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.

Information About IPv6 Source Guard and Prefix Guard

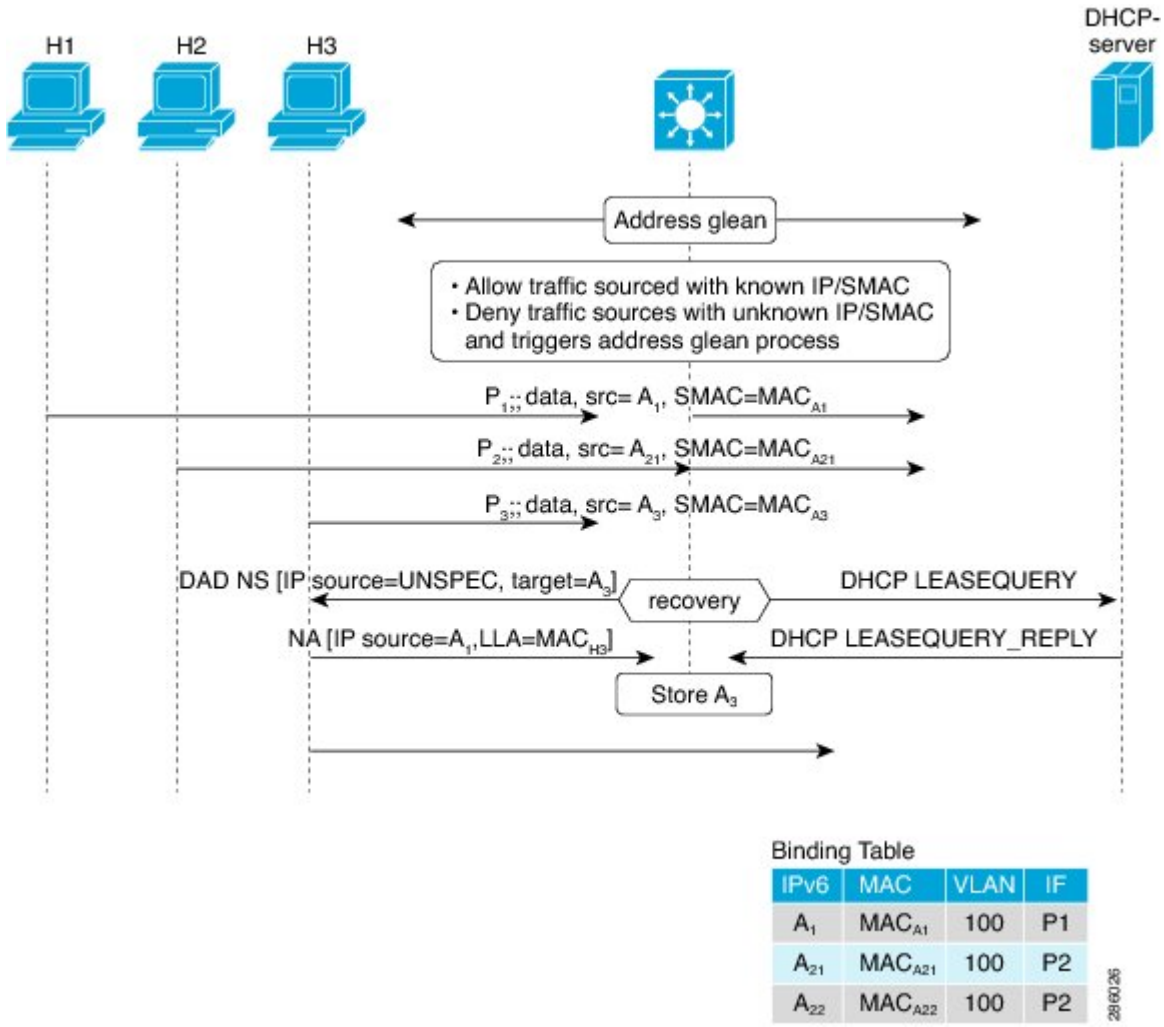
IPv6 Source Guard Overview

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 1: 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.

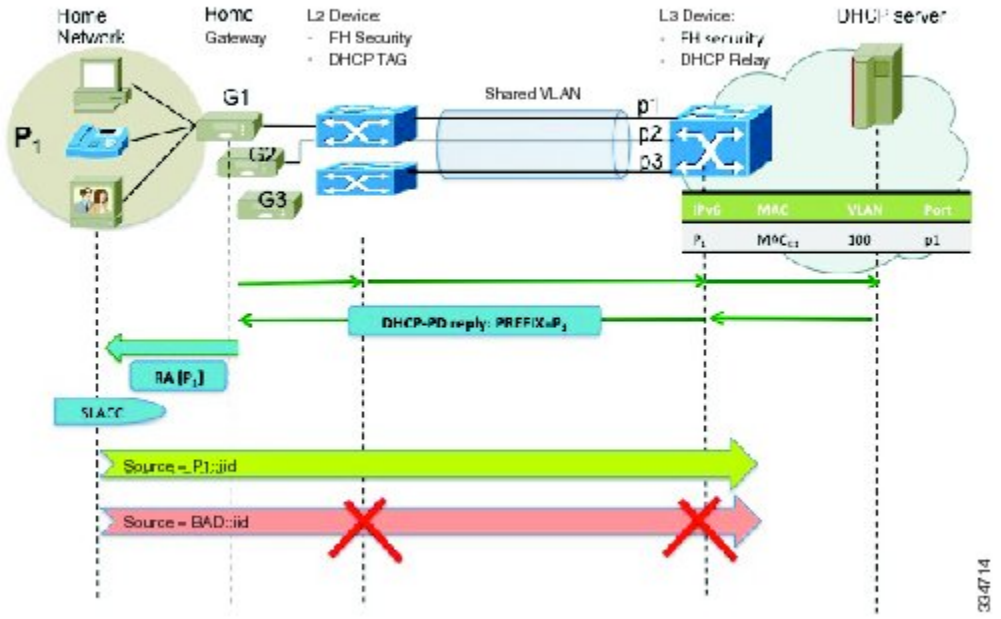
To determine which prefixes should be allowed and which prefixes should be blocked, IPv6 prefix guard uses the following:

- 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 2: 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** *source-guard-policy*
4. **permit link-local**
5. **deny global-autoconf**
6. **trusted**

7. **exit**
8. **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** *source-guard-policy* **Example:** `Device(config)# ipv6 source-guard policy my_sourceguard_policy`	Defines an IPv6 source-guard policy name and enters switch integrated security features source-guard policy configuration mode.
Step 4	**permit link-local** **Example:** `Device(config-sisf-sourceguard)# permit link-local`	Allows hardware bridging for all data traffic sourced by a link-local address.
Step 5	**deny global-autoconf** **Example:** `Device(config-sisf-sourceguard)# deny global-autoconf`	Denies data traffic from auto-configured global addresses.
Step 6	**trusted** **Example:** `Device(config-sisf-sourceguard)# trusted`	Allows hardware bridging for all data traffic on the target where the policy is applied.
Step 7	**exit** **Example:** `Device(config-sisf-sourceguard)# exit`	Exits source-guard policy configuration mode and returns to privileged EXEC mode.
Step 8	**show ipv6 source-guard policy** [*snooping-policy*] **Example:** `Device# show ipv6 source-guard policy policy1`	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.
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** *source-guard-policy*
4. **validate address**
5. **validate prefix**
6. **exit**
7. **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	**ipv6 source-guard policy** *source-guard-policy* **Example:** `Device(config)# ipv6 source-guard policy my_snooping_policy`	Defines an IPv6 source-guard policy name and enters switch integrated security features source-guard policy configuration mode.
Step 4	**validate address** **Example:** `Device(config-sisf-sourceguard)# 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-sisf-sourceguard)# validate prefix`	Enables IPv6 source guard to perform the IPv6 prefix-guard operation.
Step 6	**exit** **Example:** `Device(config-sisf-sourceguard)# exit`	Exits switch integrated security features source-guard policy configuration mode and returns to privileged EXEC mode.
Step 7	**show ipv6 source-guard policy** [*source-guard-policy*] **Example:** `Device# show ipv6 source-guard policy policy1`	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
```

Feature Information for Overview of Cisco TrustSec

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 Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
IPv6 enablement - Inline Tagging	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.