Secondary Regions

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.

- Secondary Regions, on page 2
- Information About Secondary Regions, on page 2
- Matching Routes by Path Type, Region, or Role, on page 5
- Restrictions for Secondary Regions, on page 6
- Use Cases for Secondary Regions, on page 6
- Configure a Secondary Region Using Cisco SD-WAN Manager, on page 7
- Configure a Secondary Region Using the CLI, on page 9
- Verify a Device Secondary Region Assignment Using Cisco SD-WAN Manager, on page 11
- Verify a Device Secondary Region Assignment Using the CLI, on page 11
- Verify an Interface Secondary Region Mode Using the CLI, on page 12
- Verify an Interface Secondary Region Assignment Using the CLI, on page 13

Secondary Regions

Table 1: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric: Secondary Regions	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	Secondary regions provide another facet to the Multi-Region Fabric architecture and enable direct tunnel connections between edge routers in different primary access regions. When you assign an edge router a secondary region, the router effectively operates in two regions simultaneously, and has different paths available through its primary and secondary regions.

Information About Secondary Regions

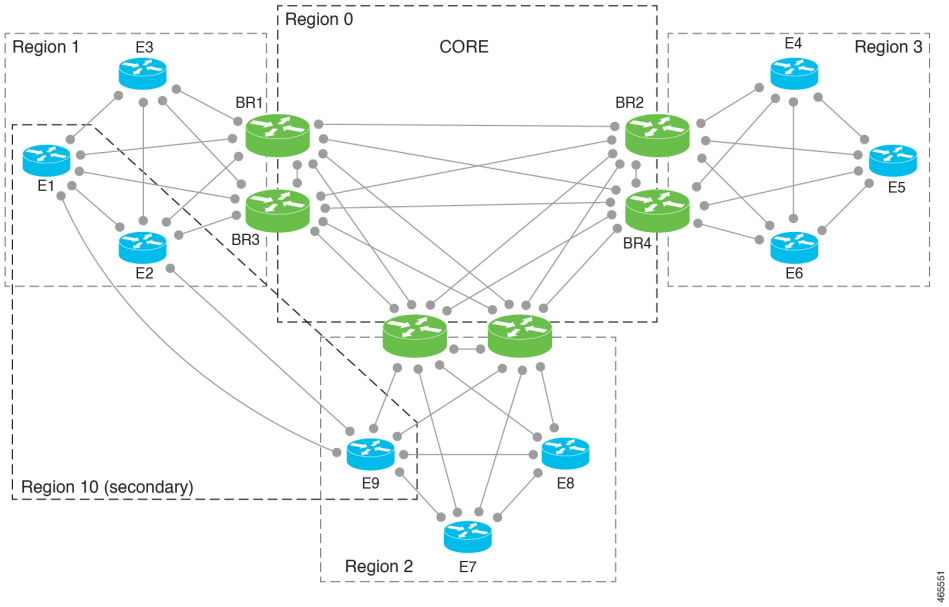
Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

In the most basic Multi-Region Fabric architecture, each device belongs to a single region. Connections from an edge router in one region to an edge router in another region are routed through border routers and region 0 and therefore require multiple hops.

Secondary regions provide another facet to the architecture and enable additional functionality. A secondary region operates more simply than a primary region: it contains only edge routers and it enables direct tunnel connections between edge routers in different primary regions. When you add an edge router to a secondary region, the router effectively operates in two regions simultaneously, and has different paths available through its primary and secondary regions.

You can create multiple secondary regions within the network to address the specific routing needs of different sets of edge routers, but an edge router cannot belong to more than one secondary region.

Figure 1: Multi-Region Fabric with a Secondary Region



Using Secondary Regions

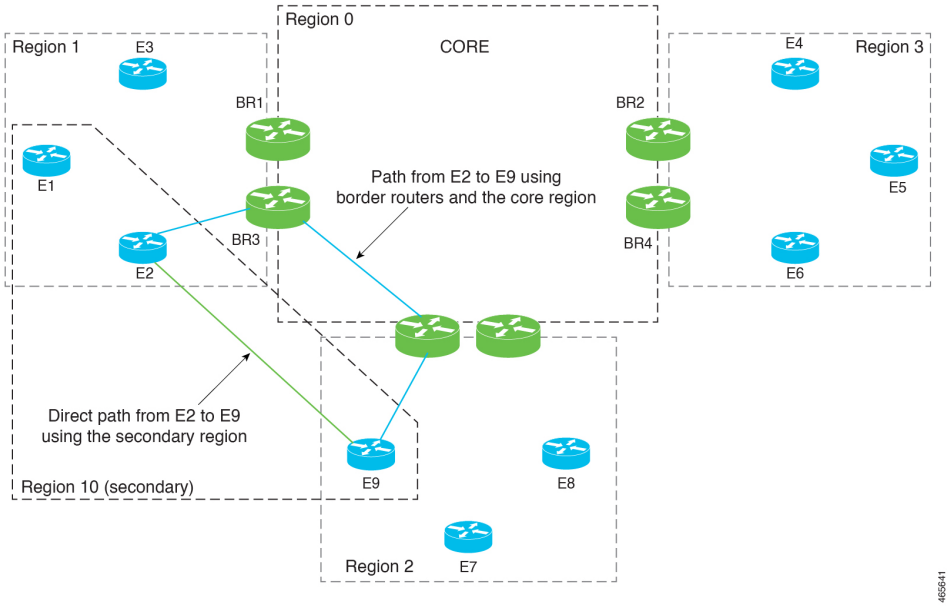
You can configure secondary region paths for any of the following:

- Load balancing using paths in the primary and secondary regions
- Directing specific applications to use a secondary-region path, which can be a premium path with better performance

Primary-Region Path and Secondary-Region Path

When a direct path is available to reach a destination, by default the overlay management protocol (OMP) enables only the direct path to the routing forwarding layer because the direct path uses fewer hops. The result is that the forwarding layer, which includes application-aware policy, can only use the direct path. You can disable this comparison of the number of hops so that traffic can use either the direct secondary-region path (fewer hops) or the primary-region path (more hops). When you disable the comparison of the number of hops, OMP applies equal-cost multi-path routing (ECMP) to all routes, and packets can use all available paths. See Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using Cisco SD-WAN Manager, on page 9.

Figure 2: Direct Path Using a Secondary Region and Multi-Hop Path Using Primary Regions and the Core Region



Control Policy

When creating a control policy for the Cisco SD-WAN Controller for the secondary region, you can match traffic according to whether it is using a primary-region path or a secondary-region path.

Workflow

1. On a device, configure a secondary region at the device level.

   See Configure a Secondary Region ID for an Edge Router Using Cisco SD-WAN Manager, on page 7.

2. On the device, specify the TLOCs that can use the secondary region.

   See Configure the Secondary Region Mode of a TLOC Using the CLI, on page 10.

3. Configure the TLOC to operate either in the secondary region only, or in both the primary and secondary regions.

   See Configure the Secondary Region Mode for a TLOC Using Cisco SD-WAN Manager, on page 8.

4. Enable the device to use both the primary region path and the secondary region path.

   See Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using Cisco SD-WAN Manager, on page 9.

5. Assign a Cisco SD-WAN Controller to the secondary region. Use a Cisco SD-WAN Controller that does not operate in any of the access regions of devices using the secondary region. To ensure this, we recommend assigning a Cisco SD-WAN Controller that operates only in a secondary region, and does not operate in any access regions. For example, you can assign a Cisco SD-WAN Controller that operates only in region 0 to operate also in a secondary region.

   See Assign Regions to a Cisco Catalyst SD-WAN Controller Using Cisco SD-WAN Manager.

Terminology

With the introduction of secondary regions to the Multi-Region Fabric architecture, it is valuable to clarify the terminology used here.

Term	Explanation or Equivalent Terms
Core region	Region 0
Access region	Any region other than region 0
Primary access region	Primary region
Secondary access region	Secondary region
Primary-region path	A path from an edge router to a border router, through the core region, to another border router, to an edge router in a different region
Secondary-region path	A direct path from an edge router 1 in one primary region to edge router 2 in another primary region, where edge routers 1 and 2 are in the same secondary region

Benefits of Secondary Regions

- Ability to route specific traffic using a direct tunnel from one edge router to another, between different primary regions.
- Ability to provide high-volume throughput, such as traffic to a data center, on a direct tunnel between different primary regions. Routing the high-volume throughput directly can prevent overloading border routers with excessive traffic volume.

Matching Routes by Path Type, Region, or Role

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

Path Type

When configuring a control policy for a Multi-Region Fabric architecture, you can match routes according to whether the route is using one of the following:

- Hierarchical path: Match a route that includes hops from an access region to a border router, through region 0, to another border router, then to an edge router in a different access region.

  To view the hierarchical path routes, use the **show sdwan omp routes** command and note the routes that list three regions in the **REGION PATH** column.

- Direct path: Match direct paths (direct routes) from one edge router to another edge router. You can enable a direct path between edge routers in different access regions by configuring a secondary region, and adding the two edge routers to the secondary region. See Information About Secondary Regions, on page 2.

To view the direct path routes, use the **show sdwan omp routes** command and note the routes that list one region in the **REGION PATH** column.

- Transport gateway path: Match a route that is re-originated by a router that has transport gateway functionality enabled.

  For information about transport gateways, see Information About Transport Gateways.

Region and Role

Similarly to matching by path type, you can match routes by the region or role (edge router or border router) of the device that originates the route.

Restrictions for Secondary Regions

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

- Secondary regions apply only to edge routers, not border routers.
- A router can belong to only one secondary region.
- A Cisco SD-WAN Controller that you assign to a secondary region must not operate in any of the primary (access) regions of devices using the secondary region. To ensure this, we recommend assigning a Cisco SD-WAN Controller that only operates in the secondary region, and does not operate in any access regions.
- You cannot configure a secondary region on a router that is configured as a transport gateway.

Note Attempting to configure a secondary region on such a router results in an error.

Use Cases for Secondary Regions

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

Use Case 1: Specific Application Traffic

An organization using a Multi-Region Fabric architecture chooses to route specific application traffic between sites in two different regions: region 1 and region 2, using a direct path route to reduce bandwidth demands on border routers. The organization arranges a carrier for this purpose between the two sites.

A network administrator configures secondary regions for an edge router in region 1 and an edge router in region 2 so that the two routers are both in secondary region 5, as follows:

- Edge router ER10

  Primary region: 1
  Secondary region: 5

- Edge router ER20

  Primary region: 2
  Secondary region: 5

The network administrator configures a direct tunnel between edge router ER10 and edge router ER20 and configures a policy that routes the specific application traffic through the direct tunnel.

Use Case 2: High Volume Data Center

An organization using a Multi-Region Fabric architecture has a data center in region 1, served by edge router ER10. Sites in regions 2, 3, and 4 (served by edge routers ER20, ER30, and ER40) connect to the data center and generate a high volume of traffic. The organization uses a premium service provider link for the core region.

To avoid routing the high-volume data center traffic through the premium link used in the core region, the network administrator configures a secondary region that includes the data center (ER10), and includes each of the remote sites (ER20, ER30, and ER40) to enable them to connect to the data center using direct tunnels. Using direct tunnels for the high-volume traffic reduces the bandwidth demands on the core region.

The primary and secondary region configuration is as follows:

- Data center: Edge router ER10

  Primary region: 1
  Secondary region: 5

- Remote site: Edge router ER20

  Primary region: 2
  Secondary region: 5

- Remote site: Edge router ER30

  Primary region: 3
  Secondary region: 5

- Remote site: Edge router ER40

  Primary region: 4
  Secondary region: 5

Configure a Secondary Region Using Cisco SD-WAN Manager

Configure a Secondary Region ID for an Edge Router Using Cisco SD-WAN Manager

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

3. Do one of the following:
   - Create a system template for the device.
   - In the table, locate the existing system template for the device. In the row for the template, click **…** and choose **Edit**.
4. In the **Basic Configuration** section, in the **Secondary Region ID** field, enable Global mode and enter the number of the secondary region, in the range 1 to 63.
5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Configure the Secondary Region Mode for a TLOC Using Cisco SD-WAN Manager

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

Before You Begin

This procedure describes how to configure the secondary region mode for a TLOC using a Cisco VPN Interface Ethernet template. For information about how to use the template in general, including how to specify the interface to which it is applied, see Configure VPN Ethernet Interface in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide*.

Configure the Secondary Region Mode for a TLOC

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create a Cisco VPN Interface Ethernet template for the device.
   - In the table, locate the existing Cisco VPN Interface Ethernet template for the device. In the row for the template, click **…** and choose **Edit**.
4. Navigate to the **Tunnel** section, and within that section the **Advanced Options** section.
5. In the **Enable Secondary Region** field, enable Global mode and choose one of the following options:

Option	Description
Only in Secondary Region	Configure the interface to handle only traffic in the secondary region.
Shared Between Primary and Secondary Regions	Configure the interface to handle traffic in the primary and secondary regions.

Note The interface inherits the secondary region assignment configured for the device at the system level.

6. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using Cisco SD-WAN Manager

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create a Cisco OMP template for the device.
   - In the table, locate the existing OMP template for the device. In the row for the template, click **…** and choose **Edit**.
4. Navigate to the **Best Path** section, and in the **Ignore Region-Path Length During Best-Path Algorithm** field, choose **On**.

   When you select **On**, the template automatically selects **Direct-Tunnel Path** and **Hierarchical Path**.

Note The default value is Off, and by default, OMP gives preference to a direct tunnel path over a hierarchical path because the direct path has fewer hops.

5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Configure a Secondary Region Using the CLI

Configure a Secondary Region ID for an Edge Router Using the CLI

1. Enter configuration mode.

   ```
   Device#config-transaction
   ```

2. Enter system configuration mode.

   ```
   Device(config)#system
   ```

3. Assign a region and secondary region.

   A device can only have a single secondary region assignment. If you have previously assigned a secondary region to the device, the new secondary region assignment replaces the previous.

   When you enable secondary region traffic for one or more TLOC interfaces, the interfaces inherit the secondary region ID that you assign at the system level.

```
Device(config-system)#region region-id secondary-region region-id
```

Example

```
Device#config-transaction
Device(config)#system
Device(config-system)#region 1 secondary-region 20
```

Configure the Secondary Region Mode of a TLOC Using the CLI

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

1. Enter configuration mode.

   ```
   Device#config-transaction
   ```

2. Enter VPN 0 configuration mode.

   ```
   Device(config)#sdwan
   ```

3. Specify an interface.

   ```
   Device(config-sdwan)#interface interface
   ```

4. Enter tunnel interface configuration mode.

   ```
   Device(config-sdwan-interface)#tunnel-interface
   ```

5. Choose one of the following modes for the TLOC to configure the TLOC to be used for primary- and secondary-region traffic, or exclusively for secondary-region traffic.

Mode	Description
secondary-only	The TLOC can handle only traffic in the device's secondary region.
secondary-shared	The TLOC can handle traffic in the device's primary and secondary regions.

   ```
   Device(config-tunnel-interface)#region {secondary-only | secondary-shared}
   ```

Example 1

This example configures the TLOC to handle primary- and secondary-region traffic.

```
Device#config-transaction
Device(config)#sdwan
Device(config-sdwan)#interface GigabitEthernet0/0/0
Device(config-interface-GigabitEthernet0/0/0)#tunnel-interface
Device(config-tunnel-interface)#region secondary-shared
```

Example 2

This example restores the default behavior, in which the TLOC does not handle secondary region traffic.

```
Device#config-transaction
Device(config)#sdwan
```

```
Device(config-sdwan)#interface GigabitEthernet0/0/0
Device(config-interface-GigabitEthernet0/0/0)#tunnel-interface
Device(config-tunnel-interface)#no region
```

Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using the CLI

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

1. Enter configuration mode.

   ```
   Device#config-transaction
   ```

2. Enter OMP configuration mode.

   ```
   Device(config)#sdwan omp
   ```

3. Enable the device to use both the primary-region path (multiple hops) and the secondary-region path (direct path).

   ```
   Device(config-omp)#best-path region-path-length ignore
   ```

Note You can use the **no** form of the command to disable this.

Verify a Device Secondary Region Assignment Using Cisco SD-WAN Manager

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. In the table, click a device.
3. Click **Real Time**.
4. In the **Device Options** field, choose **Control Local Properties**.

   The **Region ID Set** field shows the primary and secondary regions.

Verify a Device Secondary Region Assignment Using the CLI

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

Use the **show sdwan running-config system** command on a device to verify that a secondary region is configured. The **region** and **secondary-region** fields show the primary region and secondary region.

```
Device#show sdwan running-config system
system
 system-ip             175.2.55.10
 domain-id             1
 site-id               2200
 region 2
  secondary-region 20
 !
```

You can also use the **show sdwan omp summary** command on a device to verify the primary region ID (in the **region-id** field) and secondary region ID (in the **secondary-region-id** field).

```
Device#show sdwan omp summary
...
region-id                    1
secondary-region-id          20
```

Verify an Interface Secondary Region Mode Using the CLI

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

Use the **show sdwan running-config sdwan** command (Cisco IOS XE Catalyst SD-WAN device) or the **show running-config vpn 0 interface** *interface-name* command (Cisco vEdge device) to view the secondary region mode of an interface. The mode appears in the **region** field. The mode options are **secondary-only** and **secondary-shared**.

The following example is for a Cisco IOS XE Catalyst SD-WAN device.

```
Device#show sdwan running-config sdwan
sdwan
 interface GigabitEthernet1
  ip address 173.3.1.11/24
  tunnel-interface
   encapsulation ipsec
   color 3g
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   region secondary-only
  !
  no shutdown
 !
!
```

The following example is for a Cisco vEdge device.

```
Device#show running-config vpn 0 interface ge0/1
vpn 0
 interface ge0/1
  ip address 173.3.1.11/24
  tunnel-interface
   encapsulation ipsec
   color 3g
   no allow-service bgp
```

```
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   region secondary-only
  !
  no shutdown
 !
!
```

Verify an Interface Secondary Region Assignment Using the CLI

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

On a device, use the **show sdwan control local-properties** command (Cisco IOS XE Catalyst SD-WAN device) or the **show control local-properties** command (Cisco vEdge device) to view the region assignment for each interface.

In the output of the **show sdwan control local-properties** command, for each interface, the **REG IDs** column shows the region assignment.

```
Device#show sdwan control local-properties
...
                  PUBLIC           PUBLIC PRIVATE          PRIVATE   PRIVATE
      MAX   RESTRICT/           LAST         SPI TIME    NAT  VM
INTERFACE         IPv4             PORT   IPv4            IPv6      PORT    VS/VM COLOR
STATE CNTRL CONTROL/     LR/LB  CONNECTION   REMAINING   TYPE CON REG

            STUN                                                PRF IDs
-------------------------------------------------------------------------------------------
GigabitEthernet1       172.2.2.11      12366  172.2.2.11      ::        12366    4/1  lte
     up     2      no/yes/no   No/No  0:00:00:16   0:11:58:49  N    5  2
GigabitEthernet2       173.2.2.11      12366  173.2.2.11      ::        12366    4/0  3g
     up     2      no/yes/no   No/No  0:00:00:16   0:11:58:49  N    5  2,10
```

In the output of the **show control local-properties** command, for each interface, the **REGION IDs** column shows the region assignment.

```
Device#show control local-properties
           PUBLIC           PUBLIC PRIVATE          PRIVATE  PRIVATE                    MAX
     CONTROL/           LAST         SPI TIME    NAT  CON REGION
INTERFACE  IPv4           PORT   IPv4            IPv6     PORT     VS/VM COLOR  STATE CNTRL
   STUN        LR/LB  CONNECTION   REMAINING   TYPE PRF IDs
-------------------------------------------------------------------------------------------
ge0/0      172.3.1.11      12366  172.3.1.11      ::       12366    4/1  lte     up     2
     no/yes/no   No/No  0:00:00:04   0:11:59:38  N    5  3
ge0/1      173.3.1.11      12366  173.3.1.11      ::       12366    4/0  3g      up     2
     no/yes/no   No/No  0:00:00:04   0:11:59:56  N    5  10
```