IPv6 Snooping

Last Updated: August 6, 2012

The IPv6 snooping feature bundles several layer 2 IPv6 first-hop security features, including IPv6 neighbor discovery, IPv6 device tracking, and IPv6 address glean. IPv6 snooping operates at layer 2, or between layer 2 and layer 3, and provides IPv6 features with security and scalability.

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 at the end of this module.

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 Snooping

IPv6 Snooping

The IPv6 snooping feature bundles several layer 2 IPv6 first-hop security features, including IPv6 address glean, IPv6 device tracking, and IPv6 neighbor discovery. IPv6 snooping operates at layer 2, or between layer 2 and layer 3, and provides IPv6 features with security and scalability.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

When IPv6 snooping is configured on a target (which vary depending on platform target support and may include device ports, switchports, layer 2 interfaces, layer 3 interfaces, and VLANs), capture instructions are downloaded to the hardware to redirect the neighbor discovery (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 capture 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. The IPv6 snooping entry point is the last to be called, so any decision (such as drop) made by another feature supersedes the IPv6 snooping decision.

IPv6 Neighbor Discovery Inspection

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes ND messages in order to build a trusted binding table. IPv6 ND messages that do not have valid bindings are dropped.

IPv6 Global Policies

IPv6 global policies provide storage and access policy database services. IPv6 neighbor discovery (ND) inspection and the IPv6 Router Advertisement (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 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

A database table of IPv6 neighbors connected to the device is created from information sources such as Neighbor Discovery (ND) protocol 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.

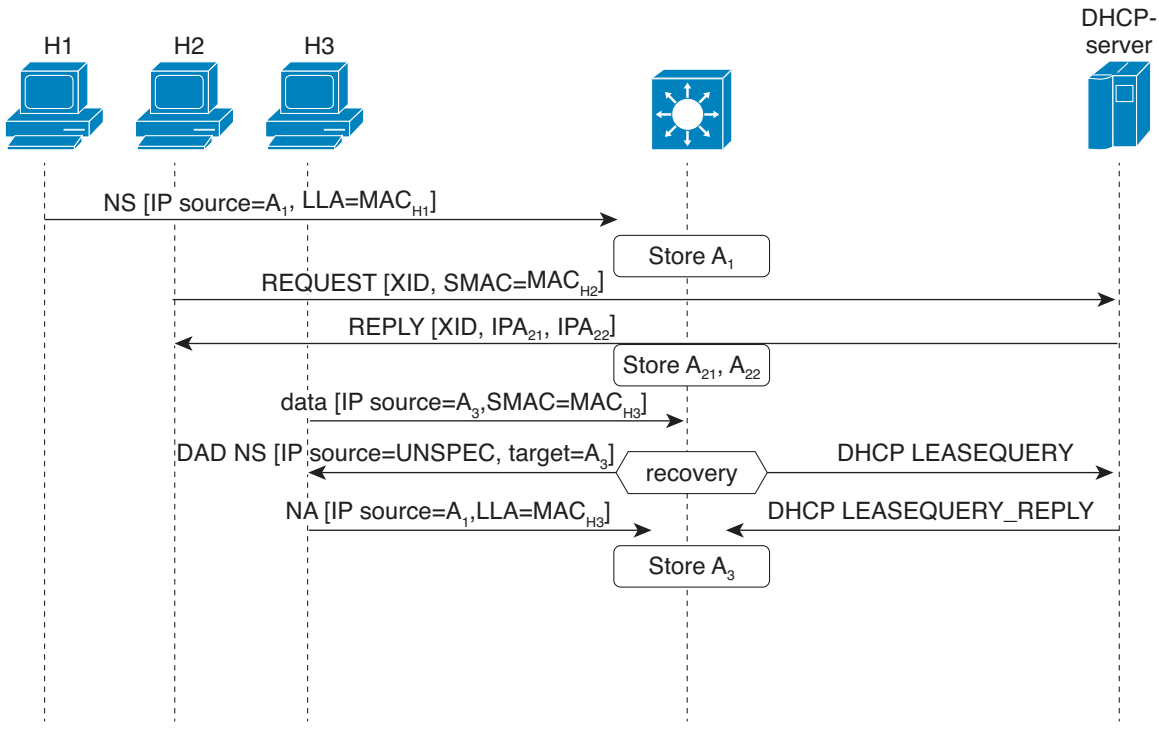
IPv6 Device Tracking

The IPv6 device tracking feature provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears. The feature tracks the liveness of the neighbors connected through the Layer 2 device on regular basis in order to revoke network access privileges as they become inactive.

IPv6 Address Glean

The IPv6 address glean feature 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.



Binding Table

IPv6	MAC	VLAN	IF
A_1	MAC_{H1}	100	P1
A_{21}	MAC_{H2}	100	P2
A_{22}	MAC_{H2}	100	P2
A_3	MAC_{H3}	100	P3

285966

How to Configure IPv6 Snooping

Configuring IPv6 Snooping

SUMMARY STEPS

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

Example:

```
Device(config)# ipv6 snooping policy policy1
```

Configures an IPv6 snooping policy named policy1 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 named policy1 to a target.

Configuring IPv6 Neighbor Discovery Inspection

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.
Step 3	**ipv6 nd inspection policy** *policy-name* **Example:** `Device(config)# ipv6 nd inspection policy policy1`	Defines the ND inspection policy name and places the device in ND inspection policy configuration mode.

	Command or Action	Purpose
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 a Specified 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 places the device in 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

These optional commands can be entered in any order to verify and troubleshoot the IPv6 ND inspection feature.

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** [**binding-table** | **classifier** | **errors** | **feature-manager** | **filter** *acl* | **ha** | **hw-api** | **interface** *interface* | **memory** | **ndp-inspection** | **policy** | **vlan** *vlanid* | **switcher** | **filter** *acl* | **interface** *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	**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 Fa 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** [**binding-table** | **classifier** | **errors** | **feature-manager** | **filter** *acl* | **ha** | **hw-api** | **interface** *interface* | **memory** | **ndp-inspection** | **policy** | **vlan** *vlanid* | **switcher** | **filter** *acl* | **interface** *interface* | *vlanid*] **Example:** `Device# debug ipv6 snooping`	Enables debugging for snooping information in IPv6.

Configuring IPv6 Device Tracking

Configuring the IPv6 Binding Table Content

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** **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* {**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.

	Command or Action	Purpose
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 places the device in 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 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.

	Command or Action	Purpose
Step 3	**ipv6 neighbor tracking** [**retry-interval** *value*] **Example:** `Device(config)# ipv6 neighbor tracking`	Tracks entries in the binding table.

Configuring IPv6 Address Glean

Note You must configure an IPv6 snooping policy and attach the policy to a target before configuring IPv6 address glean.

SUMMARY STEPS

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

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 snooping policy** *snooping-policy*

Example:

```
Device(config)# ipv6 snooping policy policy1
```

Configures an IPv6 snooping policy named policy1 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 named policy1 to a target.

Step 5 **prefix-glean** [*only*]

Example:

```
Device(config-ipv6-snooping)# prefix-glean
```

Enables the device to glean prefixes from IPv6 RAs or DHCPv6.

Configuration Examples for IPv6 Snooping

Example: Configuring IPv6 Snooping

```
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: IPv6 ND Inspection and RA Guard Configuration

This example provides information about an interface on which both the neighbor discovery (ND) inspection and router advertisement (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: IPv6 Device Tracking

```
Device# show ipv6 neighbor tracking

    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
```

Example: Configuring IPv6 Address Glean

<<Please provide an example--Thanks!>>

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 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 Address Glean	15.0(2)SE	IPv6 address glean inspects ND and DHCP messages on a link to glean addresses and then populates the binding table with these addresses. The following commands was introduced: **prefix-glean**.

Feature Name	Releases	Feature Information
IPv6 Device Tracking	12.2(50)SY 15.0(1)SY 15.0(2)SE	IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears. The following commands were introduced or modified: **ipv6 neighbor binding logging**, **ipv6 neighbor binding max-entries**, **ipv6 neighbor binding vlan**, **ipv6 neighbor tracking**, **show ipv6 neighbor binding**.
IPv6 Neighbor Discovery Inspection	12.2(50)SY 15.0(1)SY 15.0(2)SE	IPv6 neighbor discovery inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. The following commands were introduced or modified: **debug ipv6 snooping**, **device-role**, **drop-unsecure**, **ipv6 nd inspection**, **ipv6 nd inspection policy**, **sec-level minimum**, **show ipv6 snooping capture-policy**, **show ipv6 snooping counters**, **show ipv6 snooping features**, **show ipv6 snooping policies**, **tracking**, **trusted-port**.
IPv6 Snooping	15.0(2)SE	The IPv6 snooping feature bundles several layer 2 IPv6 first-hop security features, including IPv6 neighbor discovery, IPv6 device tracking, and IPv6 address glean. IPv6 snooping operates at layer 2, or between layer 2 and layer 3, and provides IPv6 features with security and scalability. The following commands were introduced or modified: **ipv6 snooping attach-policy**, **ipv6 snooping policy** .

Glossary

- **CA**—certification authority.
- **CGA**—cryptographically generated address.
- **CPA**—certificate path answer.
- **CPR**—certificate path response.
- **CPS**—certification path solicitation. The solicitation message used in the addressing process.
- **CRL**—certificate revocation list.
- **CS**—certification server.
- **CSR**—certificate signing request.
- **DAD**—duplicate address detection. A mechanism that ensures two IPv6 nodes on the same link are not using the same address.
- **DER**—distinguished encoding rules. An encoding scheme for data values.
- **nonce**—An unpredictable random or pseudorandom number generated by a node and used once. In SeND, nonces are used to assure that a particular advertisement is linked to the solicitation that triggered it.
- **non-SeND node**—An IPv6 node that does not implement SeND but uses only the Neighbor Discovery protocol without security.
- **NUD**—neighbor unreachability detection. A mechanism used for tracking neighbor reachability.
- **PACL**—port-based access list.
- **PKI**—public key infrastructure.
- **RA**—router advertisement.
- **RD**—Router discovery allows the hosts to discover what devices exist on the link and what subnet prefixes are available. Router discovery is a part of the Neighbor Discovery protocol.
- **Router Authorization Certificate**—A public key certificate.
- **SeND node**—An IPv6 node that implements SeND.
- **trust anchor**—An entity that the host trusts to authorize devices to act as devices. Hosts are configured with a set of trust anchors to protect device discovery.