Migrating to Multi-Region Fabric

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.

Migrating to Multi-Region Fabric

Table 1: Feature History

Feature Name	Release Information	Description
Migrate to Multi-Region Fabric	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco SD-WAN Release 20.9.1 Cisco vManage Release 20.9.1	Cisco SD-WAN Multi-Region Fabric provides a migration mode to facilitate migrating an enterprise network to Cisco Catalyst SD-WAN. Migration mode enables a stepwise transition of devices from Cisco SD-WAN Controllers that are not part of a Multi-Region Fabric network to Cisco SD-WAN Controllers operating in a Multi-Region Fabric architecture. The migration mode is especially useful for migrating complex networks that function similarly to a Multi-Region Fabric architecture—that is, they have multiple network segments, and have a control policy that directs inter-segmental traffic through network hubs.
Migrate a BGP-Based Hierarchical Core Network to Multi-Region Fabric	Cisco IOS XE Catalyst SD-WAN Release 17.9.2a Cisco vManage Release 20.9.2 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	This feature facilitates migrating a BGP-based hierarchical core network into a Cisco Catalyst SD-WAN Multi-Region Fabric-based topology by alleviating the need of complex control policy definitions and the existence of a BGP core.

Information About Migrating to Multi-Region Fabric

Some enterprise networks are divided into logical segments and configured to route traffic between segments through hub devices. These network architectures are similar to the Multi-Region Fabric architecture, and are well suited to being migrated to Multi-Region Fabric. Cisco Catalyst SD-WAN provides a migration mode that is useful for converting this type of network to a Multi-Region Fabric architecture.

One use case is an organization that spans multiple geographic regions and treats each geographic region as a segment within the organization's overall network architecture. The organization uses centralized control policies on the Cisco SD-WAN Controllers to configure hub-by-hub routing between segments. Configuring migration mode on the devices, and using the procedures described here, you do the following:

- Convert each segment into a Multi-Region Fabric region
- Set up border routers
- Assign the Cisco SD-WAN Controllers to operate with the Multi-Region Fabric architecture

(Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.2a, Cisco vManage Release 20.9.2, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1) Another use case is an organization that spans multiple geographic regions and clusters branch sites into logical regions. The routers in one logical region are connected to routers in another logical region through Cisco Catalyst SD-WAN gateways. The Cisco Catalyst SD-WAN gateways are configured with mutual redistribution from OMP to BGP and vice versa. The organization uses centralized control policies on the Cisco SD-WAN Controllers to ensure that the gateways receive TLOCS of only the corresponding region that they serve and don't receive the TLOCS of other gateways.

In this topology, the overlay connection exists only between the routers in a logical region and the Cisco Catalyst SD-WAN gateways. On the other hand, a BGP-to-BGP connection exists between inter-region gateways through provider edge routers as an intermediate hop. Configuring migration mode on the devices, and using the procedures described here, you do the following:

- Convert each logical region into a Multi-Region Fabric region.
- Set up the Cisco Catalyst SD-WAN gateways as border routers.
- Assign the Cisco SD-WAN Controllers to operate with the Multi-Region Fabric architecture.
- Define route maps on all provider edge devices and Cisco Catalyst SD-WAN gateways by specifying a community value.
- Modify the control policies on the Cisco SD-WAN Controllers to allow the border routers to receive the TLOCs of each other.

Benefits of Migrating to Multi-Region Fabric

For an organization that spans multiple geographic regions and treats each geographic region as a network segment, configuring the segment policy is complicated, and grows quickly in complexity as the network expands. Migrating to Multi-Region Fabric significantly simplifies the centralized control policy overhead. For an example of the complex centralized control policy that can be simplified by using Multi-Region Fabric, see Use Cases for Migrating to Multi-Region Fabric, on page 4.

Using the migration procedure described in this section migrates a network to Multi-Region Fabric while preserving the functionality of each router in the network, and each router's role in the network topology.

For example, devices that are dedicated to serving one segment of a non-Multi-Region Fabric network continue to do so in the Multi-Region Fabric architecture, with the role of edge routers. Devices that serve as hubs in a non-Multi-Region Fabric network continue to do so in the Multi-Region Fabric architecture, with the role of border routers.

Supported Devices for Migrating to 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 Migrating to Multi-Region Fabric

- Plan the role of each device in the architecture.

- 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*.
- Each edge router operating within a segment of the original network architecture has the system requirements to operate as an edge router within a single region in the Multi-Region Fabric architecture.
- Each router serving as a hub has the system requirements to operate as a Multi-Region Fabric border router.
- Determine which Cisco SD-WAN Controllers can serve each region in the Multi-Region Fabric architecture, including the core region.

Use Cases for Migrating to Multi-Region Fabric

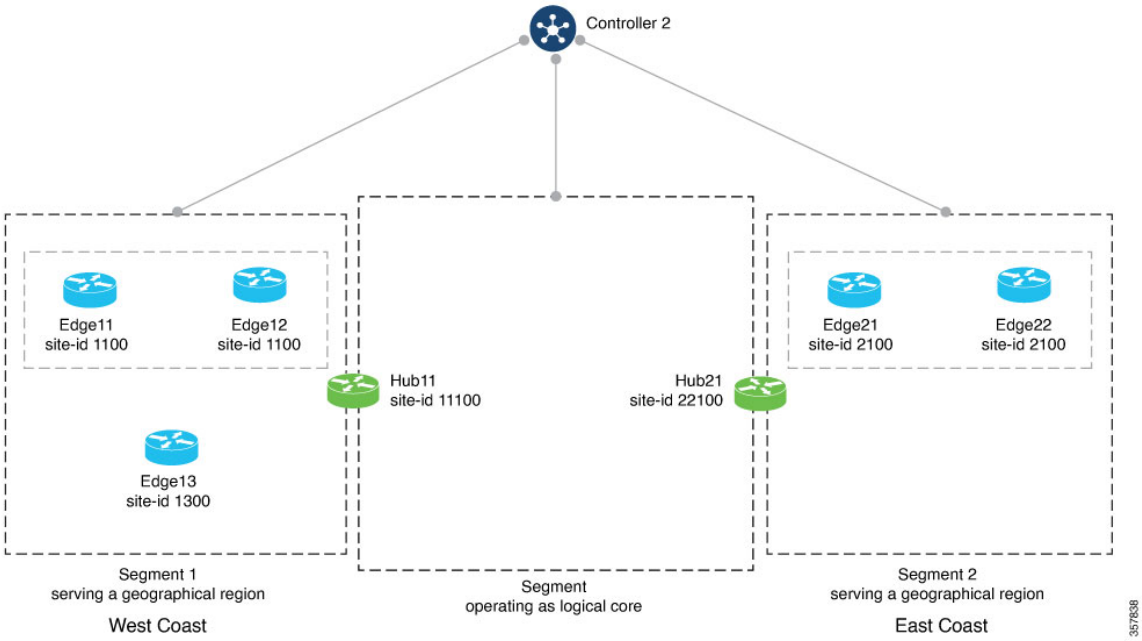
The following example provides insight into the steps for planning and executing a migration to a Multi-Region Fabric architecture. For simplification, this example includes only a small total number of routers in the organization's network, and before migration uses a single Cisco SD-WAN Controller.

The use case is an organization that spans multiple geographic regions and treats each geographic region as a network segment. Segment 1 serves the West Coast and segment 2 serves the East Coast. All traffic between the two segments is directed through hub devices in each segment.

Before and After Migration

The following illustration shows the architecture of the network. In this example, a single Cisco SD-WAN Controller serves the entire network.

Figure 1: Network Architecture Before Migration



For this network, before migration to Multi-Region Fabric, the centralized control policy, described in detail later in this section, clusters the routers into network Segments 1 and 2, and provides a hub router for Segment 1 and a hub router for Segment 2. The policy does the following:

- Enables direct routes among the devices within Segment 1, serving the West Coast geographical region.

  These include Edge11, Edge12, Edge13, and Hub11.

- Enables direct routes among the devices within Segment 2, serving the East Coast geographical region.

  These include Edge21, Edge22, and Hub21.

- Enables direct routes among devices within the logical core region.

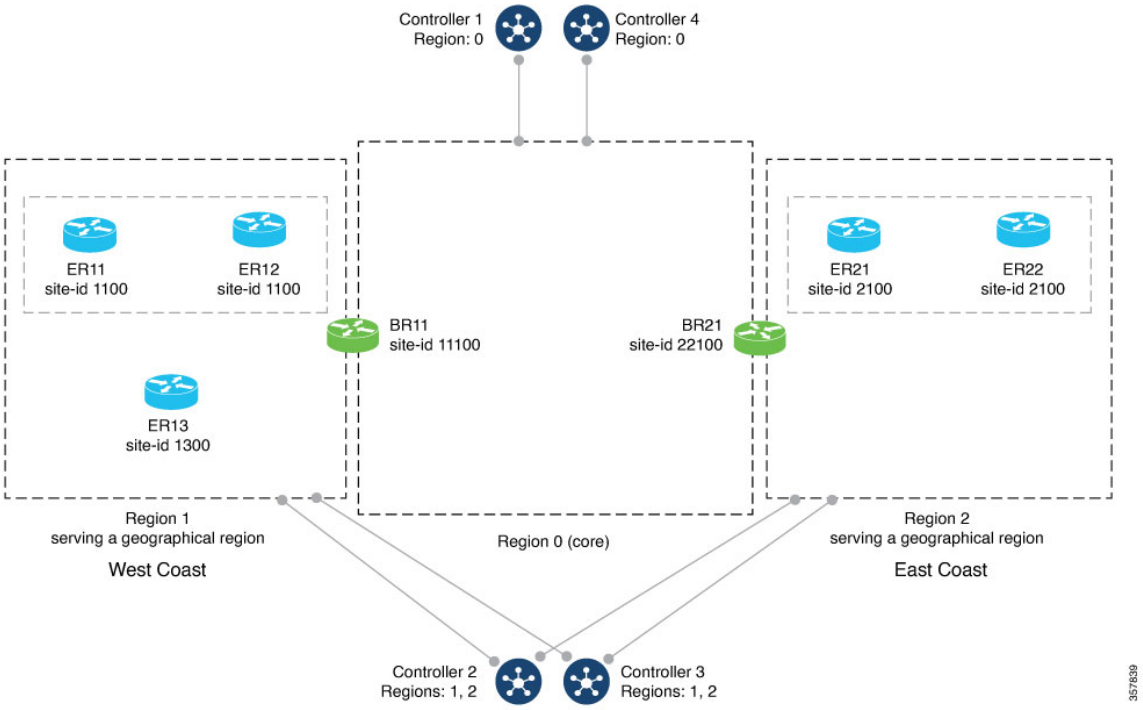
  These include Hub11 and Hub21.

- Routes inter-region traffic through the hubs, Hub11 and Hub21.

To migrate to Multi-Region Fabric, a network administrator plans the expected role and region for each router in the network architecture, plans the use of four Cisco SD-WAN Controllers, and uses the Cisco SD-WAN Manager procedure (Migrate to Multi-Region Fabric Using Cisco SD-WAN Manager, on page 21) to migrate each router.

The following illustration shows the network after migration.

Figure 2: Network Architecture After Migration to Multi-Region Fabric



In the migration shown in the preceding illustrations, each router continues to perform a similar function within the network, but the terminology describing the routers and segments changes. The following table compares the terminology that applies to each router before and after migration. Routers with a hub functionality become border routers, and network segments are formalized as regions within the Multi-Region Fabric architecture.

Geographical Region	Site	Device Name and Description Before Migration	Device Name and Description After Migration to Multi-Region Fabric
West Coast	1100	Edge11: Edge router	ER11: Edge router, Region 1
West Coast	1100	Edge12: Edge router	ER12: Edge router, Region 1
West Coast	1300	Edge13: Edge router	ER13: Edge router, Region 1
West Coast	11100	Hub11: Hub router	BR11: Border router, Region 1
East Coast	22100	Hub21: Hub	BR21: Border router, Region 2

Geographical Region	Site	Device Name and Description Before Migration	Device Name and Description After Migration to Multi-Region Fabric
East Coast	2100	Edge21: Edge router	ER21: Edge router, Region 2
East Coast	2100	Edge22: Edge router	ER22: Edge router, Region 2

Control Policy Requirements Before Migration

The following tables provide an example of the complex control policy required to accomplish (a) network segmentation, and (b) inter-segment routing through hubs, without Multi-Region Fabric. This policy example may be helpful when planning a migration of a similarly configured enterprise network to Multi-Region Fabric, and it demonstrates the advantage of accomplishing this type of network functionality using Multi-Region Fabric, significantly simplifying policy.

The tables describe the following steps:

- Part A. Define Policy Lists of Site IDs to Use in Control Policies
- Part B. Define Policy Lists of TLOCs to Use in Control Policies
- Part C. Create and Apply Control Policies Using the Lists Defined in the Previous Tables

Table 2: Part A. Define Policy Lists of Site IDs to Use in Control Policies

Brief Description of the Policy Configuration Objective	Detailed Description	Example

1. Define lists that include the edge routers in Segment 1.	Define a site list of all sites in Segment 1. These sites include all edge routers in Segment 1.	`policy`
		` lists`
		`  site-list SEGMENT1`
		`   site-id 1100`
		`   site-id 1300`
		`   !`

	Define a site list of all edge routers in Segment 1, and the hub site for Segment 1. These sites include all edge routers and hub routers in Segment 1.	`policy`
		` lists`
		`  site-list SEGMENT1_HUB1`
		`   site-id 1100`
		`   site-id 1300`
		`   site-id 11100`
		`   !`

Brief Description of the Policy Configuration Objective	Detailed Description	Example

2. Define lists that include the edge routers in Segment 2.	Define a site list of all sites in Segment 2. These sites include all edge routers in Segment 2.	`policy`
		` lists`
		`  site-list SEGMENT2`
		`   site-id 2100`
		`   !`

	Define a site list of all edge routers in Segment 2, and the hub site for Segment 2. These sites include all edge routers and hub routers in Segment 2.	`policy`
		` lists`
		`  site-list SEGMENT2_HUB2`
		`   site-id 2100`
		`   site-id 22100`
		`   !`

3. Define a list of Segment 2 destinations that will be useful when creating control policy for Segment 1 outgoing traffic.	Define a list of the following:
	• All edge routers in Segment 2
	• The hub site for Segment 2
	• The hub site for Segment 1
		`policy`
		` lists`
		`   site-list HUB1_HUB2_SEGMENT2`
		`   site-id 11100`
		`   site-id 2100`
		`   site-id 22100`
		`   !`

4. Define a list of Segment 1 destinations that will be useful when creating control policy for Segment 2 outgoing traffic.	Define a list of the following:
	• All edge routers in Segment 1
	• The hub site for Segment 1
	• The hub site for Segment 2
		`policy`
		` lists`
		`  site-list HUB1_HUB2_SEGMENT1`
		`   site-id 1100`
		`   site-id 11100`
		`   site-id 1300`
		`   site-id 22100`
		`   !`

5. Define a list of Segment 1 routers, and the hub router for Segment 2. This will be useful when creating a control policy for the Segment 1 hub router.	Define a list of the following:
	• All edge routers in Segment 1
	• The hub site for Segment 2
		`policy`
		` lists`
		`  site-list SEGMENT1_HUB2`
		`   site-id 1100`
		`   site-id 1300`
		`   site-id 22100`
		`   !`

6. Define a list of Segment 2 routers, and the hub router for Segment 1. This will be useful when creating a control policy for the Segment 2 hub router.	Define a list of the following:
	• All edge routers in Segment 2
	• The hub site for Segment 1
		`policy`
		` lists`
		`  site-list HUB1_SEGMENT2`
		`   site-id 11100`
		`   site-id 2100`
		`   !`

Table 3: Part B. Define Policy Lists of TLOCs to Use in Control Policies

Brief Description of the Policy Configuration Objective	Detailed Description	Example
1. Define lists of TLOCs for traffic between hubs. (When the network is migrated to Multi-Region Fabric, this inter-hub traffic constitutes the core region traffic.)	• Define a list of TLOCs (HUB1_CORE_TLOC) for traffic from Hub21 to Hub11. • Define a list of TLOCs (HUB2_CORE_TLOC) for traffic from Hub11 to Hub21.	policy lists tloc-list HUB1_CORE_TLOC tloc 172.16.11.10 color green encap ipsec ! tloc-list HUB2_CORE_TLOC tloc 172.17.13.10 color green encap ipsec !
2. Define lists of TLOCs for traffic between hubs and the routers in the segment that they are serving. (When the network is migrated to Multi-Region Fabric, this constitutes the access region traffic.)	• Define a list of TLOCs (HUB1_TLOCS) for traffic between Hub11 and the routers in Segment 1, for which it serves as hub. • Define a list of TLOCs (HUB2_TLOCS) for traffic between Hub21 and the routers in Segment 2, for which it serves as hub.	policy lists tloc-list HUB1_TLOCS tloc 172.16.11.10 color lte encap ipsec tloc 172.16.11.10 color 3g encap ipsec tloc 172.16.11.10 color red encap ipsec tloc 172.16.11.10 color green encap ipsec ! tloc-list HUB2_TLOCS tloc 172.17.13.10 color lte encap ipsec tloc 172.17.13.10 color 3g encap ipsec tloc 172.17.13.10 color green encap ipsec !

Table 4: Part C. Create and Apply Control Policies Using the Lists Defined in the Previous Tables

Brief Description of the Policy Configuration Objective	Detailed Description	Example

1. Create a control policy for Segment 1 that (a) enables routers within Segment 1 to send traffic to one another directly, and that (b) directs all traffic destined to Segment 2 to use Hub11 as a first hop. In this way, Hub11 serves as a hub for traffic to Segment 2.	Create a control policy called CP1 to do the following:
	• Sequence 1: Provide all devices in Segment 1 with access to the TLOCs of the other devices in Segment 1. This includes the edge routers and hub routers. This creates full-mesh connectivity in Segment 1.
	• Sequence 2: Ensure that for any traffic in Segment 1 whose destination is Hub11 or any of the devices in Segment 2, the first hop must be Hub11.
	• Sequence 3: Ensure that for any traffic within Segment 1, the devices forward the traffic directly to the destination device within the region.
		`control-policy CP1`
		`  sequence 1`
		`   match tloc`
		`    site-list SEGMENT1_HUB1`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  sequence 2`
		`   match route`
		`    site-list HUB1_HUB2_SEGMENT2`
		`   !`
		`   action accept`
		`    set`
		`     tloc-list HUB1_TLOCS`
		`    !`
		`   !`
		`  !`
		`  sequence 3`
		`   match route`
		`    site-list SEGMENT1`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  default-action reject`
		`!`

2. Apply control policy CP1, described in the previous row, to Segment 1 for outgoing traffic.		`apply-policy`
		` site-list SEGMENT1`
		`  control-policy CP1 out`

Brief Description of the Policy Configuration Objective	Detailed Description	Example

3. Create a control policy for Segment 2 that (a) enables routers within Segment 2 to send traffic to one another directly, and that (b) directs all traffic destined to Segment 1 to use Hub21 as a first hop. In this way, Hub21 serves as a hub for traffic to Segment 1.	Create a control policy called CP4 to do the following:
	• Sequence 1: Provide all devices in Segment 2 with access to the TLOCs of the other devices in Segment 2. This includes the edge routers and hub routers. This creates full-mesh connectivity in Segment 2.
	• Sequence 2: Ensure that for any traffic in Segment 2 whose destination is Hub21 or any of the devices in Segment 1, the first hop must be Hub21.
	• Sequence 3: Ensure that for any traffic within Segment 2, the devices forward traffic directly to the destination device within the region.
		`control-policy CP4`
		`  sequence 1`
		`   match tloc`
		`    site-list HUB2_SEGMENT2`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  sequence 2`
		`   match route`
		`    site-list HUB1_HUB2_SEGMENT1`
		`   !`
		`   action accept`
		`    set`
		`     tloc-list HUB2_TLOCS`
		`    !`
		`   !`
		`  !`
		`  sequence 3`
		`   match route`
		`    site-list SEGMENT2`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  default-action reject`
		`!`
		`!`

4. Apply control policy CP4, described in the previous row, to Segment 2 for outgoing traffic.		`apply-policy`
		` site-list SEGMENT2`
		`  control-policy CP4 out`

Brief Description of the Policy Configuration Objective	Detailed Description	Example

5. Create a control policy for the Segment 1 hub router Hub11 that (a) provides it with full-mesh connectivity with devices in Segment 1, and (b) provides it with full-mesh connectivity with the other hub router (Hub21).	Create a control policy called CP2 to do the following:
	• Sequence 1: Provide access to the TLOCs of devices in Segment 1 and the TLOCs of the hub router for Segment 2. This (a) creates full-mesh connectivity for the hub router for Segment 1 with the other routers in Segment 1, and (b) between the hub routers for Segments 1 and 2.
	• Sequence 2: Ensure that for any traffic whose destination is a device in Segment 1, forward the traffic directly to the device.
	• Sequence 3: Ensure that for any traffic whose destination is a device in Segment 2, including the hub and edge routers, forward the traffic to Hub21.
		`control-policy CP2`
		`  sequence 1`
		`   match tloc`
		`    site-list SEGMENT1_HUB2`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  sequence 2`
		`   match route`
		`    site-list SEGMENT1`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  sequence 3`
		`   match route`
		`    site-list HUB2_SEGMENT2`
		`   !`
		`   action accept`
		`    set`
		`     tloc-list HUB2_CORE_TLOC`
		`    !`
		`   !`
		`  !`
		`  default-action reject`
		`!`

6. Apply control policy CP2, described in the previous row, to the hub router for Segment 1.		`apply-policy`
		`site-list HUB1`
		`  control-policy CP2 out`
		`!`

Brief Description of the Policy Configuration Objective	Detailed Description	Example

7. Create a control policy for the Segment 2 hub router Hub21 that (a) provides it with full-mesh connectivity with devices in Segment 2, and (b) provides it with full-mesh connectivity with the other hub router (Hub11).	Create a control policy called CP3 to do the following:
	• Sequence 1: Provide access to the TLOCs of devices in Segment 2 and the TLOCs of the hub router for Segment 1. This (a) creates full-mesh connectivity for the hub router for Segment 2 with the other routers in Segment 2, and (b) between the hub routers for Segments 1 and 2.
	• Sequence 2: Ensure that for any traffic whose destination is a device in Segment 2, forward the traffic directly to the device.
	• Sequence 3: Ensure that for any traffic whose destination is a device in Segment 1, including the hub and edge routers, forward the traffic to Hub11.
		`control-policy CP3`
		`  sequence 1`
		`   match tloc`
		`    site-list HUB1_SEGMENT2`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  sequence 2`
		`   match route`
		`    site-list SEGMENT2`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  sequence 3`
		`   match route`
		`    site-list SEGMENT1_HUB1`
		`   !`
		`   action accept`
		`    set`
		`     tloc-list HUB1_CORE_TLOC`
		`    !`
		`   !`
		`  !`
		`  default-action reject`
		`!`

8. Apply control policy CP3, described in the previous row, to the hub router for Segment 2.		`apply-policy`
		`site-list HUB2`
		`  control-policy CP3 out`
		`!`

Use Case 2: Migration of a BGP-Based Hierarchical Core Network

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.2a, Cisco vManage Release 20.9.2, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

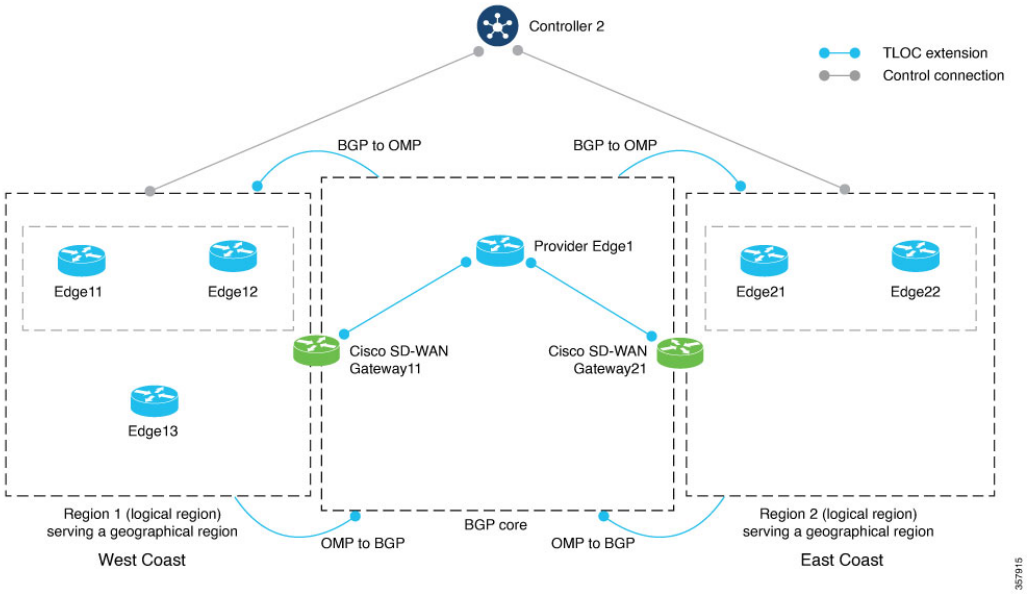
The following example provides insight into the steps for planning and executing the migration of a BGP-based hierarchical core network to a Multi-Region Fabric architecture. For simplification, this example includes only a small total number of routers in the organization's network, and before migration uses a single Cisco SD-WAN Controller.

The use case is an organization that spans multiple geographic regions and treats each geographic region as a logical region. Region 1 serves the West Coast and region 2 serves the East Coast. All traffic between the two regions is directed through Cisco Catalyst SD-WAN gateways in each region, and the inter-region gateways are connected to each other through a provider edge router by BGP peering.

Before and After Migration

The following illustration shows the architecture of the BGP-based hierarchical core network. In this example, a single Cisco SD-WAN Controller serves the entire network.

Figure 3: BGP-Based Network Architecture Before Migration



In this example:

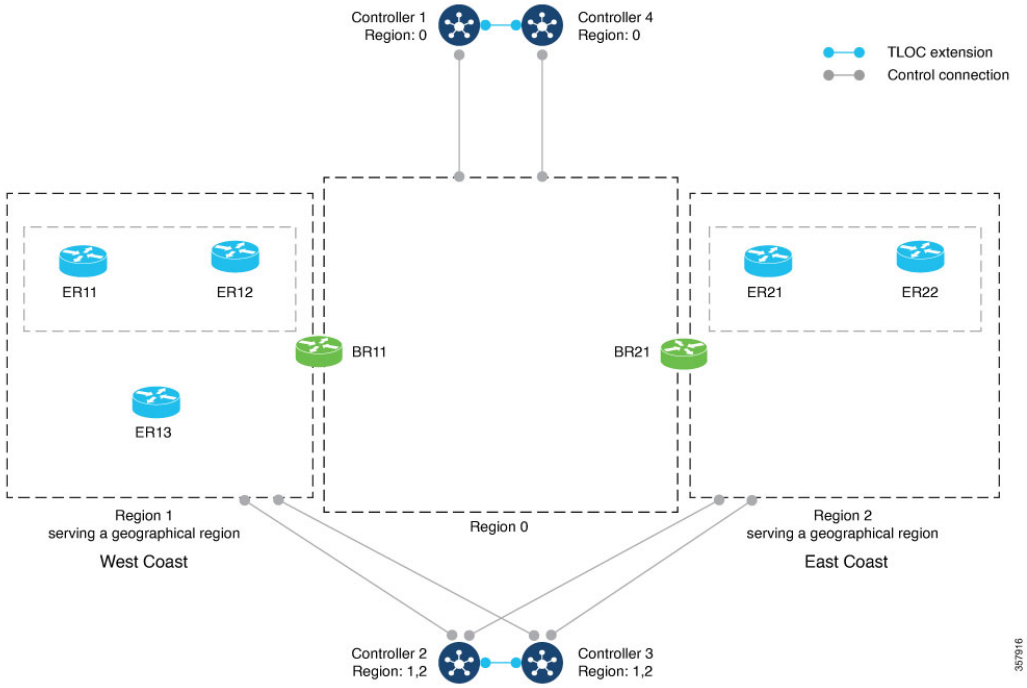
- Cisco SD-WAN Controller 2 serves logical regions 1 and 2.
- The West Coast geographical region has three devices—Edge11, Edge12, and Edge13.
- The East Coast geographical region has two devices—Edge21 and Edge22.
- Cisco Catalyst SD-WAN Gateway11 serves the West Coast geographical region and Cisco Catalyst SD-WAN Gateway21 serves the East Coast geographical region.
- A centralized control policy is defined in Cisco SD-WAN Controller 2 that facilitates hop-by-hop routing. For example, for Edge11 to reach a service-side prefix of Edge21, it must forward the traffic to Cisco Catalyst SD-WAN Gateway11 first. Cisco Catalyst SD-WAN Gateway11 then forwards the traffic from the overlay into the BGP core. The traffic is then forwarded to Cisco Catalyst SD-WAN Gateway21 through Provider Edge1. Lastly, Cisco Catalyst SD-WAN Gateway21 forwards the traffic from the BGP core into the overlay toward Edge21.

To migrate to Multi-Region Fabric, a network administrator plans the expected role and region for each router in the network architecture, and uses the Cisco SD-WAN Manager procedure (Migrate a BGP-Based Hierarchical Core Network to Multi-Region Fabric) to migrate each router.

Note In this example, the network administrator plans the use of four Cisco SD-WAN Controllers. However, only two Cisco SD-WAN Controllers are mandatory for the migration—one for the access region and one for the core region.

The following illustration shows the network after migration.

Figure 4: BGP-Based Network Architecture After Migration to Multi-Region Fabric



In the migration shown in the preceding illustrations, each router continues to perform a similar function within the network, but the terminology describing the routers and segments changes. The following table compares the terminology that applies to each router before and after migration. Cisco Catalyst SD-WAN gateways become border routers, and logical regions are formalized as regions within the Multi-Region Fabric architecture.

Geographical Region	Site	Device Name and Description Before Migration	Device Name and Description After Migration to Multi-Region Fabric
West Coast	1100	Edge11: Edge router	ER11: Edge router, Region 1
West Coast	1100	Edge12: Edge router	ER12: Edge router, Region 1
West Coast	1300	Edge13: Edge router	ER13: Edge router, Region 1
West Coast	11100	Cisco Catalyst SD-WAN Gateway11: Hub router	BR11: Border router, Region 1

Geographical Region	Site	Device Name and Description Before Migration	Device Name and Description After Migration to Multi-Region Fabric
East Coast	22100	Cisco Catalyst SD-WAN Gateway21: Hub router	BR21: Border router, Region 2
East Coast	2100	Edge21: Edge router	ER21: Edge router, Region 2
East Coast	2100	Edge22: Edge router	ER22: Edge router, Region 2

Control Policy Requirements Before Migration

The following tables provide an example of the complex control policy required to accomplish (a) network segmentation, and (b) inter-region routing through the Cisco Catalyst SD-WAN gateways, without Multi-Region Fabric. This policy example may be helpful when planning a migration of a similarly configured enterprise network to Multi-Region Fabric, and it demonstrates the advantage of accomplishing this type of network functionality using Multi-Region Fabric, significantly simplifying policy.

The tables describe the following steps:

- Part A. Define Policy Lists of Site IDs to Use in Control Policies
- Part B. Define Policy Lists of TLOCs to Use in Control Policies
- Part C. Create and Apply Control Policies Using the Lists Defined in the Previous Tables

Table 5: Part A. Define Policy Lists of Site IDs to Use in Control Policies

Brief Description of the Policy Configuration Objective	Detailed Description	Example

1. Define lists that include the edge routers in Region 1 (logical region).	Define a site list of all sites in Region 1. These sites include all edge routers in Region 1.	`policy`
		` lists`
		`  site-list REGION1`
		`   site-id 1100`
		`   site-id 1300`
		`   !`

	Define a site list of all edge routers in Region 1, and the Cisco Catalyst SD-WAN gateway for Region 1. These sites include all edge routers and the Cisco Catalyst SD-WAN gateway in Region 1.	`policy`
		` lists`
		`  site-list REGION1_GATEWAY1`
		`   site-id 1100`
		`   site-id 1300`
		`   site-id 11100`
		`   !`

Brief Description of the Policy Configuration Objective	Detailed Description	Example

2. Define lists that include the edge routers in Region 2 (logical region).	Define a site list of all sites in Region 2. These sites include all edge routers in Region 2.	`policy`
		` lists`
		`  site-list REGION2`
		`   site-id 2100`
		`   !`

	Define a site list of all edge routers in Region 2, and the Cisco Catalyst SD-WAN gateway for Region 2. These sites include all edge routers and the Cisco Catalyst SD-WAN gateway in Region 2.	`policy`
		` lists`
		`  site-list REGION2_GATEWAY2`
		`   site-id 2100`
		`   site-id 22100`
		`   !`

3. Define a list of Region 2 destinations that will be useful when creating control policy for Region 1 outgoing traffic.	Define a list of the following:
	• All edge routers in Region 2
	• The Cisco Catalyst SD-WAN gateway for Region 2
	• The Cisco Catalyst SD-WAN gateway for Region 1
		`policy`
		` lists`
		`   site-list GATEWAY1_GATEWAY2_REGION2`
		`   site-id 11100`
		`   site-id 2100`
		`   site-id 22100`
		`   !`

4. Define a list of Region 1 destinations that will be useful when creating control policy for Region 2 outgoing traffic.	Define a list of the following:
	• All edge routers in Region 1
	• The Cisco Catalyst SD-WAN gateway for Region 1
	• The Cisco Catalyst SD-WAN gateway for Region 2
		`policy`
		` lists`
		`  site-list GATEWAY1_GATEWAY2_REGION1`
		`   site-id 1100`
		`   site-id 11100`
		`   site-id 1300`
		`   site-id 22100`
		`   !`

5. Define a list of Region 1 routers, and the Cisco Catalyst SD-WAN gateway for Region 2. This will be useful when creating a control policy for the Region 1 Cisco Catalyst SD-WAN gateway.	Define a list of the following:
	• All edge routers in Region 1
	• The Cisco Catalyst SD-WAN gateway for Region 2
		`policy`
		` lists`
		`  site-list REGION1_GATEWAY2`
		`   site-id 1100`
		`   site-id 1300`
		`   site-id 22100`
		`   !`

6. Define a list of Region 2 routers, and the Cisco Catalyst SD-WAN gateway for Region 1. This will be useful when creating a control policy for the Region 2 Cisco Catalyst SD-WAN gateway.	Define a list of the following:
	• All edge routers in Region 2
	• The Cisco Catalyst SD-WAN gateway for Region 1
		`policy`
		` lists`
		`  site-list GATEWAY1_REGION2`
		`   site-id 11100`
		`   site-id 2100`
		`   !`

Table 6: Part B. Define Policy Lists of TLOCs to Use in Control Policies

Brief Description of the Policy Configuration Objective	Detailed Description	Example

1. Define lists of TLOCs for traffic between the Cisco Catalyst SD-WAN gateways.
(When the network is migrated to Multi-Region Fabric, this inter-gateway traffic constitutes the core region traffic.)
	• Define a list of TLOCs (GATEWAY1_CORE_TLOC) for traffic from Cisco Catalyst SD-WAN Gateway21 to Cisco Catalyst SD-WAN Gateway11.
	• Define a list of TLOCs (GATEWAY2_CORE_TLOC) for traffic from Cisco Catalyst SD-WAN Gateway11 to Cisco Catalyst SD-WAN Gateway21.
		`policy`
		`lists`
		`  tloc-list GATEWAY1_CORE_TLOC`
		`   tloc 172.16.11.10 color green encap ipsec`
		`  !`
		`  tloc-list GATEWAY2_CORE_TLOC`
		`   tloc 172.17.13.10 color green encap ipsec`
		`  !`

2. Define lists of TLOCs for traffic between the Cisco Catalyst SD-WAN gateways and the routers in the region that they are serving.
(When the network is migrated to Multi-Region Fabric, this constitutes the access region traffic.)
	• Define a list of TLOCs (GATEWAY1_TLOCS) for traffic between Cisco Catalyst SD-WAN Gateway11 and the routers in Region 1, for which it serves as hub.
	• Define a list of TLOCs (GATEWAY2_TLOCS) for traffic between Cisco Catalyst SD-WAN Gateway21 and the routers in Region 2, for which it serves as hub.
		`policy`
		`lists`
		`  tloc-list GATEWAY1_TLOCS`
		`   tloc 172.16.11.10 color lte encap ipsec`
		`   tloc 172.16.11.10 color 3g encap ipsec`
		`   tloc 172.16.11.10 color red encap ipsec`
		`   tloc 172.16.11.10 color green encap ipsec`
		`  !`
		`  tloc-list GATEWAY2_TLOCS`
		`   tloc 172.17.13.10 color lte encap ipsec`
		`   tloc 172.17.13.10 color 3g encap ipsec`
		`   tloc 172.17.13.10 color green encap ipsec`
		`  !`

Table 7: Part C. Create and Apply Control Policies Using the Lists Defined in the Previous Tables

Brief Description of the Policy Configuration Objective	Detailed Description	Example

1. Create a control policy for Region 1 that (a) enables routers within Region 1 to send traffic to one another directly, and that (b) directs all traffic destined to Region 2 to use Cisco Catalyst SD-WAN Gateway11 as a first hop. In this way, Cisco Catalyst SD-WAN Gateway11 serves as a hub for traffic to Region 2.	Create a control policy called CP1 to do the following:
	• Sequence 1: Provide all devices in Region 1 with access to the TLOCs of the other devices in Region 1. This includes the edge routers and the Cisco Catalyst SD-WAN gateways. This creates full-mesh connectivity in Region 1.
	• Sequence 2: Ensure that for any traffic in Region 1 whose destination is Cisco Catalyst SD-WAN Gateway21 or any of the devices in Region 2, the first hop must be Cisco Catalyst SD-WAN Gateway11.
	• Sequence 3: Ensure that for any traffic within Region 1, the devices forward the traffic directly to the destination device within the region.
		control-policy CP1
		  sequence 1
		  match tloc
		  site-list REGION1_GATEWAY1
		  !
		  action accept
		  !
		  !
		  sequence 2
		  match route
		  site-list GATEWAY2_REGION2
		  !
		  action accept
		  set
		  tloc-list GATEWAY1_TLOCS
		  !
		  !
		  !
		  sequence 3
		  match route
		  site-list REGION1_GATEWAY1
		  !
		  action accept
		  !
		  !
		  default-action reject
		!

2. Apply control policy CP1, described in the previous row, to Region 1 for outgoing traffic.		apply-policy site-list REGION1 control-policy CP1 out

Brief Description of the Policy Configuration Objective	Detailed Description	Example
3. Create a control policy for Region 2 that (a) enables routers within Region 2 to send traffic to one another directly, and that (b) directs all traffic destined to Region 1 to use Cisco Catalyst SD-WAN Gateway21 as a first hop. In this way, Cisco Catalyst SD-WAN Gateway21 serves as a hub for traffic to Region 1.	Create a control policy called CP4 to do the following: • Sequence 1: Provide all devices in Region 2 with access to the TLOCs of the other devices in Region 2. This includes the edge routers and the Cisco Catalyst SD-WAN gateways. This creates full-mesh connectivity in Region 2. • Sequence 2: Ensure that for any traffic in Region 2 whose destination is Cisco Catalyst SD-WAN Gateway11 or any of the devices in Region 1, the first hop must be Cisco Catalyst SD-WAN Gateway21. • Sequence 3: Ensure that for any traffic within Region 2, the devices forward traffic directly to the destination device within the region.	control-policy CP4 sequence 1 match tloc site-list GATEWAY2_REGION2 ! action accept ! ! sequence 2 match route site-list GATEWAY1_REGION1 ! action accept set tloc-list GATEWAY2_TLOCS ! ! ! sequence 3 match route site-list GATEWAY2_REGION2 ! action accept ! ! default-action reject ! !
4. Apply control policy CP4, described in the previous row, to Region 2 for outgoing traffic.		apply-policy site-list REGION2 control-policy CP4 out
5. Create a control policy for Cisco Catalyst SD-WAN Gateway11 that provides it with full-mesh connectivity with devices in Region 1.	Create a control policy called CP2 to do the following: • Sequence 1: Provide access to the TLOCs of devices in Region 1. This creates full-mesh connectivity for the gateway with the other routers in Region 1. • Sequence 2: Ensure that for any traffic within Region 1, the devices forward the traffic directly to the destination device within the region.	control-policy CP2 sequence 1 match tloc site-list REGION1_GATEWAY1 ! action accept ! ! sequence 2 match route site-list REGION1_GATEWAY1 ! action accept ! ! default-action reject !

Brief Description of the Policy Configuration Objective	Detailed Description	Example

6. Apply control policy CP2, described in the previous row, to Cisco Catalyst SD-WAN Gateway11 for Region 1.		`apply-policy`
		`site-list GATEWAY1`
		`  control-policy CP2 out`
		`!`

7. Create a control policy for Cisco Catalyst SD-WAN Gateway21 that provides it with full-mesh connectivity with devices in Region 2.	Create a control policy called CP3 to do the following:
	• Sequence 1: Provide access to the TLOCs of devices in Region 2. This creates full-mesh connectivity for the gateway with the other routers in Region 2.
	• Sequence 2: Ensure that for any traffic within Region 2, the devices forward traffic directly to the destination device within the region.
		`control-policy CP3`
		`  sequence 1`
		`   match tloc`
		`    site-list GATEWAY2_REGION2`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  sequence 2`
		`   match route`
		`    site-list GATEWAY2_REGION2`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  default-action reject`
		`!`
		`!`

8. Apply control policy CP3, described in the previous row, to Cisco Catalyst SD-WAN Gateway21 for Region 2.		`apply-policy`
		`site-list GATEWAY2`
		`  control-policy CP3 out`
		`!`

Migrate to Multi-Region Fabric Using Cisco SD-WAN Manager

Before You Begin

- Starting with the existing network architecture, plan which devices in the network to migrate to Multi-Region Fabric. Plan the role and region for each of these devices, as they will function within a Multi-Region Fabric architecture.
- Plan which Cisco SD-WAN Controllers you will require in the network after migration. Following migration, the default Cisco SD-WAN Controller in use before migration will not be in service. We recommend repurposing this Cisco SD-WAN Controller for use in the core region.

Migrate to Multi-Region Fabric

1. For each device in the network, create a Cisco System template (Cisco IOS XE Catalyst SD-WAN device) or Cisco vEdge System template (Cisco vEdge device) for the device, or open the existing template already assigned to the device.
2. In the **Basic Configuration** section, set the **Enable Migration Mode to Multi-Region Fabric** field to **Enable**.
3. Apply the templates to the devices. This places the devices into migration mode.

4. Deploy a Cisco SD-WAN Controller to serve the Multi-Region Fabric core region.

   For information about deploying a Cisco SD-WAN Controller, see the "Cisco SD-WAN Overlay Network Bring-Up Process" chapter of the *Cisco Catalyst SD-WAN Getting Started Guide*.

   - Apply the same feature templates, device template, and policy templates as are currently active on the default region Cisco SD-WAN Controllers.
   - Set the Multi-Region Fabric region of the Cisco SD-WAN Controller to 0.

     For information about assigning a region to a Cisco SD-WAN Controller, see Assign Regions to a Cisco Catalyst SD-WAN Controller Using Cisco SD-WAN Manager.

5. Deploy Cisco SD-WAN Controllers to serve the Multi-Region Fabric access regions.

   - Apply the same feature templates, device template, and policy templates as are currently active on the default region Cisco SD-WAN Controllers.
   - Set the Multi-Region Fabric region of each Cisco SD-WAN Controller to the region number that it is intended to serve.

6. For each device that will function as a border router, apply a configuration to enable the device to connect to the core region, the relevant access region, and the default region Cisco SD-WAN Controller.

   For additional information, see Assign a Role and Region to a Device Using Cisco SD-WAN Manager and Assign Border Router TLOCs to the Core Region Using Cisco SD-WAN Manager.

7. For each device that will function as a border router, view the OMP peers to confirm connectivity to the default region Cisco SD-WAN Controller, the core region Cisco SD-WAN Controllers, and the access region Cisco SD-WAN Controllers. For information about viewing the OMP peers, see View OMP Peers Using Cisco SD-WAN Manager, on page 27.

8. For each device that will function as an edge router, do the following:

   a. Apply a configuration to enable the device to connect to the default region Cisco SD-WAN Controllers and the Cisco SD-WAN Controllers for the access region to which the edge router belongs.

   b. Configure the region.

      For information about configuring the region, see Assign a Role and Region to a Device Using Cisco SD-WAN Manager.

9. For each border router, do the following to disable migration mode:

   a. Open the Cisco System template (Cisco IOS XE Catalyst SD-WAN device) or Cisco vEdge System template (Cisco vEdge device) for the device.

   b. In the **Basic Configuration** section, set the **Enable Migration Mode to Multi-Region Fabric** field to **Default**. (After choosing **Default**, the field is blank.)

   c. Apply the template to the device.

   When you complete this step on a device, the border router no longer connects to the default region Cisco SD-WAN Controllers.

10. View the OMP peers to verify that the device has the following peers:

- The Cisco SD-WAN Controllers serving the access region for which this devices serves as a border router
- The Cisco SD-WAN Controllers serving the core region

For information about viewing the OMP peers, see View OMP Peers Using Cisco SD-WAN Manager, on page 27.

11. For each edge router, do the following to disable migration mode:
    a. Open the Cisco System template (Cisco IOS XE Catalyst SD-WAN device) or Cisco vEdge System template (Cisco vEdge device) for the device.
    b. In the **Basic Configuration** section, set the **Enable Migration Mode to Multi-Region Fabric** field to **Default**. (After choosing **Default**, the field is blank.)
    c. Apply the template to the device.
12. After disabling migration mode for each device, the devices in the network no longer use the default region Cisco SD-WAN Controller. Optionally, if your network planning involves using this controller for the core region, as recommended in the **Before You Begin** section, you can reassign this Cisco SD-WAN Controller to serve the core region.
13. After completing the migration, the control policies that were previously in use to divide the network into segments and to route traffic through hubs, are no longer required. On the Cisco SD-WAN Controller that served as the default region Cisco SD-WAN Controller, remove the control policies by detaching the policy templates for these policies from each Cisco SD-WAN Controller.

    For information about removing a policy template from a Cisco SD-WAN Controller, see the "Centralized Policy" chapter of the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*.

Migrate a BGP-Based Hierarchical Core Network to Multi-Region Fabric

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.2a, Cisco vManage Release 20.9.2, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

Before You Begin

- Starting with the existing network architecture, plan which devices in the network to migrate to Multi-Region Fabric. Plan the role and region for each of these devices, as they will function within a Multi-Region Fabric architecture.
- Plan which Cisco SD-WAN Controllers you will require in the network after migration. Following migration, the default Cisco SD-WAN Controller in use before migration will not be in service. We recommend repurposing this Cisco SD-WAN Controller for use in the core region.

Migrate to Multi-Region Fabric

1. For each device in the network, create a Cisco System template (Cisco IOS XE Catalyst SD-WAN device) or Cisco vEdge System template (Cisco vEdge device) for the device, or open the existing template already assigned to the device.
2. For each device that will function as an edge router, in the **Basic Configuration** section, set the **Enable Migration Mode to Multi-Region Fabric** field to **Enable**.
3. Apply the templates to the devices. This places the devices into migration mode.
4. Deploy a Cisco SD-WAN Controller to serve the Multi-Region Fabric core region.

   For information about deploying a Cisco SD-WAN Controller, see the "Cisco SD-WAN Overlay Network Bring-Up Process" chapter of the *Cisco Catalyst SD-WAN Getting Started Guide*.

   - Apply the same feature templates, device template, and policy templates as are currently active on the default region Cisco SD-WAN Controllers.
   - Set the Multi-Region Fabric region of the Cisco SD-WAN Controller to 0.

     For information about assigning a region to a Cisco SD-WAN Controller, see Assign Regions to a Cisco Catalyst SD-WAN Controller Using Cisco SD-WAN Manager.

5. Deploy Cisco SD-WAN Controllers to serve the Multi-Region Fabric access regions.
   - Apply the same feature templates, device template, and policy templates as are currently active on the default region Cisco SD-WAN Controllers.
   - Set the Multi-Region Fabric region of each Cisco SD-WAN Controller to the region number that it is intended to serve.
6. Configure a route map to append the community string in additive manner, and apply the route map on the Cisco Catalyst SD-WAN gateways toward the provider edge router for BGP peering. In addition, apply a similar route map on the provider edge router toward the Cisco Catalyst SD-WAN gateways for BGP peering.

Note The community string used across all the steps—either in a route map or in the **Migration BGP Community** field—must be the same.

7. For each device that will have the role of border router, in the Cisco BGP feature template for the device, do the following:
   a. In the **Basic Configuration** section, enable **Propagate Community**.
   b. In the **Neighbor** section, for each configured neighbor, enable **Send Community**, which is enabled by default.
8. Configure the propagate-community parameter on the Cisco Catalyst SD-WAN gateways.
9. Configure the send-community parameter on the provider edge router for BGP peering to the Cisco Catalyst SD-WAN gateways.
10. Configure a route map on the Cisco Catalyst SD-WAN gateways, which allows only those routes that match the community string used for migration.

This route map is used for OMP to BGP redistribution on all the gateway routers.

11. For each Cisco Catalyst SD-WAN gateway that will function as a border router, open the device template in Cisco SD-WAN Manager in the draft mode, modify all the relevant feature templates associated with the device template, and then move the template out of the draft mode.

    Configure the following on the Cisco Catalyst SD-WAN gateways:

    - Migration mode: Enabled from BGP core
    - Migration community: <*value*>
    - Role: Border router
    - Corresponding access gegion it is intended to serve
    - Route map in the OMP to BGP redistribution direction that matches and permits routes which are tagged with the community <*value*>
    - TLOCs in the core region

12. For each device that will function as a border router, view the OMP peers to confirm connectivity to the default region Cisco SD-WAN Controller, the core region Cisco SD-WAN Controllers, and the access region Cisco SD-WAN Controllers. For information about viewing the OMP peers, see View OMP Peers Using Cisco SD-WAN Manager, on page 27.

13. Modify the control policies on the Cisco SD-WAN Controller to allow the Cisco Catalyst SD-WAN gateways, which are now border routers, to receive the TLOCs of each other.

14. For each device that will function as an edge router, configure the region.

    For information about configuring the region, see Assign a Role and Region to a Device Using Cisco SD-WAN Manager.

15. Remove the route-map definition from the provider edge router that was appended with the community string.

16. Remove the route maps from the border routers that were configured for BGP peering and for OMP to BGP redistribution.

17. For each border router, do the following to disable migration mode:

    a. Open the Cisco System template (Cisco IOS XE Catalyst SD-WAN device) or Cisco vEdge System template (Cisco vEdge device) for the device.

    b. In the **Basic Configuration** section, set the **Enable Migration Mode to Multi-Region Fabric** field to **Default**. (After choosing **Default**, the field is blank.)

    c. Apply the template to the device.

    When you complete this step on a device, the border router no longer connects to the default region Cisco SD-WAN Controllers.

18. View the OMP peers to verify that the device has the following peers:

    - The Cisco SD-WAN Controllers serving the access region for which this device is a border router
    - The Cisco SD-WAN Controllers serving the core region

For information about viewing the OMP peers, see View OMP Peers Using Cisco SD-WAN Manager, on page 27.

19. For each edge router, do the following to disable migration mode:
    a. Open the Cisco System template (Cisco IOS XE Catalyst SD-WAN device) or Cisco vEdge System template (Cisco vEdge device) for the device.
    b. In the **Basic Configuration** section, set the **Enable Migration Mode to Multi-Region Fabric** field to **Default**. (After choosing **Default**, the field is blank.)
    c. Apply the template to the device.
20. After disabling migration mode for each device, the devices in the network no longer use the default region Cisco SD-WAN Controller. Optionally, if your network planning involves using this controller for the core region, as recommended in the **Before You Begin** section, you can reassign this Cisco SD-WAN Controller to serve the core region.
21. After completing the migration, the control policies that were previously in use to divide the network into segments and to route traffic through hubs, are no longer required. Remove the control policies by detaching the policy templates for these policies from each Cisco SD-WAN Controller.

    For information about removing a policy template from a Cisco SD-WAN Controller, see the "Centralized Policy" chapter of the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*.

Enable or Disable Migration Mode Using the CLI

Enable Migration Mode

1. Enter system mode.

   ```
   system
   ```

2. Enable migration mode.

   ```
   multi-region-fabric migration-mode enabled
   ```

Disable Migration Mode

1. Enter system mode.

   ```
   system
   ```

2. Disable migration mode.

   ```
   no multi-region-fabric migration-mode
   ```

Enable or Disable Migration Mode in a BGP-Based Network Using the CLI

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.2a, Cisco vManage Release 20.9.2, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

Enable Migration Mode

1. Enter system mode.

   system

2. Enable migration mode on the edge devices.

   multi-region-fabric migration-mode enabled

3. Enable migration mode on the Cisco Catalyst SD-WAN gateways.

   ```
   multi-region-fabric
   migration-mode enabled-from-bgp-core
   migration-bgp-community community value
   ```

Disable Migration Mode

1. Enter system mode.

   system

2. Disable migration mode on the Cisco Catalyst SD-WAN gateways.

   no multi-region-fabric

3. Disable migration mode on the edge devices.

   no multi-region-fabric

Verification Procedures for Migration to Multi-Region Fabric

The following procedures are helpful for verifying the connectivity and other information after migrating a network to Multi-Region Fabric.

View OMP Peers Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. In the table of devices, click **…** at the right of the desired border router and choose **Real Time**.
3. In the left pane, click **Real Time**.
4. In the **Device Options** field, enter **OMP Peers**.

   A table shows peer information, similarly to the **show sdwan omp peers** CLI command. In the output, check the **REGION ID** column, which shows one of the following for each peer.

- **None**: A Cisco SD-WAN Controller that has not been configured to operate with Multi-Region Fabric. This includes the default region Cisco SD-WAN Controllers configured before migration to Multi-Region Fabric.
- **0**: Core region Cisco SD-WAN Controllers.
- *access-region-id*: Access region Cisco SD-WAN Controllers.

Verify Connectivity Between Devices Using Cisco SD-WAN Manager

Use this procedure to trace the route between two devices, such as two edge devices in different regions to verify connectivity between the devices.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. In the table of devices, click **…** adjacent to the desired border router and choose **Real Time**.
3. In the left pane, click **Troubleshooting**.
4. Click **Trace Route**.
5. In the **Destination IP** field, enter an IP address for the endpoint of the route tracing.
6. Click the **VPN** drop-down list and choose the VPN for the route tracing.

Verify That a Border Router is Re-Originating Routes Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. In the table of devices, click **…** adjacent to the desired border router and choose **Real Time**.
3. In the left pane, click **Real Time**.
4. In the **Device Options** field, enter **OMP Received Routes**.

Locate the rows of the table that show 0.0.0.0 in the **Peer** column. These rows correspond to routes from the border router itself. If the border router is re-originating routes, then in those rows, the **Region Path** column shows two numbers for the route, including a 0 for the core region, and the **Status** column shows **BR-R** (border router re-originated).

Verify That a Border Router is Re-Originating Routes Using the CLI

On a border router, use the following command:

show sdwan omp routes *ip-number/subnet-mask*

Locate the rows of the table that show 0.0.0.0 in the **Peer** column. These rows correspond to routes from the border router itself. If the border router is re-originating routes, then in those rows, the **Region Path** column shows two numbers for the route, including a **0** for the core region, and the **Status** column shows **BR-R** (border router re-originated).

Example:

```
show sdwan omp routes 10.1.1.0/24
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved
BR-R -> Border-Router reoriginated
TGW-R -> Transport-Gateway reoriginated

         AFFINITY                                    PATH                    ATTRIBUTE
         GROUP
TENANT   VPN PREFIX       FROM PEER      ID     LABEL  STATUS   TYPE       TLOC IP       COLOR  ENCAP
PREFERENCE  NUMBER    REGION ID  REGION PATH
------------------------------------------------------------------------------------------------------------------------
0        1   10.1.1.0/24 0.0.0.0        21474  1003   C,Red,R, installed  172.18.11.10  green ipsec  -
         None      0          0 1
                                        83721          BR-R

                         172.16.122.10   104    1003    C,I,R   installed  172.18.51.10  lte   ipsec  -
         None      1          1
                         172.16.122.10   105    1003    C,I,R   installed  172.18.51.10  red   ipsec  -
         None      1          1
                         172.16.123.10   118    1003    C,R     installed  172.18.51.10  lte   ipsec  -
         None      1          1
                         172.16.123.10   119    1003    C,R     installed  172.18.51.10  red   ipsec  -
         None      1          1
```