IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third Party Devices

Note   To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices

Table 1: Feature History

Feature Name	Release Information	Description
IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN and Third-Party Devices Over a Service VPN	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.x	This feature allows you to configure an IPv6 GRE or IPsec tunnel from a Cisco IOS XE Catalyst SD-WAN device to a third-party device over a service VPN.

Information About IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and third party devices

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

This feature allows you to configure an IPv6 GRE or IPSEC tunnel from Cisco IOS XE Catalyst SD-WAN devices to a third-party device over a service VPN. The following types are supported for a tunnel in a service VPN:

• IPv6 GRE tunnel over IPv4 underlay

• IPv6 GRE tunnel over IPv6 underlay

• IPsec IPv6 tunnel over IPv4 underlay

• IPsec IPv6 tunnel over IPv6 underlay

Restrictions for IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices

• This feature is configurable only through the device CLI template. Feature templates are not supported.

• Configuration groups is not supported.

• Dual stack is not supported for IPsec SVTI tunnels but supported for GRE tunnels.

• The interface name as loopback for tunnel source is not supported. When you use a loopback interface as a tunnel source, you must provide either an IPv4 or IPv6 address as the tunnel source field. You can provide an interface name as tunnel source field for the physical interface and sub-interface.

Supported Devices for IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices

Table 2: Supported Devices and Releases

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and later	• Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8500L Edge Platforms • Cisco Catalyst 8000V Edge Software • Cisco ASR 1001-HX Router • Cisco ASR 1002-HX Router • Cisco ISR1100 Series Routers • Cisco 4461 Integrated Services Router

Configure IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices Using a CLI Template

Configure a Common Source Interface

This section provides an example CLI configuration to configure a common source interface.

1. Enter the global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode.

   ```
   interface GigabitEthernet1
   ```

3. Enable the interface.

   ```
   no shutdown
   ```

4. Set an IP address for the interface.

   ```
   ip address 209.165.200.225 255.255.255.0
   ```

5. Configure an IPv6 address.

   ```
   ipv6 address 2001:DB8:200::225/64
   ```

6. Exit the interface configuration mode.

IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third Party Devices

Configure IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices Using a CLI Template

```
exit
```

This section provides an example CLI configuration to configure a loopback interface.

1. Configure a loopback interface.

   ```
   interface Loopback 0
   ```

2. Set an IP address for the interface.

   ```
   ip address 209.165.201.1 255.255.255.0
   ```

3. Configure an IPv6 address.

   ```
   ipv6 address 2001:DB8:201::1/64
   ```

4. Exit the interface configuration mode.

   ```
   exit
   ```

Here's the complete configuration example for configuring a common source interface.

```
interface GigabitEthernet5
 no shutdown
 ip address 209.165.202.129 255.255.255.0
 ipv6 address 2001:DB8:202::129/64
exit
interface Loopback0
 no shutdown
 ip address 209.165.201.1 255.255.255.0
 ipv6 address 2001:DB8:201::1/64
exit
```

Configure an IPv6 GRE Tunnel Over IPv4 Underlay

This section provides an example CLI configuration to configure an IPv6 GRE tunnel over IPv4 underlay.

1. Enter the global configuration mode.

   ```
   configure terminal
   ```

2. Create an interface tunnel.

   ```
   interface Tunnel64
   ```

3. Enable the interface.

   ```
   no shutdown
   ```

4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.

   ```
   vrf forwarding 1
   ```

5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.

   ```
   ipv6 address 2001:DB8:64::1/64
   ```

6. Set the source address for the tunnel interface in interface configuration mode.

   ```
   tunnel source 209.165.202.129
   ```

7. Set the destination address for the GRE tunnel interface in interface configuration mode.

   ```
   tunnel destination 209.165.202.158
   ```

IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third Party Devices

Configure IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices Using a CLI Template

8. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

```
tunnel route-via GigabitEthernet5 mandatory
```

Here's the complete configuration example for configuring an IPv6 GRE tunnel over IPv4 underlay.

```
interface Tunnel64
no shutdown
 vrf forwarding 1
 ipv6 address 2001:DB8:64::1/64
 tunnel source 209.165.202.129
 tunnel destination 209.165.202.158
 tunnel route-via GigabitEthernet5 mandatory
```

Configure an IPv6 GRE Tunnel Over IPv6 Underlay

This section provides an example CLI configuration to configure a IPv6 GRE tunnel over IPv6 underlay.

1. Enter the global configuration mode.

```
configure terminal
```

2. Enter the tunnel interface mode.

```
interface Tunnel66
```

3. Enable the interface.

```
no shutdown
```

4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.

```
vrf forwarding 1
```

5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.

```
ipv6 address 2001:DB8:166::1/64
```

6. Set the source address for the tunnel interface in interface configuration mode.

```
tunnel source 2001:DB8:15::15
```

7. Set the destination address for the GRE tunnel interface in interface configuration mode.

```
tunnel destination 2001:DB8:15::16
```

8. Set the encapsulation mode for the tunnel interface, in interface configuration mode.

```
tunnel mode gre ipv6
```

9. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

```
tunnel route-via GigabitEthernet5 mandatory
```

Here's the complete configuration example for configuring an IPv6 GRE tunnel over IPv6 underlay.

```
interface Tunnel66
 no shutdown
  vrf forwarding 1
  ipv6 address 2001:DB8:66::1/64
  tunnel source 2001:DB8:15::15
  tunnel destination 2001:DB8:15::16
```

IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third Party Devices

Configure IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices Using a CLI Template

```
tunnel mode gre ipv6
tunnel route-via GigabitEthernet5 mandatory
```

Configure an IPsec IPv6 Tunnel Over IPv4 Underlay

This section provides an example CLI configuration to configure an IPsec IPv6 tunnel over IPv4 underlay.

1. Enter the global configuration mode.

```
configure terminal
```

2. Enter the tunnel interface mode.

```
interface Tunnel164
```

3. Enable the interface.

```
no shutdown
```

4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.

```
vrf forwarding 1
```

5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.

```
ipv6 address 2001:DB8:164::1/64
```

6. Set the source address for the tunnel interface in interface configuration mode.

```
tunnel source 209.165.202.129
```

7. Set the destination address for the IPsec tunnel interface in interface configuration mode.

```
tunnel destination 209.165.202.158
```

8. Set the encapsulation mode for the tunnel interface, in interface configuration mode.

```
tunnel mode ipsec ipv4 v6-overlay
```

9. Associate the tunnel interface with an IPsec profile.

```
tunnel protection ipsec profile if-ipsec1-ipsec-profile164
```

10. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

```
tunnel route-via GigabitEthernet5 mandatory
```

Here's the complete configuration example for configuring an IPsec IPv6 tunnel over IPv4 underlay.

```
interface Tunnel164
no shutdown
 vrf forwarding 1
 ipv6 address 2001:DB8:164::1/64
 tunnel source 209.165.202.129
 tunnel destination 209.165.202.158
 tunnel mode ipsec ipv4 v6-overlay
 tunnel protection ipsec profile if-ipsec1-ipsec-profile164
 tunnel route-via GigabitEthernet5 mandatory
```

Configure an IPsec IPv6 Tunnel Over IPv6 Underlay

This section provides an example CLI configuration to configure an IPsec IPv6 tunnel over IPv6 underlay.

1. Enter the global configuration mode.

IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third Party Devices

Verify IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Device Devices and Third-Party Devices in Service VPN

```
configure terminal
```

2. Enter the tunnel interface mode.

```
interface Tunnel166
```

3. Enable the interface.

```
no shutdown
```

4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.

```
vrf forwarding 1
```

5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.

```
ipv6 address 2001:DB8:166::1/64
```

6. Set the source address for the tunnel interface in interface configuration mode.

```
tunnel source 2001:DB8:15::15
```

7. Set the destination address for the IPsec tunnel interface in interface configuration mode.

```
tunnel destination 2001:DB8:15::16
```

8. Set the encapsulation mode for the tunnel interface, in interface configuration mode.

```
tunnel mode ipsec ipv6
```

9. Associate the tunnel interface with an IPsec profile.

```
tunnel protection ipsec profile if-ipsec1-ipsec-profile166
```

10. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

```
tunnel route-via GigabitEthernet5 mandatory
```

Here's the complete configuration example for configuring an IPsec IPv6 tunnel over IPv6 underlay.

```
interface Tunnel166
no shutdown
 vrf forwarding 1
 ipv6 address 2001:DB8:166::1/64
 tunnel source 2001:DB8:15::15
 tunnel destination 2001:DB8:15::16
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile if-ipsec1-ipsec-profile166
 tunnel route-via GigabitEthernet5 mandatory
```

Verify IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Device Devices and Third-Party Devices in Service VPN

The following is a sample output from the **show run interface** *type/number* command.

```
Device#show run interface tunnel 164
interface Tunnel164
no shutdown
```

IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third Party Devices

Verify IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Device Devices and Third-Party Devices in Service VPN

```
vrf forwarding 1
ipv6 address 2001:DB8:164::1/64
tunnel source 209.165.202.129
tunnel destination 209.165.202.158
tunnel mode ipsec ipv4 v6-overlay
tunnel protection ipsec profile if-ipsec1-ipsec-profile164
tunnel route-via GigabitEthernet5 mandatory
```

The following is a sample output from the **show adjacency tunnel164 internal** command.

```
Device#show adjacency tunnel164 internal
Protocol Interface           Address
IPV6     Tunnel164           point2point(7)
                             0 packets, 0 bytes
                             epoch 0
                             sourced in sev-epoch 14
                             empty encap string
                             P2P-ADJ
                             Next chain element:
                               IP adj out of GigabitEthernet5, addr 209.165.202.158
718424FDE3D8
                               parent oce 0x718424FDE498
                               frame originated locally (Null0)
                             L3 mtu 1500
                             Flags (0x5938C4)
                             Fixup enabled (0x400000)
                                   IPSec tunnel
                             HWIDB/IDB pointers 0x71842EA25C50/0x71842EA30E90
                             IP redirect enabled
                             Switching vector: IPv6 midchain adjacency oce
                        Post encap features: IPSEC Post-encap output classification
Protocol Interface           Address
                             Next-hop cannot be inferred
                             IOSXE-RP Inject sbublock:
                               pak transmitted 14
                               last inject at 00:00:02 ago
                             IP Tunnel stack to 209.165.202.158 in Default (0x0)
                              nh tracking enabled: 209.165.202.158/32
                              route-via enabled: GigabitEthernet5 (mandatory)
                              IP adj out of GigabitEthernet5, addr 209.165.202.158
                             Platform adj-id: 0xF80001D7, 0x0, tun_qos_dpidx:0
                             Adjacency pointer 0x718424FDD8E8
                             Next-hop unknown
```