



IPv6 First-Hop Security Binding Table

Last Updated: July 25, 2012

A database table of IPv6 neighbors connected to a device is created from information sources such as Neighbor Discovery Protocol (NDP) snooping. This database, or binding, table is used by various IPv6 guard features to prevent spoofing and redirect attacks.

The IPv6 first-hop security binding table recovery mechanism enables the binding table to recover in the event of a device reboot.

- [Finding Feature Information, page 1](#)
- [Prerequisites for IPv6 First-Hop Security Binding Table, page 1](#)
- [Restrictions for IPv6 First-Hop Security Binding Table, page 2](#)
- [Information About IPv6 First-Hop Security Binding Table, page 2](#)
- [How to Configure IPv6 First-Hop Security Binding Table, page 3](#)
- [Configuration Examples for IPv6 First-Hop Security Binding Table, page 9](#)
- [Additional References, page 10](#)
- [Feature Information for IPv6 First-Hop Security Binding Table, page 11](#)

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.

Prerequisites for IPv6 First-Hop Security Binding Table

- 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 Destination Guard feature. For information, see the “IPv6 Destination Guard” module.



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

Restrictions for IPv6 First-Hop Security Binding Table

- The IPv6 first-hop security binding table is supported only on the Cisco 7600 series platform and Cisco Catalyst 3750 series switches.

Information About IPv6 First-Hop Security Binding Table

- [Overview of the IPv6 First-Hop Security Binding Table, page 2](#)
- [IPv6 First-Hop Security Binding Table Recovery Mechanism, page 2](#)
- [Recovery Protocols and Prefix Lists, page 2](#)

Overview of the IPv6 First-Hop Security Binding Table

A database table of IPv6 neighbors connected to the device is created from information sources such as NDP 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 the prefix binding of the neighbors to prevent spoofing and redirect attacks.

IPv6 First-Hop Security Binding Table Recovery Mechanism

The IPv6 first-hop security binding table recovery 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 learnt via NDP or Dynamic Host Configuration Protocol (DHCP) gleaning.

The IPv6 First-Hop Security Binding Table Recovery Mechanism feature recovers the missing binding table entries when the resolution for a destination address fails in the destination guard. Upon a failure, a binding table entry is recovered by querying the DHCP server or the destination host depending on the configuration.



Note

For more information on the IPv6 destination guard, see the “IPv6 Destination Guard” module.

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]**.

For more information on how to configure IPv6 prefix lists, see the “[How to Implement RIP for IPv6](#)” module.

How to Configure IPv6 First-Hop Security Binding Table

- [Configuring IPv6 Binding Table Content, page 3](#)
- [Configuring the IPv6 First-Hop Security Binding Table Recovery Mechanism, page 5](#)
- [Associating Recovery Protocols with Prefix Lists, page 8](#)

Configuring 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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ipv6 neighbor binding vlan <i>vlan-id</i> { interface <i>type number</i> <i>ipv6-address</i> <i>mac-address</i> } [tracking [disable enable retry-interval <i>value</i>] reachable-lifetime <i>value</i>] Example: Device(config)# ipv6 neighbor binding vlan 100 interface Ethernet 0/0 reachable-lifetime 100	Adds a static entry to the binding table database.

Command or Action	Purpose
Step 4 ipv6 neighbor binding max-entries <i>entries</i> [vlan-limit <i>number</i> interface-limit <i>number</i> mac-limit <i>number</i>] 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 <i>vlan-id</i> interface <i>type number</i> ipv6 <i>ipv6-address</i> mac <i>mac-address</i>] 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	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
	Example: Device> enable	
Step 2	configure terminal	Enters global configuration mode.
	Example: Device# configure terminal	

	Command or Action	Purpose
Step 3	ipv6 neighbor binding vlan <i>vlan-id</i> ipv6-address interface <i>type number</i> 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 <i>list-name</i> permit ipv6-prefix/prefix-length 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	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 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 <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 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 <i>policy-name</i> 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.
Step 15	vlan configuration <i>vlan-list-id</i> 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 <i>policy-name</i> Example: Device(config-vlan-config)# ipv6 snooping attach-policy xyz	Attaches the IPv6 snooping policy to a VLAN.

Command or Action	Purpose
Step 17 <code>ipv6 destination-guard attach-policy <i>policy-name</i></code> Example: <pre>Device(config-vlan-config)# ipv6 destination-guard attach-policy xyz</pre>	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 <code>end</code> Example: <pre>Device(config-vlan-config)# end</pre>	Exits VLAN configuration mode and returns to privileged EXEC mode.

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 <code>enable</code> Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>ipv6 snooping policy <i>snooping-policy-id</i></code> Example: <pre>Device(config)# ipv6 snooping policy 200</pre>	Enters IPv6 snooping configuration mode and allows you to modify the configuration of the snooping policy specified.

Command or Action	Purpose
Step 4 <code>protocol { dhcp ndp } [prefix-list prefix-list-name]</code> Example: Device(config-ipv6-snooping)# protocol dhcp prefix-list dhcp_prefix_list	Associates a recovery protocol (DHCP or NDP) with a prefix list.
Step 5 <code>end</code> Example: Device(config-ipv6-snooping)# exit	Exits IPv6 snooping configuration mode and returns to privileged EXEC mode.

Configuration Examples for IPv6 First-Hop Security Binding Table

- [Example: Configuring IPv6 Binding Table Content, page 9](#)
- [Example: Configuring IPv6 First-Hop Security Binding Table Recovery, page 9](#)
- [Example: Associating Recovery Protocols with Prefix Lists, page 10](#)

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: 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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
IPv6 commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS IPv6 Command Reference
IPv6 neighbor discovery	“Implementing IPv6 Addressing and Basic Connectivity” module
IPv6 destination guard	“IPv6 Destination Guard” module
IPv6 prefix lists	“How to Implement RIP for IPv6” module

Standards and RFCs

Standard/RFC	Title
RFC 3756	<i>IPv6 Neighbor Discovery (ND) Trust Models and Threats</i>
RFC 3971	<i>Secure Neighbor Discovery (SeND)</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 First-Hop Security Binding Table

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 First-Hop Security Binding Table*

Feature Name	Releases	Feature Information
IPv6 First-Hop Security Binding Table	15.2(4)S	A database table of IPv6 neighbors connected to the device is created from information sources such as NDP snooping. This database, or binding, table is used by various IPv6 guard features to prevent spoofing and redirect attacks.
IPv6 First-Hop Security Binding Table Recovery Mechanism	15.2(4)S	<p>The IPv6 first-hop security binding table recovery mechanism enables the binding table to recover in the event of a device reboot.</p> <p>The following commands were introduced: destination-glean, protocol (IPv6).</p>