# Cisco Catalyst SD-WAN Carrier Supporting Carrier

**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.

***Table 1: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Cisco Catalyst SD-WAN Support for Carrier Supporting Carrier Connectivity | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a<br><br>Cisco vManage Release 20.6.1 | The feature adds support for carrier supporting carrier (CSC) connectivity on Cisco IOS XE Catalyst SD-WAN devices.<br><br>CSC enables you to interconnect IP or multiprotocol label switching (MPLS) networks operating at different sites over an MPLS backbone network. Using CSC requires an edge router that supports CSC functionality, called a carrier edge (CE) device, at each site. This feature enables a Cisco IOS XE Catalyst SD-WAN device to serve as a CE device, making it unnecessary to have a separate dedicated CE device at each site managed by Cisco Catalyst SD-WAN. |

# Prerequisites for Cisco Catalyst SD-WAN Carrier Supporting Carrier

A Cisco IOS XE Catalyst SD-WAN device that functions as a CSC customer edge (CSC-CE) device must have an external border gateway protocol (eBGP) peer connection with the CSC provider edge (CSC-PE) router.

# Restrictions for Cisco Catalyst SD-WAN Carrier Supporting Carrier

- IPv6 addressing is not supported.
- Network address translation (NAT) for the MPLS link is not supported.
- Firewall services on the MPLS link are not supported.
- Cloud OnRamp for SaaS is not supported.
- VPN route leak is not supported.

# Information About Cisco Catalyst SD-WAN Carrier Supporting Carrier

### Carrier Supporting Carrier

Carrier supporting carrier (CSC) is a hierarchical VPN model that allows organizations to interconnect their IP or MPLS networks located at different sites over an MPLS backbone network. This eliminates the need for the organizations to build and maintain their own MPLS backbone.

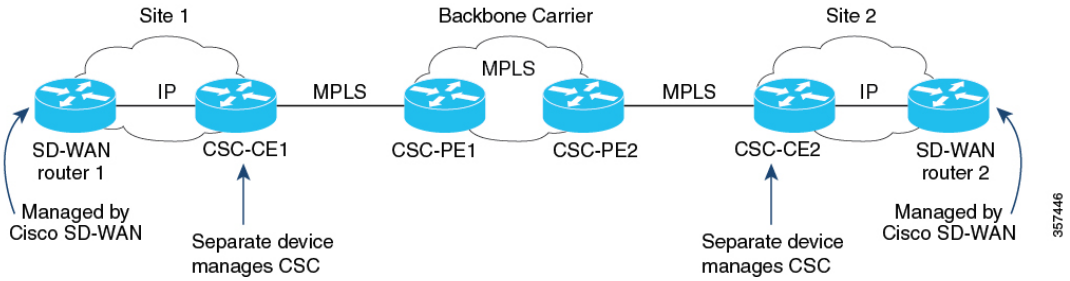
The following are components of CSC:

- Backbone carrier: The service provider that provides the backbone network. Typically, the backbone carrier network employs multiple segments to segregate the traffic of different customer carriers that share the backbone carrier network. The backbone carrier may be managed by the same organization or by a different organization as the customer carriers.
- Customer carrier: An organization that uses the backbone network to route traffic from one site to another. The customer carrier may be part of the organization that operates the backbone network, or may be independent.
- CSC-CE: Customer edge (CE) device. This device operates within a local site network and connects the site to the backbone carrier, using an MPLS connection. It utilizes the backbone carrier to connect to other sites.
- CSC-PE: Provider edge (PE) device. This device operates within the backbone carrier network and connects to CSC-CE devices at customer sites, using an MPLS connection.

### Cisco Catalyst SD-WAN Carrier Supporting Carrier

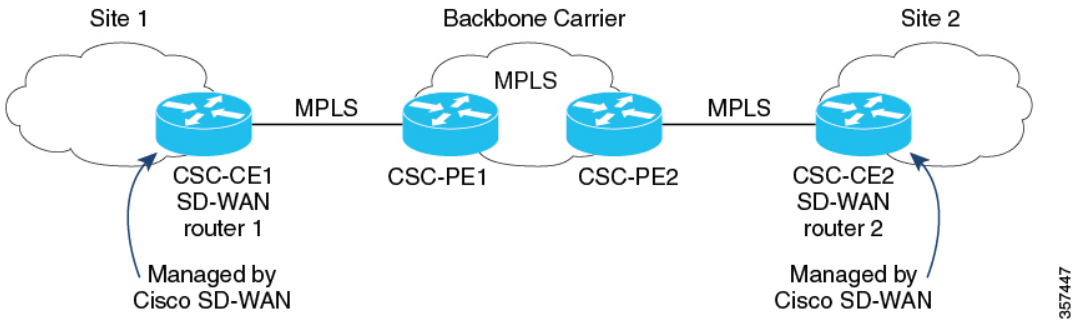
The following illustration shows a CSC network topology with a Cisco IOS XE Catalyst SD-WAN device at each site, using a release earlier than Cisco IOS XE Catalyst SD-WAN Release 17.6.1a. Because the Cisco IOS XE Catalyst SD-WAN devices cannot function as a CSC-CE when using these releases, the topology requries two separate devices at each site: an edge device managed by Cisco Catalyst SD-WAN and a separate CSC-CE device.

***Figure 1: Carrier Supporting Carrier with Cisco Catalyst SD-WAN, Before Cisco IOS XE Catalyst SD-WAN Release 17.6.1a***




From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, a Cisco IOS XE Catalyst SD-WAN device can serve as a CSC-CE device, making it unnecessary to have a separate dedicated CSC-CE device. As compared with the previous illustration, the following illustration shows a simpler CSC network topology, with Cisco IOS XE Catalyst SD-WAN devices providing CSC-CE functionality.

***Figure 2: Carrier Supporting Carrier with Cisco Catalyst SD-WAN, Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Later***




### Traffic Flow

If a CSC-CE device only has an MPLS connection to the neighbor CSC-PE device, then all traffic from the CSC-CE device uses the MPLS connection, including the following traffic types:

- Service VPN traffic
- Control traffic
- Cisco Catalyst SD-WAN bidirectional forwarding detection (BFD) probe traffic

If a CSC-CE device has an MPLS connection to the neighbor CSC-PE device and also has a separate connection to the internet, then the traffic from the CSC-CE device may use different connections, as follows:

- Based on the configured traffic policy, control traffic and BFD probe traffic can use the internet and MPLS connections.

- Service VPN traffic uses only the MPLS connection.

### Label Switching

For traffic that uses an MPLS connection between a CSC device and the backbone carrier, the backbone carrier manages the traffic using label-switched paths, and has no information about the customer carrier routes.

# Benefits of Cisco Catalyst SD-WAN Carrier Supporting Carrier

Cisco Catalyst SD-WAN support for CSC enables a Cisco IOS XE Catalyst SD-WAN device to serve as an edge device at a site where CSC is required. With the Cisco IOS XE Catalyst SD-WAN device providing CSC-CE functionality, it is not necessary to have a separate router serving the CE role.

# Use Cases for Cisco Catalyst SD-WAN Carrier Supporting Carrier

Cisco Catalyst SD-WAN support for CSC is useful for global organizations that use CSC with a backbone carrier to support multiple, separate divisions of the organization. Each division's traffic is private but shares a common backbone carrier.

Service providers that use a CSC topology may benefit from Cisco Catalyst SD-WAN support for CSC. Carrier edge devices managed by Cisco Catalyst SD-WAN can support CSC, making it unnecessary to have a separate device to manage CSC functionality.

# Configure Carrier Supporting Carrier

You can configure the CE devices for CSC in the following ways:

- (Recommended) In Cisco SD-WAN Manager, use a BGP feature template.
- In Cisco SD-WAN Manager, use a CLI template to configure CSC by CLI.

## Configure Carrier Supporting Carrier

Perform the following steps to configure a CE device for CSC using a new feature template.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and click **Create Template**. From the drop-down, choose **From Feature Template**.

**Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**.

3. In the **Device Model** field, choose the correct device model.
4. In the **Device Role** field, choose **SDWAN Edge**.
5. In the **Template Name** field, enter a name for the template.

6. In the **Transport & Management VPN** section, in the **Cisco VPN 0** field, choose a template to configure VPN 0 according to the network architecture.

   For information about configuring VPN 0, see Configure Interfaces in the WAN Transport VPN (VPN 0) in the Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x.

7. In the **Cisco VPN Interface Ethernet** field, choose a template to configure the interface.

   For information about configuring this field, see Configure VPN Ethernet Interface in the Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x.

8. In the **Transport & Management VPN** section, click **Cisco BGP** to add the Cisco BGP field.

   For information about configuring a BGP template, see Configure BGP Using SD-WAN Manager Templates in the Cisco Catalyst SD-WAN Routing Configuration Guide, Cisco IOS XE Release 17.x.

9. In the **MPLS Interface** section, in the **Interface Name 1** field, enter the interface used to connect the device to the backbone carrier.

10. In the **Neighbor** section, click **Advanced Options** to display CSC options.

11. Configure the following fields, which are specific to CSC support:

| Field | Description |
|---|---|
| Send Label | Choose **On** to enable CSC support. |
| Explicit Null | If the device uses a loopback WAN interface, choose **On**. |
| As Override | If the two CE devices (CE1 and CE2) that connect through the backbone carrier use the same autonomous system (AS) number, choose **On**. |
| Allowas In | Similarly to **As Override**, if the two CE sites use the same AS number, choose **On**. |

12. Click **Save** to save the BGP configuration.

13. Click **Create** to create the feature template.

    The **Configuration** > **Templates** page appears, showing available templates.

14. Attach the template to the device.

    a. On the **Configuration** > **Templates** page.

    b. Click **Device Templates**.

**Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**.

    c. For the new template, click **…** and choose **Attach Devices**.

    d. Move a device to the **Selected Devices** column and click **Attach**.

# Configure Carrier Supporting Carrier Using the CLI

We recommend that you use the BGP feature template in Cisco SD-WAN Manager to configure Cisco IOS XE Catalyst SD-WAN devices for use with CSC. If it is necessary to configure a device by CLI, use a CLI template in Cisco SD-WAN Manager.

### Before You Begin

Before you configure a Cisco IOS XE Catalyst SD-WAN device to provide CSC-CE functionality, apply a BGP configuration to the device. The following steps add CSC functionality.

### Configure Carrier Supporting Carrier the CLI

1. Configure the following on CSC-CE1:

   a. Configure the device to map MPLS labels to VRFs. For incoming traffic, the router checks the MPLS label of the traffic and uses the IP loookup table of the VRF mapped to that label. For example, if MPLS label 10 is mapped to VRF 1, then for incoming traffic with the MPLS label 10, the router uses the IP lookup table of VRF 1. For information about mmapping MPLS labels to VRFs, see the Cisco documentation for MPLS forwarding commands.

   ```
   Device# config-transaction
   Device(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
   Device(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
   Device(config)# mpls label range min-label max-label static min-static-label
   max-static-label
   ```

   b. Enable multiprotocol label switching (MPLS) on the interface.

   ```
   Device(config)# interfaceinterface
   Device(config-if)# mpls bgp forwarding
   ```

   c. Enter router configuration mode and configure the router to run a BGP process.

   ```
   Device(config-if)# router bgp bgp-number
   ```

   d. Configure a CSC-PE device as the neighbor, where *neighbor-ip* is the address of the neighbor CSC-PE device.

   ```
   Device(config-router)# neighbor neighbor-ip allowas-in
   ```

   e. If the device uses a loopback WAN interface, advertise the ability of the router to send MPLS labels with BGP routes. The **explicit-null** keyword enables a CSC-CE router to send labels with a value of 0 to its neighbor.

   **Note** If you include the **neighbor** *neighbor-ip* **send-label explicit-null** command on a device that does not use a loopback WAN interface, it does not adversely impact performance.

   ```
   Device(config-router)# neighbor neighbor-ip send-label explicit-null
   ```

2. Configure the following on CSC-CE2:

   a. Configure the device to map MPLS labels to VRFs. For incoming traffic, the router checks the MPLS label of the traffic and uses the IP loookup table of the VRF mapped to that label. For example, if MPLS label 10 is mapped to VRF 1, then for incoming traffic with the MPLS label 10, the router uses

the IP lookup table of VRF 1. For information about mmapping MPLS labels to VRFs, see the Cisco documentation for MPLS forwarding commands.

```
Device# config-transaction
Device(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
Device(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
Device(config)# mpls label range min-label max-label static min-static-label
max-static-label
```

**b.** Enable multiprotocol label switching (MPLS) on the interface.

```
Device(config)# interfaceinterface
Device(config-if)# mpls bgp forwarding
```

**c.** Enter router configuration mode and configure the router to run a BGP process.

```
Device(config-if)# router bgp bgp-number
```

**d.** Configure a CSC-PE device as the neighbor, where *neighbor-ip* is the address of the neighbor CSC-PE device.

```
Device(config-router)# neighbor neighbor-ip as-override
```

**e.** If the device uses a loopback WAN interface, advertise the ability of the router to send MPLS labels with BGP routes.

```
Device(config-router)# neighbor neighbor-ip send-label explicit-null
```

### Example

The following examples show a complete BGP configuration, including CSC functionality, for two devices: CSC-CE1 and CSC-CE2.

- CSC-CE1 has the address 10.1.1.10.
- CSC-CE2 has the address 10.1.1.20.
- CSC-PE1 (the neighbor of CSC-CE1) has the address 10.2.2.10.
- CSC-PE2 (the neighbor of CSC-CE2) has the address 10.2.2.20.

The following is the configuration for CSC-CE1:

```
mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
mpls label range 100000 1048575 static 16 99
interface GigabitEthernet2
 no shutdown
 mpls bgp forwarding
 ip address 10.1.1.15 255.255.255.0

router bgp 10
 bgp log-neighbor-changes
 bgp router-id 172.16.255.15
 neighbor 10.1.1.20 remote-as 100
 neighbor 10.1.1.20 fall-over bfd
address-family ipv4 unicast
  maximum-paths 4
  neighbor 10.1.1.20 activate
  neighbor 10.1.1.20 advertisement-interval 30
  neighbor 10.2.2.10 allowas-in
  neighbor 10.2.2.10 send-label explicit-null
```

```
  neighbor 10.1.1.20 send-community both
  exit-address-family
 !
 timers bgp 60 180
```

The following is the configuration for CSC-CE2:

```
mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
mpls label range 100000 1048575 static 16 99
interface GigabitEthernet5
 ip address 10.0.6.11 255.255.255.0
 negotiation auto
 mpls bgp forwarding

router bgp 10
 bgp log-neighbor-changes
 bgp router-id 172.16.255.11
 neighbor 10.1.1.10 remote-as 200
 address-family ipv4 unicast
  neighbor 10.1.1.10 activate
  neighbor 10.1.1.10 advertisement-interval 30
    neighbor 10.2.2.20 as-override
    neighbor 10.2.2.20 send-label explicit-null
  network 10.0.7.0 mask 255.255.255.0
  redistribute connected
  redistribute static
  exit-address-family
```

# Verify That a Device is Configured for Carrier Supporting Carrier

To verify that a device is configured correctly to reach a remote CSC-CE device, execute the **show ip route** *remote-csc-ce-device-address* command on the device. Verify that the command output shows the following:

- A routing entry for the remote site IP address.
- One or more routing descriptor blocks describing the next-hop addresses for the path to the remote CSC-CE device. Verify that each descriptor block includes an MPLS label.

### Example

```
Device# show ip route 10.0.1.100
Routing entry for 10.0.1.0/24
...
Routing Descriptor Blocks:
* 10.1.1.100, from 10.1.1.100, 00:00:50 ago
...
MPLS label: 26
…
```

If the device is not configured correctly, the output displays the following:

```
% Subnet not in table
```