

Bidirectional SXP Support

- Feature History for Bidirectional SXP, on page 1
- Cisco TrustSec and SXP Roles, on page 1
- Bidirectional SXP Support, on page 2
- SXPv4 Loop Detection, on page 2
- Configure Bidirectional SXP Support , on page 2
- Configuration Examples for Bidirectional SXP Support, on page 4

Feature History for Bidirectional SXP

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	Bidirectional Security Group Tag (SGT) Exchange Protocol (SXP): Bidirectional SXP feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	Bidirectional SXP: With bidirectional SXP support, a single peer can function as both a speaker and a listener, allowing SXP bindings to flow in both directions over a single connection.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Cisco TrustSec and SXP Roles

Cisco TrustSec establishes secure network domains where devices authenticate one another. Within this system, the device originating data is called the "speaker," while the receiving device is the "listener."

Bidirectional SXP Support

With bidirectional SXP support, a single peer can function as both a speaker and a listener, allowing SXP bindings to flow in both directions over a single connection. This setup requires only one pair of IP addresses, with the listener initiating the connection and the speaker accepting it.

SXPv4 Loop Detection

SXP version 4 maintains support for loop detection, helping to prevent stale bindings within the network.

Configure Bidirectional SXP Support

To configure bidirectional SXP support, 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 sxp enable**

Example:

```
Device(config)# cts sxp enable
```

Enables the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4).

Step 4 **cts sxp default password** *password*

Example:

```
Device(config)# cts sxp default password Cisco123
```

(Optional) Specifies the Cisco TrustSec SGT SXP default password.

Step 5 **cts sxp default source-ip** *ipv4-address*

Example:

```
Device(config)# cts sxp default source-ip 10.20.2.2
```

(Optional) Configures the Cisco TrustSec SGT SXP source IPv4 address.

Step 6 **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} **both** [**vrf** *vrf-name*]

Example:

```
Device(config)# cts sxp connection peer 10.20.2.2 password default mode local both
```

Configures the Cisco TrustSec SXP peer address connection for a bidirectional SXP configuration.

- The **both** keyword configures the bidirectional SXP configuration.
- The **source** keyword specifies the IPv4 address of the source device. If no address is specified, the connection uses the default source address, if configured, or the address of the port.
- The **password** keyword specifies the password that Cisco TrustSec SXP uses for the connection using the following options:
  - **default**: Use the default Cisco TrustSec SXP password you configured using the cts sxp default password command.
  - **none**: A password is not used.
- 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.
  - **both**: Specifies that the device is both the speaker and the listener in the bidirectional SXP connection.
- The **optional** vrf keyword specifies the VRF to the peer. The default is the default VRF.

Step 7 **cts sxp speaker** *hold-time minimum-period*

Example:

```
Device(config)# cts sxp speaker hold-time 950
```

(Optional) Configures the global hold time (in seconds) of a speaker network device for Cisco TrustSec SGT SXPv4.

The valid range is from 1 to 65534. The default is 120.

Step 8 **cts sxp listener hold-time** *minimum-period maximum-period*

Example:

```
Device(config)# cts sxp listener hold-time 750 1500
```

(Optional) Configures the global hold time (in seconds) of a listener network device for Cisco TrustSec SGT SXPv4.

The valid range is from 1 to 65534. The default is 90 to 180.

Note
The *maximum-period* value must be greater than or equal to the minimum-period value.

Step 9 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode.

Step 10 **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

Example:

```
Device# show cts sxp connections
```

Displays Cisco TrustSec Exchange Protocol (SXP) status and connections.

Configuration Examples for Bidirectional SXP Support

These sections provide configuration examples for Bidirectional SXP support.

Example: Configure Bidirectional SXP Support

The following example shows how to enable bidirectional CTS-SXP and configure the SXP peer connection on Device-A to connect to Device-B:

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

The following example shows how to configure the bidirectional CTS-SXP peer connection on Device-B to connect to Device-A:

```
Device-B> enable
Device-B# configure terminal
Device-B(config)# cts sxp enable
Device-B(config)# cts sxp default password Password123
Device-B(config)# cts sxp default source-ip 10.20.2.2
Device-B(config)# cts sxp connection peer 10.10.1.1 password default mode local both
Device-B(config)# exit
```

Example: Verify Bidirectional SXP Support

The followinge example is a sample output of the **show cts sxp connections** command.

```
Device# show cts sxp connections

        SXP : Enabled
        Highest Version Supported: 4
        Default Password : Set
        Default Source IP: Not Set
        Connection retry open period: 120 secs
        Reconcile period: 120 secs
        Retry open timer is running
        ------------------------------------------
        Peer IP : 2.0.0.2
        Source IP : 1.0.0.2
```

```
        Conn status : On (Speaker) :: On (Listener)
        Conn version : 4
        Local mode : Both
        Connection inst# : 1
        TCP conn fd : 1(Speaker) 3(Listener)
        TCP conn password: default SXP password
        Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46
(dd:hr:mm:sec)
```

The followinge example is a sample output of the **show cts sxp connections brief** command.

```
        Device# show cts sxp connection brief

        SXP : Enabled
        Highest Version Supported: 4
        Default Password : Set
        Default Source IP: Not Set
        Connection retry open period: 120 secs
        Reconcile period: 120 secs
        Retry open timer is running
        ------------------------------------------------------
        Peer_IP Source_IP Conn Status Duration
        ------------------------------------------------------
        2.0.0.2 1.0.0.2 On(Speaker)::On(Listener) 0:00:37:17 (dd:hr:mm:sec)::0:00:37:19
(dd:hr:mm:sec)
```

The following table describes the various scenarios for the connection status output.

Node1	Node2	Node1 CLI Output for Connection Status	Node2 CLI Output for Connection Status
Both	Both	On (Speaker) On (Listener)	On (Listener) On (Speaker)
Speaker	Listener	On	On
Listener	Speaker	On	On