

IPv6 Support for SGT and SGACL

- Feature History for IPv6 support SGT and SGACL, on page 1
- IPv6 Support for SGT and SGACL, on page 1
- IPv6 Dynamic Learning Components, on page 2
- IPv6 address-to-SGT mapping priorities, on page 2
- How to Configure IPv6 Support for SGT and SGACL, on page 2
- Verify IPv6 Support for SGT and SGACL, on page 7
- Configuration Examples for IPv6 Support for SGT and SGACL, on page 7

Feature History for IPv6 support SGT and SGACL

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 26.2.1ea	IPv6 support SGT and SGACL: The IPv6 Support for Security Group Tags (SGT) and Security Group Access Control Lists (SGACL) feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	IPv6 support SGT and SGACL: SGT and SGACL support seamless mapping between IPv6 addresses and SGTs.	Cisco C9610 Series Smart Switches

IPv6 Support for SGT and SGACL

The IPv6 Support for Security Group Tags (SGT) and Security Group Access Control Lists (SGACL) feature enables seamless mapping between IPv6 addresses and SGTs. These mapped SGTs play a crucial role in enforcing security policies via SGACLs.

IPv6 Dynamic Learning Components

Dynamic learning of IPv6 addresses relies on three core components:

- Switch Integrated Security Features (SISF):

  An infrastructure responsible for security, address assignment, resolution, neighbor discovery, and exit point discovery.

- Cisco Enterprise Policy Manager (EPM):

  Registers with SISF to receive IPv6 address notifications. EPM then uses IPv6 addresses and SGTs obtained from Cisco Identity Services Engine (ISE) to create IP-SGT bindings.

- Cisco TrustSec:

  Protects devices from unauthorized access by assigning SGTs to incoming traffic and enforcing access policies based on these tags across the network.

IPv6 address-to-SGT mapping priorities

IPv6 address-to-SGT mapping can be achieved through several methods, prioritized as follows (from lowest to highest):

1. VLAN:

   IPv6 addresses learned through SISF on VLANs with SGT-VLAN mappings, using ICMPv6 Neighbor Discovery.

2. CLI:

   Manual address bindings set using the **cts role-based sgt-map** global configuration command (IP-SGT format).

3. Layer 3 Interface:

   Bindings created from FIB forwarding entries traversing interfaces with consistent Layer 3 interface-SGT or identity port mapping (IPM).

4. SXP:

   Bindings received from SGT Exchange Protocol (SXP) peers.

5. Local:

   Bindings for authenticated hosts, identified through EPM and device tracking (SISF).

6. Internal:

   Bindings between locally configured IP addresses and the device's SGT.

How to Configure IPv6 Support for SGT and SGACL

This section describes how to configure IPv6 support for SGT and SGACL.

Learn IPv6 Addresses for IP-SGT Bindings

SISF is a feature that learns IPv6 addresses for use in IP-SGT bindings.

To learn IPv6 addresses for IP-SGT bindings, configure this task.

Procedure

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** *host-address/prefix* **sgt** *sgt-value*

Example:

```
Device(config)# cts role-based sgt-map 2001::db8::1/64 sgt 120
```

Manually maps a source IPv6 address to an SGT on either a host or a virtual routing and forwarding (VRF) instance.

Step 4 **device-tracking policy** *policy-name*

Example:

```
Device(config)# device-tracking policy policy1
```

Enables device tracking and enters device tracking configuration mode.

Step 5 **tracking enable**

Example:

```
Device(config-device-tracking)# tracking enable
```

Overrides the default tracking policy on a port.

Step 6 **end**

Example:

```
Device(config-device-tracking)# end
```

Exits device tracking configuration mode and returns to privileged EXEC mode.

Configure IPv6 IP-SGT Binding Using Local Binding

To configure IPv6 IP-SGT Binding Using Local Binding, perform this task.

Before you begin

- In local binding, SGT values are downloaded from Cisco Identity Service Engine (ISE). For more information, see the *Configuring Cisco Security Group Access Policies* document.
- SISF must be enabled and populated before IPv6 address can be generated.



Note This task uses Cisco Identity Based Networking Services (IBNS) Version 2.0.

Procedure

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 **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 configuredbefore 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 **exit**

Example:

```
Device(config-action-control-policymap)# exit
```

Exits action control policy-map configuration mode and returns to global configuration mode.

Step 8 **interface gigabitethernet** *interface-number*

Example:

```
Device(config)# interface gigabitethernet 1/0/1
```

Configures an interface and enters interface configuration mode.

Step 9 **description** *interface-description*

Example:

```
Device(config-if)# description downlink to ipv6 clients
```

Describes the configured interface.

Step 10 **switchport access vlan** *vlan-id*

Example:

```
Device(config-if)# switchport access vlan 20
```

Sets access mode characteristics of the interfaceand configures VLAN when the interface is in access mode.

Step 11 **switchport mode access**

Example:

```
Device(config-if)# switchport mode access
```

Sets the trunking mode to access mode.

Step 12 **device-tracking attach-policy** *policy-name*

Example:

```
Device(config-if)# device-tracking attach-policy snoop
```

Applies a policy to the IPv6 Snooping feature.

Step 13 **access-session port-control auto**

Example:

```
Device(config-if)# access-session port-control auto
```

Sets the authorization state of a port.

Step 14 **mab eap**

Example:

```
Device(config-if)# mab eap
```

Uses Extensible Authentication Protocol (EAP) for MAC authentication bypass.

Step 15 **dot1x pae authenticator**

Example:

```
Device(config-if)# dot1x pae authenticator
```

Enables dot1x authentication on the port.

Step 16 **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 sessionsthat come up on this interface. The policy map has rules for authentication and authorization.

Step 17 **end**

Example:

```
Device(config-if)# end
```

Exits interface configuration mode and returns to privileged EXEC mode.

Step 18 **show cts role-based sgt-map all ipv6**

Example:

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

Displays active IPv6 IP-SGT bindings.

Configure IPv6 IP-SGT Binding Using a VLAN

In a VLAN, a network administrator assigns SGT values to a particular VLAN.

To configure IPv6 IP-SGT BindinguUsing a VLAN, perform this task.

Procedure

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.

sgt-value: The range must be from 2 to 65519.

Step 4 **end**

Example:

```
Device(config)# end
```

Exits global configuration mode and returns to privileged EXEC mode.

Verify IPv6 Support for SGT and SGACL

Command	Description
show cts role-based sgt-map all	Displays active IPv4 and IPv6 IP-SGT bindings.
show cts role-based sgt-map all ipv6	Displays active IPv6 IP-SGT bindings.

Configuration Examples for IPv6 Support for SGT and SGACL

The following sections show how to configure IPv6 Support for SGT and SGACL.

Example: Learn IPv6 Addresses for IP-SGT Bindings

The following example shows how to learn IPv6 addresses for IP-SGT bindings:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map 2001::db8::1/64 sgt 120
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# tracking enable
Device(config-device-tracking)# end
```

Example: Configure IPv6 IP-SGT Binding Using Local Binding

The following example uses IBNS Version 2.0

```
Device> enable
Device# configure terminal
Device(config)# policy-map type control subscriber policy1
Device(config-event-control-policymap)# event session-started 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)# exit
Device(config)# interface gigabitethernet 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)# device-tracking 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 policy
Device(config-if)# end
```

Example: Configure IPv6 IP-SGT Binding Using a VLAN

The following example shows how to configure IP-SGT binding using a VLAN:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map vlan-list 20 sgt 3
Device(config)# end
```