IPv6 Support for SGT and SGACL

The IPv6 Support for SGT and SGACL feature facilitates dynamic learning of mappings between IP addresses and Security Group Tags (SGTs) for IPv6 addresses. The SGT is later used to derive the Security Group Access Control List (SGACL).

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 Support for SGT and SGACL

Enforcement of IPv6 addresses is not supported by this feature.

Information About IPv6 Support for SGT and SGACL

Components of IPv6 Dynamic Learning

Dynamic learning of IPv6 addresses require three components:

- Switch Integrated Security Features (SISF)—An infrastructure built to take care of security, address assignment, address resolution, neighbor discovery, exit point discovery, and so on.
- Cisco Enterprise Policy Manager (EPM)—A solution that registers to SISF to receive IPv6 address notifications. The Cisco EPM then uses these IPv6 addresses and the Security Group Tags (SGTs) downloaded from the Cisco Identity Services Engine (ISE) to generate IP-SGT bindings.
- Cisco TrustSec—A solution that protects devices from unauthorized access. Cisco TrustSec assigns an SGT to the ingress traffic of a device and enforces the access policy based on the tag anywhere in the network.

Learning of IPv6 addresses can be done using the following methods, which are listed starting from lowest priority (1) to highest priority (7):

1. VLAN—Bindings learned from snooped Address Resolution Protocol (ARP) packets on a VLAN that has VLAN-SGT mapping.
2. CLI—Address bindings configured using the IP-SGT form of the **cts role-based sgt-map** global configuration command.
3. Layer 3 Interface (L3IF)—Bindings added due to forwarding information base (FIB) forwarding entries that have paths through one or more interfaces with consistent L3IF-SGT mapping or identity port mapping (IPM) on routed ports.
4. SXP—Bindings learned from SGT Exchange Protocol (SXP) peers.
5. IP_ARP—Bindings learned when tagged ARP packets are received on a CTS-capable link.
6. Local—Bindings of authenticated hosts that are learned via EPM and device tracking.
7. Internal—Bindings between locally configured IP addresses and the device's own SGT.

How to Configure IPv6 Support for SGT and SGACL

Generating IPv6 Addresses for IP-SGT Bindings

Switch Integrated Security Features (SISF) is a feature that generates IPv6 addresses for use in IP-SGT bindings.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *policy-name*
4. **tracking enable**
5. **exit**
6. **ipv6 dhcp pool** *dhcp-pool-name*
7. **address prefix** *ipv6-address/prefix*
8. **exit**
9. **interface vlan** *interface-number*
10. **ipv6 enable**
11. **no ipv6 address**
12. **ipv6 address** *ipv6-address/prefix*
13. **ipv6 address autoconfiguration**
14. **ipv6 dhcp server** *dhcp-pool-name*
15. **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** *policy-name* **Example:** `Device(config)# ipv6 snooping policy policy1`	Generates IPv6 addresses for IP-SGT bindings and enters IPv6 snooping configuration mode.
Step 4	**tracking enable** **Example:** `Device(config-ipv6-snooping)# tracking enable`	Overrides the default tracking policy on a port.
Step 5	**exit** **Example:** `Device(config-ipv6-snooping)# exit`	Exits IPv6 snooping configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**ipv6 dhcp pool** *dhcp-pool-name* **Example:** `Device(config)# ipv6 dhcp pool dhcp-pool`	Assigns an IPv6 DHCP pool to the DHCP server and enters IPv6 DHCP pool configuration mode.
Step 7	**address prefix** *ipv6-address/prefix* **Example:** `Device(config-dhcpv6)# address prefix 2001:DB8::1/64`	Sets the IPv6 address for an end host.
Step 8	**exit** **Example:** `Device(config-dhcpv6)# exit`	Exits IPv6 DHCP pool configuration mode and returns to global configuration mode.
Step 9	**interface vlan** *interface-number* **Example:** `Device(config)# interface vlan 20`	Creates a VLAN interface and enters interface configuration mode.
Step 10	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 on an interface.
Step 11	**no ipv6 address** **Example:** `Device(config-if)# no ipv6 address`	Removes the existing IPv6 address set for an interface.
Step 12	**ipv6 address** *ipv6-address/prefix* **Example:** `Device(config-if)# ipv6 address 2001:DB8:1:1::1/64`	Assigns an IPv6 address for the interface.
Step 13	**ipv6 address autoconfiguration** **Example:** `Device(config-if)# ipv6 address autoconfiguration`	Enables stateless autoconfiguration on an interface.
Step 14	**ipv6 dhcp server** *dhcp-pool-name* **Example:** `Device(config-if)# ipv6 dhcp server dhcp-pool`	Assigns an IPv6 DHCP pool to the DHCP server.

Step 15	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

Configure IPv6-SGT binding by using either local binding or a VLAN.

Configuring IPv6 IP-SGT Binding Using Local Binding

In local binding, the Security Group Tag (SGT) value is downloaded from the Identity Services Engine (ISE).

Before You Begin

-
- An IPv6 address must be generated through Switch Integrated Security Features (SISF) to configure an IP-SGT binding.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control subscriber** *control-policy-name*
4. **event session-started match-all**
5. *priority-number* **class always do-until-failure**
6. *action-number* **authenticate using mab**
7. **end**
8. **configure terminal**
9. **interface gigabitethernet** *interface-number*
10. **description** *interface-description*
11. **switchport access vlan** *vlan-id*
12. **switchport mode access**
13. **ipv6 snooping attach-policy** *policy-name*
14. **access-session port-control auto**
15. **mab eap**
16. **dot1x pae authenticator**
17. **service-policy type control subscriber** *policy-name*
18. **end**
19. **show cts role-based sgt-map all ipv6**

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	**policy-map type control subscriber** *control-policy-name* **Example:** `Device(config)# policy-map type control subscriber policy1`	Defines a control policy for subscriber sessions and enters control policy-map configuration mode.
Step 4	**event session-started match-all** **Example:** `Device(config-event-control-policymap)# event session-started match-all`	Specifies the type of event that triggers actions in a control policy if conditions are met.
Step 5	*priority-number* **class always do-until-failure** **Example:** `Device(config-class-control-policymap)# 10 class always do-until-failure`	Associates a control class with one or more actions in a control policy and enters action control policy-map configuration mode. • A named control class must first be configured before specifying it with the *control-class-name* argument.
Step 6	*action-number* **authenticate using mab** **Example:** `Device(config-action-control-policymap)# 10 authenticate using mab`	Initiates the authentication of a subscriber session using the specified method.

Step 7	**end**
	Example:
	`Device(config-action-control-policymap)# end`
		Exits action control policy-map configuration mode and returns to privileged EXEC mode.

Step 8	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 9	**interface gigabitethernet** *interface-number* **Example:** `Device(config)# interface gigabitehternet 1/0/1`	Enters interface configuration mode.
Step 10	**description** *interface-description* **Example:** `Device(config-if)# description downlink to ipv6 clients`	Describes the configured interface.

	Command or Action	Purpose
Step 11	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 20`	Sets access mode characteristics of the interface and configures VLAN when the interface is in access mode.
Step 12	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Sets the trunking mode to access mode.
Step 13	**ipv6 snooping attach-policy** *policy-name* **Example:** `Device(config-if)# ipv6 snooping attach-policy snoop`	Applies a policy to the IPv6 snooping feature.
Step 14	**access-session port-control auto** **Example:** `Device(config-if)# access-session port-control auto`	Sets the authorization state of a port.
Step 15	**mab eap** **Example:** `Device(config-if)# mab eap`	Uses Extensible Authentication Protocol (EAP) for MAC authentication bypass.
Step 16	**dot1x pae authenticator** **Example:** `Device(config-if)# dot1x pae authenticator`	Enables dot1x authentication on the port.
Step 17	**service-policy type control subscriber** *policy-name* **Example:** `Device(config-if)# service-policy type control subscriber policy`	Specifies the policy map that is used for sessions that come up on this interface. The policy map has rules for authentication and authorization.

Step 18	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Step 19	**show cts role-based sgt-map all ipv6** **Example:** `Device# show cts role-based sgt-map all ipv6`	Displays active IPv6 IP-SGT bindings.

Configuring IPv6 IP-SGT Binding Using a VLAN

In a VLAN, a network administrator assigns a Security Group Tag (SGT) value to a particular VLAN.

Before You Begin

-
- An IPv6 address must be generated through Switch Integrated Security Features (SISF) to configure an IP-SGT binding.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts role-based sgt-map vlan-list** *vlan-id* **sgt** *sgt-value*
4. **end**
5. **show cts role-based sgt-map all ipv6**

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	**cts role-based sgt-map vlan-list** *vlan-id* **sgt** *sgt-value* **Example:** `Device(config)# cts role-based sgt-map vlan-list 20 sgt 3`	Assigns an SGT value to the configured VLAN. **Note** The range of the *sgt-value* argument must be from 2 to 65519.

Step 4	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Step 5	**show cts role-based sgt-map all ipv6** **Example:** `Device# show cts role-based sgt-map all ipv6`	Displays active IPv6 IP-SGT bindings.

Verifying IPv6 Support for SGT and SGACL

SUMMARY STEPS

1. **enable**
2. **show cts role-based sgt-map all**
3. **show cts role-based sgt-map all ipv6**

DETAILED STEPS

Command or Action | **Purpose**

Step 1 **enable**

Example:

```
Device> enable
```

Purpose: Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show cts role-based sgt-map all**

Example:

```
Device# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
192.0.2.1                8       INTERNAL
192.0.2.2                8       INTERNAL
192.0.2.3                11      LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of INTERNAL bindings = 2
Total number of active   bindings = 3

Active IPv6-SGT Bindings Information

IP Address                                  SGT     Source
================================================================
2001:DB8:0:ABCD::1                          8       INTERNAL
2001:DB8:1::1                               11      LOCAL
2001:DB8:1::1                               11      LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of INTERNAL bindings = 1
Total number of active   bindings = 3
```

Purpose: Displays active IPv4 and IPv6 IP-SGT bindings.

Step 3 **show cts role-based sgt-map all ipv6**

Example:

```
Device# show cts role-based sgt-map all ipv6

Active IP-SGT Bindings Information
```

Purpose: Displays active IPv6 IP-SGT bindings.

	Command or Action	Purpose

```
IP Address                                  SGT     Source
================================================================
2001:DB8:1::1                                  10      CLI
2001:DB8:1:FFFF::1                             27      VLAN
2001:DB8:9798:8294:753F::1                     5       LOCAL
2001:DB8:8E99:DA94:8A6A::2                     5       LOCAL
2001:DB8:104:2001::139                         27      VLAN
2001:DB8:104:2001:14FE:9798:8294:753F          5       LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of VLAN     bindings = 2
Total number of CLI      bindings = 1
Total number of LOCAL    bindings = 3
Total number of active   bindings = 6
```

Configuration Examples for IPv6 Support for SGT and SGACL

Example: Generating IPv6 Addresses for IP-SGT Bindings

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy-name
Device(config-ipv6-snooping)# tracking enable
Device(config-ipv6-snooping)# exit
Device(config)# ipv6 dhcp pool dhcp-pool
Device(config-dhcpv6)# address prefix 2001:DB8::1/64
Device(config-dhcpv6)# exit
Device(config)# interface vlan 20
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:DB8::2/64
Device(config-if)# ipv6 address autoconfiguration
Device(config-if)# ipv6 enable
Device(config-if)# ipv6 dhcp server dhcp-pool
Device(config-if)# end
```

Example: Configuring IPv6 IP-SGT Binding Using Local Binding

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy-name
Device(config-ipv6-snooping)# tracking enable
Device(config-ipv6-snooping)# exit
Device(config)# ipv6 dhcp pool dhcp-pool
Device(config-dhcpv6)# address prefix 2001:DB8::1/64
Device(config-dhcpv6)# exit
Device (config)# interface vlan 20
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:DB8::2/64
Device(config-if)# ipv6 address autoconfiguration
Device(config-if)# ipv6 enable
Device(config-if)# ipv6 dhcp server dhcp-pool
Device(config-if)# exit
Device(config)# policy-map type control subscriber policy1
Device(config-event-control-policymap)# event session match-all
Device(config-class-control-policymap)# 10 class always do-until-failure
Device(config-action-control-policymap)# 10 authenticate using mab
Device(config-action-control-policymap)# end
Device# configure terminal
Device(config)# interface gigabitehternet 1/0/1
Device(config-if)# description downlink to ipv6 clients
Device(config-if)# switchport access vlan 20
Device(config-if)# switchport mode access
Device(config-if)# ipv6 snooping attach-policy snoop
Device(config-if)# access-session port-control auto
Device(config-if)# mab eap
Device(config-if)# dot1x pae authenticator
Device(config-if)# service-policy type control subscriber example
Device(config-if)# end
```

Example: Configuring IPv6 IP-SGT Binding Using a VLAN

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy-name
Device(config-ipv6-snooping)# tracking enable
Device(config-ipv6-snooping)# exit
Device(config)# ipv6 dhcp pool dhcp-pool
Device(config-dhcpv6)# address prefix 2001:DB8::1/64
Device(config-dhcpv6)# domain name domain.com
Device(config-dhcpv6)# exit
Device  (config)# interface vlan 20
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:DB8::2/64
Device(config-if)# ipv6 address autoconfiguration
Device(config-if)# ipv6 enable
Device(config-if)# ipv6 nd other-config-flag
Device(config-if)# ipv6 dhcp server dhcp-pool
Device(config-if)# end
```

Additional References for IPv6 Support for SGT and SGACL

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	• Cisco IOS Security Command Reference Commands A to C • Cisco IOS Security Command Reference Commands D to L • Cisco IOS Security Command Reference Commands M to R • Cisco IOS Security Command Reference Commands S to Z
Security group ACL	"Enablement of Security Group ACL at Interface Level" module of *Cisco TrustSec Configuration Guide*
IEEE 802.1X authentication	"Configuring IEEE 802.1X Port-Based Authentication" module of *802.1X Authentication Services Configuration Guide*
MAC Authentication Bypass	"Configuring MAC Authentication Bypass" module of *Authentication Authorization and Accounting Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for IPv6 Support for SGT and SGACL

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 . An account on Cisco.com is not required.

Table 1: Feature Information for IPv6 Support for SGT and SGACL

Feature Name	Releases	Feature Information
IPv6 Support for SGT and SGACL	Cisco IOS XE 3.6E	The IPv6 Support for SGT and SGACL feature introduces dynamic learning of mappings between IP addresses and Security Group Tags (SGTs) for IPv6 addresses. The SGT is later used to derive the Security Group Access Control List (SGACL). In Cisco IOS XE Release 3.6E, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Catalyst 3850 Series Switches • Catalyst 4500E Supervisor Engine 7L-E • Catalyst 4500-X Series Switches • Catalyst 4900 Series Switches • Catalyst 4500E Supervisor Engine 8-E The following command was modified: **cts role-based sgt-map**.