Configuring SGT Exchange Protocol

You can use the SGT Exchange Protocol (SXP) to propagate the Security Group Tags (SGTs) across network devices that do not have hardware support for Cisco Group-Based Policy. This module describes how to configure Cisco Group-Based Policy SXP on switches in your network.

Cisco Group-Based Policy builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

The Security Group Tag (SGT) Exchange Protocol (SXP) is one of several protocols that supports CTS and is referred to in this document as Cisco Group-Based Policy SXP. Cisco Group-Based Policy SXP is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. Cisco Group-Based Policy SXP passes IP to SGT bindings from authentication points to upstream devices in the network. This process allows security services on switches, routers, or firewalls to learn identity information from access devices.

- Prerequisites for SGT Exchange Protocol, on page 1
- Restrictions for SGT Exchange Protocol, on page 2
- Information About SGT Exchange Protocol, on page 2
- How to Configure SGT Exchange Protocol, on page 4
- Configuration Examples for SGT Exchange Protocol, on page 13
- Verifying SGT Exchange Protocol Connections, on page 13
- Feature History for SGT Exchange Protocol, on page 15

Prerequisites for SGT Exchange Protocol

The Cisco SGT Exchange Protocol (SXP) network needs to be established before implementing SXP. This network has the following prerequisites:

- To use the Cisco Group-Based Policy functionality on your existing router, ensure that you have purchased a Cisco Group-Based Policy security license. If the router is being ordered and needs the Cisco Group-Based Policy functionality, ensure that this license is pre-installed on your router before it is shipped to you
- Cisco Group-Based Policy SXP software must run on all network devices.
- Connectivity should exist between all network devices.

Restrictions for SGT Exchange Protocol

- Cisco Group-Based Policy Exchange Protocol is not supported on logical interfaces; supported only on physical interfaces.
- In Cisco IOS XE Everest 16.6.4 and later releases, when the Dynamic Host Control Protocol (DHCP) snooping is enabled, Cisco Group-Based Policy enforcement for DHCP packets are bypassed by enforcement polices.
- Modifying a peer list under an SXP group is not supported when the peer connection configuration is present.
- Modifying export-list or import-list under speaker or listener export-import-group is not allowed when SXP connection configuration is present for any of the peers in the group. To modify the configuration under export-import-group, the corresponding peer SXP connection configuration must be removed. You can also shut down SXP by using the **no cts sxp enable** command.
- One peer cannot be configured under multiple export-import-groups in the same direction, that is, a peer can be part of speaker export-import-group as well as listener export-import-group but cannot be part of a second speaker or listener group at the same time.
- Global export-import-group and per peer export-import-group configuration are mutually exclusive.

Information About SGT Exchange Protocol

This section provides information about SGT Exchange Protocol.

SGT Exchange Protocol Overview

The Security Group Tag (SGT) Exchange Protocol (SXP) is one of several protocols that supports Cisco Group-Based Policy. SXP is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. Cisco Group-Based Policy filters packets at the egress interface. During endpoint authentication, a host accessing the Cisco Group-Based Policy domain (the endpoint IP address) is associated with an SGT at the access device through Dynamic Host Control Protocol (DHCP) snooping and IP device tracking. The access device transmits that association or binding through SXP to Cisco Group-Based Policy hardware-capable egress devices. These devices maintain a table of source IP-to-SGT bindings. Packets are filtered on the egress interface by Cisco Group-Based Policy hardware-capable devices by applying security group access control lists (SGACLs). SXP passes IP-to-SGT bindings from authentication points to upstream devices in the network. This process allows security services on switches, routers, or firewalls to learn identity information from access devices.

SGTs can be assigned through any of the following Endpoint Admission Control (EAC) access methods:

- 802.1X port-based authentication
- MAC Authentication Bypass (MAB)
- Web Authentication

SXP uses TCP as the transport protocol, and the TCP port 64999 for connection initiation. SXP uses Message Digest 5 (MD5) and TCP Authentication Option (TCP-AO) for authentication and integrity check. It has two defined roles—speaker (initiator) and listener (receiver).

Security Group Tagging

Security Group Tag is a unique 16 bit tag that is assigned to a unique role. It represents the privilege of the source user, device, or entity and is tagged at the ingress of the Cisco Group-Based Policy domain. SXP uses the device and user credentials acquired during authentication for classifying packets by security groups (SGs) as they enter a network. This packet classification is maintained by tagging packets on the ingress to the Cisco Group-Based Policy network so that they can be identified for the purpose of applying security and other policy criteria along the data path. The Security Group Tag (SGT) allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic. Static port Identification is used to lookup the SGT value for a particular endpoint connected to a port.

SGT Assignment

The Security Group Tag (SGT) of a packet can be assigned at the port level when the packet comes tagged on a Cisco Group-Based Policy link, or when a single endpoint authenticates on a port. SGT of an incoming packet is determined in the following ways:

- When a packet that is tagged with an SGT comes on a trusted port, the tag in the packet is considered as the source SGT.
- When a packet is tagged with an SGT, but comes on an untrusted port, the packet is ignored and the source SGT is set as configured on the port.
- When a packet does not have an SGT, the source SGT is set as configured on the port.

The following methods of assigning SGTs are supported:

- IPM (dot1x, MAB, and Web Authentication)
- VLAN-to-SGT mapping is a low priority classification method where IP addresses used within the VLAN are learned through IP device tracking. The learned IP addresses are assigned to the static SGT.
- SXP (SGT Exchange Protocol) Listener
- IP SGT
- Subnet SGT
- Port SGT
- Caching SGT

SXP Version 5

The deployment of VRFs is dependent on SXP connections and IP-SGT mappings. With an increase in the number of VRFs, an increase in SXP connections along with IP-SGT mappings are required. To improve this dependency, SXP version 5 has been designed to export and import SXP mappings between specified SXP peers. SXP version 5 can export IP-SGT bindings under various user defined VRFs over a single connection, unlike SXP version 4 which can export only the connection VRF IP-SGT bindings over a single connection.

- SXP version 5 exports certain mappings on the SXP speaker side based on binding source type or VRF.
- SXP version 5 imports certain mappings on the SXP listener side into the specified VRF.

Based on your configuration, which VRF associated IP-SGT binding should be exported to the remote peer device is decided. If an SXP connection is created between two devices which support SXP version 5, then the SXP connection negotiates to operate in SXP version 5 mode. If a device at either end of the SXP connection supports a lower version of SXP, then the SXP connection negotiates to operate at the lowest of the supported versions.

You can configure the VRF or list of VRF tables on which IP-SGT binding should be exported to peer devices by using the **cts sxp** global configuration command.

How to Configure SGT Exchange Protocol

This section describes how to configure SGT Exchange Protocol.

Configuring a Device SGT Manually

In normal Cisco Group-Based Policy operation, the authentication server assigns an SGT to the device for packets originating from the device. You can manually configure an SGT to be used if the authentication server is not accessible, but an authentication server-assigned SGT will take precedence over a manually-assigned SGT.

To manually configure an SGT on the device, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**cts sgt** *tag* **Example:** `Device(config)# cts sgt tag`	Configures the SGT for packets sent from the device. The tag argument is in decimal format. The range is 1 to 65533.
Step 3	**exit** **Example:** `Device(config)# exit`	Exits configuration mode.

Configuring an SXP Peer Connection

You must configure the SXP peer connection on both of the devices. One device is the speaker and the other is the listener, or you can also set both speaker and listener in both the devices. When using password protection, make sure to use the same password on both ends.

Note If a default SXP source IP address is not configured and you do not configure an SXP source address in the connection, the Cisco Group-Based Policy software derives the SXP source IP address from existing local IP addresses. The SXP source address might be different for each TCP connection initiated from the device.

To configure an SXP peer connection, perform this task:

Procedure

	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 sxp connection peer** *peer-ipv4-addr*[**source** *src-ipv4-addr*] **password** {**default** | **none**} **mode** {**local** | **peer**} {**speaker** | **listener**} {**vrf** *vrf-name*} **Example:** `Device(config)# cts sxp connection peer 10.10.1.1 password default mode local listener`	Configures the SXP address connection. The optional **source** keyword specifies the IPv4 address of the source device. If no address is specified, the connection will use the default source address, if configured, or the address of the port. The **password** keyword specifies the password that SXP will use for the connection using the following options: - **default**—Use the default SXP password you configured using the **cts sxp default password** command. - **none**—Do not use a password. The mode keyword specifies the role of the remote peer device: - **local**—The specified mode refers to the local device. - **peer**—The specified mode refers to the peer device. - **speaker**—Default. Specifies that the device is the speaker in the connection. - **listener**—Specifies that the device is the listener in the connection.

	Command or Action	Purpose
		The optional **vrf** keyword specifies the VRF to the peer. The default is the default VRF.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode
Step 5	**show cts sxp connections** **Example:** `Device# show cts sxp connections`	(Optional) Displays the SXP connection information.

Configuring the Default SXP Password

By default, SXP uses no password when setting up connections.

To configure a default SXP password, perform this task:

Procedure

	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 sxp default password** [**0** | **6** | **7**] *password* **Example:** `Device(config)# cts sxp default password 0 hello`	Configures the SXP default password. You can enter either a clear text password (using the **0** or no option) or an encrypted password (using the **6** or **7** option). The maximum password length is 32 characters.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode

Configuring the Default SXP Source IP Address

SXP uses the default source IP address for all new TCP connections where a source IP address is not specified. There is no effect on existing TCP connections when you configure the default SXP source IP address.

To configure a default SXP source IP address, perform this task:

Procedure

	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 sxp default source-ip** *src-ip-addr* **Example:** `Device(config)# cts sxp default source-ip 10.0.1.2`	Configures the SXP default source IP address.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Changing the SXP Reconciliation Period

After a peer terminates an SXP connection, an internal hold-down timer starts. If the peer reconnects before the internal hold-down timer expires, the SXP reconciliation period timer starts. While the SXP reconciliation period timer is active, the Cisco Group-Based Policy software retains the SGT mapping entries learned from the previous connection and removes invalid entries. The default value is 120 seconds (2 minutes). Setting the SXP reconciliation period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

To change the SXP reconciliation period, perform this task:

Procedure

	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 sxp reconciliation period** *seconds* **Example:** `Device(config)# cts sxp reconciliation period 360`	Changes the SXP reconciliation timer. The default value is 120 seconds (2 minutes). The range is from 0 to 64000.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Changing the SXP Retry Period

The SXP retry period determines how often the Cisco Group-Based Policy software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco Group-Based Policy software makes a new attempt to set up the connection after the SXP retry period timer expires. The default value is 120 seconds. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

To change the SXP retry period, perform this task:

Procedure

	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 sxp retry period** *seconds* **Example:** `Device(config)# cts sxp retry period 360`	Changes the SXP retry timer. The default value is 120 seconds (2 minutes). The range is from 0 to 64000.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Creating Syslogs to Capture Changes of IP Address-to-SGT Mapping Learned Through SXP

When the **cts sxp log binding-changes** command is configured in global configuration mode, SXP syslogs (sev 5 syslog) are generated whenever a change to IP address to SGT binding occurs (add, delete, change). These changes are learned and propagated on the SXP connection. The default is **no cts sxp log binding-changes**.

To enable logging of binding changes, perform the following task:

Procedure

	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 sxp log binding-changes** **Example:** `Device(config)# cts sxp log binding-changes`	Enables logging for IP to SGT binding changes.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an SXP Export-list

To configure an SXP export list, perform this task:

Note Export-list configurations cannot be removed if it is associated with any SXP group. To remove it you must first disable the SXP connection.

Procedure

	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 sxp export-list** *export_list_name* **Example:** `Device(config)# cts sxp export-list export_list_1`	Configures an SXP export list, and enters export-list configuration mode.

	Command or Action	Purpose

Step 4	**binding-source-type** {**all** | **caching** | **cli** | **l3if** | **lisp-local-host** | **lisp-remote-host** | **local** | **omp** | **vlan**}
	Example:
	`Device(config-export-list)# binding-source-type all`
		(Optional) Configures bindings of corresponding source type that are to be exported to the peer.
		• **all**: Exports all bindings.
		• **caching**: Exports cached bindings to the peer.
		• **cli**: Exports CLI bindings to the peer.
		• **l3if**: Exports L3IF bindings to the peer.
		• **lisp-local-host**: Exports LISP local bindings to the peer.
		• **lisp-remote-host**: Exports LISP remote bindings to the peer.
		• **local**: Exports local bindings to the peer.
		• **omp**: Exports OMP bindings to the peer.
		• **vlan**: Exports VLAN bindings to the peer.

Step 5	**vrf** {*instance_name* | **Default-vrf** | **all**}
	Example:
	`Device(config-export-list)# vrf all`
		(Optional) Configures a VPN routing and forwarding instance.
		• *instance_name*: Specifies a VPN routing and forwarding instance name.
		• **Default-vrf**: Exports default VRF bindings.
		• **all**: Exports all IP-SGT bindings.
		Note **vrf all** and **vrf** *instance_name* configuration are mutually exclusive.

Step 6	**end**
	Example:
	`Device(config-export-list)# end`
		Exits export list configuration mode, and returns to privileged EXEC mode

Configuring an SXP Import-list

To configure an SXP import list, perform this task:

Note Import-list configurations cannot be removed if it is associated with any SXP group. To remove it you must first disable the SXP connection.

Procedure

	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 sxp import-list** *import_list_name* **Example:** `Device(config)# cts sxp import-list import_list_1`	Configures an SXP import-list, and enters import list configuration mode.
Step 4	**vlan-list** **Example:** `Device(config-import-list)# vlan-list`	(Optional) Configures import VRF based on the VLAN in the received binding update. **Note** If there is no VRF mapping in the device for a VLAN received in the update, the bindings that are received are added to the default VRF table.

Step 5	**vrf** {*instance_name* | **Default-vrf**}}
	Example:
	`Device(config-import-list)# vrf vrf_1`
		(Optional) Configures the VRF used to import the bindings.
		• *instance_name*: Specifies a VPN routing and forwarding instance name.
		• **Default-vrf**: Configures the default VPN routing and forwarding instance.
		Note **vrf** *instance_name* and **vlan-list** configuration are mutually exclusive.

Step 6	**end**
	Example:
	`Device(config-import-list)# end`
		Exits export list configuration mode, and returns to privileged EXEC mode

Configuring an SXP Export-import-group

The export-import-groups are defined as either speaker or listener groups to control the export or import of SXP bindings for the group.

Procedure

	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 sxp export-import-group** {**listener** | **speaker**} {**global** | *list_name*}
	Example:
	`Device(config)# cts sxp export-import-group listener group_1`
		Configures an SXP export-import-group, and enters export-import-group configuration mode.
		- **global**: Configures either an SXP listener global import-group or SXP speaker global export-group.
		Global speaker or listener export-import-group is applied to all SXP connections configured in the device.
		- *list_name*: Specifies the default VPN routing and forwarding instance name.

Step 4	**import-list** *list_name*
	Example:
	`Device(config-export-import-group)# import-list import_1`
		(Optional) Specifies the import list name to be applied to the export-import-group.
		An empty import-list or export-list cannot be attached to a listener or speaker export-import-group respectively.

Step 5	**export-list** *list_name* **Example:** `Device(config-export-import-group)# export-list export_1`	(Optional) Specifies the export list name to be applied to the export-import-group. An empty import-list or export-list cannot be attached to a listener or speaker export-import-group respectively.
Step 6	**peer** *address_name* **Example:** `Device(config-export-import-group)# peer 1.1.1.1 2.2.2.2`	(Optional) Configures a list of peers to be applied to the export-import-group. A maximum of eight peers can be configured.

Step 7	**end**
	Example:
	`Device(config-export-import-group)# end`
		Exits export-import-group configuration mode, and returns to privileged EXEC mode

Configuration Examples for SGT Exchange Protocol

The following sections show configuration examples of SGT Exchange Protocol:

Example: Enabling Cisco Group-Based Policy SXP and an SXP Peer Connection

The following example shows how to enable SXP and configure an SXP peer connection between device A, the speaker, and device B, the listener:

```
Device# configure terminal
Device(config)# cts sxp enable
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.10.1.1
Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the SXP peer connection between device B, the listener, and device A, the speaker:

```
Device# configure terminal
Device(config)# cts sxp enable
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.20.2.2
Device(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

Example: Configuring the Default SXP Password and Source IP Address

The following example shows how to configure a default SXP password and source IP address:

```
Device# configure terminal
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.20.2.2
Device(config)# end
```

Verifying SGT Exchange Protocol Connections

To view SXP connections, perform this task:

Command	Purpose
show cts sxp connections	Displays detailed information about the SXP status and connections.
show cts sxp connections [brief]	Displays brief information about the SXP status and connections.
show cts sxp export-list	Displays the list of VRF associated to a given export list name or all export lists.

Command	Purpose
show cts sxp import-list	Displays the list of VRF associated to a given import list name or all import lists.
show cts sxp export-import-group [detailed]	Displays the export list or import list applied with the given export-import-group along with the list of peers that are part of this export-import-group.

The following is sample output from the **show cts sxp connections** command:

```
Device# show cts sxp connections

SXP                      : Enabled
Default Password         : Set
Default Source IP        : 10.10.1.1
Connection retry open period: 10 secs
Reconcile period         : 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP                  : 10.20.2.2
Source IP                : 10.10.1.1
Conn status              : On
Conn Version             : 2
Connection mode          : SXP Listener
Connection inst#         : 1
TCP conn fd              : 1
TCP conn password        : default SXP password
Duration since last state change: 0:00:21:25 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

The following is sample output from the **show cts sxp connections brief** command:

```
Device# show cts sxp connections brief

SXP                      : Enabled
Default Password         : Set
Default Source IP        : Not Set
Connection retry open period: 120 secs
Reconcile period         : 120 secs
Retry open timer is not running
-----------------------------------------------------------------------------
Peer_IP          Source_IP          Conn Status    Duration
-----------------------------------------------------------------------------
10.1.3.1         10.1.3.2           On             6:00:09:13 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

The **show cts sxp export-list** command displays the list of VRF associated for a given export list name or all the export list configured on the device.

```
Device# show cts sxp export-list export_list_1

   Export-list-name: export_list_1
   vrf red_vrf
   vrf blue_vrf

Device# show cts sxp export-list

   Export-list-name: export_list_1
       vrf red_vrf
       vrf blue_vrf
       vrf green_vrf
   Export-list-name: export_list_2
       vrf all
```

The **show cts sxp export-import-group** command displays the export list or import list applied with a given export-import-group along with the list of peers that are part of this export-import-group. It can also list details of all the export-import-groups configured on the device. Use the **detailed** keyword to display the export list or import list contents along with the export-list or import-list name and the list of peers. The **global** keyword displays the details of only the global listener and speaker.

```
Device# show cts sxp export-import-group speaker group_1

   Export-import-group: group_1
   Export-list-name: export_list_1
   Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

Device# show cts sxp export-import-group listener

Global Listener export-import-group: Not configured

   Export-import-group: group_1
   Export-list-name:  export_list_1
   Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

   Export-import-group: group_2
   Import-list-name: import_list_1
   Peer-list: 4.4.4.4, 5.5.5.5, 6.6.6.6


Device# show cts sxp export-import-group speaker group_1 detailed

    Export-import-group: group_1
    Export-list-name: export_list_1
    Export-list-content:
       vrf Red_vrf
       vrf Blue_vrf
    Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

Device# show cts sxp export-import-group listener detailed

    Global Listener export-import-group: Not configured

    Export-import-group: group_1
    Import-list-name: import_list_1
    Import-list-content:
       vlan-list
    Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

Device# show cts sxp export-import-group global

   Global Listener export-import-list Name: group_1
   Global Speaker export-import-list Name: group_2
```

Feature History for SGT Exchange Protocol

This table provides release and related 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	Feature Information
Cisco IOS XE Gibraltar 16.11.1	SGT Exchange Protocol	The SXP propagates the SGTs across network devices that do not have hardware support for Cisco Group-Based Policy.
Cisco IOS XE Cupertino 17.7.1	SGT Exchange Protocol	Support for this feature was introduced on the Cisco Catalyst 9600 Series Supervisor 2 Module (C9600X-SUP-2).
Cisco IOS XE Cupertino 17.9.1	SXP Version 5	SXP version 5 supports exporting VRF and VLAN information on the SXP packet to peer devices.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.