)**, **sec-level minimum**, **show ipv6 neighbor binding**, **show ipv6 snooping capture-policy**, **show ipv6 snooping counters**, **show ipv6 snooping features**, **show ipv6 snooping policies**, **tracking**, **trusted-port**.



CHAPTER 3

DHCP—DHCPv6 Guard

This module describes the Dynamic Host Configuration Protocol version 6 (DHCPv6) Guard feature. This feature blocks DHCP reply and advertisement messages that originate from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked. The filtering decision is determined by the device role assigned to the receiving switch port, trunk, or VLAN. In addition, to provide a finer level of filter granularity, messages can be filtered based on the address of the sending server or relay agent, or by the prefixes and addresses ranges listed in the reply message. This functionality helps to prevent traffic redirection or denial of service (DoS).

- Finding Feature Information, on page 27
- Restrictions for DHCPv6 Guard, on page 27
- Information About DHCPv6 Guard, on page 28
- How to Configure DHCPv6 Guard, on page 28
- Configuration Examples for DHCPv6 Guard, on page 31
- Additional References, on page 31
- Feature Information for DHCP—DHCPv6 Guard, on page 32

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for DHCPv6 Guard

- The DHCPv6 guard feature is not supported on Etherchannel ports.

Information About DHCPv6 Guard

DHCPv6 Guard Overview

The DHCPv6 Guard feature blocks reply and advertisement messages that come from unauthorized DHCP servers and relay agents.

Packets are classified into one of the three DHCP type messages. All client messages are always switched regardless of device role. DHCP server messages are only processed further if the device role is set to server. Further processing of server messages includes DHCP server advertisements (for source validation and server preference) and DHCP server replies (for permitted prefixes).

If the device is configured as a DHCP server, all the messages need to be switched, regardless of the device role configuration.

How to Configure DHCPv6 Guard

Configuring DHCP—DHCPv6 Guard

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit host** *address* **any**
5. **exit**
6. **ipv6 prefix-list** *list-name* **permit** *ipv6-prefix* **128**
7. **ipv6 dhcp guard policy** *policy-name*
8. **device-role** {**client** | **server**}
9. **match server access-list** *ipv6-access-list-name*
10. **match reply prefix-list** *ipv6-prefix-list-name*
11. **preference min** *limit*
12. **preference max** *limit*
13. **trusted-port**
14. **exit**
15. **interface** *type number*
16. **switchport**
17. **exit**
18. **exit**
19. **show ipv6 dhcp guard policy** [*policy-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 access-list** *access-list-name* **Example:** `Device(config)# ipv6 access-list acl1`	Defines the IPv6 access list and enters IPv6 access list configuration mode.
Step 4	**permit host** *address* **any** **Example:** `Device(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any`	Sets the conditions in the named IP access list.
Step 5	**exit** **Example:** `Device(config-ipv6-acl)# exit`	Exits IPv6 access list configuration mode and returns to global configuration mode.
Step 6	**ipv6 prefix-list** *list-name* **permit** *ipv6-prefix* **128** **Example:** `Device(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128`	Creates an entry in an IPv6 prefix list.
Step 7	**ipv6 dhcp guard policy** *policy-name* **Example:** `Device(config)# ipv6 dhcp guard policy pol1`	Defines the DHCPv6 guard policy name and enters DHCP guard configuration mode.
Step 8	**device-role** {**client** | **server**} **Example:** `Device(config-dhcp-guard)# device-role server`	Specifies the device role of the device attached to the target (interface or VLAN).
Step 9	**match server access-list** *ipv6-access-list-name* **Example:**	(Optional) Enables verification of the advertised DHCP server and relay address in inspected messages from the configured authorized server access list. If not configured,

	Command or Action	Purpose
	`Device(config-dhcp-guard)# match server access-list acl1`	this check will be bypassed. An empty access list is treated as a permit.
Step 10	**match reply prefix-list** *ipv6-prefix-list-name* **Example:** `Device(config-dhcp-guard)# match reply prefix-list abc`	(Optional) Enables verification of the advertised prefixes in DHCP reply messages from the configured authorized prefix list. If not configured, this check will be bypassed. An empty prefix list is treated as a permit.
Step 11	**preference min** *limit* **Example:** `Device(config-dhcp-guard)# preference min 0`	(Optional) Enables verification that the advertised preference (in preference option) is greater than the specified limit. If not specified, this check will be bypassed.
Step 12	**preference max** *limit* **Example:** `Device(config-dhcp-guard)# preference max 255`	(Optional) Enables verification that the advertised preference (in preference option) is less than the specified limit. If not specified, this check will be bypassed.
Step 13	**trusted-port** **Example:** `Device(config-dhcp-guard)# trusted-port`	(Optional) Specifies that this policy is being applied to trusted ports. All DHCP guard policing will be disabled.
Step 14	**exit** **Example:** `Device(config-dhcp-guard)# exit`	Exits DHCP guard configuration mode and returns to global configuration mode.
Step 15	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/2/0`	Specifies an interface and enters interface configuration mode.
Step 16	**switchport** **Example:** `Device(config-if)# switchport`	Puts an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 17	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 18	**exit** **Example:**	Exits global configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config)# exit`	
Step 19	**show ipv6 dhcp guard policy** [*policy-name*] **Example:** `Device# show ipv6 dhcp policy guard pol1`	(Optional) Displays the policy configuration as well as all the interfaces where the policy is applied.

Configuration Examples for DHCPv6 Guard

Example: Configuring DHCP—DHCPv6 Guard

The following example displays a sample configuration for DHCPv6 Guard:

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
DHCP conceptual and configuration information	*Cisco IOS IP Addressing Services Configuration Guide*

Standards/RFCs

Standard	Title
No new or modified standards/RFCs are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

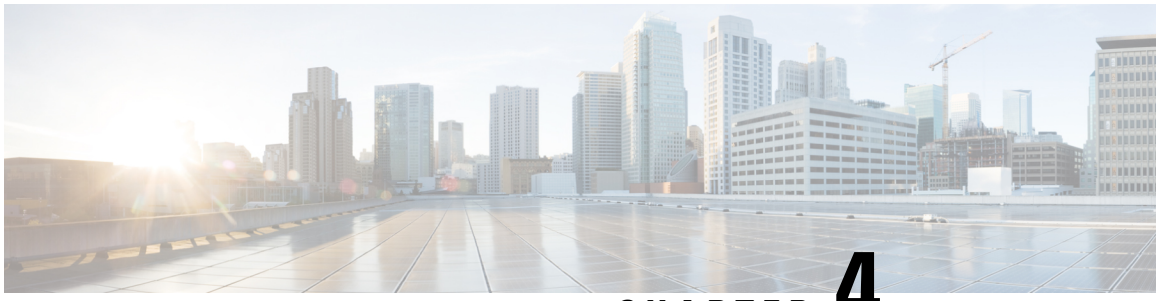
Feature Information for DHCP—DHCPv6 Guard

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for DHCP—DHCPv6 Guard

Feature Name	Releases	Feature Information
DHCP—DHCPv6 Guard		The DHCP—DHCPv6 Guard feature blocks DHCP reply and advertisement messages that originate from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked. The following commands were introduced or modified: **device-role** , **ipv6 dhcp guard attach-policy (DHCPv6 Guard)**, **ipv6 dhcp guard policy**, **match reply prefix-list**, **match server access-list**, **preference (DHCPv6 Guard)**, **show ipv6 dhcp guard policy**, **trusted-port (DHCPv6 Guard)**.



CHAPTER 4

IPv6 Source Guard and Prefix Guard

IPv6 Source Guard and IPv6 Prefix Guard are Layer 2 snooping features that validate the source of IPv6 traffic. IPv6 Source Guard blocks any data traffic from an unknown source. For example, one that is not already populated in the binding table or previously learned through Neighbor Discovery (ND) or Dynamic Host Configuration Protocol (DHCP) gleaning. IPv6 Prefix Guard prevents home-node sourcing traffic outside of the authorized and delegated traffic.

- Finding Feature Information, on page 33
- Information about IPv6 Source Guard and Prefix Guard, on page 33
- How to Configure IPv6 Source Guard and Prefix Guard, on page 35
- Configuration Examples for IPv6 Source Guard and Prefix Guard, on page 39
- Additional References for IPv6 Source Guard and Prefix Guard, on page 39
- Feature Information for IPv6 Source Guard and Prefix Guard, on page 40

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information about IPv6 Source Guard and Prefix Guard

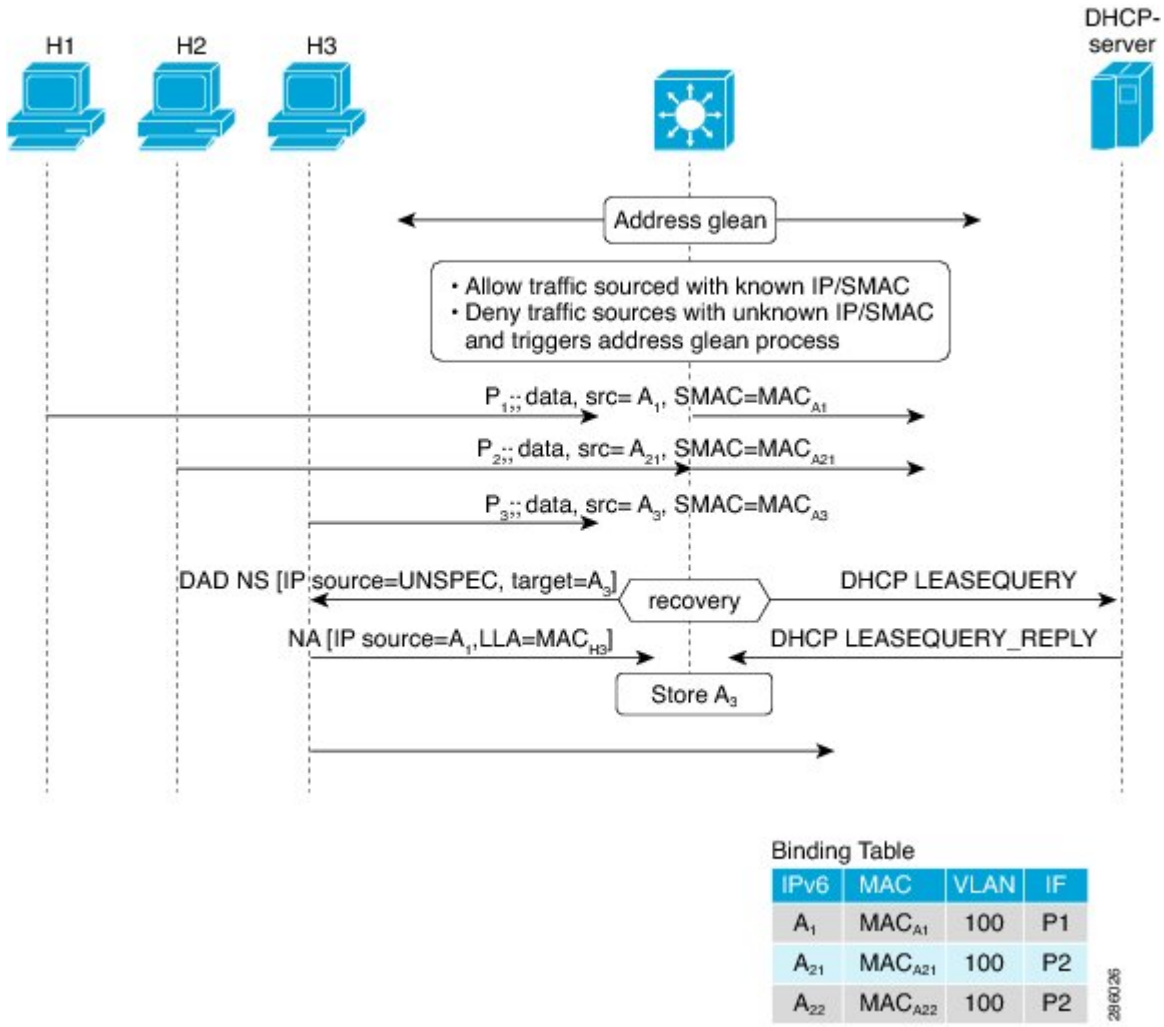
IPv6 Source Guard Overview

IPv6 source guard is an interface feature between the populated binding table and data traffic filtering. This feature enables the device to deny traffic when it is originated from an address that is not stored in the binding table. IPv6 source guard does not inspect ND or DHCP packets; rather, it works in conjunction with IPv6 neighbor discovery (ND) inspection or IPv6 address glean, both of which detect existing addresses on the link and store them into the binding table. IPv6 source guard is an interface between the populated binding table and data traffic filtering, and the binding table must be populated with IPv6 prefixes for IPv6 source guard to work.

IPv6 source guard can deny traffic from unknown sources or unallocated addresses, such as traffic from sources not assigned by a DHCP server. When traffic is denied, the IPv6 address glean feature is notified so that it can try to recover the traffic by querying the DHCP server or by using IPv6 ND. The data-glean function prevents the device and end user from getting deadlocked, whereupon a valid address fails to be stored into the binding table, there is no recovery path, and the end user is unable to connect.

The following illustration provides an overview of how IPv6 source guard works with IPv6 address glean.

Figure 2: IPv6 Source Guard and Address Glean Overview



IPv6 Prefix Guard Overview

The IPv6 Prefix Guard feature works within the IPv6 Source Guard feature, enabling the device to deny traffic originated from nontopologically correct addresses. IPv6 prefix guard is often used when IPv6 prefixes are delegated to devices (for example, home gateways) using DHCP prefix delegation. The feature discovers ranges of addresses assigned to the link and blocks any traffic sourced with an address outside this range.

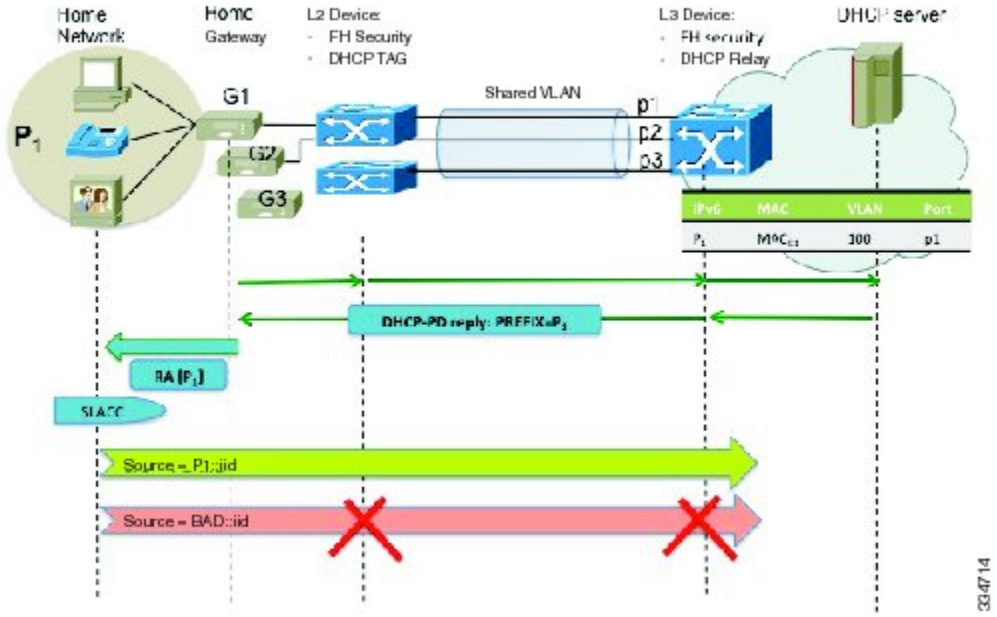
To determine which prefixes should be allowed and which prefixes should be blocked, IPv6 prefix guard uses the following:

- Prefix glean in Router Advertisements (RAs)
- Prefix glean in DHCP prefix delegation
- Static configuration

Whenever a prefix is to be allowed, IPv6 prefix guard downloads it to the hardware table. Whenever a packet is switched, the hardware matches the source of the packet against this table and drops the packet if no match is found.

The following figure shows a service provider (SP) scenario in which prefixes are gleaned in DHCP-PD messages.

Figure 3: Prefixes Gleaned in DHCP-PD Messages Scenario



How to Configure IPv6 Source Guard and Prefix Guard

Configuring IPv6 Source Guard

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **ipv6 source-guard policy** *snooping-policy*
4. **permit link-local**
5. **deny global-autoconfig**
6. trusted
7. **exit**
8. **show ipv6 source-guard policy** [*snooping-policy*]

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **ipv6 source-guard policy** *snooping-policy*

Example:

```
Device(config)# ipv6 source-guard policy
```

Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.

Step 4 **permit link-local**

Example:

```
Device(config-source-guard)# permit link-local
```

Allows hardware bridging for all data traffic sourced by a link-local address.

Step 5 **deny global-autoconfig**

Example:

```
Device(config-source-guard)# deny global-autoconfig
```

Denies data traffic from auto-configured global addresses.

Step 6 trusted

Example:

```
trusted
```

Step 7 **exit**

Example:

```
Device(config-if)# exit
```

Exits source-guard policy configuration mode and places the device in privileged EXEC mode.

Step 8 **show ipv6 source-guard policy** [*snooping-policy*]

Displays the IPv6 source-guard policy configuration.

Configuring IPv6 Source Guard on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 source-guard attach-policy** *source-guard-policy*
5. **exit**
6. **show ipv6 source-guard policy** *source-guard-policy*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface fastethernet 3/13`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 source-guard attach-policy** *source-guard-policy* **Example:** `Device(config-if)# ipv6 source-guard attach-policy my_source_guard_policy`	Applies IPv6 source guard on an interface.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and places the device in privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show ipv6 source-guard policy** *source-guard-policy* **Example:** `Device# show ipv6 source-guard policy policy1`	Displays all the interfaces on which IPv6 source guard is applied.

Configuring IPv6 Prefix Guard

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 source-guard policy** *snooping-policy*
4. **validate address**
5. **validate prefix**
6. **exit**
7. **show ipv6 source-guard policy** [*snooping-policy*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 source-guard policy** *snooping-policy* **Example:** `Device(config)# ipv6 source-guard policy`	Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.
Step 4	**validate address** **Example:** `Device(config-source-guard)# no validate address`	Disables the validate address feature and enables the IPv6 prefix guard feature to be configured.
Step 5	**validate prefix** **Example:** `Device(config-source-guard)# validate prefix`	Enables IPv6 source guard to perform the IPv6 prefix-guard operation.
Step 6	**exit** **Example:**	Exits source-guard policy configuration mode and places the device in privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-if)# exit`	
Step 7	**show ipv6 source-guard policy** [*snooping-policy*]	Displays the IPv6 source-guard policy configuration.

Configuration Examples for IPv6 Source Guard and Prefix Guard

Example: Configuring IPv6 Source Guard and Prefix Guard

```
Device# ipv6 source-guard policy policy1

Policy guard configuration:
  validate prefix
  validate address
```

Additional References for IPv6 Source Guard and Prefix Guard

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
IPv4 addressing	*IP Addressing: IPv4 Addressing Configuration Guide*
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

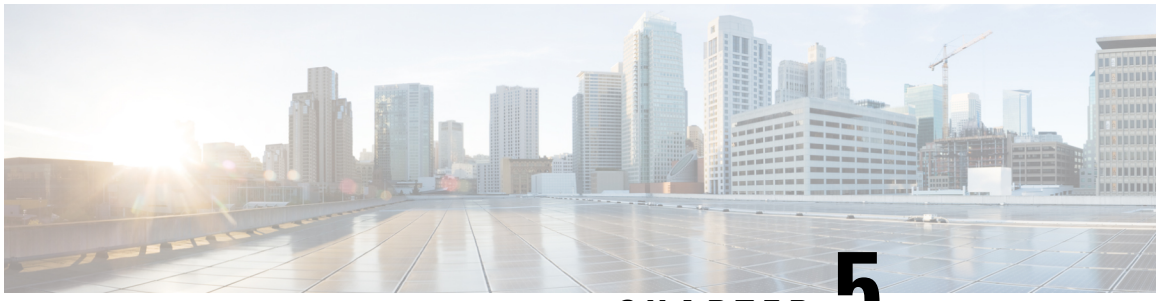
Feature Information for IPv6 Source Guard and Prefix Guard

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for IPv6 Source Guard and Prefix Guard

Feature Name	Releases	Feature Information
IPv6 Prefix Guard	15.3(1)S	The IPv6 Prefix Guard feature enables a device to deny traffic originated from nontopologically correct addresses. The following commands were introduced or modified: **ipv6 source-guard policy**, **permit link-local**, **show ipv6 source-guard policy**, **validate address**, **validate prefix**.
IPv6 Source Guard	15.0(2)SE 15.3(1)S IOS XE 3.6.0E, IOS 15.2(2)E	The IPv6 source guard feature blocks any data traffic sourced from an unknown source. For example, one that is not already populated in the binding table or previously learned through ND or DHCP gleaning. The following commands were introduced or modified: **deny global-autoconfig**, **ipv6 source-guard attach-policy**, **ipv6 source-guard policy**, **permit link-local**, **show ipv6 source-guard policy**, **trusted**.



CHAPTER 5

IPv6 Destination Guard

The IPv6 Destination Guard feature works with IPv6 neighbor discovery to ensure that the device performs address resolution only for those addresses that are known to be active on the link. It relies on the address glean functionality to populate all destinations active on the link into the binding table and then blocks resolutions before they happen when the destination is not found in the binding table.

- Finding Feature Information, on page 41
- Prerequisites for IPv6 Destination Guard, on page 41
- Information About IPv6 Destination Guard, on page 42
- How to Configure the IPv6 Destination Guard, on page 42
- Configuration Examples for IPv6 Destination Guard, on page 43
- Additional References, on page 44
- Feature Information for IPv6 Destination Guard, on page 44

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IPv6 Destination Guard

- You should be familiar with the IPv6 Neighbor Discovery feature. For information about IPv6 neighbor discovery, see the “Implementing IPv6 Addressing and Basic Connectivity” module.
- You should be familiar with the IPv6 First-Hop Security Binding Table feature. For information, see the “IPv6 First-Hop Security Binding Table” module.

Information About IPv6 Destination Guard

IPv6 Destination Guard Overview

The IPv6 Destination Guard feature works with IPv6 neighbor discovery to ensure that the device performs address resolution only for those addresses that are known to be active on the link. It relies on the address glean functionality to populate all destinations active on the link into the binding table and then blocks resolutions before they happen when the destination is not found in the binding table.

Prior to filtering incoming routed traffic, the device gleans addresses on the link, by snooping Neighbor Discovery Protocol (NDP) and DHCP messages. When a packet reaches the device and there is not yet an adjacency for the destination or for the next hop, the NDP consults the device binding table to verify that the destination on link or the next-hop have been previously gleaned. If the destination is not found in the binding table, the packet is dropped. Otherwise, neighbor discovery resolution is performed.

How to Configure the IPv6 Destination Guard

Configuring IPv6 Destination Guard

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 destination-guard policy** *policy-name*
4. **enforcement** {**always** | **stressed**}
5. **exit**
6. **vlan configuration** *vlan-list*
7. **ipv6 destination-guard attach-policy** [*policy-name*]
8. **exit**
9. **show ipv6 destination-guard policy** [*policy-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ipv6 destination-guard policy** *policy-name* **Example:** `Device(config)# ipv6 destination-guard policy pol1`	Defines the destination guard policy name and enters destination-guard configuration mode.
Step 4	**enforcement** {**always** | **stressed**} **Example:** `Device(config-destguard)# enforcement always`	Sets the enforcement level for the target address.
Step 5	**exit** **Example:** `Device(config-destguard)# exit`	Exits destination-guard configuration mode and returns to global configuration mode.
Step 6	**vlan configuration** *vlan-list* **Example:** `Device(config)# vlan configuration 1`	Enters VLAN configuration mode.
Step 7	**ipv6 destination-guard attach-policy** [*policy-name*] **Example:** `Device(config-vlan-config)# ipv6 destination-guard attach-policy pol1`	Attaches a destination guard policy to a VLAN.
Step 8	**exit** **Example:** `Device(config-vlan-config)# end`	Exits VLAN configuration mode and rreturns to privileged EXEC configuration mode.
Step 9	**show ipv6 destination-guard policy** [*policy-name*] **Example:** `Device# show ipv6 destination-guard policy pol1`	(Optional) Displays the policy configuration and all interfaces where the policy is applied.

Configuration Examples for IPv6 Destination Guard

Example: Configuring an IPv6 Destination Guard Policy

The following example shows how to configure a destination guard policy:

```
Router> enable
```

```
Router# configure terminal
Router(config)# vlan configuration 300
Router(config-vlan-config)# ipv6 destination-guard attach-policy destination
% Warning - 'ipv6 snooping' should be configured before destination-guard


Router(config-vlan-config)# ipv6 snooping attach-policy ND
Router(config)# vlan configuration 300
Router(config-vlan-config)# ipv6 destination-guard attach-policy destination
Router(config-vlan-config)#

Router# show ipv6 destination-guard policy destination
Destination guard policy Destination:
  enforcement always
        Target: vlan 300
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

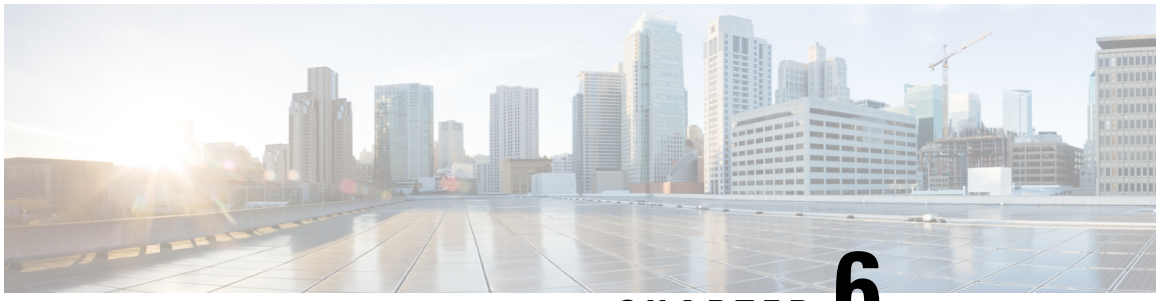
Feature Information for IPv6 Destination Guard

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for IPv6 Destination Guard

Feature Name	Releases	Feature Information
IPv6 Destination Guard	15.2(4)S 15.1(2)SG IOS XE 3.6.0E, IOS 15.2(2)E	The IPv6 Destination Guard feature blocks data traffic from an unknown source and filters IPv6 traffic based on the destination address. The following commands were introduced or modified: **enforcement**, **ipv6 destination-guard attach-policy**, **ipv6 destination-guard policy**, **show ipv6 destination-guard policy**.



CHAPTER 6

IPv6 RFCs

Standards and RFCs

RFCs	Title
RFC 1195	*Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
RFC 1267	*A Border Gateway Protocol 3 (BGP-3)*
RFC 1305	*Network Time Protocol (Version 3) Specification, Implementation and Analysis*
RFC 1583	*OSPF version 2*
RFC 1772	*Application of the Border Gateway Protocol in the Internet*
RFC 1886	*DNS Extensions to Support IP version 6*
RFC 1918	*Address Allocation for Private Internets*
RFC 1981	*Path MTU Discovery for IP version 6*
RFC 2080	*RIPng for IPv6*
RFC 2281	*Cisco Hot Standby Router Protocol (HSRP)*
RFC 2332	*NBMA Next Hop Resolution Protocol (NHRP)*
RFC 2373	*IP Version 6 Addressing Architecture*
RFC 2374	*An Aggregatable Global Unicast Address Format*
RFC 2375	*IPv6 Multicast Address Assignments*
RFC 2401	*Security Architecture for the Internet Protocol*
RFC 2402	*IP Authentication Header*
RFC 2404	*The Use of Hash Message Authentication Code Federal Information Processing Standard 180-1 within Encapsulating Security Payload and Authentication Header*
RFC 2406	*IP Encapsulating Security Payload (ESP)*

RFCs	Title
RFC 2407	*The Internet Security Domain of Interpretation for ISAKMP*
RFC 2408	*Internet Security Association and Key Management Protocol*
RFC 2409	*Internet Key Exchange (IKE)*
RFC 2427	*Multiprotocol Interconnect over Frame Relay*
RFC 2428	*FTP Extensions for IPv6 and NATs*
RFC 2460	*Internet Protocol, Version 6 (IPv6) Specification*
RFC 2461	*Neighbor Discovery for IP Version 6 (IPv6)*
RFC 2462	*IPv6 Stateless Address Autoconfiguration*
RFC 2463	*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
RFC 2464	*Transmission of IPv6 Packets over Ethernet*
RFC 2467	*Transmission of IPv6 Packets over FDDI*
RFC 2472	*IP Version 6 over PPP*
RFC 2473	*Generic Packet Tunneling in IPv6 Specification*
RFC 2474	*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
RFC 2475	*An Architecture for Differentiated Services Framework*
RFC 2492	*IPv6 over ATM*
RFC 2545	*Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
RFC 2590	*Transmission of IPv6 Packets over Frame Relay Specification*
RFC 2597	*Assured Forwarding PHB*
RFC 2598	*An Expedited Forwarding PHB*
RFC 2640	*Internet Protocol, Version 6 Specification*
RFC 2684	*Multiprotocol Encapsulation over ATM Adaptation Layer 5*
RFC 2697	*A Single Rate Three Color Marker*
RFC 2698	*A Two Rate Three Color Marker*
RFC 2710	*Multicast Listener Discovery (MLD) for IPv6*
RFC 2711	*IPv6 Router Alert Option*
RFC 2732	*Format for Literal IPv6 Addresses in URLs*

RFCs	Title
RFC 2765	*Stateless IP/ICMP Translation Algorithm (SIIT)*
RFC 2766	*Network Address Translation-Protocol Translation (NAT-PT)*
RFC 2858	*Multiprotocol Extensions for BGP-4*
RFC 2893	*Transition Mechanisms for IPv6 Hosts and Routers*
RFC 3056	*Connection of IPv6 Domains via IPv4 Clouds*
RFC 3068	*An Anycast Prefix for 6to4 Relay Routers*
RFC 3095	*RObust Header Compression (ROHC): Framework and Four Profiles: RTP, UDP, ESP, and Uncompressed*
RFC 3107	*Carrying Label Information in BGP-4*
RFC 3137	*OSPF Stub Router Advertisement*
RFC 3147	*Generic Routing Encapsulation over CLNS*
RFC 3152	*Delegation of IP6.ARPA*
RFC 3162	*RADIUS and IPv6*
RFC 3315	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
RFC 3319	*Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiated Protocol (SIP) Servers*
RFC 3392	*Capabilities Advertisement with BGP-4*
RFC 3414	*User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
RFC 3484	*Default Address Selection for Internet Protocol version 6 (IPv6)*
RFC 3513	*Internet Protocol Version 6 (IPv6) Addressing Architecture*
RFC 3576	*Change of Authorization*
RFC 3587	*IPv6 Global Unicast Address Format*
RFC 3590	*Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*
RFC 3596	*DNS Extensions to Support IP Version 6*
RFC 3633	*DHCP IPv6 Prefix Delegation*
RFC 3646	*DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
RFC 3697	*IPv6 Flow Label Specification*
RFC 3736	*Stateless DHCP Service for IPv6*

RFCs	Title
RFC 3756	*IPv6 Neighbor Discovery (ND) Trust Models and Threats*
RFC 3759	*RObust Header Compression (ROHC): Terminology and Channel Mapping Examples*
RFC 3775	*Mobility Support in IPv6*
RFC 3810	*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
RFC 3846	*Mobile IPv4 Extension for Carrying Network Access Identifiers*
RFC 3879	*Deprecating Site Local Addresses*
RFC 3898	*Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
RFC 3954	*Cisco Systems NetFlow Services Export Version 9*
RFC 3956	*Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*
RFC 3963	*Network Mobility (NEMO) Basic Support Protocol*
RFC 3971	*SEcure Neighbor Discovery (SEND)*
RFC 3972	*Cryptographically Generated Addresses (CGA)*
RFC 4007	*IPv6 Scoped Address Architecture*
RFC 4075	*Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6*
RFC 4087	*IP Tunnel MIB*
RFC 4091	*The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework*
RFC 4092	*Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)*
RFC 4109	*Algorithms for Internet Key Exchange version 1 (IKEv1)*
RFC 4191	*Default Router Preferences and More-Specific Routes*
RFC 4193	*Unique Local IPv6 Unicast Addresses*
RFC 4214	*Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*
RFC 4242	*Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
RFC 4282	*The Network Access Identifier*
RFC 4283	*Mobile Node Identifier Option for Mobile IPv6*
RFC 4285	*Authentication Protocol for Mobile IPv6*
RFC 4291	*IP Version 6 Addressing Architecture*

RFCs	Title
RFC 4292	*IP Forwarding Table MIB*
RFC 4293	*Management Information Base for the Internet Protocol (IP)*
RFC 4302	*IP Authentication Header*
RFC 4306	*Internet Key Exchange (IKEv2) Protocol*
RFC 4308	*Cryptographic Suites for IPsec*
RFC 4364	*BGP MPLS/IP Virtual Private Networks (VPNs)*
RFC 4382	*MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base*
RFC 4443	*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
RFC 4552	*Authentication/Confidentiality for OSPFv3*
RFC 4594	*Configuration Guidelines for DiffServ Service Classes*
RFC 4601	*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification*
RFC 4610	*Anycast-RP Using Protocol Independent Multicast (PIM)*
RFC 4649	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*
RFC 4659	*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
RFC 4724	*Graceful Restart Mechanism for BGP*
RFC 4798	*Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*
RFC 4818	*RADIUS Delegated-IPv6-Prefix Attribute*
RFC 4861	*Neighbor Discovery for IP version 6 (IPv6)*
RFC 4862	*IPv6 Stateless Address Autoconfiguration*
RFC 4884	*Extended ICMP to Support Multi-Part Messages*
RFC 4885	*Network Mobility Support Terminology*
RFC 4887	*Network Mobility Home Network Models*
RFC 5015	*Bidirectional Protocol Independent Multicast (BIDIR-PIM)*
RFC 5059	*Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*
RFC 5072	*IPv6 over PPP*
RFC 5095	*Deprecation of Type 0 Routing Headers in IPv6*
RFC 5120	*M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*

RFCs	Title
RFC 5130	*A Policy Control Mechanism in IS-IS Using Administrative Tags*
RFC 5187	*OSPFv3 Graceful Restart*
RFC 5213	*Proxy Mobile IPv6*
RFC 5308	*Routing IPv6 with IS-IS*
RFC 5340	*OSPF for IPv6*
RFC 5460	*DHCPv6 Bulk Leasequery*
RFC 5643	*Management Information Base for OSPFv3*
RFC 5838	*Support of Address Families in OSPFv3*
RFC 5844	*IPv4 Support for Proxy Mobile IPv6*
RFC 5845	*Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6*
RFC 5846	*Binding Revocation for IPv6 Mobility*
RFC 5881	*Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)*
RFC 5905	*Network Time Protocol Version 4: Protocol and Algorithms Specification*
RFC 5969	*IPv6 Rapid Deployment on IPv4 Infrastructures (6RD) -- Protocol Specification*
RFC 6105	*IPv6 Router Advertisement Guard*
RFC 6620	*FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses*