

Cisco Catalyst SD-WAN Multi-Region Fabric

- Configure Cisco Catalyst SD-WAN Multi-Region Fabric, on page 1
- Information About Multi-Region Fabric, on page 2
- Supported Devices for Multi-Region Fabric, on page 8
- Prerequisites for Multi-Region Fabric, on page 8
- Restrictions for Multi-Region Fabric, on page 9
- Use Cases for Multi-Region Fabric, on page 11
- Enable Multi-Region Fabric, on page 12
- Configure Multi-Region Fabric Using Configuration Groups in Cisco SD-WAN Manager, on page 12
- Configure Multi-Region Fabric Using Feature Templates in Cisco SD-WAN Manager, on page 19
- Use Regions With a Centralized Policy, on page 25
- Configure Multi-Region Fabric Using the CLI, on page 27
- Verify Multi-Region Fabric, on page 29
- Monitor Multi-Region Fabric, on page 30

Configure Cisco Catalyst SD-WAN Multi-Region Fabric

Table 1: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric (also Hierarchical SD-WAN)	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	You can use Cisco SD-WAN Manager to enable and configure Multi-Region Fabric, which provides the ability to divide the architecture of the Cisco Catalyst SD-WAN overlay network into multiple regional networks that operate distinctly from one another.

Feature Name	Release Information	Description
Re-Origination Dampening	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	In networks experiencing instability, TLOCs and bidirectional forwarding detection (BFD) tunnels may alternate repeatedly between being available and unavailable. This causes the overlay management protocol (OMP) to repeatedly withdraw and re-originate routes. This churn adversely affects Cisco SD-WAN Controller performance. Adding a delay before re-originating routes that have gone down repeatedly prevents excessive churn, and prevents this type of network instability from diminishing Cisco SD-WAN Controller performance.
Cisco Catalyst SD-WAN Controller Optimizations	Cisco Catalyst SD-WAN Control Components Release 20.10.1	There are two optimizations of Cisco SD-WAN Controller performance: • Cisco SD-WAN Controller optimization of outbound control policy: This feature helps to optimize Cisco SD-WAN Controller performance by streamlining the evaluation of outbound control policies. The controller evaluates the policy only once for all peers rather than reevaluating for each peer. • Cisco SD-WAN Controller resistance to TLOC flapping: When TLOCs cycle between unavailable and available, called flapping, they cause Cisco SD-WAN Controllers to continually readvertise the list of routes to devices in the network. This degrades the performance of Cisco SD-WAN Controllers and devices in the network. To address this and improve performance, Cisco SD-WAN Controllers isolate the disruption to devices that use the same control policy, leaving other devices unaffected.
Configure Multi-Region Fabric and Related Features Using Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Control Components Release 20.13.1	Configure Multi-Region Fabric features, such as role, region, and so on, and configure transport gateway path behavior on routers, using configuration groups.

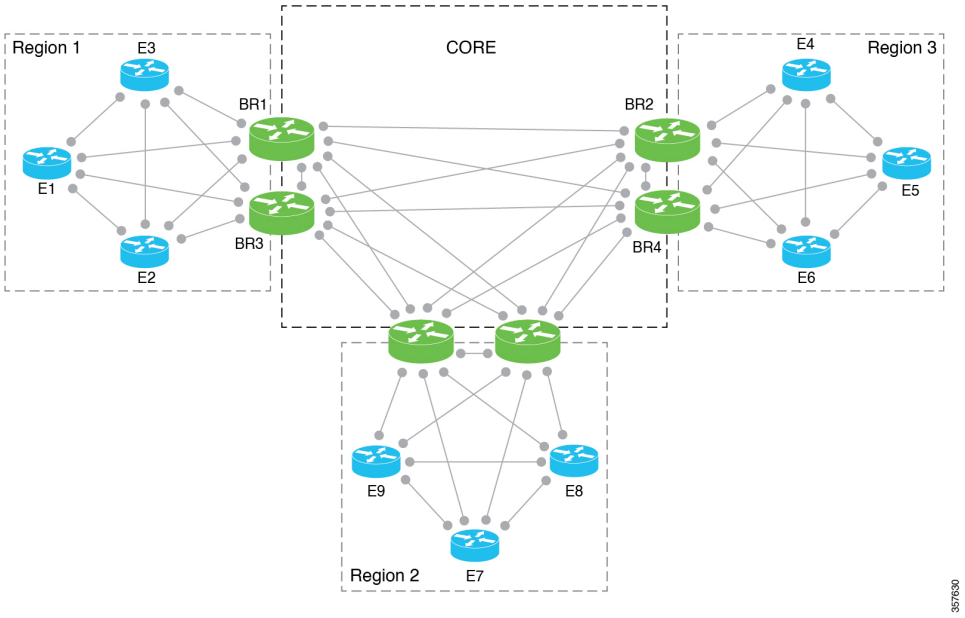
Information About Multi-Region Fabric

Cisco Catalyst SD-WAN Multi-Region Fabric (formerly Hierarchical SD-WAN) provides the option to divide the architecture of the overlay network into the following:

- A core overlay network: This network, called region 0, consists of border routers (BR in the illustration below) that connect to regional overlays and connect to each other.
- One or more regional overlay networks: Each regional network consists of edge routers that connect to other edge routers within the same region, and can connect to core region border routers that are assigned to the region.

The following figure shows a core overlay network with six border routers (BR1 to BR6), two assigned to each of three regions. In the three regional overlay networks, edge routers connect only to other edge routers within the same region or to core border router assigned to the region.

Figure 1: Multi-Region Fabric Architecture



Intra-Region and Inter-Region Traffic

The division into regions creates a distinction between intra-region traffic and inter-region traffic.

- Intra-region traffic: Edge routers connect directly to other edge routers within the region.

  The traffic traverses direct tunnels between source devices and destination devices.

- Inter-region traffic: Edge routers in one region do not connect directly to edge routers in a different region. For inter-region traffic, the edge routers connect to core border routers, which forward the traffic to the core border routers assigned to the target region, and those border routers forward the traffic to the edge routers within the target region.

  The traffic traverses three tunnels between the source device and the destination device.

Disaggregated Transport

An important principle in Multi-Region Fabric is that after you define regions and a core-region network, you can arrange to use different traffic transport services for each region and for the core-region network.

In a common use case, the core region is used for traffic between distant geographic regions. In this scenario, the core region uses a premium transport service to provide the required level of performance and cost effectiveness for long-distance connectivity.

Network Topology

Multi-Region Fabric provides the flexibility to use different network topologies in different regions. For example, region 1 can use a full mesh of Cisco Catalyst SD-WAN tunnels, while region 2 can use a hub-and-spoke topology, and Region3 can use a full mesh topology with dynamic tunnels.

We recommend using a full mesh of tunnels for the overlay topology of the core region (region 0). This means that each border router in the core region requires a tunnel to each other border router in the core. These direct tunnels provide optimal connectivity for forwarding traffic from one region to another.

The implementation of a full mesh topology minimizes the complexity of routing within the core overlay network. By contrast, partial mesh topology would require topology-aware routing to compute inter-region paths. For scaling limitations, see Restrictions for Multi-Region Fabric, on page 9.

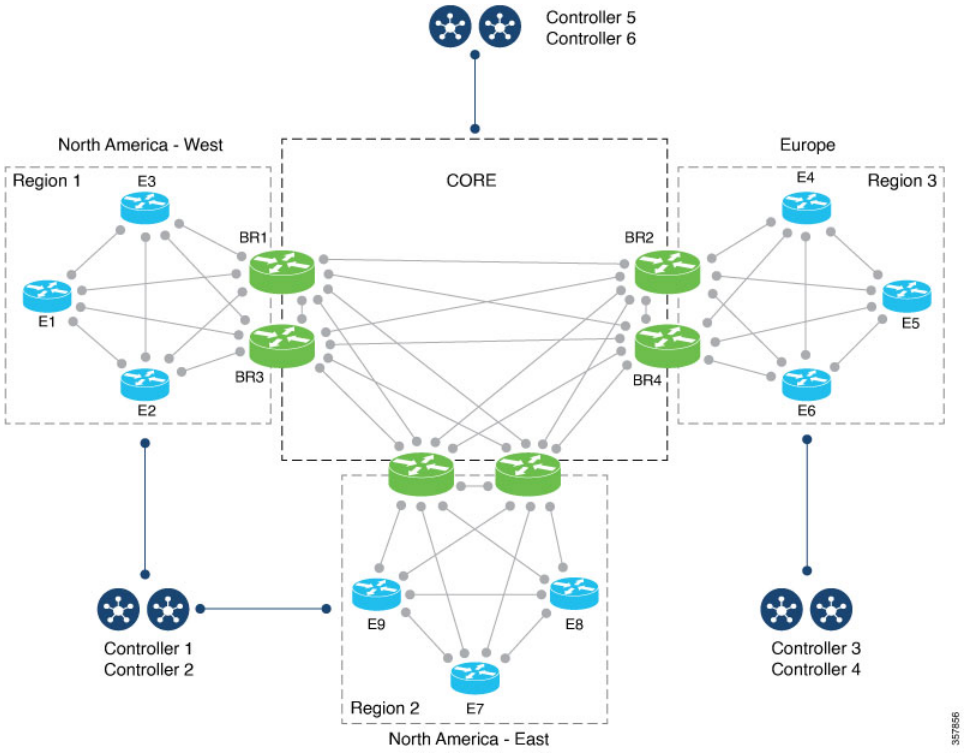
Distributed Cisco Catalyst SD-WAN Controllers

Multi-Region Fabric enables you to assign Cisco SD-WAN Controllers to serve specific regions. If your organization's network contains only a small number of devices, a single Cisco SD-WAN Controller, or typically a pair of Cisco SD-WAN Controllers, can serve all regions in the network. For larger numbers of devices, we recommend that you assign Cisco SD-WAN Controllers to serve specific regions.

Note the following for the example below:

- Cisco SD-WAN Controllers 1 and 2 serve regions 1 and 2.
- Cisco SD-WAN Controllers 3 and 4 serve region 3.
- Cisco SD-WAN Controllers 5 and 6 serve the core region (region 0).

Figure 2: Cisco Catalyst SD-WAN Controllers Serving Different Regions



Note For Cisco SD-WAN Controller restrictions, see Restrictions for Multi-Region Fabric, on page 9.

Re-Origination Dampening

Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

In networks experiencing instability, TLOCs and bidirectional forwarding detection (BFD) tunnels may alternate repeatedly between being available and unavailable. This type of network stability may have various causes, including the following:

- Malfunctioning physical connections
- Network issues that interfere with connectivity
- Weak signals in a cellular network

The alternating between availability and unavailability can cause the overlay management protocol (OMP) operating on border routers and transport gateways to repeatedly withdraw routes that become unavailable and then re-originate the routes when they become available again. This churn propagates to the Cisco SD-WAN Controllers managing the network, creating unnecessary demands on Cisco SD-WAN Controller resources and diminishing performance.

To prevent network instability from diminishing Cisco SD-WAN Controller performance, from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, when border routers and transport gateways detect repeated problems

with network stability, they introduce a delay before re-originating routes after the routes become available. This reduces unnecessary load on the Cisco SD-WAN Controllers and keeps the control plane stable.

Re-origination dampening is enabled by default and does not require any configuration.

Cisco Catalyst SD-WAN Controller Optimization of Outbound Control Policy

Beginning with Cisco Catalyst SD-WAN Control Components Release 20.10.x, Cisco SD-WAN Controllers use a caching feature to optimize performance when applying a control policy to multiple peers.

When a Cisco SD-WAN Controller applies an outbound control policy to a peer, it evaluates each sequence (each of which specifies a match condition and an action) in the policy. For each action in the policy, the controller creates what is called an attribute, which represents the action. For example, if the action in a sequence is to set an OMP tag to 100, the Cisco SD-WAN Controller generates an attribute for setting the OMP tag of a route to 100.

When the Cisco SD-WAN Controller applies the policy to a peer in the outbound direction, for each path that is matched, the controller saves the action attribute to a cache. When the Cisco SD-WAN Controller applies the same control policy to another peer, it does not have to evaluate the policy again. It can use the cached attributes. Minimizing the number of times the Cisco SD-WAN Controller must evaluate a policy improves the performance of the controller.

You can confirm that this feature is operating on a Cisco SD-WAN Controller by running the **show running-config omp** command on the controller. The output includes the following line:

```
outbound-policy-caching
```

On a Cisco SD-WAN Controller, to view the attributes for a path (VPN and prefix), resulting from its evaluating a control policy, run the **show support omp rib vroute** *vpn*:*prefix* **detail** command, and view the RIB-CACHE sections of the output, as shown in the following example:

```
vsmart#show support omp rib vroute 1:192.168.30.0/24 detail | begin RIB-CACHE
  RIB-CACHE-ENTRY: (0xc733cb0), Policy-name: sc_test, Policy-seq-num: 100, RI-ID: 64, attr:
 0xc77bb40
    Attribute: (0xc77bb40), ROUTE-IPV4, Length: 1160, Ref: 6
      Flags: (0x8000c25) WEIGHT TLOC SITE-ID OVERLAY-ID ORIGIN ORIGINATOR
      Region-id: 65534, Secondary-Region-id: 65535, Orig-Access-Region-id: 65534,
Sub-Region-ID: 0, Pref: 0, Weight: 1, Tag: 0, Stale: 0 Version: 0, Restrict: 0, on-Demand:
 0, Domain: 0, BR-Preference: 0, Affinity:0, MRF-Route-Originator:None
      Distance: 0, Site-ID: 300, Carrier: 0, Query: 0, Gen-ID: 0x0, Border: 0 Overlay: 1
Site-Type: 0 0 0 0
      Originator: 172.16.255.30
      Origin: Protocol: connected[1], Sub-Type: none[0], Metric: 0
      TLOC: ((nil)) 172.16.255.30 : biz-internet : ipsec
    TE count 2
     TE: TLOC: 172.16.255.40 : mpls : ipsec, Label: 8389618, Pref: 0, Affinity: 0
     TE: TLOC: 172.16.255.40 : biz-internet : ipsec, Label: 8389618, Pref: 0, Affinity: 0
  RIB-CACHE-ENTRY: (0xc7deb20), Policy-name: sc_test, Policy-seq-num: 100, RI-ID: 70, attr:
 0xc7de3b0
    Attribute: (0xc7de3b0), ROUTE-IPV4, Length: 1160, Ref: 6
      Flags: (0x8000c25) WEIGHT TLOC SITE-ID OVERLAY-ID ORIGIN ORIGINATOR
      Region-id: 65534, Secondary-Region-id: 65535, Orig-Access-Region-id: 65534,
Sub-Region-ID: 0, Pref: 0, Weight: 1, Tag: 0, Stale: 0 Version: 0, Restrict: 0, on-Demand:
 0, Domain: 0, BR-Preference: 0, Affinity:0, MRF-Route-Originator:None
      Distance: 0, Site-ID: 300, Carrier: 0, Query: 0, Gen-ID: 0x0, Border: 0 Overlay: 1
Site-Type: 0 0 0 0
      Originator: 172.16.255.30
      Origin: Protocol: connected[1], Sub-Type: none[0], Metric: 0
      TLOC: ((nil)) 172.16.255.30 : mpls : ipsec
    TE count 2
```

```
TE: TLOC: 172.16.255.40 : mpls : ipsec, Label: 8389618, Pref: 0, Affinity: 0
TE: TLOC: 172.16.255.40 : biz-internet : ipsec, Label: 8389618, Pref: 0, Affinity: 0
```

Cisco Catalyst SD-WAN Controller Resistance to TLOC Flapping

Sometimes TLOCs cycle between unavailable and available—this is called flapping. This flapping can degrade the performance of the Cisco SD-WAN Controllers that advertise routes based on available TLOCs by causing the Cisco SD-WAN Controllers to review and readvertise the routes repeatedly.

Beginning with Cisco Catalyst SD-WAN Control Components Release 20.9.x, Cisco SD-WAN Controllers minimize wasting resources when TLOCs in the network flap by creating an interest list of all of the TLOCs used in all control policies, cumulatively. The Cisco SD-WAN Controller ignores flapping of TLOCs that are not on the interest list, meaning that if a TLOC that is not on the interest list experiences flapping, the Cisco SD-WAN Controller does not have to readvertise the routes based on available TLOCs.

To further optimize Cisco SD-WAN Controller performance, beginning with Cisco Catalyst SD-WAN Control Components Release 20.10.x, the controllers maintain a separate TLOC interest list for each control policy, limiting the disruption caused by TLOC flapping. If a TLOC used by a specific control policy experiences flapping, it affects only the Cisco SD-WAN Controller instances that make use of that control policy. This minimizes the performance impact of TLOC flapping on Cisco SD-WAN Controller instances in the network.

You can use the **show support policy route-policy** command on a Cisco SD-WAN Controller to show the TLOCs of interest for each control policy.



Note This strategy, introduced with Cisco Catalyst SD-WAN Control Components Release 20.10.1, limits the number of TLOCs that you can include in a control policy to 64.

Benefits of Multi-Region Fabric

- Simplified policy design
- Prevention of certain traffic routing failures caused by policy—specifically, routing failures that can occur when a device responsible for one of the hops between the source and destination of a traffic flow is unavailable
- End-to-end encryption of inter-region traffic
- Flexibility to select the best transport for each region

  This flexibility can provide better performance for traffic across geographical regions. In the typical use case, an organization arranges to use premium traffic transport for the core region, providing better traffic performance across distant geographical regions.
- Better control over traffic paths between domains

  In some scenarios, it is advantageous to control how traffic is routed between domains, such as between geographical regions. The Multi-Region Fabric architecture simplifies this.

  For an example of how this is useful, see “Control over traffic paths between domains” in Use Cases for Multi-Region Fabric, on page 11.
- Enabling site-to-site traffic paths between disjoint providers

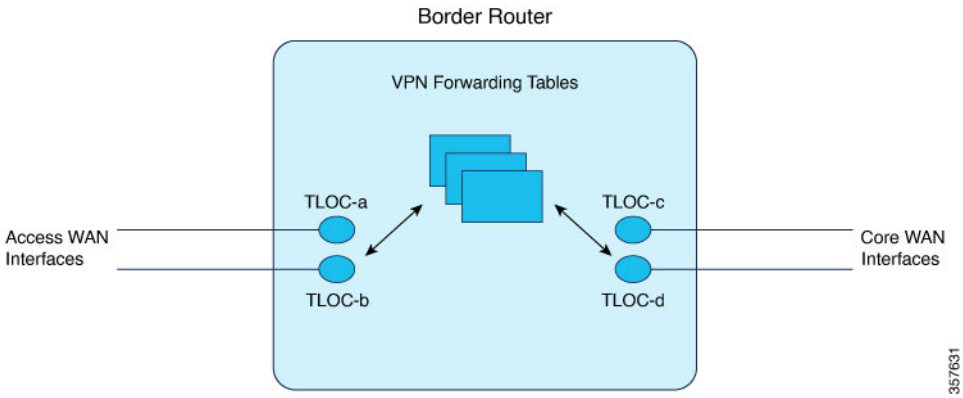
The architecture of Multi-Region Fabric separates between edge routers and border routers. This enables you to establish site-to-site traffic paths between disjoint providers, which are two providers that cannot provide direct IP routing reachability between them. If each site connects to a core-region border router, then the core-region network can provide connectivity between the two sites.

The core-region network can provide this connectivity because each border router has the following:

- A set of (one or more) WAN interfaces to connect to regional edge routers
- A separate set of WAN interfaces for connectivity within the core region

The border router uses VPN forwarding tables to route traffic flows between its two sets of WAN interfaces.

Figure 3: Disjoint Providers



- Optimized tunnel encapsulation

  You can use different types of tunnel encapsulation for the core region and for regional networks.

  For example, you might use IPsec tunnel encapsulation, which is encrypted, between a regional edge router and a core border router. If the core-region infrastructure does not require encryption, you might use generic routing encapsulation (GRE) for tunnels within the core region to provide better throughput. The advantage of selecting the optimal tunnel encapsulation method for each region is better performance for inter-regional traffic.

Supported Devices for Multi-Region Fabric

- Edge router role: All Cisco IOS XE Catalyst SD-WAN devices, all Cisco vEdge devices
- Border router role: All Cisco IOS XE Catalyst SD-WAN devices

Prerequisites for Multi-Region Fabric

- Minimum software version for Cisco IOS XE Catalyst SD-WAN devices: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a
- Minimum software version for Cisco vEdge devices: Cisco SD-WAN Release 20.7.1

Restrictions for Multi-Region Fabric

General Restrictions

- If you configure the devices in a network to use Multi-Region Fabric (assigning a region to each device), then all devices in the network must be configured to use Multi-Region Fabric. A device that is not configured for Multi-Region Fabric cannot connect to a device that is configured forMulti-Region Fabric.

Note Because of this restriction, the process of enabling Multi-Region Fabric for an existing network may temporarily disrupt connectivity between devices within the network.

- We recommend that you use a full mesh topology for the Multi-Region Fabric core-region network, with tunnels from each border router in the core region to each other border router in the core. While this has the advantage of simpler configuration, it limits the ability to scale number of border routers in the core region.
- Only Cisco IOS XE Catalyst SD-WAN devices can have the border router role.

Note For an explanation of edge router and border router terminology, see Information About Multi-Region Fabric, on page 2.

- A border router can serve only one access region. (Regions other than the core region are called access regions.)

Routing Restrictions

Multi-Region Fabric does not support the following routing features:

- End-to-end SLA aware routing
- Multi-tenancy support for edge routers and border routers
- IP multicast on overlay support
- Per-region SLA policies. A border router always applies its region's SLA policy to traffic to and from other regions, irrespective of the SLA configurations in the other regions.
- Fast convergence by backup path selection in border routers
- When you add a new region on Cisco SD-WAN Controller, the control connection fails. When control connection fails, TLOC is removed and BFD goes down.

The following routing feature requires Cisco IOS XE Catalyst SD-WAN Release 17.11.1a or later, and Cisco Catalyst SD-WAN Control Components Release 20.11.1 or later:

- Overlay management protocol (OMP) route aggregation on border routers

Cisco Catalyst SD-WAN Controller Restrictions

- Region 0 restriction: If you assign a Cisco SD-WAN Controller to the core-region (region 0) network, you cannot assign it to any other region.
- Region parity: Cisco SD-WAN Controllers can serve multiple regions. If you configure two Cisco SD-WAN Controllers to serve any one region in common, then those controllers must serve all of the same regions. They cannot have only partial overlap in their coverage of regions.

  The following examples show valid and invalid Cisco SD-WAN Controller scenarios:

  - Valid (non-overlapping):

    Controller A serves region 1.
    Controller B serves region 2.

  - Valid (overlapping single region):

    Controller A serves region 1.
    Controller B serves region 1.

  - Valid (overlapping multiple regions):

    Controller A serves regions 1, 2, and 3.
    Controller B serves regions 1, 2, and 3.

  - Invalid (partially overlapping regions):

    Controller A serves regions 1, 2, and 3.
    Controller B serves only regions 1 and 2.

Scale Limitations

The scale limitations described here are for the Multi-Region Fabric feature. Other limitations may apply to your network configuration.

Multi-Region Fabric has the following scale limitations, as shown in the table. For detailed scaling information for Cisco SD-WAN Control Components, see Recommended Computing Resources in *Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Recommended Computing Resources*.

Item	Supported Scale
Maximum validated number of regions	12
Maximum validated number of regions per Cisco SD-WAN Controller	7

Note If your network requirements exceed these validated limits, contact your Cisco account team.

Use Cases for Multi-Region Fabric

Control of Traffic Paths Between Domains

One advantage of Multi-Region Fabric is the separation between individual regional networks and the core region. Each of these component networks can employ a different type of routing infrastructure, different service providers, and a different set of traffic policies.

In some scenarios, it is advantageous to use different types of traffic transport for intra-regional traffic and for inter-regional traffic. For example, you might use a specific transport service only for inter-regional traffic, to provide the performance that you need at a reasonable cost. The separation of component networks in Multi-Region Fabric architecture simplifies the configuration required to accomplish this.

For example, an organization operating in North America with offices and network infrastructure on the West Coast, and offices and network infrastructure on the East Coast might use different service providers in those two regions to support traffic within the region. Those service providers might not offer the optimal cost or performance for inter-regional traffic between the West Coast and the East Coast.

Without Multi-Region Fabric, one approach has been the following:

- Create a cloud service gateway in the West Coast region.
- Create another cloud service gateway in the East Coast region.
- For traffic between the two regions, configure edge devices to route the traffic to the West Coast gateway or the East Coast gateway, whichever is closest.
- Rely on the cloud services provider for transport between the two gateways.

With Multi-Region Fabric, you can use the core region to manage all traffic between the West Coast and the East Coast, and you can choose the optimal type of backbone infrastructure specifically for the core region to meet your cost and performance requirements. For example, the organization might use the following:

- A West Coast regional service provider for intra-regional West Coast traffic
- An East Coast regional service provider for intra-regional East Coast traffic
- A cloud services provider, or Cisco Catalyst SD-WAN Cloud Interconnect, for the backbone infrastructure

Using Multi-Region Fabric in this scenario offers the following advantages:

- The routing configuration is far simpler.
- The Multi-Region Fabric method prevents certain routing failures—specifically, routing failures that can occur when a device responsible for one of the hops between the source and destination of a traffic flow is unavailable. These failures can occur if you use one of the more complex configuration methods for accomplishing a similar result. The Multi-Region Fabric core region that manages these intermediate hops is more responsive than other methods (such as configuring traffic to use regional gateways, as described above) to device failure and reroutes such traffic to avoid the routing failure.

In general, this disaggregation of transport providers enables you to optimize the cost and performance of operating each regional segment of the organization’s network.

Enable Multi-Region Fabric

Before You Begin

From Cisco Catalyst SD-WAN Manager Release 20.13.1, by default, you can configure regions and subregions without enabling Multi-Region Fabric. For full Multi-Region Fabric functionality, such as using a core region or secondary regions, enable the feature using this procedure.

Note In some scenarios, it is useful to use regions to isolate segments of a network, even without enabling Multi-Region Fabric. For example, you can use regions to achieve network segmentation.

Enable Multi-Region Fabric, Cisco Catalyst SD-WAN Manager Release 20.13.1 and Later

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Enable the **Multi-Region Fabric** control.

Enable Multi-Region Fabric, Cisco Catalyst SD-WAN Manager Release 20.12.x and Earlier

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Multi-Region Fabric** area, enable Multi-Region Fabric.

Note In Cisco SD-WAN Manager Releases 20.7.x and 20.8.x, this area was labeled **Hierarchical SDWAN**.

Configure Multi-Region Fabric Using Configuration Groups in Cisco SD-WAN Manager

For configuring by configuration group, see the Multi-Region Fabric feature for a System profile.

Configure the Multi-Region Fabric Role Using a Configuration Group

Before You Begin

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

- The default role is edge router.
- Use separate configuration groups to configure edge routers and border routers.

Configure the Multi-Region Fabric Role

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Create and configure a **Multi-Region Fabric** feature in a System profile.
3. In the **Basic Settings** section, in the **Role** field, choose a role.

Table 2: Basic Settings

Parameter Name	Description
Region	Beginning with Cisco Catalyst SD-WAN Manager Release 20.13.1, this field has been removed. Set the region in the deployment phase. • Border routers: Configure the access region for the border router to serve. • Edge routers: Configure the access region for the edge router. Range: 1 to 63
Role	• Border routers: Use **border-router**. • Edge routers: Use **edge-router**.
Secondary Region ID	Secondary regions provide another layer to the Multi-Region Fabric architecture. A secondary region contains only edge routers and 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. Range: 1 to 63
Enable Migration Mode to Multi-Region Fabric	Beginning with Cisco Catalyst SD-WAN Manager Release 20.13.1, this field has moved to the **Advanced** tab. Use this parameter when migrating devices from a non-Multi-Region Fabric architecture to Multi-Region Fabric. To prepare for migration, do the following: • Use the **enabled** option for devices that will function as edge routers after migration. • Use the **enabled-from-bgp-core** option for Cisco Catalyst SD-WAN gateway routers that will function as border routers after migration.

Also see Deploy a configuration group.

Configure a Secondary Region Using a Configuration Group

Before You Begin

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

- Create a configuration group for Cisco IOS XE Catalyst SD-WAN devices. For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17x*.
- The default role is edge router.
- Enable Multi-Region Fabric. For information, see Enable Multi-Region Fabric, on page 12.
- Define at least one secondary region.

  Define secondary regions in the network hierarchy manager (**Configuration** > **Network Hierarchy**). See Network Hierarchy and Resource Management in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Configure a Secondary Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group for Cisco IOS XE Catalyst SD-WAN devices and choose **Edit**.
3. In the **System Profile**, add or edit the **Multi-Region Fabric** feature.
4. In the **Advanced Settings** section, in the **Secondary Region** field, choose a secondary region.
5. Click **Save**.

Configure Which Traffic a Border Router Interface Handles, Using a Configuration Group

Before You Begin

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

- Create a configuration group for Cisco IOS XE Catalyst SD-WAN devices. For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17x*.
- This option applies only to a device with a role of border router.
- Configure the role using the Multi-Region Fabric feature in the System Profile. For information, see Configure the Multi-Region Fabric Role Using a Configuration Group, on page 12.

Configure How a Border Router Interface Handles Access and Core Region Traffic

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group for Cisco IOS XE Catalyst SD-WAN devices and choose **Edit**.
3. In the **Transport & Management Profile**, add or edit an interface feature (such as Internet, MPLS, or LTE).
4. Click **Tunnel**.
5. In the **Multi-Region Fabric** section, enable the **Connect to Core Region** option.

6. Choose one of the following to determine how the interface handles access region and core region traffic:
   - **Share Interface with Access Region**: Share the interface between the access region and core region.
   - **Keep Exclusive to Core Region**: Use the interface only for the core region.
7. Click **Save**.

Configure Which Traffic an Edge Router Interface Handles, Using a Configuration Group

Before You Begin

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

- Create a configuration group for Cisco IOS XE Catalyst SD-WAN devices. For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17x*.
- This option applies only to a device with a role of edge router.
- Configure the role using the Multi-Region Fabric feature in the System Profile.

Configure How an Edge Router Interface Handles Secondary Region Traffic

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group for Cisco IOS XE Catalyst SD-WAN devices and choose **Edit**.
3. In the **Transport & Management Profile**, add or edit an interface feature (such as Internet, MPLS, or LTE).
4. Click **Tunnel**.
5. In the **Multi-Region Fabric** section, enable the **Connect to Secondary Region** option.
6. Choose one of the following to determine how the interface handles access region and core region traffic:
   - **Share Interface with Access Region**: Share the interface between the primary and secondary regions.
   - **Keep Exclusive to Secondary Region**: Use the interface only for the secondary region.
7. Click **Save**.

Configure a Router to Treat Hierarchical and Direct Paths Equally, Using a Configuration Group

Before You Begin

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, Cisco Catalyst SD-WAN Manager Release 20.12.1

Note From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1, configuring a router to treat hierarchical and direct paths equally feature is not supported.

- Create a configuration group for Cisco IOS XE Catalyst SD-WAN devices. For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17x*.
- This option applies only to a router in a Multi-Region Fabric scenario, with one or more secondary regions configured.

  In a Multi-Region Fabric scenario, if using secondary regions, configure this option to enable traffic to use all available paths rather than only direct paths.

  By default, when a direct path is available to reach a destination, the overlay management protocol (OMP) enables only the direct path to the routing forwarding layer because the direct path uses fewer hops. This logic is part of route optimization. The result is that the forwarding layer, which includes application-aware routing policy, can only use the direct path.

  The **Treat Hierarchical and Direct Paths Equally** option described in this procedure disables this comparison of the number of hops between the direct paths and alternate paths. This enables traffic to 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.

Configure a Router to Treat Hierarchical and Direct Paths Equally

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group for Cisco IOS XE Catalyst SD-WAN devices and choose **Edit**.
3. In the **System Profile**, edit the **OMP** feature.
4. In the **Best Path** section, enable the **Treat Hierarchical and Direct Paths Equally** option.
5. Click **Save**.

Configure the Regions for Route Aggregation Using a Configuration Group

Before You Begin

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

- Create a configuration group for Cisco IOS XE Catalyst SD-WAN devices. For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17x*.
- This option applies only in a Multi-Region Fabric scenario, and only to a device with a role of border router.

  Configure the role using the Multi-Region Fabric feature in the System Profile.

- In a Multi-Region Fabric scenario, route aggregation is a method for reducing the number of entries that routers in a network must maintain in routing tables, for better scaling. You can choose to apply route aggregation only to the core region, to access regions, or to both.

Configure the Regions for Route Aggregation

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group for Cisco IOS XE Catalyst SD-WAN devices that is used to configure border routers, and choose **Edit**.
3. In the **Service Profile**, edit the feature for a specific service VPN ID.
4. Click **Advertise OMP**.
5. Click **Add OMP Advertise IPv4** or **Add OMP Advertise IPv6**.
6. In the **Protocol** field, choose **aggregate**.
7. In the **Applied to Region** field, choose **core**, **access**, or **core-and-access**, to apply route aggregation only to the core region, access regions, or both.
8. Click **Save**.

Configure Transport Gateway Path Behavior Using a Configuration Group

Before You Begin

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

Create a configuration group for Cisco IOS XE Catalyst SD-WAN devices. For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17x*.

Configure Transport Gateway Path Behavior

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group for Cisco IOS XE Catalyst SD-WAN devices and choose **Edit**.
3. In the **System Profile**, edit the **OMP** feature.
4. In the **Best Path** section, enable the **Transport Gateway Path Behavior** option.
5. Choose one of the following options:
   - **Prefer Transport Gateway Path**: For devices that can connect through a transport gateway, use only the transport gateway paths, even if other paths are available.
   - **Do ECMP Between Direct and Transport Gateway Paths**: For devices that can connect through a transport gateway and through direct paths, apply equal-cost multi-path (ECMP) to all available paths.

6. (Optional) In the **Site Type** field, choose one or more site types to apply the transport gateway path behavior only to those site types.
7. Click **Save**.

Configure the Region and Subregion When Deploying a Configuration Group

Before You Begin

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

From Cisco Catalyst SD-WAN Manager Release 20.13.1, configure the region and subregion while deploying a configuration group to devices. Applying these during deployment enables you to create a configuration group and associate it with a broad range of devices that may be in different network regions. When you deploy the configuration group, you can choose a subset of the devices and configure the region and subregion to apply to that subset of the associated devices.

For information about assigning a region and subregion using a CLI template, see Cisco Catalyst SD-WAN Multi-Region Fabric.

Configure the Region and Subregion When Deploying a Configuration Group

1. When deploying a configuration group to associated devices, choose the devices to which to deploy the configuration group.



Note For information about deploying a configuration group to associated devices, see Using Configuration Groups in *Cisco Catalyst SD-WAN Configuration Groups*.

2. On the **Add and Review Device Configuration** page, in the **Region** drop-down list, choose a region.
3. If the region has one or more subregions defined, in the **Subregion** drop-down list, choose a subregion.

Configure Multi-Region Fabric Using Feature Templates in Cisco SD-WAN Manager

Table 3: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric (also Hierarchical SD-WAN)	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	You can use Cisco SD-WAN Manager to enable and configure Multi-Region Fabric, which provides the ability to divide the architecture of the Cisco Catalyst SD-WAN overlay network into multiple regional networks that operate distinctly from one another.
Re-Origination Dampening	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	In networks experiencing instability, TLOCs and bidirectional forwarding detection (BFD) tunnels may alternate repeatedly between being available and unavailable. This causes the overlay management protocol (OMP) to repeatedly withdraw and re-originate routes. This churn adversely affects Cisco SD-WAN Controller performance. Adding a delay before re-originating routes that have gone down repeatedly prevents excessive churn, and prevents this type of network instability from diminishing Cisco SD-WAN Controller performance.

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Controller Optimizations	Cisco Catalyst SD-WAN Control Components Release 20.10.1	There are two optimizations of Cisco SD-WAN Controller performance: • Cisco SD-WAN Controller optimization of outbound control policy: This feature helps to optimize Cisco SD-WAN Controller performance by streamlining the evaluation of outbound control policies. The controller evaluates the policy only once for all peers rather than reevaluating for each peer. • Cisco SD-WAN Controller resistance to TLOC flapping: When TLOCs cycle between unavailable and available, called flapping, they cause Cisco SD-WAN Controllers to continually readvertise the list of routes to devices in the network. This degrades the performance of Cisco SD-WAN Controllers and devices in the network. To address this and improve performance, Cisco SD-WAN Controllers isolate the disruption to devices that use the same control policy, leaving other devices unaffected.
Configure Multi-Region Fabric and Related Features Using Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Control Components Release 20.13.1	Configure Multi-Region Fabric features, such as role, region, and so on, and configure transport gateway path behavior on routers, using configuration groups.

Before You Begin

Before you begin assigning regions and roles to configure Multi-Region Fabric, review the following.

Note The process of enabling Multi-Region Fabric for an existing network may temporarily disrupt connectivity between devices within the network. See Restrictions for Multi-Region Fabric, on page 9.

1. Determine whether your network requires a hierarchical architecture: If your enterprise networking is limited to one geographic region, where one type of traffic transport suffices for traffic between all points in the network, it is not necessary to employ Multi-Region Fabric. A flat network can address those network requirements.
2. Plan the regions: When you plan a hierarchical architecture, decide which devices to include in each region. In addition, plan the core region, including which devices to use as border routers. Plan which Cisco SD-WAN Controller will serve each region. For an example of a Multi-Region Fabric architecture, see Information About Multi-Region Fabric, on page 2.

3. Granularity: When you plan regions, apply a level of granularity that addresses your organization's network requirements. For example, if you are planning regions for North America, it might be sufficient to use only West Coast and East Coast if your organization's offices are located only in those areas. But if your organization has offices in Canada, and uses a service provider that is local to that area, it might be necessary to include a separate region for Canada.
4. Core-region network requirements: Typically, the core region provides a premium level of transport between distant regions. With this consideration, decide from which location it is most effective for traffic to enter the core region. This often depends on the geographic regions that your organization's network includes, and the type of transport that you intend to use between distant regions.

   Consider the following examples of different core region requirements:

   - Example 1: North America

     For an enterprise network spanning North America, you might intend to use the core region to manage traffic transport between the East and West Coast regions, using a premium transport service. In this case, traffic originating in the West Coast should be routed to core-region border routers on the West Coast rather than crossing to the East Coast outside of the core region. Similarly, traffic originating on the East Coast should be routed to core-region border routers on the East Coast.

   - Example 2: North America and Europe

     For an enterprise network spanning North America and Europe, you might intend to use the core region to manage traffic transport only between North America and Europe, using a transport service that is optimal for the intercontinental traffic. In this case, it might be acceptable for traffic originating on the West Coast to enter the core region through any border router in North America. Similarly, traffic originating anywhere in Europe would be routed to core-region border routers in Europe.

Assign a Role and Region to a Device Using Cisco SD-WAN Manager

Before You Begin

- Plan the Multi-Region Fabric architecture, and decide on the roles (edge router or border router) and regions for each device in the network.
- This procedure uses a feature template to assign a role. For full information about configuring devices using templates, see Configure Devices.
- For information about the number of interfaces that are supported for each device, see the scale limitations in Restrictions for Multi-Region Fabric.
- From Cisco vManage Release 20.9.1, use Network Hierarchy and Resource Management to create the region that you will use in the following procedure. Creating the region includes assigning a region ID to the region. For information about creating a region, see the Network Hierarchy and Resource Management chapter in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x*.

Assign a Role and Region to a Device

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. Select the device type to display the templates available for the device.
5. Click the **System** template.
6. In the **Template Name** field, enter a name for the template.
7. In the **Basic Configuration** section, configure the following fields:

Field	Description
Region ID	Choose a value between 1 and 63 for a region. **Note** From Cisco vManage Release 20.9.1, enter the number of the region that you created for the device using Network Hierarchy and Resource Management, as described in Before You Begin. **Note** By default, all interfaces on the device use the region configured here. For a border router, configure one or more TLOC interfaces to connect to the core region. Other TLOC interfaces on the border router use the region configured here. See Assign Border Router TLOCs to the Core Region Using Cisco SD-WAN Manager.
Role	Choose **Edge Router** or **Border Router**. **Note** Only Cisco IOS XE Catalyst SD-WAN devices can have the **Border Router** role.

8. For a border router, enable the device to function in the core region.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

   c. Click **Add Template**.
   d. Select the device type to display the templates available for the device.
   e. Click the **Cisco VPN Interface Ethernet** template.
   f. In the **Tunnel** section, in the **Tunnel Interface** field, click **On** to enable tunnels.

g. In the **Enable Core Region** field, click **On** to enable connections to the core region.

Assign Border Router TLOCs to the Core Region Using Cisco SD-WAN Manager

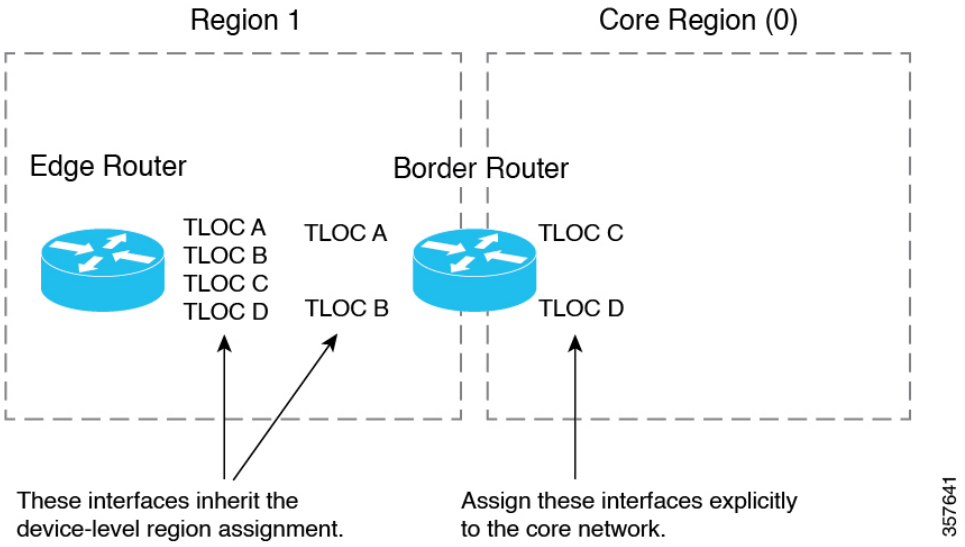
Before You Begin

- Assign the role of border router to the device and assign the device to a region. By default, all interfaces on a device use the region configured for the device. See Assign a Region and Role to a Device Using Cisco SD-WAN Manager.

  For a border router, configure one or more TLOC interfaces to connect to the core region. Other TLOC interfaces on the border router use the region configured for the device.

- This procedure creates a template that assigns interfaces of a specified color to the core region. Before creating the template, configure a color for the interfaces that you want to assign to the core region, or verify that they have a color configured already.

Figure 4: TLOC Interface Region Assignments



Assign Border Router TLOCs to the Core Region

1. Create a Cisco VPN Interface Ethernet template for the TLOC interfaces that you want to connect to the core region.

   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

   b. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

   c. Click **Add Template**.

d. In the **Template Name** field, provide a template name.

e. In the **Tunnel** section, in the **Tunnel Interface** field, click **On**.

f. In the **Color** field, specify a color that identifies the interfaces that you want to assign to the core region.

g. Click **Advanced Options**.

h. In the **Settings** section, in the **Enable Core Region** field, click **On**.

i. In the **Basic Configuration** section, in the **Interface Name** field, enter an interface name.

j. Click **Save**.

2. Add the Cisco VPN Interface Ethernet template that you created in the previous step to a device template.

   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

   b. Click **Device Templates**.



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

   c. Click **Create Template** and choose **From Feature Template**.

   d. In the **Transport & Management VPN** section, locate the **Additional Cisco VPN 0 Templates** list and click **Cisco VPN Interface Ethernet**.

      This adds a new line to the **Transport & Management VPN** section, labelled **Cisco VPN Interface Ethernet**, with a menu for selecting an interface.

   e. In the new **Cisco VPN Interface Ethernet** line, click the menu and select the Cisco VPN Interface Ethernet template that you created in an earlier step.

   f. Click **Update**.

3. Apply the device template to the border router device.

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

Before You Begin

- Plan the Multi-Region Fabric architecture, and decide on the roles (edge router or border router) and regions for each device in the network. Plan which Cisco SD-WAN Controllers should serve each region.
- This procedure uses a feature template to assign a role. For full information about configuring devices using templates, see Configure Devices.
- For restrictions that apply to Cisco SD-WAN Controllers, see Restrictions for Multi-Region Fabric.

Assign Regions to a Cisco SD-WAN Controller

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



Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. For the device type, select **Controller**.
5. Click the **System** template.
6. In the **Template Name** field, enter a name for the template.
7. In the **Basic Configuration** section, in the **Region ID List** field, enter a region or region list.
8. Apply the template to the Cisco SD-WAN Controller.

Use Regions With a Centralized Policy

Create a Region List Using Cisco SD-WAN Manager

Region lists are useful when creating a region match condition for a centralized policy.

Create a Region List

1. In the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policy**.
3. Click **Add Policy**.
4. In the list area, click **Region**.
5. Click **New Region List**.
6. Enter the following:
   - **Region List Name**: Name for the new list.
   - **Add Region**: One or more region numbers in the range of 1 to 63, using to the instructions in the field.
7. Click **Add**.

Add a Region Match Condition to a Centralized Policy

After you configure regions for Multi-Region Fabric, you can specify a region or region list as a match condition when configuring centralized route policy.

For complete information about working with centralized policy, see the Centralized Policy section of the Cisco SD-WAN Policies Configuration Guide.

For complete information about working with centralized policy, see the Centralized Policy section of the Policies Configuration Guide for vEdge Routers.

Add a Region Match Condition to a Centralized Policy

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Custom Options** and in the **Centralized Policy** section, choose **Topology**.
3. Click **Add Topology** and choose **Custom Control**.
4. Click **Sequence Type** and choose **Route**.
5. Click **Sequence Rule**.
6. Click **Match**.
7. Click **Region**.
8. In the **Match Conditions** area, enter a region or region list.

   See Create a Region List Using Cisco SD-WAN Manager.

Attach a Centralized Policy to a Region

After you configure regions for Multi-Region Fabric, specify a region or region list when attaching a centralized policy.

For complete information about working with centralized policy, see the Centralized Policy section of the Cisco SD-WAN Policies Configuration Guide.

For complete information about working with centralized policy, see the Centralized Policy section of the Policies Configuration Guide for vEdge Routers.

Attach a Centralized Policy to a Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policy**.
3. In the table, locate the policy to attach. In the row of the policy, click **…** and choose **Edit**.

   For the **Topology**, **Application-Aware Routing**, and **Traffic Data** options, you can choose to add a new site or new region.
4. Click **New Site/Region List**.
5. Click **Region**.
6. Enter a region ID or region list.
7. Proceed with attaching the policy.

Configure Multi-Region Fabric Using the CLI

Assign a Role to a Device Using the CLI

Use the **role** command on a device to assign a role of border router, for Multi-Region Fabric functionality. The default role is edge router. To change the role from border router to edge router, use the **no** form of the command.

Example (border router)

```
Device#config-transaction
Device(config)#system
Device(config-system)#role border-router
```

Example (edge router)

```
Device#config-transaction
Device(config)#system
Device(config-system)#no role border-router
```

Assign a Region ID to Edge Router TLOCs Using a CLI Template

Minimum release for the **subregion** keyword: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global configuration mode.

All TLOC interfaces on a device inherit the region ID that you assign to the device.

Use the **region** command to assign a region (range: 1 to 63) for a device, and optionally a subregion (range: 1 to 63).

```
system
region region-id [subregion subregion-id]
```

Example 1

```
system
  region 1
```

Example 2

The following example assigns region 1, subregion 3.

```
system
 region 1
  sub-region 3
```

Assign a Region ID to Border Router TLOCs Using a CLI Template

Minimum release for the **subregion** keyword: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global configuration mode.

By default, all TLOCs on a device inherit the region ID that you assign to the device. For a border router, you must explicitly assign one or more TLOC interfaces to the core region. For information about how many TLOCs can be assigned to the core region, see Restrictions for Multi-Region Fabric, on page 9.

1. Use the **region** command to assign a region (range: 1 to 63), and optionally a subregion (range: 1 to 63).

   ```
   system
   region region-id [subregion subregion-id]
   ```

   By default, all interfaces on the device operate in the assigned region.

2. To assign a TLOC interface to the core region, use the **region core** command.

   ```
   sdwan
     interface interface
       tunnel-interface
       region core
   ```

Example 1

The following example assigns a border router to region 1.

```
system
 region 1
!
sdwan
 interface GigabitEthernet1
  tunnel-interface
  region core
 !
!
```

Example 2

The following example assigns a router to region 1, subregion 5.

```
system
 system-ip 192.0.2.1
 domain-id 1
 site-id 1100
 region 1
  subregion 5
```

Assign Regions to a Cisco Catalyst SD-WAN Controller Using the CLI

When setting up Multi-Region Fabric, you can assign existing Cisco SD-WAN Controllers to a region, or you can create new Cisco SD-WAN Controllers to use for Multi-Region Fabric.

You can use the same set of Cisco SD-WAN Controllers to serve devices in every region of the organization's network, with the exception of the core region Cisco SD-WAN Controller, which must be provisioned to serve only the core region. In a network with a small number of devices, this may be feasible. However, for a network with a large number of devices, we recommend that you assign the controllers to specific regions.

Assign Regions to a Cisco Catalyst SD-WAN Controller

On the Cisco SD-WAN Controller, use the **region** command to assign the Cisco SD-WAN Controller to one or more regions.

region {*region*} [*region ...*]

Example:

This example assigns the Cisco SD-WAN Controller to regions 1 and 2.

```
vSmart(config-system)#region 1 2
```

Verify Multi-Region Fabric

Use the **show omp summary** and **show control local-properties** commands to verify the role and region for devices, or assigned regions for Cisco SD-WAN Controllers.

show omp summary

Use this command on a device to display the device role. The device-role field indicates either Edge-Router or Border-Router.

```
vEdge# show omp summary
oper-state UP
admin-state UP
personality vedge
device-role Edge-Router
...
```

Use this command on a Cisco SD-WAN Controller to display the regions that the controller is configured to manage. The region-id field indicates the list of regions.

```
vSmart1# show omp summary
oper-state              UP
admin-state             UP
personality             vsmart
...
vsmart-peers            1
vedge-peers             0
region-id               0 1 2 3 4 5
```

show control local-properties

Use this command on a device to display which region has been configured for each TLOC interface.

```
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 ID
------------------------------------------------------------------------------------------------------------
GigabitEthernet0/0/0     10.0.0.1    12366  10.0.0.1     ::       12366    1/1  public-internet  up
 2     yes/yes/no   No/No  0:00:00:04   0:11:59:27  N    8  0
GigabitEthernet0/0/1     10.0.0.2    12366  10.0.0.2     ::       12366    1/0  green            up
 2      no/yes/no   No/No  0:00:00:07   0:11:57:39  N    5  2
GigabitEthernet0/1/1.10  10.0.0.3    5062   10.0.0.5     ::       12346    1/0  gold             up
 2      no/yes/no  Yes/No  0:00:00:07   0:11:57:41  N    5  2
Loopback300              10.10.0.10  12366  10.10.0.10   ::       12366    0/0  blue             up
 0      no/ no/no   No/No  0:00:10:37   0:11:54:42  N    5  2
```

Monitor Multi-Region Fabric

To monitor the status of the Multi-Region Fabric configuration, you can use the following commands to display information about device region, device role, and so on.

Command	Description
show control local-properties	Use this command on a device to display which region has been configured for each TLOC interface.
show omp summary	Use this command on a device or a Cisco SD-WAN Controller to display the region configuration, device roles, and so on.
show omp routes	Use this command on a device or a Cisco SD-WAN Controller to display region information for each route managed by the device or Cisco SD-WAN Controller.
show bfd sessions	Use this command on a device to display region information for each BFD session on the device.