



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, page 1](#)
- [Restrictions for IPv6 Snooping, page 1](#)
- [Information About IPv6 Snooping, page 2](#)
- [How to Configure IPv6 Snooping, page 5](#)
- [Configuration Examples for IPv6 Snooping, page 14](#)
- [Additional References for IPv6 Source Guard and Prefix Guard, page 15](#)
- [Feature Information for IPv6 Snooping, page 16](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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 Snooping

The IPv6 Snooping feature bundles several Layer 2 IPv6 first-hop security features, including IPv6 Address Glean and IPv6 Device Tracking. The feature 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 Snooping 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.

When IPv6 Snooping 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 Snooping 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 snooping entry point. This entry point is the last to be called, so any decision (such as drop) made by another feature supersedes the IPv6 Snooping decision.

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

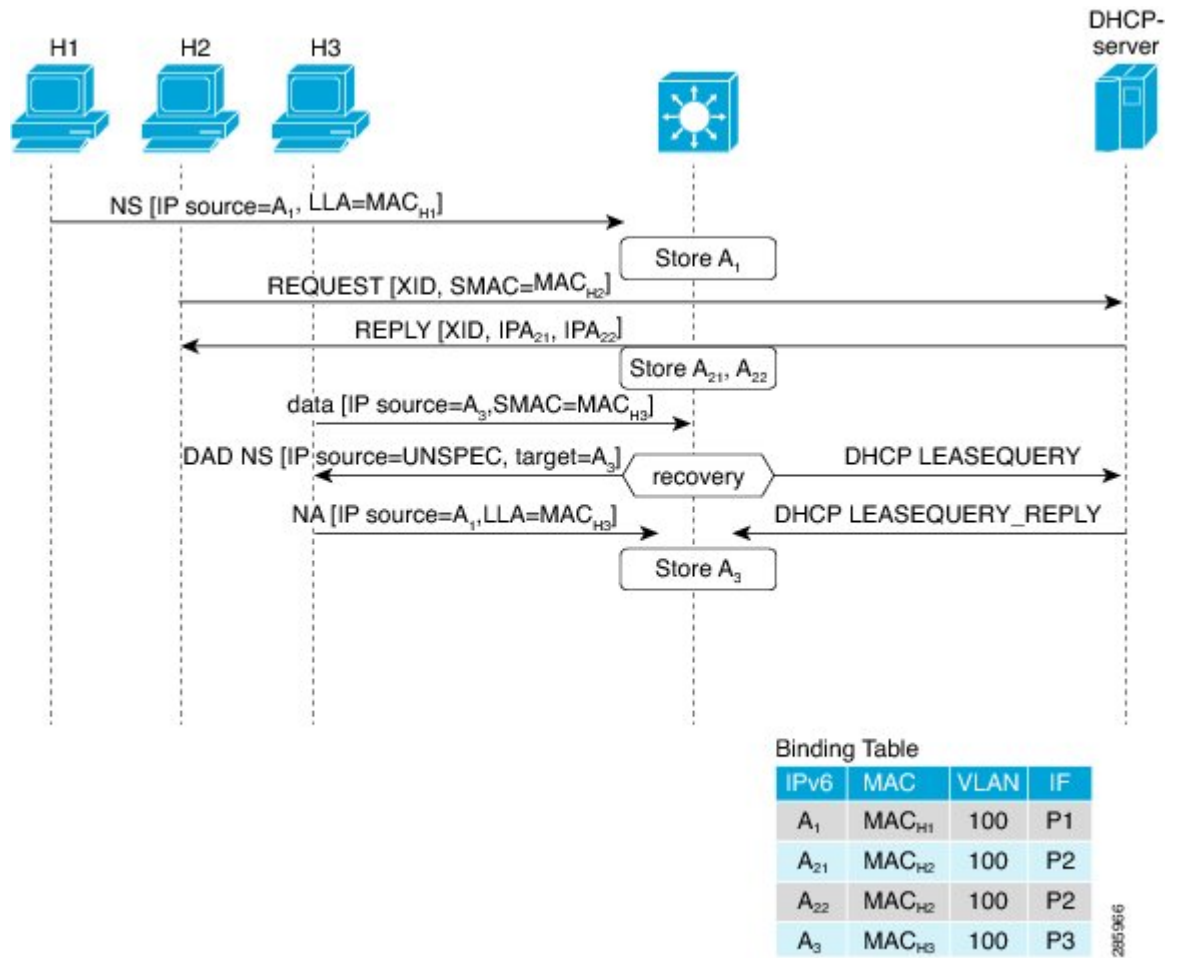
IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

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 Snooping on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy *snooping-policy***
4. **exit**
5. **interface *type number***
6. **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 <i>snooping-policy</i> Example: Device(config)# ipv6 snooping policy policy1	Configures an IPv6 snooping policy and enters IPv6 snooping configuration mode.
Step 4	exit Example: Device(config-ipv6-snooping)# exit	Exits IPv6 snooping configuration mode.
Step 5	interface <i>type number</i> Example: Device(config)# interface Gigabitethernet 0/0/1	Enters interface configuration mode.

	Command or Action	Purpose
Step 6	ipv6 snooping attach-policy <i>snooping-policy</i> Example: Device(config-if)# ipv6 snooping attach-policy policy1	Attaches the IPv6 snooping policy to 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: Device# show ipv6 snooping capture-policy interface ethernet 0/0	Displays snooping ND message capture policies.
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.

	Command or Action	Purpose
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 Content

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ipv6 neighbor binding {ipv6-address ipv6-prefix} interface type number [hardware-address mac-address][tracking [disable enable retry-interval value] reachable-lifetime value] Example: Device(config)# ipv6 neighbor binding 2001:DB8:0:ABCD::1 interface GigabitEthernet 0/0/1 reachable-lifetime 100	Adds a static entry to the binding table database.
Step 4	ipv6 neighbor binding max-entries entries 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 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 *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. data-glean {recovery | log-only} [ndp | dhcp]
8. prefix-glean
9. protocol dhcp [prefix-list *prefix-list-name*]
10. exit
11. ipv6 destination-guard policy *policy-name*
12. enforcement {always | stressed}
13. exit
14. interface *type number*
15. ipv6 snooping attach-policy *snooping-policy*
16. ipv6 destination-guard attach-policy *policy-name*
17. 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 <i>ipv6-address</i> interface <i>type number</i> Example: Device(config)# ipv6 neighbor binding 2001:db8::1 interface GigabitEthernet3/0/1	Adds a static entry to the binding table database.

	Command or Action	Purpose
Step 4	ipv6 prefix-list <i>list-name</i> permit <i>ipv6-prefix/prefix-length</i> ge <i>ge-value</i> 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 <i>snooping-policy-id</i> Example: Device(config)# ipv6 snooping policy xyz	Enters IPv6 snooping configuration mode and allows you to modify the configuration of the snooping policy specified.
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	data-glean {recovery log-only} [ndp dhcp] Example: Device(config-ipv6-snooping)# data-glean recovery ndp	Enables IPv6 first-hop security binding table recovery using source (or “data”) address gleaning. Note If logging (without recovery) is required, use the data-glean log-only command.
Step 8	prefix-glean Example: Device(config-ipv6-snooping)# prefix-glean	Enables the device to glean prefixes from IPv6 router advertisements (RAs) or Dynamic Host Configuration protocol (DHCP)
Step 9	protocol dhcp [prefix-list <i>prefix-list-name</i>] 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 10	exit Example: Device(config-ipv6-snooping)# exit	Exits IPv6 snooping configuration mode and returns to global configuration mode.
Step 11	ipv6 destination-guard policy <i>policy-name</i> 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.

	Command or Action	Purpose
Step 12	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 13	exit Example: Device(config-destguard)# exit	Exits destination guard configuration mode and returns to global configuration mode.
Step 14	interface type number Example: Device(config)# interface GigabitEthernet 0/0/1	Enters interface configuration mode.
Step 15	ipv6 snooping attach-policy snooping-policy Example: Device(config-if)# ipv6 snooping attach-policy xyz	Attaches the IPv6 snooping policy to the interface.
Step 16	ipv6 destination-guard attach-policy policy-name Example: Device(config-if)# ipv6 destination-guard attach-policy xyz	Attaches the destination guard policy to the specified interface. Note For information about how to configure an IPv6 destination guard policy, see the “IPv6 Destination Guard” module.
Step 17	end Example: Device(config-if)# end	Exits interface 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.
Step 3	ipv6 snooping policy <i>snooping-policy-id</i> 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} [<i>prefix-list prefix-list-name</i>] 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.

	Command or Action	Purpose
Step 3	ipv6 snooping policy <i>snooping-policy</i> 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 on an Interface

```

Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# exit
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ipv6 snooping attach-policy policy1
.
.
.
Device# show ipv6 snooping policies interface gigabitEthernet 0/0/1
Target      Type  Policy      Feature      Target range
Gi0/0/1     PORT  my_policy   Destination  Gu vlan all
Gi0/0/1     PORT  policy1     Snooping     vlan all

```

Example: Configuring IPv6 Binding Table Content

```

Device(config)# ipv6 neighbor binding 2001:DB8:0:ABCD::1 interface GigabitEthernet 0/0/1
reachable-lifetime 100
Device(config)# ipv6 neighbor binding max-entries 100
Device(config)# ipv6 neighbor binding logging
Device(config)# exit

```

Example: Configuring IPv6 First-Hop Security Binding Table Recovery

```

Device> enable
Device# configure terminal
Device(config)# ipv6 neighbor binding 2001:db8::1 interface GigabitEthernet3/0/1
Device(config)# ipv6 prefix-list abc permit 2001:DB8::/64 ge 128
Device(config)# ipv6 snooping policy xyz
Device(config-ipv6-snooping)# destination-glean recovery dhcp
Device(config-ipv6-snooping)# data-glean recovery ndp
Device(config-ipv6-snooping)# prefix-glean
Device(config-ipv6-snooping)# protocol dhcp prefix-list abc
Device(config-ipv6-snooping)# exit
Device(config)# ipv6 destination-guard policy xyz
Device(config-destguard)# enforcement stressed

```

```
Device(config-destguard)# exit
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ipv6 snooping attach-policy xyz
Device(config-if)# ipv6 destination-guard attach-policy xyz
Device(config-if)# end
```

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
```

Additional References for IPv6 Source Guard and Prefix Guard

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

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 1: 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 XE Release 3.9S	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. In Cisco IOS XE Release 3.9S, support was added for the Cisco CSR 1000V and the Cisco ASR 1000 Series Routers. 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.

