

Cisco Catalyst SD-WAN Multi-Region Fabric Configuration Guide, Releases 26.x and Later

First Published: 2026-03-04

Last Modified: 2026-05-04

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1 **Read Me First** 1

CHAPTER 2 **Quick Start: Multi-Region Fabric and Related Features** 3

Configure Multi-Region Fabric and Related Features 3

CHAPTER 3 **Cisco Catalyst SD-WAN Multi-Region Fabric** 5

Configure Cisco Catalyst SD-WAN Multi-Region Fabric 5

Information About Multi-Region Fabric 6

Benefits of Multi-Region Fabric 11

Supported Devices for Multi-Region Fabric 12

Prerequisites for Multi-Region Fabric 12

Restrictions for Multi-Region Fabric 13

Use Cases for Multi-Region Fabric 15

Enable Multi-Region Fabric 16

Configure Multi-Region Fabric Using Configuration Groups in Cisco SD-WAN Manager 16

Configure the Multi-Region Fabric Role Using a Configuration Group 16

Configure a Secondary Region Using a Configuration Group 17

Configure Which Traffic a Border Router Interface Handles, Using a Configuration Group 18

Configure Which Traffic an Edge Router Interface Handles, Using a Configuration Group 19

Configure a Router to Treat Hierarchical and Direct Paths Equally, Using a Configuration Group 19

Configure the Regions for Route Aggregation Using a Configuration Group 20

Configure Transport Gateway Path Behavior Using a Configuration Group 21

Configure the Region and Subregion When Deploying a Configuration Group 22

Configure Multi-Region Fabric Using Feature Templates in Cisco SD-WAN Manager 22

Assign a Role and Region to a Device Using Cisco SD-WAN Manager 24
Assign Border Router TLOCs to the Core Region Using Cisco SD-WAN Manager 26
Assign regions to a Cisco Catalyst SD-WAN Controller using templates 28
Use Regions With a Centralized Policy 28
Create a Region List Using Cisco SD-WAN Manager 28
Add a Region Match Condition to a Centralized Policy 29
Attach a Centralized Policy to a Region 29
Configure Multi-Region Fabric Using the CLI 30
Assign a Role to a Device Using the CLI 30
Assign a Region ID to an Edge Router TLOCs Using a CLI Template 30
Assign a Region ID to a Border Router TLOCs Using a CLI Template 31
Assign Regions to a Cisco Catalyst SD-WAN Controller Using the CLI 31
Verify Multi-Region Fabric 32
Monitor Multi-Region Fabric 33

CHAPTER 4 **Migrating to Multi-Region Fabric** 35
Migrating to Multi-Region Fabric 35
Information About Migrating to Multi-Region Fabric 36
Benefits of Migrating to Multi-Region Fabric 37
Supported Devices for Migrating to Multi-Region Fabric 37
Prerequisites for Migrating to Multi-Region Fabric 37
Use Cases for Migrating to Multi-Region Fabric 38
Use Case 2: Migration of a BGP-Based Hierarchical Core Network 46
Migrate to Multi-Region Fabric Using Cisco SD-WAN Manager 54
Migrate a BGP-Based Hierarchical Core Network to Multi-Region Fabric 56
Enable or Disable Migration Mode Using the CLI 59
Enable or Disable Migration Mode in a BGP-Based Network Using the CLI 59
Verification Procedures for Migration to Multi-Region Fabric 60
View OMP Peers Using Cisco SD-WAN Manager 60
Verify Connectivity Between Devices Using Cisco SD-WAN Manager 60
Verify That a Border Router is Re-Originating Routes Using Cisco SD-WAN Manager 61
Verify That a Border Router is Re-Originating Routes Using the CLI 61

CHAPTER 5 **Create Regions and Assign Controllers Workflow** 63

Information about the Create WAN Regions and Assign Controllers Workflow 63
Prerequisites for the Create Regions and Assign Controllers Workflow 64
Restrictions for the Create Regions and Assign Controllers Workflow 64
Use Cases for the Create Regions and Assign Controllers Workflow 64
Create Regions and Assign Controllers Workflow 64
Verify Regions 65

CHAPTER 6 **Multi-Region Fabric Secondary Regions** 67
Multi-Region Fabric Secondary Regions 67
Information About Secondary Regions 68
Benefits of Secondary Regions 71
Matching Routes by Path Type, Region, or Role 71
Restrictions for secondary regions 72
Use Cases for Secondary Regions 72
Configure a Secondary Region Using Cisco SD-WAN Manager 74
Configure a Secondary Region ID for an Edge Router Using Cisco SD-WAN Manager 74
Configure the Secondary Region Mode for a TLOC Using Cisco SD-WAN Manager 74
Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using Cisco SD-WAN Manager 75
Configure a Secondary Region Using the CLI 76
Configure a Secondary Region ID for an Edge Router Using the CLI 76
Configure the Secondary Region Mode of a TLOC Using the CLI 76
Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using the CLI 77
Verify a Device Secondary Region Assignment Using Cisco SD-WAN Manager 78
Verify a Device Secondary Region Assignment Using the CLI 78
Verify an Interface Secondary Region Mode Using the CLI 78
Verify an Interface Secondary Region Assignment Using the CLI 79

CHAPTER 7 **Multi-Region Fabric Management Region** 81
Multi-Region Fabric Management Region 81
Information About Management Regions 82
Benefits of Management Regions 83
Restrictions for Management Regions 83

Configure a Management Region 83
Configure a Cisco SD-WAN Controller to Support a Management Region, Using CLI Commands 84
Enable the Management Region for a Management Gateway, Using a Configuration Group 85
Enable the Management Region for a Management Gateway, Using CLI Commands 85
Configure a Router to Support a Management Region, Using a Configuration Group 87
Configure a Router to Support a Management Region, Using CLI Commands 88
Verify the Management Region Configuration 88

CHAPTER 8 **Transport Gateways** 91
Transport Gateways 91
Information About Transport Gateways 91
Benefits of Transport Gateways 93
Supported Devices for Transport Gateways 94
Restrictions for Transport Gateways 94
Configure Transport Gateways Using Cisco SD-WAN Manager 95
Enable Transport Gateway Functionality on a Router Using Cisco SD-WAN Manager 95
Configure the Transport Gateway Path Preference Using Cisco SD-WAN Manager 96
Configure Transport Gateways Using the CLI 96
Enable Transport Gateway Functionality on a Router Using a CLI Template 96
Configure the Transport Gateway Path Preference Using a CLI Template 97
Verify a Transport Gateway Configuration Using the CLI 98

CHAPTER 9 **Router Affinity** 99
Router Affinity 99
Information About Router Affinity Groups 100
Benefits of Router Affinity Groups 104
Information About Setting an Affinity Group by Control Policy 104
Benefits of Setting an Affinity Group by Control Policy 105
Information About Support for Affinity Groups with Service Routes and TLOC Routes 105
Benefits of Support for Affinity Groups with Service Routes and TLOC Routes 106
Supported Devices for Router Affinity Groups 108
Supported Platforms for Setting an Affinity Group by Control Policy 108
Supported Devices for Support for Affinity Groups with Service Routes and TLOC Routes 108
Prerequisites for Support for Affinity Groups with Service Routes and TLOC Routes 108

Restrictions for Router Affinity Groups 109
Use Cases for Router Affinity Groups 109
Use Cases for Setting an Affinity Group by Control Policy 111
Use Cases Support for Affinity Groups with Service Routes and TLOC Routes 113
Use Case: Network Services and Control Policy 113
Use Case: TLOC Route Filtering by Affinity Group 115
Configure Router Affinity Groups Using Cisco SD-WAN Manager 116
Configure an Affinity Group or Affinity Group Preference on a Device, Using Cisco SD-WAN Manager 116
Configure a Cisco SD-WAN Controller to Provide Only Paths in the Affinity Preference List, Using Cisco SD-WAN Manager 117
Configure Affinity Group by Control Policy Using Cisco SD-WAN Manager 118
Configure Router Affinity Groups Using the CLI 118
Configure an Affinity Group on a Router Using the CLI 118
Configure Affinity Group Preference on a Router Using the CLI 119
Configure a Cisco SD-WAN Controller to Provide Only Paths in an Affinity Group Preference List Using a CLI Template 119
Configure Affinity Group by Control Policy Using a CLI Template 120
Verify an Affinity Group and Affinity Group Preference Using Cisco SD-WAN Manager 122
Verify the Affinity Group and Affinity Group Preference Using the CLI 122

CHAPTER 10 **Multi-Region Fabric Subregions** 123
Multi-Region Fabric Subregions 123
Information About Subregions 124
Benefits of Subregions 127
Supported Devices for Subregions 127
Restrictions for Subregions 127
Use Cases for Subregions 128
Use Case: Sharing Border Routers 128
Use Case: Border Router Failover 129
Use Case: Sharing Transport Gateways Across Subregions 130
Use Case: Dedicated Transport Gateways 131
Configure and Use Subregions 131

CHAPTER 11 **Multi-Region Fabric Using Multicloud and SDCI** 133

Multi-Region Fabric Using Multicloud and SDCI 133

Information About Multi-Region Fabric Using Multicloud and SDCI 133

Benefits of Multi-Region Fabric Using Multicloud and SDCI 134

Supported Devices for Multi-Region Fabric Using Multicloud and SDCI 135

Prerequisites for Multi-Region Fabric Using Multicloud and SDCI 135

Restrictions for Multi-Region Fabric Using Multicloud and SDCI 135

Use Cases for Multi-Region Fabric Using Multicloud and SDCI 135

Use Case 1: Multi-Region Fabric Deployment with Cloud Service Provider as Backbone 135

Use Case 2: Multi-Region Fabric Deployment with SDCI as Backbone: Edge-Cloud Topology 136

Use Case 3: Multi-Region Fabric Hybrid Deployment with SDCI as Backbone and Cloud Gateway as Edge Router 137

Workflow for Configuring Multi-Region Fabric with a Cloud Service Core Region 138

CHAPTER 12 **Multi-Region Fabric Policy** 141

Multi-Region Fabric Policy 141

Information About Configuring Policies for Multi-Region Fabric 142

Matching Routes by Path Type, Region, or Role 142

Matching Traffic-To 143

Matching by Region and Role 147

Information About Matching Traffic According to the Destination Region 147

Information About Configuring Path Preference 148

Prioritization of Policy 149

Supported Devices for Multi-Region Fabric Policy Options 149

Restrictions for Multi-Region Fabric Policy Options 149

Multi-Region Fabric Use Cases 150

Use Cases for Configuring Path Preference 150

Configure Multi-Region Fabric Policy Using Cisco SD-WAN Manager 151

Configure a Data Policy or Application Route Policy to Match Traffic-To Using Cisco SD-WAN Manager 151

Configure a Control Policy to Match Region and Role Using Cisco SD-WAN Manager 153

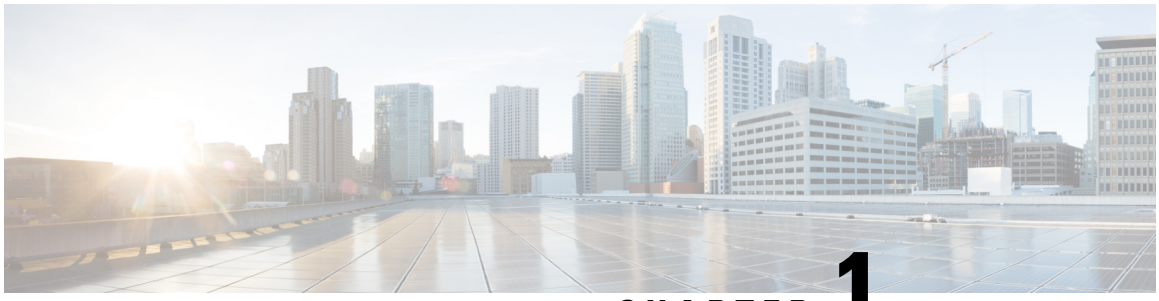
Match Traffic According to the Destination Region Using Cisco SD-WAN Manager 154

Configure the Path Preference for a Preferred Color Group List Using Cisco SD-WAN Manager 155

Use a Preferred Color Group in a Policy 156
Configure Multi-Region Fabric Policy Using the CLI 158
Match Routes According to Path Type Using the CLI 158
Match Routes According to Region and Role Using the CLI 159
Create a Region List Using a CLI Template 159
Configure a Data Policy or Application Route Policy to Match Traffic-To Using a CLI Template 160
Configure a Control Policy to Match Region and Role Using a CLI Template 161
Apply a Policy Using a CLI Template 162
Match Traffic According to the Destination Region Using the CLI 163
Configure the Path Preference for a Preferred Color Group List Using the CLI 165

CHAPTER 13 **Route Aggregation on Border Routers and Transport Gateways** 169
Route Aggregation on Border Routers and Transport Gateways 169
Information About Route Aggregation on Border Routers and Transport Gateways 169
Benefits of Route Aggregation on Border Routers and Transport Gateways 172
Supported Platforms for Route Aggregation on Border Routers and Transport Gateways 172
Use Cases for Route Aggregation on Border Routers and Transport Gateways 173
Configure Route Aggregation on Border Routers and Transport Gateways Using Cisco SD-WAN Manager 173
Configure Route Aggregation on Border Routers and Transport Gateways Using a CLI Template 175

APPENDIX A **End of support for three types of regions** 177
Overview of end of support for three types of regions 177
Secondary regions 177
Subregions 178
Replace Subregion Configurations with Tunnel Groups 180
Management regions 180



CHAPTER 1

Read Me First

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.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17
- User Documentation for Cisco SD-WAN Release 20

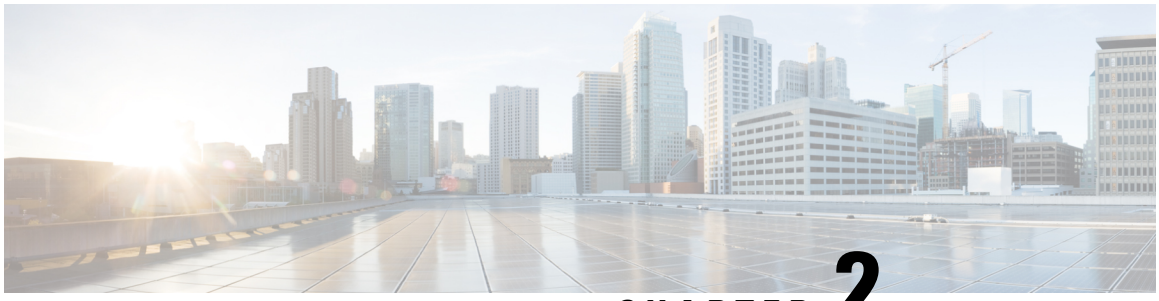
Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.

- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



CHAPTER 2

Quick Start: Multi-Region Fabric and Related Features

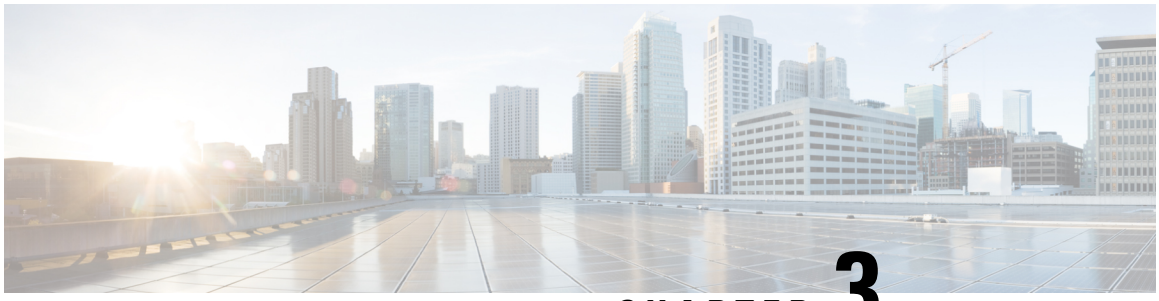
- Configure Multi-Region Fabric and Related Features, on page 3

Configure Multi-Region Fabric and Related Features

Table 1: Configure Multi-Region Fabric and Related Features

Configuration Task	Information
Enable full Multi-Region Fabric functionality.	Enable Multi-Region Fabric, on page 16
Manage the network hierarchy, including creating regions, subregions, and secondary regions.	*Network Hierarchy Management* in the *Cisco Catalyst SD-WAN Network Hierarchy Configuration Guide*
Configure the Multi-Region Fabric role for a router.	Configure the Multi-Region Fabric Role Using a Configuration Group, on page 16
Configure a secondary region for a router.	Configure a Secondary Region Using a Configuration Group, on page 17
Configure how a border router interface handles access and core region traffic.	Configure Which Traffic a Border Router Interface Handles, Using a Configuration Group, on page 18
Configure how an edge router interface handles secondary region traffic.	Configure Which Traffic an Edge Router Interface Handles, Using a Configuration Group, on page 19
Configure a router to treat hierarchical and direct paths equally.	Configure a Router to Treat Hierarchical and Direct Paths Equally, Using a Configuration Group, on page 19
Configure transport gateway path behavior.	Configure Transport Gateway Path Behavior Using a Configuration Group, on page 21

Configuration Task	Information
Configure the regions for route aggregation.	Configure the Regions for Route Aggregation Using a Configuration Group, on page 20
Configure the region and subregion when deploying a configuration group to routers.	Configure the Region and Subregion When Deploying a Configuration Group, on page 22



CHAPTER 3

Cisco Catalyst SD-WAN Multi-Region Fabric

- Configure Cisco Catalyst SD-WAN Multi-Region Fabric, on page 5
- Information About Multi-Region Fabric, on page 6
- Supported Devices for Multi-Region Fabric, on page 12
- Prerequisites for Multi-Region Fabric, on page 12
- Restrictions for Multi-Region Fabric, on page 13
- Use Cases for Multi-Region Fabric, on page 15
- Enable Multi-Region Fabric, on page 16
- Configure Multi-Region Fabric Using Configuration Groups in Cisco SD-WAN Manager, on page 16
- Configure Multi-Region Fabric Using Feature Templates in Cisco SD-WAN Manager, on page 22
- Use Regions With a Centralized Policy, on page 28
- Configure Multi-Region Fabric Using the CLI, on page 30
- Verify Multi-Region Fabric, on page 32
- Monitor Multi-Region Fabric, on page 33

Configure Cisco Catalyst SD-WAN Multi-Region Fabric

Table 2: 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.

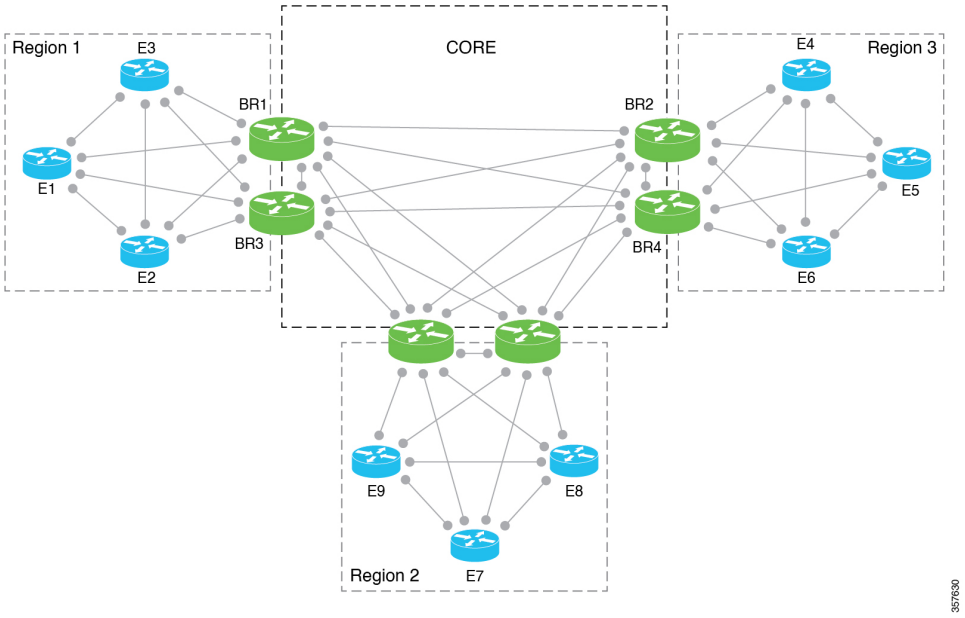
Information About Multi-Region Fabric

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 13.

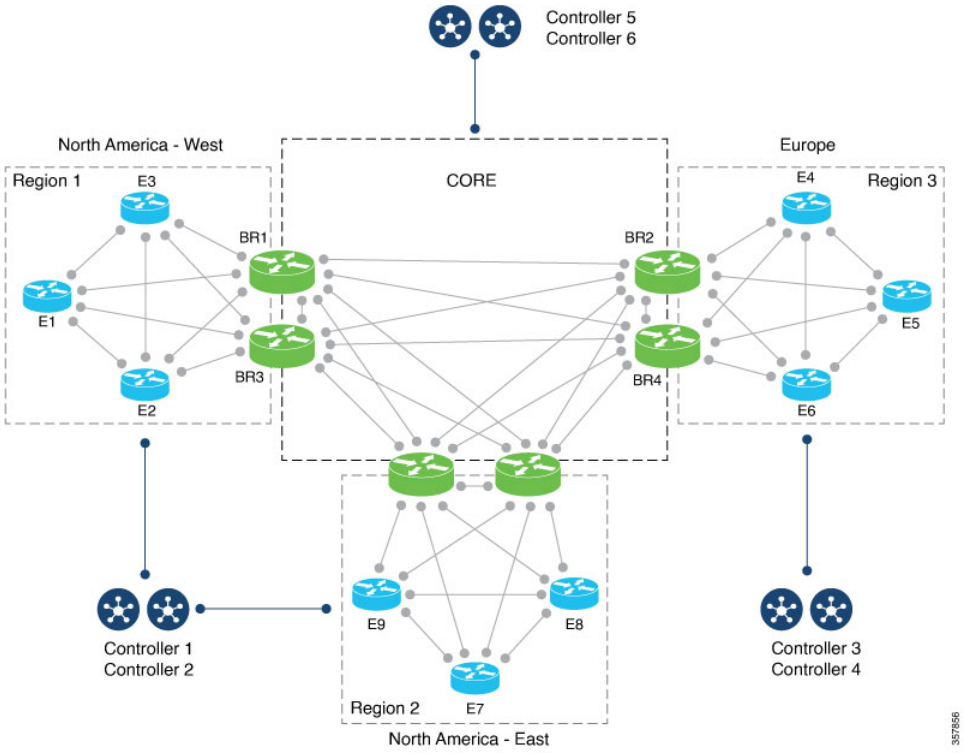
Distributed Cisco Catalyst SD-WAN Controllers

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 13.

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 15.
- Enabling site-to-site traffic paths between disjoint providers

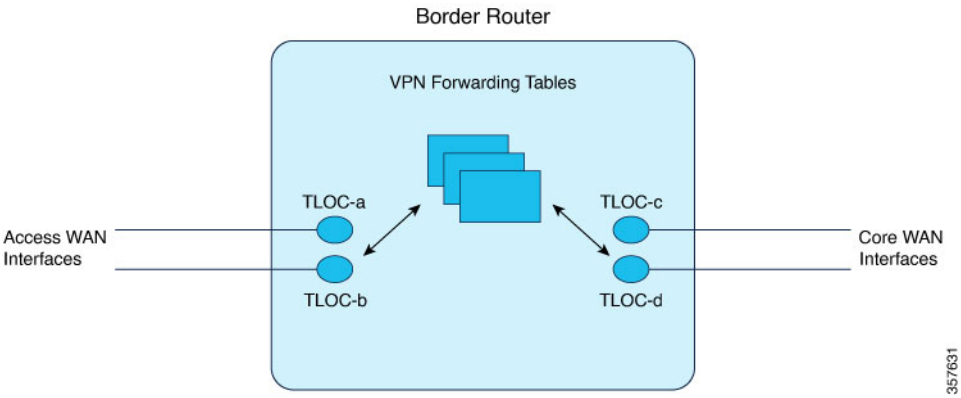
The architecture of Multi-Region Fabric separates between edge routers and border routers. This enables you to establish site-to-site traffic paths between disjoint providers, which are two providers that cannot provide direct IP routing reachability between them. If each site connects to a core-region 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 6.

- 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, in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

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 3: 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 the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.
- The default role is edge router.
- Enable Multi-Region Fabric. For information, see Enable Multi-Region Fabric, on page 16.
- Define at least one secondary region.

  Define secondary regions in the network hierarchy manager (**Configuration** > **Network Hierarchy**). See the *Cisco Catalyst SD-WAN Network Hierarchy Configuration Guide*.

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 Reference Guide*.
- 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 16.

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 the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.
- 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 Reference Guide*.
- 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 the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide* .
- 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 the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide* .

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.

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 the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide* .

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 4: 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.

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 13.

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 6.
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, on page 13.
- 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 *Cisco Catalyst SD-WAN Network Hierarchy Configuration Guide*.

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, on page 26.
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

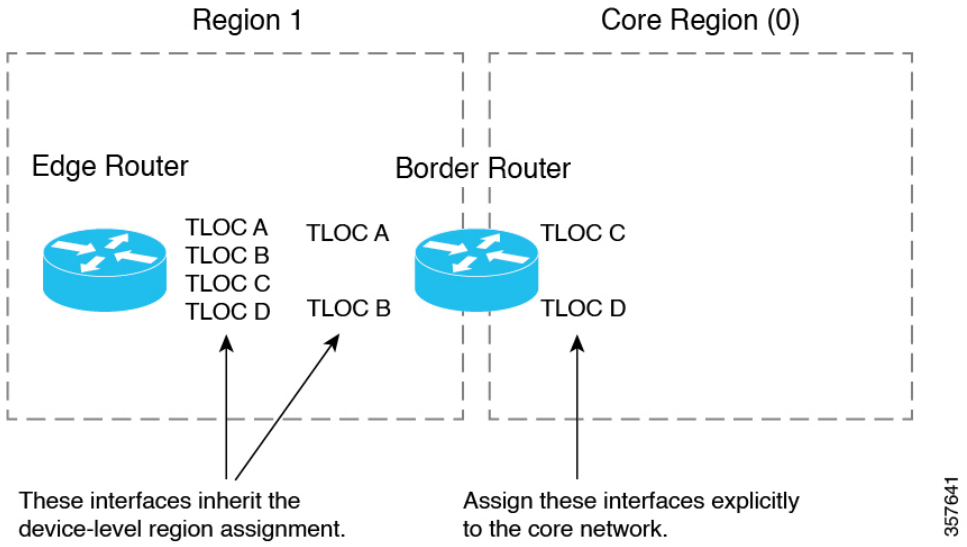
Before You Begin

- 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 Role and Region to a Device Using Cisco SD-WAN Manager, on page 24.

  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 templates

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.
- For restrictions that apply to Cisco SD-WAN Controllers, see Restrictions for Multi-Region Fabric, on page 13.

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 *Cisco Catalyst SD-WAN Policies Configuration Guide*.

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, on page 28.

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 *Cisco Catalyst SD-WAN Policies Configuration Guide*.

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 an 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, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*. 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 a 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, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*. 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 13.

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

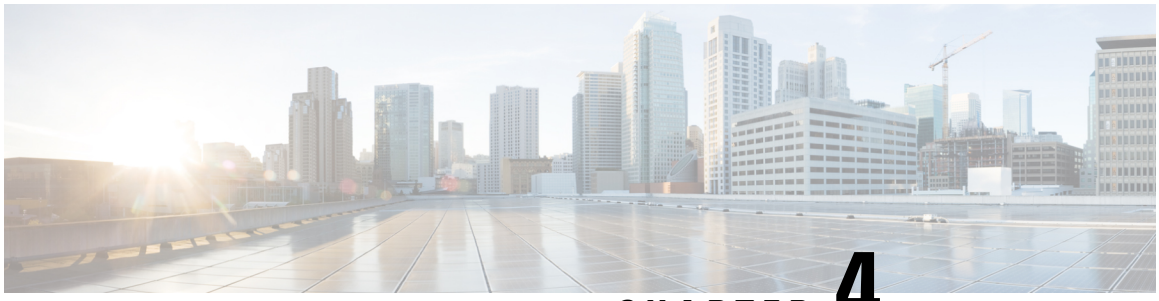
      STUN                                          PRF ID
------------------------------------------------------------------------------------------------------------
GigabitEthernet0/0/0     10.0.0.1    12366  10.0.0.1     ::       12366    1/1  public-internet  up
 2     yes/yes/no   No/No  0:00:00:04   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.



CHAPTER 4

Migrating to Multi-Region Fabric

- Migrating to Multi-Region Fabric, on page 35
- Information About Migrating to Multi-Region Fabric, on page 36
- Supported Devices for Migrating to Multi-Region Fabric, on page 37
- Prerequisites for Migrating to Multi-Region Fabric, on page 37
- Use Cases for Migrating to Multi-Region Fabric, on page 38
- Migrate to Multi-Region Fabric Using Cisco SD-WAN Manager, on page 54
- Migrate a BGP-Based Hierarchical Core Network to Multi-Region Fabric, on page 56
- Enable or Disable Migration Mode Using the CLI, on page 59
- Enable or Disable Migration Mode in a BGP-Based Network Using the CLI, on page 59
- Verification Procedures for Migration to Multi-Region Fabric, on page 60

Migrating to Multi-Region Fabric

Table 5: 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.

Feature Name	Release Information	Description
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 38.

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, refer to the *Cisco Catalyst SD-WAN Network Hierarchy Configuration Guide*.
- 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

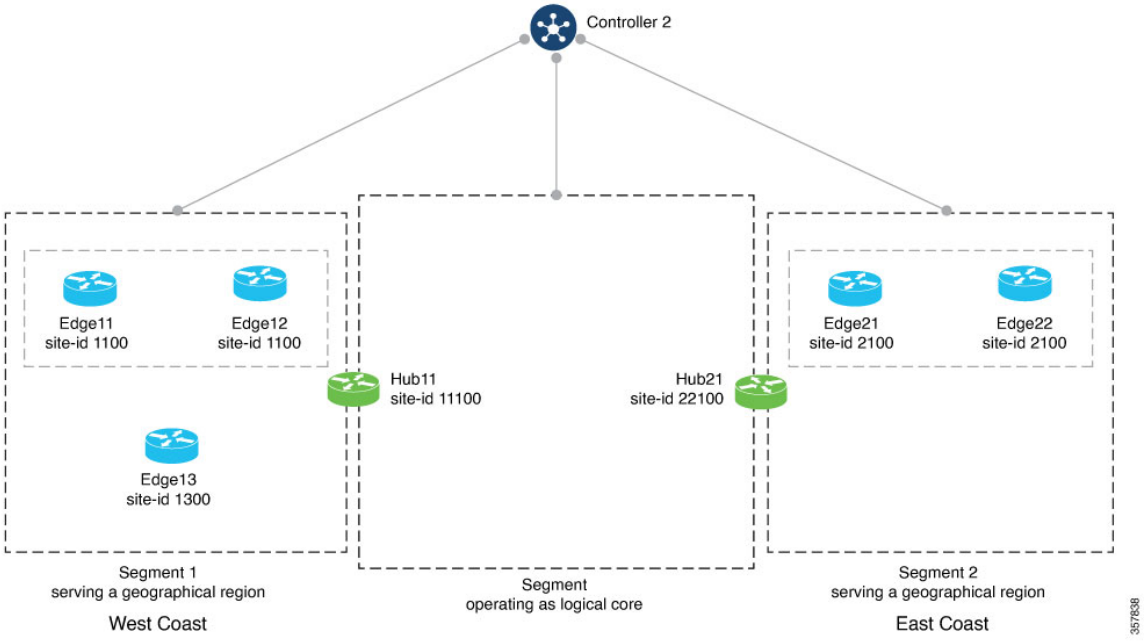
The following example provides insight into the steps for planning and executing a migration to a Multi-Region Fabric architecture. For simplification, this example includes only a small total number of routers in the organization's network, and before migration uses a single Cisco SD-WAN Controller.

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 5: 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.

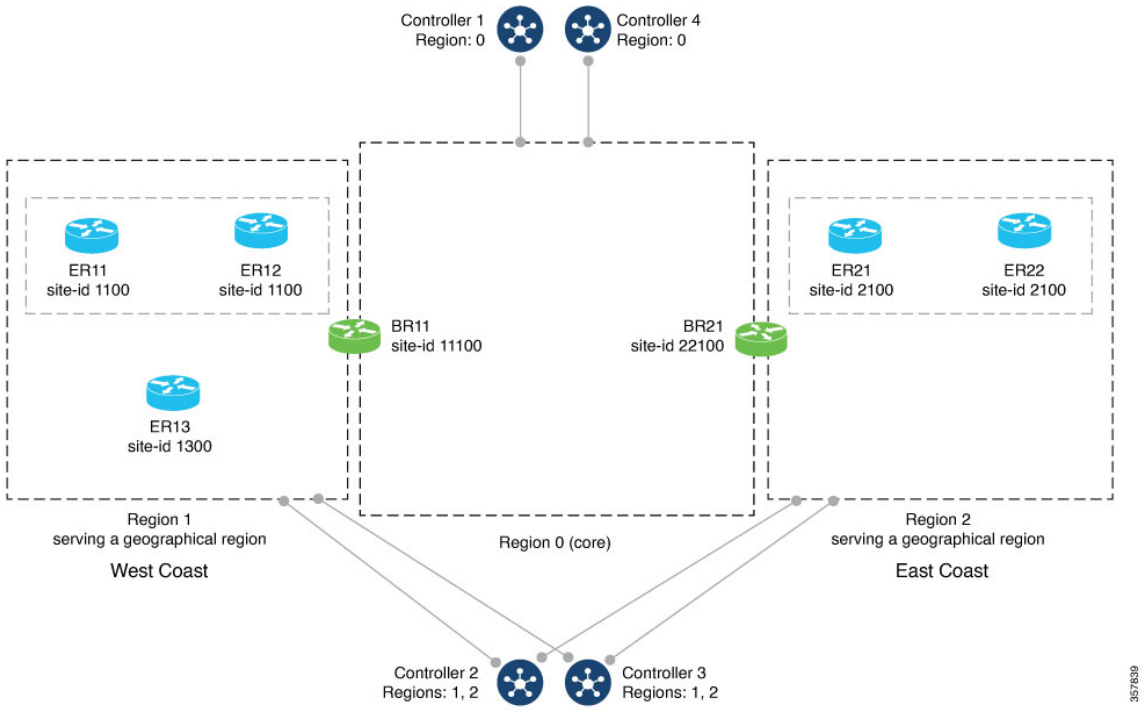
  These include Hub11 and Hub21.

- 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 54) to migrate each router.

The following illustration shows the network after migration.

Figure 6: 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

Geographical Region	Site	Device Name and Description Before Migration	Device Name and Description After Migration to Multi-Region Fabric
West Coast	11100	Hub11: Hub router	BR11: Border router, Region 1
East Coast	22100	Hub21: Hub	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-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 6: 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 7: 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 8: 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

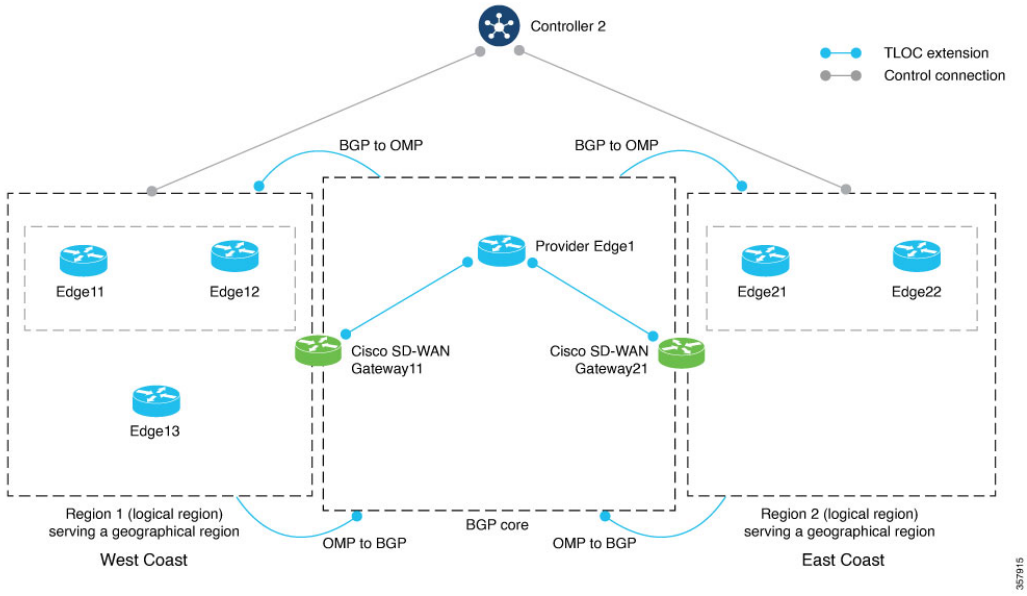
The following example provides insight into the steps for planning and executing the migration of a BGP-based hierarchical core network to a Multi-Region Fabric architecture. For simplification, this example includes only a small total number of routers in the organization's network, and before migration 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 7: BGP-Based Network Architecture Before Migration



In this example:

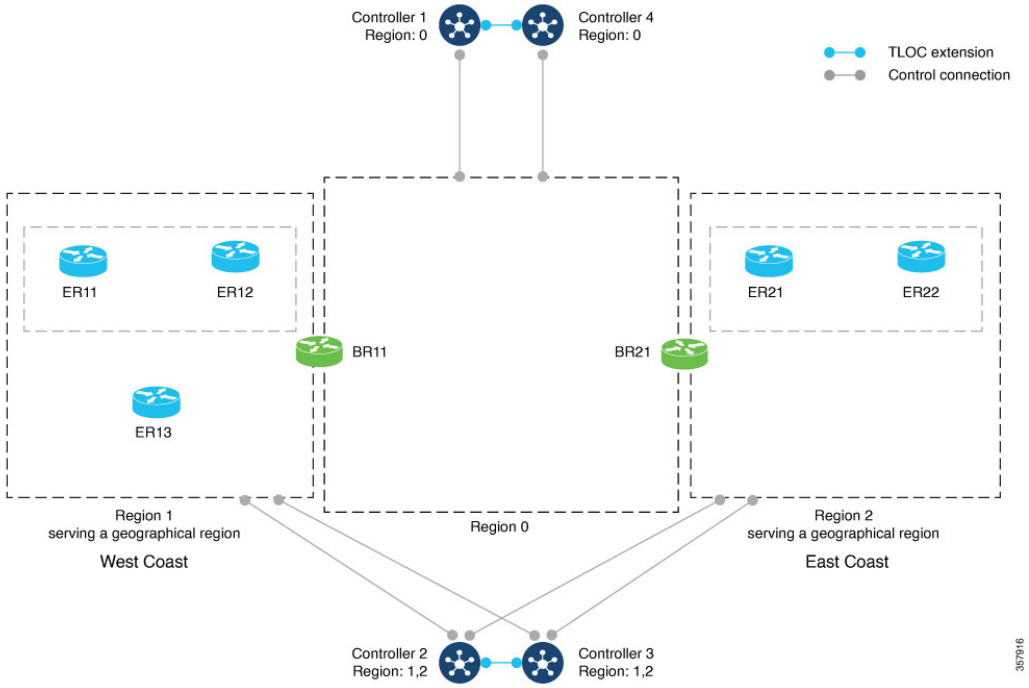
- Cisco SD-WAN Controller 2 serves logical regions 1 and 2.
- The West Coast geographical region has three devices—Edge11, Edge12, and Edge13.
- The East Coast geographical region has two devices—Edge21 and Edge22.
- Cisco Catalyst SD-WAN Gateway11 serves the West Coast geographical region and Cisco 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, on page 56 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 8: 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 9: 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 10: 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 11: 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.
   - 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 templates, on page 28.

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, on page 24 and Assign Border Router TLOCs to the Core Region Using Cisco SD-WAN Manager, on page 26.

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 60.

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, on page 24.

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 60.

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.
   - 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 templates, on page 28.
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 60.
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, on page 24.
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 60.
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, refer to the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

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).

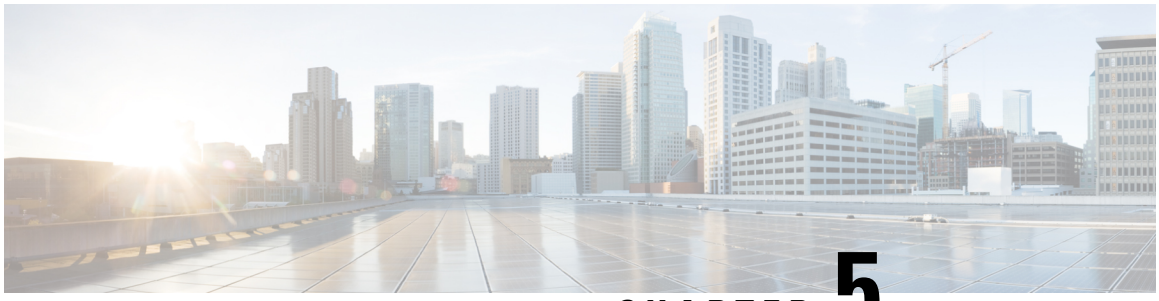
Example:

```
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
```



CHAPTER 5

Create Regions and Assign Controllers Workflow

Table 12: Feature History

Feature Name	Release Information	Description
Create Regions and Assign Controllers Workflow	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Cisco SD-WAN Manager introduces a fully guided workflow that allows you to create multiple regions within your Cisco Catalyst SD-WAN fabric and assign Cisco SD-WAN Controllers to them.

- Information about the Create WAN Regions and Assign Controllers Workflow, on page 63
- Prerequisites for the Create Regions and Assign Controllers Workflow, on page 64
- Restrictions for the Create Regions and Assign Controllers Workflow, on page 64
- Use Cases for the Create Regions and Assign Controllers Workflow, on page 64
- Create Regions and Assign Controllers Workflow, on page 64
- Verify Regions, on page 65

Information about the Create WAN Regions and Assign Controllers Workflow

Cisco SD-WAN Manager introduces a comprehensive fully guided workflow to create multiple WAN regions within your Cisco Catalyst SD-WAN fabric and assign Cisco SD-WAN Controllers to them. Before the introduction of the Create Regions and Assign Controllers workflow, you would have to create regions using a different page and assign Cisco SD-WAN Controllers using a different page. For more information about Network Hierarchy and Resource Management, refer to the *Cisco Catalyst SD-WAN Network Hierarchy Configuration Guide*. The Create Regions and Assign Controllers workflow makes it easier to complete the entire process of creating regions and assigning Cisco SD-WAN Controllers. Starting from Cisco Catalyst SD-WAN Manager Release 20.15.1, you can deploy policy groups and match TLOC conditions in a centralized policy to a particular region.

Prerequisites for the Create Regions and Assign Controllers Workflow

You can create a region only if you enable the **Multi-Region Fabric** option in Cisco SD-WAN Manager. Perform the following procedure to enable Multi-Region Fabric:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy** > **Multi Region Fabric (MRF)**.
2. Enable the **Multi-Region Fabric Routing** option.



Note MRF core routing can't be disabled once enabled. You can remove all the MRF related configuration manually.

Restrictions for the Create Regions and Assign Controllers Workflow

- A minimum of 2 Cisco SD-WAN Controllers must be available in the Cisco SD-WAN Manager and they need to be in the SD-WAN Manager mode.
- Manage Cisco SD-WAN Controllers using a device template, not a CLI template.
- The edge devices must run Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and later releases.

Use Cases for the Create Regions and Assign Controllers Workflow

- New or less experienced network administrators can quickly become proficient in managing the Cisco Catalyst SD-WAN network, as the guided workflow provides step-by-step instructions, reducing the learning curve and the potential for misconfiguration.
- As your business grow and you need to add new regions or branch offices to your network, the guided workflow allows for quick and error-free expansion.

Create Regions and Assign Controllers Workflow

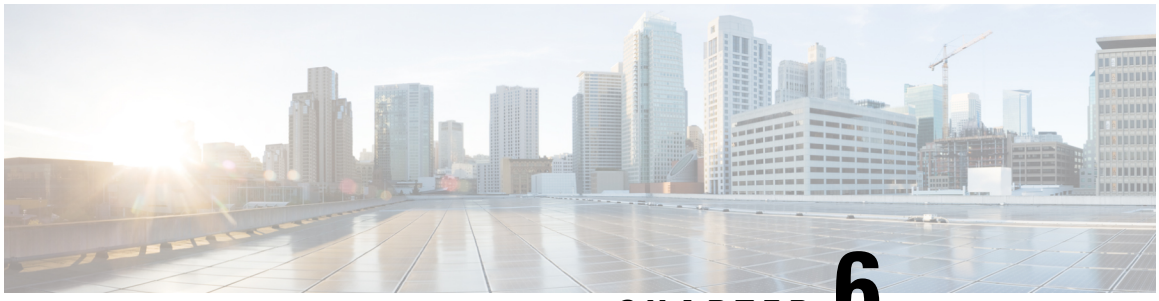
1. In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflows Library** > **Create regions and assign controllers**.
2. Follow the workflow instructions to create regions and assign Cisco SD-WAN Controllers.



Note Create a region ID in the Network Hierarchy page, before assigning a region to the controllers.

Verify Regions

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. View the regions in the left pane, under **Global**.



CHAPTER 6

Multi-Region Fabric Secondary Regions

- Multi-Region Fabric Secondary Regions, on page 67
- Information About Secondary Regions, on page 68
- Matching Routes by Path Type, Region, or Role, on page 71
- Restrictions for secondary regions, on page 72
- Use Cases for Secondary Regions, on page 72
- Configure a Secondary Region Using Cisco SD-WAN Manager, on page 74
- Configure a Secondary Region Using the CLI, on page 76
- Verify a Device Secondary Region Assignment Using Cisco SD-WAN Manager, on page 78
- Verify a Device Secondary Region Assignment Using the CLI, on page 78
- Verify an Interface Secondary Region Mode Using the CLI, on page 78
- Verify an Interface Secondary Region Assignment Using the CLI, on page 79

Multi-Region Fabric Secondary Regions

Note Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1 are the last releases to support these features:

- Secondary regions
- Subregions
- Management regions

From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1, configuration of secondary regions and subregions is possible only by API. Because later releases do not support these features, we advise you to update your network design and configuration to use alternative solutions where possible. Refer to End of support for three types of regions, on page 177.

Table 13: Feature History

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

Information About Secondary Regions

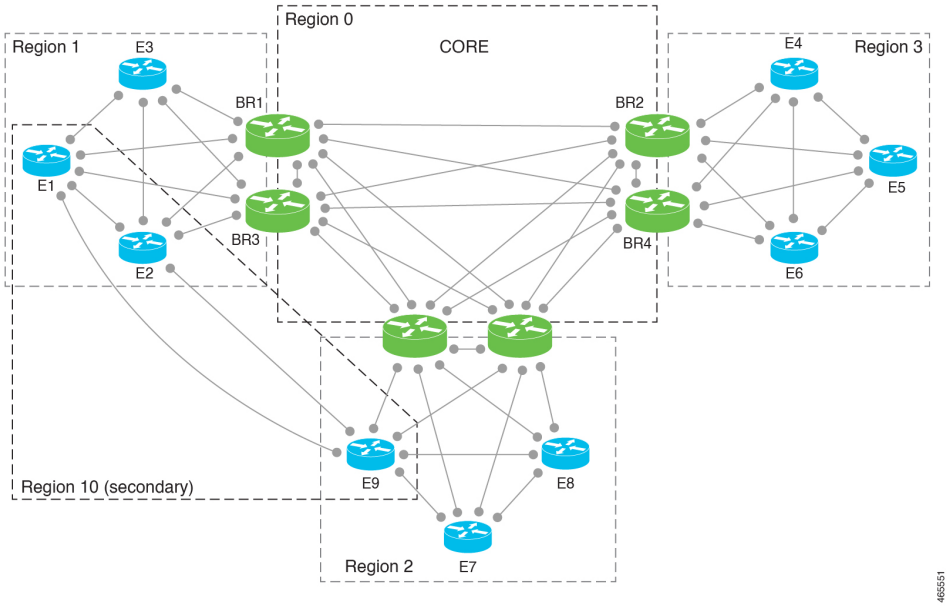
Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

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

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

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

Figure 9: Multi-Region Fabric with a Secondary Region



Using Secondary Regions

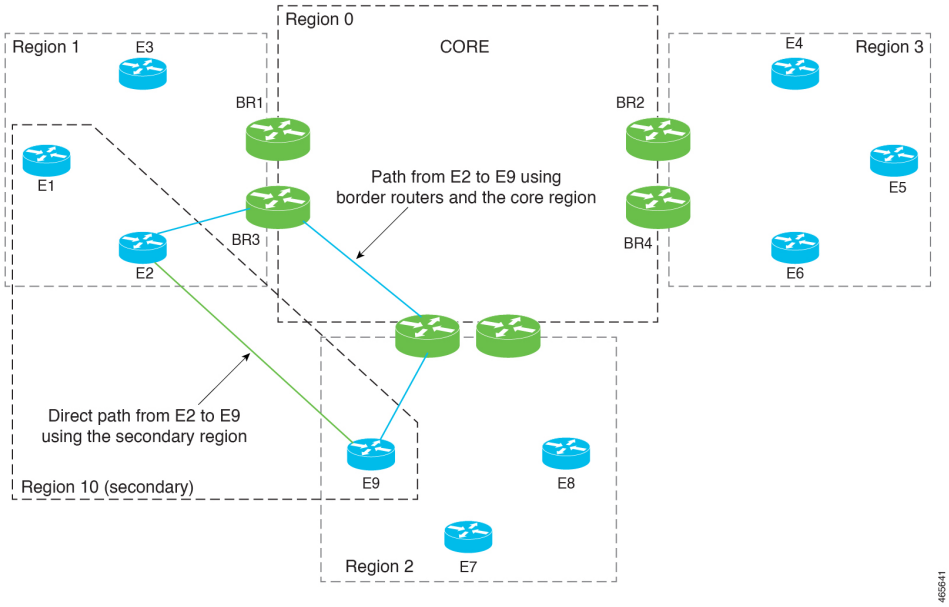
You can configure secondary region paths for any of the following:

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

Primary-Region Path and Secondary-Region Path

When a direct path is available to reach a destination, by default the overlay management protocol (OMP) enables only the direct path to the routing forwarding layer because the direct path uses fewer hops. The result is that the forwarding layer, which includes application-aware policy, can only use the direct path. You can disable this comparison of the number of hops so that traffic can use either the direct secondary-region path (fewer hops) or the primary-region path (more hops). When you disable the comparison of the number of hops, OMP applies equal-cost multi-path routing (ECMP) to all routes, and packets can use all available paths. See Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using Cisco SD-WAN Manager, on page 75.

Figure 10: Direct Path Using a Secondary Region and Multi-Hop Path Using Primary Regions and the Core Region



Control Policy

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

Workflow

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

   See Configure a Secondary Region ID for an Edge Router Using Cisco SD-WAN Manager, on page 74.

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

   See Configure the Secondary Region Mode of a TLOC Using the CLI, on page 76.

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

   See Configure the Secondary Region Mode for a TLOC Using Cisco SD-WAN Manager, on page 74.

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

   See Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using Cisco SD-WAN Manager, on page 75.

5. Assign a Cisco SD-WAN Controller to the secondary region. Use a Cisco SD-WAN Controller that does not operate in any of the access regions of devices using the secondary region. To ensure this, assign a Cisco SD-WAN Controller that operates only in a secondary region, and does not operate in any access regions. Or assign an Cisco SD-WAN Controller that operates in the core region (region 0) to operate also in a secondary region.

   See Assign regions to a Cisco Catalyst SD-WAN Controller using templates, on page 28.

Terminology

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

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

Benefits of Secondary Regions

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

Matching Routes by Path Type, Region, or Role

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

Path Type

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

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

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

- Direct path: Match direct paths (direct routes) from one edge router to another edge router. You can enable a direct path between edge routers in different access regions by configuring a secondary region, and adding the two edge routers to the secondary region. See Information About Secondary Regions, on page 68.

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

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

  For information about transport gateways, see Information About Transport Gateways, on page 91.

Region and Role

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

Restrictions for secondary regions

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

SD-WAN Controller for a secondary region

When assigning an SD-WAN Controller to a secondary region, do not assign an SD-WAN Controller that is also assigned to a primary access region of any device using the secondary region. To avoid this, apply this simple rule: Do not assign an SD-WAN Controller to a primary access region and to a secondary region.

Secondary regions apply to edge routers

Secondary regions apply only to edge routers, not border routers.

Router in only one secondary region

A router can belong to only one secondary region.

Router configured as a transport gateway

You cannot configure a secondary region on a router that is configured as a transport gateway.



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

Use Cases for Secondary Regions

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

Use Case 1: Specific Application Traffic

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

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

- Edge router ER10

  Primary region: 1
  Secondary region: 5

- Edge router ER20

  Primary region: 2
  Secondary region: 5

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

Use Case 2: High Volume Data Center

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

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

The primary and secondary region configuration is as follows:

- Data center: Edge router ER10

  Primary region: 1
  Secondary region: 5

- Remote site: Edge router ER20

  Primary region: 2
  Secondary region: 5

- Remote site: Edge router ER30

  Primary region: 3
  Secondary region: 5

- Remote site: Edge router ER40

  Primary region: 4
  Secondary region: 5

Configure a Secondary Region Using Cisco SD-WAN Manager

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

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

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

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

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

Before You Begin

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

Configure the Secondary Region Mode for a TLOC

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create a Cisco VPN Interface Ethernet template for the device.
   - In the table, locate the existing Cisco VPN Interface Ethernet template for the device. In the row for the template, click **…** and choose **Edit**.

4. Navigate to the **Tunnel** section, and within that section the **Advanced Options** section.
5. In the **Enable Secondary Region** field, enable Global mode and choose one of the following options:

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



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

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

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

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

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

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



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

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

Configure a Secondary Region Using the CLI

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

1. Enter configuration mode.

   ```
   Device#config-transaction
   ```

2. Enter system configuration mode.

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

3. Assign a region and secondary region.

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

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

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

Example

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

Configure the Secondary Region Mode of a TLOC Using the CLI

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

1. Enter configuration mode.

   ```
   Device#config-transaction
   ```

2. Enter VPN 0 configuration mode.

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

3. Specify an interface.

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

4. Enter tunnel interface configuration mode.

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

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

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

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

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

Example 1

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

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

Example 2

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

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

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

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

1. Enter configuration mode.

   ```
   Device#config-transaction
   ```

2. Enter OMP configuration mode.

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

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

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

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

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

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

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

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

Verify a Device Secondary Region Assignment Using the CLI

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

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

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

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

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

Verify an Interface Secondary Region Mode Using the CLI

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

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

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

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

The following example is for a Cisco vEdge device.

```
Device#show running-config vpn 0 interface ge0/1
vpn 0
 interface ge0/1
  ip address 173.3.1.11/24
  tunnel-interface
   encapsulation ipsec
   color 3g
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   region secondary-only
  !
  no shutdown
 !
!
```

Verify an Interface Secondary Region Assignment Using the CLI

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

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

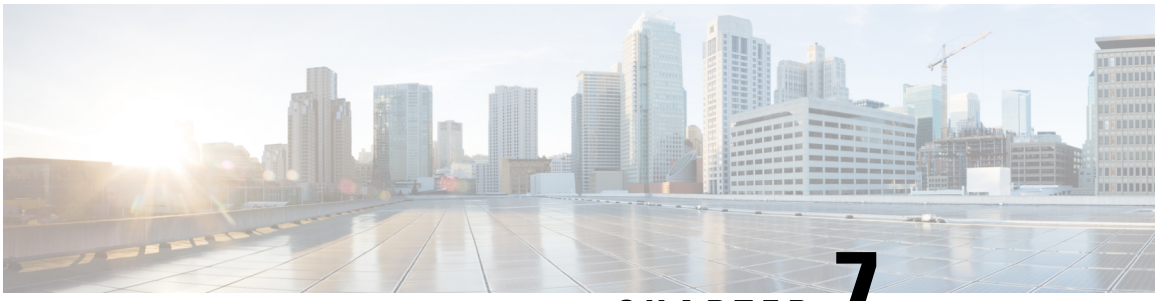
In the output of the **show sdwan control local-properties** command, for each interface, the **REG IDs** column shows the region assignment.

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

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

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

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



CHAPTER 7

Multi-Region Fabric Management Region

- Multi-Region Fabric Management Region, on page 81
- Information About Management Regions, on page 82
- Restrictions for Management Regions, on page 83
- Configure a Management Region, on page 83
- Verify the Management Region Configuration, on page 88

Multi-Region Fabric Management Region

Note Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1 are the last releases to support these features:

- Secondary regions
- Subregions
- Management regions

From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1, configuration of secondary regions and subregions is possible only by API. Because later releases do not support these features, we advise you to update your network design and configuration to use alternative solutions where possible. Refer to End of support for three types of regions, on page 177.

Table 14: Feature History

Feature Name	Release Information	Feature Description
Management Region	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco Catalyst SD-WAN Control Components Release 20.13.1	A management region is a specialized region that can span all access regions in a Multi-Region Fabric architecture. A management region enables hub-and-spoke connectivity between any router in the network and one or more management gateways. Connectivity between a router and a management gateway uses access region transport services. The connectivity does not use the core region transport service, even when the router and management gateway are in different access regions.

Information About Management Regions

Some organizations employ management gateways, which are devices that connect to all or a subset of the routers in a network, and provide a point of connectivity to another device or network. Management gateways carry only management traffic, not user data traffic.

Challenge

In a Multi-Region Fabric scenario, the separation of edge routers into separate access regions presents a connectivity challenge for management gateways. All edge routers in the network can, in fact, connect to a management gateway, regardless of its location. If the management gateway is within the same access region, then connectivity is simple within an access region, and if the management gateway is in a different access region, a router can reach it by connecting through the core region.

However, the transport service used for the core region may be a higher-cost premium service, employed to optimize network performance for performance-sensitive traffic. Traffic to the management gateway is not performance-sensitive, so it is helpful to be able to separate that management traffic from the core region pathways, and use a lower-cost transport service.

Management Region

To provide the routers in a Multi-Region Fabric network with connectivity to one or more management gateways, configure a management region. The management region provides an overlay that connects the various routers in the network to the management gateways. The connectivity between network routers and the management gateways follows a hub-and-spoke pattern, where each management gateway is a hub connecting to the various routers in the network as spokes. However, the management region overlay is separate from the access region overlay, so the use of hub-and-spoke connectivity within the management region has no bearing on the connectivity architecture of the rest of the network.

To use a management region, do the following:

- Designate one or more Cisco SD-WAN Controllers to manage the management region.

- On these Cisco SD-WAN Controllers, enable the management region.
- On the management gateways, configure the management region and a VRF for management region traffic, and enable the devices as management gateways.
- The management region uses a hidden region ID and does not consume a region ID from the user-configurable range (1 through 63).
- On each device that connects to the management gateway, configure the management region and the VRF used for management region traffic.

Benefits of Management Regions

A management region provides easily configured hub-and-spoke connectivity between network routers and one or more management gateways, without requiring use of the core region.

Restrictions for Management Regions

- A Cisco SD-WAN Controller that is managing an access region cannot also manage the management region. We recommend dedicating one or more Cisco SD-WAN Controllers to exclusively manage the management region. Alternatively, you can use one or more Cisco SD-WAN Controllers that are managing the core region.
- You cannot configure a router to serve as a management gateway and also a transport gateway simultaneously.
- Use the same VRF for the management region across all the devices, including the management gateways. This ensures that all management region traffic uses the same VRF, as required.

Configure a Management Region

Use the following workflow to configure a management region. The steps include links to the relevant procedures.

1. As a planning step, designate one or more Cisco SD-WAN Controllers to manage the management region.



Note We recommend dedicating one or more Cisco SD-WAN Controllers to exclusively manage the management region. As noted in Restrictions for Management Regions, you can use one or more Cisco SD-WAN Controllers that are managing the core region. A Cisco SD-WAN Controller that is managing an access region cannot also manage the management region.

2. On the designated Cisco SD-WAN Controllers, enable the management region:

   Configure a Cisco SD-WAN Controller to Support a Management Region, Using CLI Commands, on page 84

3. On each of the one or more management gateways, configure the management region, and assign a single VRF to use, using one of the following procedures:

Enable the Management Region for a Management Gateway, Using a Configuration Group, on page 85
Enable the Management Region for a Management Gateway, Using CLI Commands, on page 85

4. On each device that connects to the management gateway, configure the management region, using one of the following procedures. In case there are multiple management gateways, you can configure an order of preference among them.

Configure a Router to Support a Management Region, Using a Configuration Group, on page 87
Configure a Router to Support a Management Region, Using CLI Commands, on page 88

Configure a Cisco SD-WAN Controller to Support a Management Region, Using CLI Commands

Configure a Cisco SD-WAN Controller to support a management region, using a CLI Profile in a configuration group or using a CLI template:

- For information about using the CLI Profile, see CLI Profile.
- For information about using CLI templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.

1. Enter system configuration mode.

   system

2. Enable support for a management region.

   management-region

Example 1

The following sample configuration configures a Cisco SD-WAN Controller that is dedicated to managing the management region. Note that the example does not include configuration of a core region (region 0).

```
system
  host-name controller01
  system-ip 10.100.1.1
  site-id 100
  management-region
  no daemon-restart
  admin-tech-on-failure
  !
```

Example 2

The following sample configuration configures a Cisco SD-WAN Controller that is managing the core region, to also support a management region.

```
system
  host-name controller01
  system-ip 10.100.1.1
  site-id 100
  region 0
  management-region
  no daemon-restart
```

```
admin-tech-on-failure
!
```

Enable the Management Region for a Management Gateway, Using a Configuration Group

Before You Begin

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

Configure a Router to Support a Management Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group for a Cisco IOS XE Catalyst SD-WAN device and choose **Edit**.
3. Open the **System Profile** section and add or edit the **Multi Region Fabric** feature.
4. In the **Advanced** section, do the following:
   a. For the **Management Region** field, choose **Global** and enable the management region.
   b. For the **Enable as Management Gateway** field, choose **Global** and enable the device as a management gateway.
   c. For the **Management VPN** field, choose **Global** and enter a VRF to use for the management region traffic.

Note Configure the same VRF number on the management gateway and on the routers in the network that communicate with the management gateway. This ensures that all management region traffic uses the same VRF, as required.

5. Click **Save**.

Enable the Management Region for a Management Gateway, Using CLI Commands

Enable the management region for a management gateway, using a CLI Profile in a configuration group or using a CLI template:

- For information about using the CLI Profile, refer to CLI Profile.
- For information about using CLI templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.

1. Enter system configuration mode.

```
system
```

2. Enter the access region ID in which the management gateway is located.

   ```
   region region-id
   ```

3. Configure the region as a management region and configure the VRF to use exclusively for management region traffic.

   Configure the same VRF number on the management gateway and on the routers in the network. Use this VRF only for management region traffic, not for any other network traffic.



Note After you enable the use of a management region with a specific VRF, OMP sends only the management VRF routes into the management region; it does not send routes of other VRFs to the management region.

```
management-region
vrf vrf-id
```

4. Enable the management-gateway functionality for the router.

   ```
   management-gateway enable
   ```

Example 1

The following sample configuration enables the management region for a management gateway, configures access region 5 (meaning that the device is located in access region 5), and designates VRF 3 for the management traffic.

Configuring an affinity group number is optional, but when you are configuring a router in the network, you can configure a preference order among multiple management gateways, according to their affinity group numbers. This configuration assigns a system-level affinity group number of 1.

```
system
  system-ip 10.1.1.1
  domain-id 1
  site-id 100
  region 5
    management-region
      vrf 3
      !
    !
  !
management-gateway enable
affinity-group affinity-group-number 1
```

Example 2

The following sample configuration enables the management region for a management gateway, configures access region 5 (meaning that the device is located in access region 5), and designates VRF 3 for the management traffic.

Configuring an affinity group number is optional, but when you are configuring a router in the network, you can configure a preference order among multiple management gateways, according to their affinity group numbers. This configuration assigns a system-level affinity group number of 1, and an affinity group number of 2 specifically for VRF 3 traffic.

```
system
  system-ip 10.1.1.1
```

```
  domain-id 1
  site-id 100
  region 5
    management-region
      vrf 3
      !
    !
  !
management-gateway enable
affinity-group affinity-group-number 1
affinity-per-vrf 2
  vrf-range 3
```

Configure a Router to Support a Management Region, Using a Configuration Group

Before You Begin

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

Configure a Router to Support a Management Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group for a Cisco IOS XE Catalyst SD-WAN device and choose **Edit**.
3. In the **System Profile** add or edit the **Multi Region Fabric** feature.
4. In the **Advanced** section, do the following:
   a. For the **Management Region** field, choose **Global** and enable the management region.
   b. For the **Management VPN** field, choose **Global** and enter a VRF to use for the management region traffic.

Note Configure the same VRF number on the management gateway and on the routers in the network that communicate with the management gateway.

Note You can also choose **Device Specific** and provide a variable to define at the time of deployment.

5. (Optional) Enter affinity group numbers, separated by commas with no spaces, to configure a preference order among management gateways, according to the affinity group number of the management gateways.

   Maximum number of preference numbers: 12

Note To enable use of a preference order, configure an affinity group number on each management gateway.

6. Click **Save**.

Configure a Router to Support a Management Region, Using CLI Commands

Configure a router to support a management region, using a CLI Profile in a configuration group or using a CLI template:

- For information about using the CLI Profile, refer to CLI Profile.
- For information about using CLI templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.

1. Enter system configuration mode.

   ```
   system
   ```

2. Enter the access region number of the region where the device is located.

   ```
   region region-id
   ```

3. Configure the region as a management region and configure the VRF to use for management region traffic. Configure the same VRF number on the management gateway and on the routers in the network.

   ```
   management-region
   vrf vrf-id
   ```

Example

The following sample configuration configures a border router to use the management region, using VRF 3 for management traffic.

```
system
  system-ip 10.1.1.2
  domain-id 1
  site-id 100
  region 1
    management-region
      vrf 3
      !
    !
  !
role border-router
```

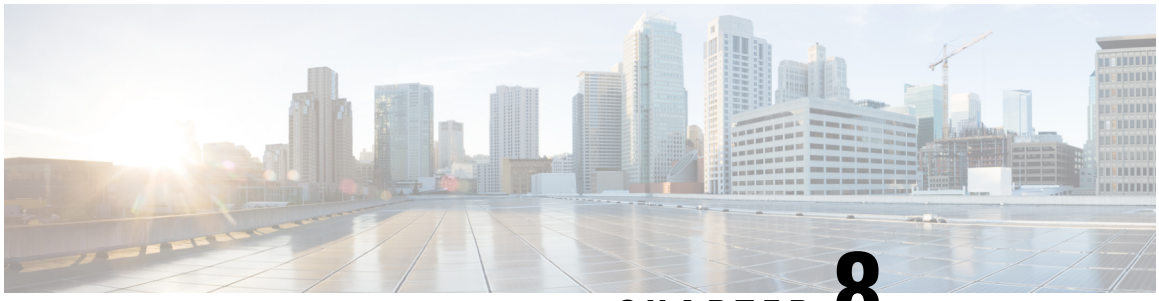
Verify the Management Region Configuration

Use the **show sdwan omp summary** command to view the details of the management region configuration.

Example

```
Device#show sdwan omp summary
…
```

```
region-id                       1,0,Mgmt
management-gateway              disabled
management-region               enabled
management-region-vpn           3
management-gateway-preference   52
```



CHAPTER 8

Transport Gateways

- Transport Gateways, on page 91
- Information About Transport Gateways, on page 91
- Supported Devices for Transport Gateways, on page 94
- Restrictions for Transport Gateways, on page 94
- Configure Transport Gateways Using Cisco SD-WAN Manager, on page 95
- Configure Transport Gateways Using the CLI, on page 96
- Verify a Transport Gateway Configuration Using the CLI, on page 98

Transport Gateways

Table 15: Feature History

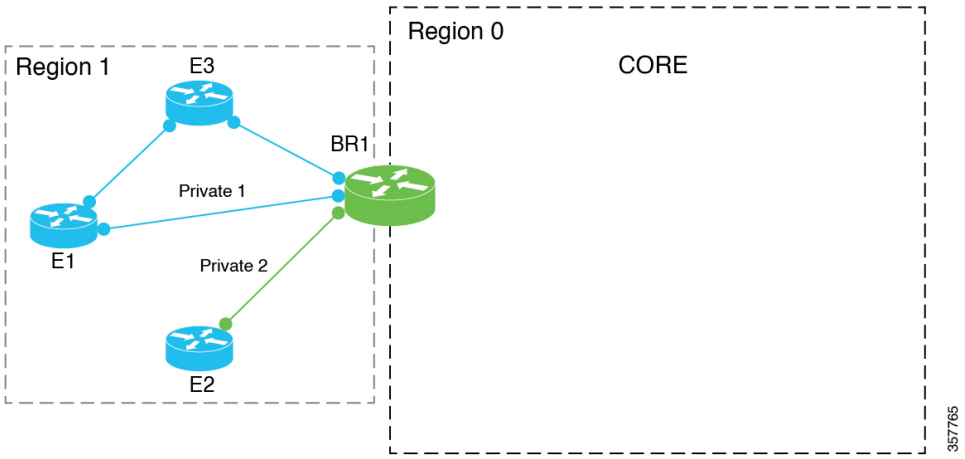
Feature Name	Release Information	Description
Multi-Region Fabric: Transport Gateways	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	An edge router or border router that has connections to two networks that lack direct connectivity can function as a transport gateway. This is helpful for enabling connectivity between routers that are configured to be within the same access region, but which do not have direct connectivity.

Information About Transport Gateways

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

Various devices assigned to the same access region may operate in networks that lack direct connectivity—so-called disjoint networks. If there is an edge router or a border router that operates in the same access region, and has connections to the two disjoint networks, you can configure that router to function as a transport gateway. As a transport gateway, the router provides connectivity to the edge routers in the disjoint networks.

Figure 11: Border Router Functioning as a Transport Gateway for Edge Routers that Lack Direct Connectivity



The Problem That Transport Gateways Address

Without transport gateway functionality, one method for enabling traffic between devices that lack direct connectivity is to create a control policy that routes traffic between the devices in disjoint networks using an intermediate device that has connectivity to both networks, and configuring specific routes.

There are problems with this approach:

- Complexity: Configuring a control policy to advertise prefixes is complicated.
- Potential traffic black hole: The control policy cannot detect whether a device or a configured route is unavailable. This can lead to packet loss if a route becomes unavailable.

Routing Mechanism

When a router is configured to function as a transport gateway, it does the following for each route between devices within its primary region.

1. Installs each route that it learns from the Cisco SD-WAN Controllers for the access region.
2. Re-originates each route that it learns from the Cisco SD-WAN Controllers, substituting its own TLOCs as the next hop for the routes. This means that it substitutes its TLOCs as the next hop for each route and advertises the route to the Cisco SD-WAN Controllers for its region.

Note Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, routes that are reoriginated from a site through the transport gateway are filtered out by the Cisco Catalyst SD-WAN Controller. These reoriginated routes are not sent back to the originating site or the sites which share same site ID as the originating site. The reoriginated routes are only distributed to different sites within the Cisco Catalyst SD-WAN network.

This change in routing mechanism is also backported to Cisco Catalyst SD-WAN Manager Release 20.15.2, and Cisco Catalyst SD-WAN Manager Release 20.12.5.

Note that this process does not re-originate primary region routes into the core region, or core region routes into an access region.

The effect of configuring a router as a transport gateway is that it can provide routes for all intra-region traffic. A device in the network uses the transport gateway route only if it lacks a direct route to the destination.

Primary Region Only

If you configure an edge router to act as a transport gateway, the edge router re-originates only routes in a primary access region. For information about primary and secondary regions, see Information About Secondary Regions, on page 68.

If you configure a border router to act as a transport gateway, it re-originates only routes in the access region, not the core region.

Preference for a Transport Gateway Route

After configuring a transport gateway, there may be multiple paths available between two routers in an access region. When multiple paths are available between two routers, the overlay management protocol (OMP) applies best path selection logic to choose the best path. The best path selection logic is biased toward paths with the smallest number of hops, which may possibly exclude the transport gateway path. OMP best path selection logic includes the following:

- By default, OMP selects a direct path if one is available.
- If no direct path is available, OMP selects a path with more hops, such as through a transport gateway.

You can configure the OMP logic as follows:

- Prefer a transport gateway path over a direct path.
- Consider direct paths and transport gateway paths as equal.

See Configure the Transport Gateway Path Preference Using Cisco SD-WAN Manager, on page 96.

Multiple Transport Gateways

If there are multiple transport gateways active in a region, then a device applies equal-cost multi-path routing (ECMP) across all of the available transport gateways.

Benefits of Transport Gateways

Advantages of Using Transport Gateways

- Enables easier configuration than the control policy method.
- If a route becomes unavailable, the transport gateway withdraws the route to the edge router and stops re-originating the paths to it, preventing networking black holes.

Traffic Protocols

Transport gateway routers can handle IPv4 and IPv6 traffic.

Supported Devices for Transport Gateways

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

- Transport gateway functionality: Cisco IOS XE Catalyst SD-WAN devices only
- Ability to use transport gateway paths: Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices

Restrictions for Transport Gateways

Restrictions from Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1

- Cloud onRamp for SaaS routes

  Does not affect Cloud onRamp for SaaS routes.

- Secondary regions

  Transport gateway functionality is not supported on routers that have a secondary region configured.



Note Attempting to configure transport gateway functionality on such a router results in an error.

- Multiple devices within the same region

  If you enable transport gateway functionality on multiple devices within the same region, providing more than one transport gateway path between edge routers in disjoint networks, the edge routers apply best path selection logic to determine the best path.

  If there are multiple transport gateways and OMP selected transport gateway paths, then it applies ECMP to all available transport gateway paths.

  By default, OMP selects a direct path if one is available, and if not, selects a path with more hops, such as through a transport gateway, if available. However, you can configure the OMP logic differently. Refer to Information About Transport Gateways, on page 91.

- Not advertising a transport gateway route to another transport gateway

  If you enable transport gateway functionality on multiple devices within the same region, the Cisco SD-WAN Controller for the region ensures that a route that is re-originated by one transport gateway is not advertised to another transport gateway. By preventing the advertising of a transport gateway route to another transport gateway, the Cisco SD-WAN Controller helps to prevent any potential routing loops.

- Resource demands

  Due to the resource demands of transport gateway functionality, we recommend enabling this only on a high-performance device with CPU and memory resources to handle the additional load. The specific resource requirements depend on your networking environment.

- Dynamic on-demand tunnels

You cannot configure dynamic on-demand tunnels for a device configured as a transport gateway. This restriction applies in MRF- and non-MRF architectures. For information about dynamic on-demand tunnels, refer to Dynamic On-Demand Tunnels in the *Cisco Catalyst SD-WAN Network Configuration Guide*.

- Edge router and a border router in the same region

  Do not configure both an edge router and a border router in the same region as transport gateways.

- Border router requirement

  For a network using Multi-Region Fabric, Cisco IOS XE Catalyst SD-WAN Release 17.15.x and Cisco Catalyst SD-WAN Control Components Release 20.15.x are the last releases to support configuring non-border-routers as transport gateways. From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Control Components Release 20.16.1, in such a network, only configure border routers as transport gateways. Do not configure other types of routers as transport gateways.

  If you're not using Multi-Region Fabric, you can still configure the transport gateway independently. The border router concept does not apply to a flat design (non-Multi-Region Fabric). For example, you may need to enable the transport gateway for the purpose of intent-based hub and spoke configuration.

Restrictions from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Control Components Release 20.16.1

Border router requirement

For a network using Multi-Region Fabric, Cisco IOS XE Catalyst SD-WAN Release 17.15.x and Cisco Catalyst SD-WAN Control Components Release 20.15.x are the last releases to support configuring non-border-routers as transport gateways. From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Control Components Release 20.16.1, in such a network, only configure border routers as transport gateways. Do not configure other types of routers as transport gateways.

Configure Transport Gateways Using Cisco SD-WAN Manager

Enable Transport Gateway Functionality on a Router Using Cisco SD-WAN Manager

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create a system template for the device.
   - In the table, locate the existing system template for the device. In the row for the template, click **…** and choose **Edit**.
4. In the **Basic Configuration** section, in the **Transport Gateway** field, choose **On**.

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

Configure the Transport Gateway Path Preference Using Cisco SD-WAN Manager

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create an OMP template for the device.
   - In the table, locate the existing OMP template for the device. In the row for the template, click **…** and choose **Edit**.
4. In the **Best Path** section, in the **Transport Gateway Path Behavior** field, choose Global mode and choose one of the following options:

Option	Description
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.
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.

5. (Optional) From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, you can click the **Site Types** field and choose one or more site types to which to apply the transport gateway behavior. For information about how the Site Types parameter operates together with the Transport Gateway Path Behavior parameter, refer to the section about OMP best path logic and transport gateway path preference in the *Cisco Catalyst SD-WAN Routing Configuration Guide*.
6. Click **Save** if creating a new template, or **Update** if editing an existing template.

Configure Transport Gateways Using the CLI

Enable Transport Gateway Functionality on a Router Using a CLI Template

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

Do the following on a device to configure it as a transport gateway:

1. Enter system configuration mode.

```
system
```

2. Enable transport gateway functionality.

```
transport-gateway enable
```



Note To disable transport gateway functionality, use the **no** form of the command.

Example

```
system
  transport-gateway enable
```

Configure the Transport Gateway Path Preference Using a CLI Template

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

Do the following on a device to configure it to use a transport gateway:

1. Enter sdwan configuration mode.

```
sdwan
```

2. Enter system OMP configuration mode.

```
omp
```

3. Configure the transport gateway path preference, using one of the following options:

```
best-path transport-gateway {prefer | ecmp-with-direct-path}
```

Option	Description
ecmp-with-direct path	For devices that can connect through a transport gateway and through direct paths, apply equal-cost multi-path (ECMP) to all available paths.
prefer	For devices that can connect through a transport gateway, use only the transport gateway paths, even if other paths are available.

4. Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, you can specify which types of traffic use a transport gateway route. Other types of traffic do not use a transport gateway.

```
omp best-path transport-gateway-settings site-types site-types
```

Option	Description
site-types	Include one or more of the following site types, separated by spaces: **cloud**, **branch**, **br**, **type-1**, **type-2**, **type-3**



Note To use this command, ensure that you use **omp best-path transport-gateway prefer** in the previous step.

Example

The following example configures a device to prefer transport gateway routes.

```
sdwan
omp
  omp best-path transport-gateway prefer
```

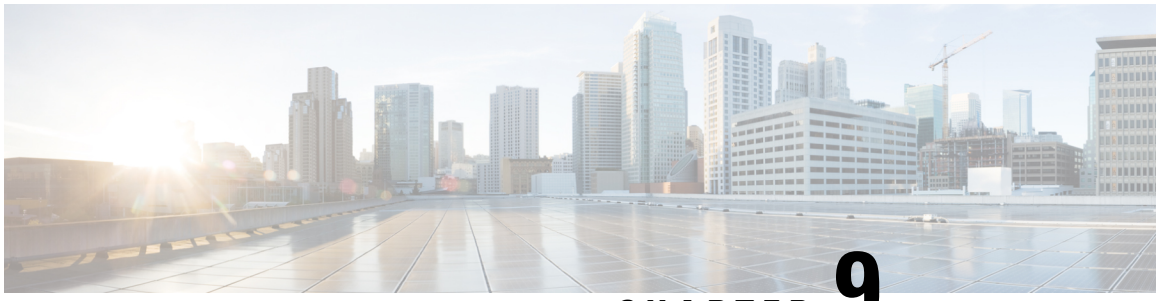
Verify a Transport Gateway Configuration Using the CLI

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

Use the **show sdwan running-config system** command on a device to check whether it is configured as a transport gateway. In the output, **transport-gateway enable** indicates that it is configured.

```
Device#show sdwan running-config system
system
system-ip             192.168.1.1
domain-id             1
site-id               11100
region 1
!
role                  border-router
transport-gateway enable
...
```

You can also use the **show sdwan omp summary** command on a device to check whether it is configured as a transport gateway. In the output, **transport-gateway enabled** indicates that transport gateway functionality is enabled.



CHAPTER 9

Router Affinity

- Router Affinity, on page 99
- Information About Router Affinity Groups, on page 100
- Information About Setting an Affinity Group by Control Policy, on page 104
- Information About Support for Affinity Groups with Service Routes and TLOC Routes, on page 105
- Supported Devices for Router Affinity Groups, on page 108
- Supported Platforms for Setting an Affinity Group by Control Policy, on page 108
- Supported Devices for Support for Affinity Groups with Service Routes and TLOC Routes, on page 108
- Prerequisites for Support for Affinity Groups with Service Routes and TLOC Routes, on page 108
- Restrictions for Router Affinity Groups, on page 109
- Use Cases for Router Affinity Groups, on page 109
- Use Cases for Setting an Affinity Group by Control Policy, on page 111
- Use Cases Support for Affinity Groups with Service Routes and TLOC Routes, on page 113
- Configure Router Affinity Groups Using Cisco SD-WAN Manager, on page 116
- Configure Router Affinity Groups Using the CLI, on page 118
- Configure Affinity Group by Control Policy Using a CLI Template, on page 120
- Verify an Affinity Group and Affinity Group Preference Using Cisco SD-WAN Manager, on page 122
- Verify the Affinity Group and Affinity Group Preference Using the CLI, on page 122

Router Affinity

Table 16: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric: Router Affinity	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	Often a router has multiple options to choose for the next hop when routing a flow to its destination. When multiple devices can serve as the next hop for a flow, you can specify the order of preference among the devices by configuring router affinity groups. The result is that a router attempts to use a route to the next-hop device of highest preference first, and if that device is not available, it attempts to use a route to the next-hop device of the next lower preference. Affinity groups enable this functionality without requiring complex control policies.

Feature Name	Release Information	Description
Improved Prioritization of Routes to Peer Devices in the Affinity Group Preference List	Cisco Catalyst SD-WAN Control Components Release 20.9.1	This feature introduces a change to the order in which Cisco SD-WAN Controllers advertise routes to devices. From this release, when Cisco SD-WAN Controllers advertise routes to a device, they (a) give higher priority to routes to peer devices in the affinity group preference list, and (b) lower priority to routes that may have a higher best path score, but are not routes to a device associated with a preferred affinity group. The effect is to prioritize routes to peer devices in preferred affinity groups.
Support for Affinity Groups for Service Routes and TLOC Routes	Cisco Catalyst SD-WAN Control Components Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This feature extends support of affinity group assignments to service routes and TLOC routes. A common use for this is to add further control to routing by using affinity group preference together with control policies that match service routes and TLOC routes.
Set Affinity Group by Control Policy	Cisco Catalyst SD-WAN Control Components Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	You can configure a control policy to match specific TLOCs or routes and assign them an affinity group value, overriding the affinity group that they inherit from the router.

Information About Router Affinity Groups

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

Router affinity groups enable you to specify the order of preference for choosing among multiple routers that can serve as the next transit hop for a network flow. This applies in circumstances in which (a) a router is determining its next hop for a flow, and (b) more than one router in the Multi-Region Fabric architecture can serve as the next hop. There are two aspects to configuring the functionality:

- On a router, assigning a router affinity group ID (a number from 1 to 63).
- On a router, assigning the order of preference for choosing the router for a next hop. This is a list of affinity group IDs.

When the overlay management protocol (OMP), operating on a router, chooses the best path for a flow, it does the following:

1. Determines the possible next-hop routers, based on which routers are advertising the prefix for the destination of the flow. (This is standard OMP functionality.)
2. From the possible next-hop routers, OMP considers the affinity group preferences when choosing the best path, prioritizing the possible next hop routers accordingly. (This is specific to affinity group functionality.)

The result is that a router first attempts to use a route to the next-hop device of highest preference, and if that device is not available, it attempts to use a route to the next-hop device of the next lower preference. If none of the devices on the affinity preference list are available, then the router attempts to use a route to any other device that can serve as the next hop. One effect of this is an automatic failover from one possible next hop router to a different next hop router if the first one is not available. Affinity groups enable this functionality without requiring complex control policies.

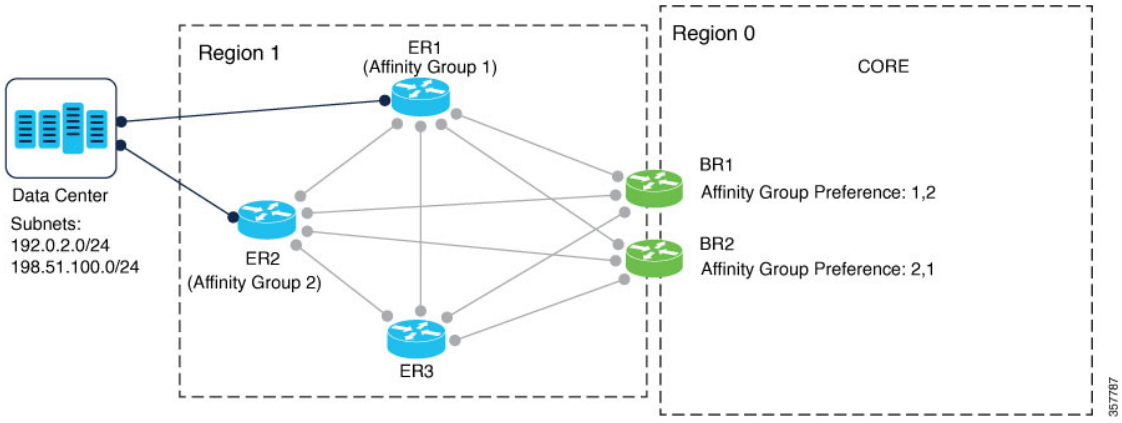
Routing Mechanism

Router affinity affects route selection as follows:

- Within a given network, or region in the case of Multi-Region Fabric, the overlay management protocol (OMP) manages the advertisement of prefixes by devices in the network.
- When a device routes a network flow to its destination, OMP enables the device to select a next-hop device that is advertising the prefix of the destination.
- Only devices that can serve as a next hop toward the prefix advertise the prefix.
- Among the possible next-hop devices, the configured affinity group preference determines the preference order for the next hop.

In the following example, edge routers ER1 and ER2 advertise the subnets used in the data center. If border router BR1 is routing a flow to a prefix in one of the data center subnets, it can use ER1 or ER2 as the next hop. Based on the affinity groups configured on ER1 and ER2, and based on the affinity group preference order configured on BR1, as shown in the illustration, BR1 chooses ER1 as the next hop. If ER1 is not available, then BR1 routes the flow to ER2 as the next hop.

Figure 12: Router Affinity Example



Filter Out Paths Configured with an Affinity Group Not in the Affinity Preference List

Optionally, you can configure Cisco Catalyst SD-WAN to enable routers to connect only to routers that are on their affinity list. To do this, use the **filter route outbound affinity-group preference** option on the Cisco SD-WAN Controllers that manage a region. The Cisco SD-WAN Controllers provide each device in the region with only the routes to routers in their affinity list, or routers that have no affinity group assignment. See Configure a Cisco SD-WAN Controller to Provide Only Paths in the Affinity Preference List, Using Cisco SD-WAN Manager, on page 117.

Use this option only when you are certain that you do not want a router to connect to any device that has an affinity group assignment that is not on its affinity list. The advantage is that managing fewer routes saves memory resources on the Cisco SD-WAN Controllers and on edge routers.

Prioritization of Routes to Peer Devices in the Affinity Group Preference List

From Cisco Catalyst SD-WAN Control Components Release 20.9.x, when Cisco SD-WAN Controllers advertise routes to a device, they give higher priority to advertising routes to peer devices in the affinity group preference list, and a lower priority to routes that may have a higher best path score, but which are not routes to a device associated with a preferred affinity group. This is especially important when a send path limit is configured for the Cisco SD-WAN Controller, limiting the number of routes advertised to any given device. It ensures that when a router is managing a limited number of routes, the routes include the peer devices on the affinity group preference list.

The following explains how this works in more detail:

For each affinity group, a Cisco SD-WAN Controller maintains link lists for each route advertised by devices in the network. For each defined affinity group, the Cisco SD-WAN Controller creates two link lists:

- List of routes that (a) are for devices in the affinity group, and (b) are chosen by the best path selection algorithm (meaning that they have a high best path score and are favored by the algorithm)
- List of routes that (a) are for devices in the affinity group, but (b) are not chosen by the best path selection algorithm

Note that the best path selection algorithm designates a route as chosen based on route characteristics, policy, and other factors.

When the Cisco SD-WAN Controller advertises routes to a particular device, it uses the link lists to favor routes to peer devices in the affinity group preference list of the device.

For example, for a network loosely matching the preceding illustration, but with more available routes, consider the following scenario:

Device	Devices Advertise Routes to the Cisco SD-WAN Controller	Results of Best Path Selection Algorithm	Resulting Link Lists
ER1, which is assigned to affinity group 1	ER1 has four routes, and it advertises them to the Cisco SD-WAN Controller as routes associated with affinity group 1.	In this example, the best path selection algorithm designates two of the routes as chosen and two as not chosen.	The Cisco SD-WAN Controller adds each of the routes to link lists: • Link list for affinity group 1, chosen routes: 2 routes • Link list for affinity group 1, not chosen routes: 2 routes **Note** "Chosen" means chosen by the best path selection algorithm, as described in the explanation that precedes this table.

Device	Devices Advertise Routes to the Cisco SD-WAN Controller	Results of Best Path Selection Algorithm	Resulting Link Lists
ER2, which is assigned to affinity group 2	ER2 has three routes, and it advertises them to the Cisco SD-WAN Controller as routes associated with affinity group 2.	In this example, the best path selection algorithm designates two of the routes as chosen and one as not chosen.	The Cisco SD-WAN Controller adds each of the routes to link lists: • Link list for affinity group 2, chosen routes: 2 routes • Link list for affinity group 2, not chosen routes: 1 route
ER3, which is not assigned to an affinity group	ER3 has three routes, and it advertises them to the Cisco SD-WAN Controller as routes associated with affinity group 0. (Affinity group 0 corresponds to devices that are not assigned to an affinity group.)	In this example, the best path selection algorithm designates two of the routes as chosen and one as not chosen.	The Cisco SD-WAN Controller adds each of the routes to link lists: • Link list for affinity group 0, chosen routes: 2 routes • Link list for affinity group 0, not chosen routes: 1 route

As shown in the illustration, device BR1 has an affinity group preference list of 1, 2. Given this, there are the following possibilities for advertising routes to BR1:

- No send path limit defined:

  If the Cisco SD-WAN Controller does not have a send path limit defined, it can advertise to BR1 all six routes in the link lists for chosen routes, as described in the table: two for ER1, two for ER2, and two for ER3.

- Send path limit defined:

  If the Cisco SD-WAN Controller has a send path limit of 4, it advertises to BR1 first the two routes in the link list for affinity group 1 chosen routes, for ER1. In addition, it advertises the two routes in the link list for affinity group 2 chosen routes, for ER2. At this point, it has advertised four routes, which is its limit, and it does not advertise the routes in the link list for chosen routes for affinity group 0 (devices not assigned to any affinity group). So no routes for ER3 are included. The result is that if BR1 has an affinity group preference list of 1, 2, the Cisco SD-WAN Controller favors providing it with routes to peer devices ER1 and ER2 (devices in affinity groups 1 and 2), even if the best path score for the ER3 routes was higher.

Workflow

- On a router, configure an affinity group ID number.

  See Configure an Affinity Group or Affinity Group Preference on a Device, Using Cisco SD-WAN Manager, on page 116.

- On a router, configure a list of affinity group ID numbers, in order of preference from highest to lowest, to specify the order of preference for connecting to routers.

  Configure an Affinity Group or Affinity Group Preference on a Device, Using Cisco SD-WAN Manager, on page 116.

- Optionally, on the Cisco SD-WAN Controllers serving an access region, restrict routers to connecting only to devices on their affinity group preference list.

  See Configure a Cisco SD-WAN Controller to Provide Only Paths in the Affinity Preference List, Using Cisco SD-WAN Manager, on page 117.

Benefits of Router Affinity Groups

Router affinity groups can help with capacity planning and load balancing by enabling you to preferentially direct traffic from a device to specific routers when more than one router is available for a next hop.

Information About Setting an Affinity Group by Control Policy

Minimum releases: Cisco Catalyst SD-WAN Control Components Release 20.11.1, Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

When you configure an affinity group for a router, each TLOC of the router inherits the affinity group. Routes that originate from the TLOCs also inherit the affinity group.

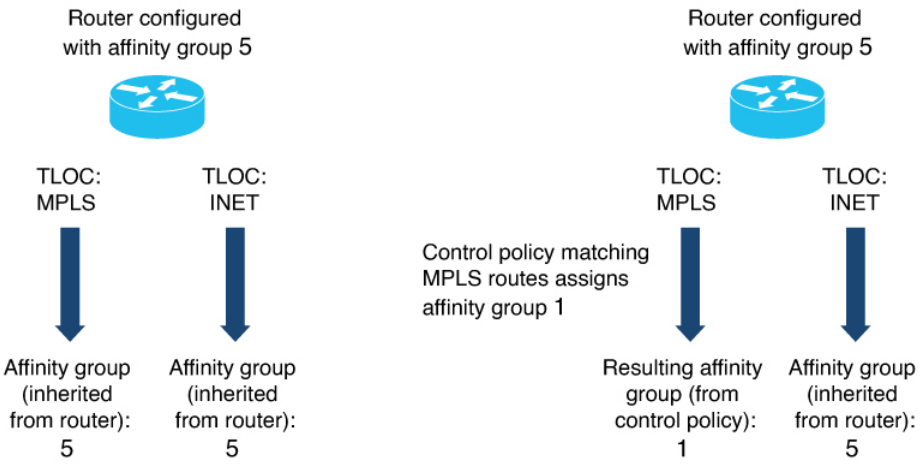
In addition to configuring the affinity at the router level, you can configure a control policy to match specific TLOCs or routes and assign them an affinity group value, overriding the affinity group that they inherit from the router.

Table 17: Methods for Configuring an Affinity Group

Affinity Configuration Method	Effect
Router affinity: Configure an affinity group at the router level.	The TLOCs on the router, and any routes that originate on the router have the configured affinity group. By default, routes from all TLOCs on the router inherit the same affinity group. For example, consider a router has two TLOCs, A and B, each using a different transport method. The routes from both of the TLOCs inherit the same affinity group from the router. This does not provide a way to configure a preference for TLOC A over TLOC B.
Control policy: Assign an affinity group to a TLOC or route.	A control policy can match TLOCs or routes, and assign them an affinity group. This overrides the affinity group that the TLOCs or routes inherit from the router. For example, you can match a TLOC using multiprotocol label switching (MPLS) and assign it a different affinity group than that of the router itself.

The following illustration shows how a TLOC can inherit its affinity group from a router or receive the affinity group from a control policy. The same affinity group applies to routes originating from the TLOC. The illustration shows that you can override the inherited affinity group of routes, to assign a specific affinity group to MPLS routes.

Figure 13: Affinity Group Configuration



Benefits of Setting an Affinity Group by Control Policy

Assigning affinity groups by control policy provides an additional layer of control of affinity group values for TLOCs and routes. This offers additional flexibility in controling routing.

Information About Support for Affinity Groups with Service Routes and TLOC Routes

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, Cisco Catalyst SD-WAN Control Components Release 20.11.1

Affinity groups provide additional control of routing traffic that has multiple possible destinations or intermediate hops. Affinity group preferences prioritize among the options for next hop. Multi-Region Fabric supports affinity groups for service routes and TLOC routes. Service routes and TLOC routes inherit the affinity group of the router they are associated with.

The addition of support for affinity groups in Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco Catalyst SD-WAN Control Components Release 20.11.1 does not change the process of configuring affinity groups or affinity group preference lists. For information about configuring these, see Configure Router Affinity Groups Using Cisco SD-WAN Manager, on page 116.

Behavior When Filtering by Affinity Group

When you configure Cisco SD-WAN Controllers to filter by affinity group, they provide each router with only the routes associated with an affinity group in the router's affinity group preference list, or with routes associated with no affinity group. For example, if router A has an affinity group preference list of 1, 2, then Cisco SD-WAN Controllers provide router A with the following:

- Routes, including service routes and TLOC routes, associated with a router with affinity groups 1 or 2
- Routes, including service routes and TLOC routes, associated with a router with no affinity group configured

In this case, Cisco SD-WAN Controllers do not provide router A with routes associated with affinity group 3.

A benefit of filtering out routes according to the preference list is that it reduces the demand on router and Cisco SD-WAN Controller resources.

For information about filtering by affinity group, refer to Configure a Cisco SD-WAN Controller to Provide Only Paths in the Affinity Preference List, Using Cisco SD-WAN Manager, on page 117.

Benefits of Support for Affinity Groups with Service Routes and TLOC Routes

Affinity Groups and Service Routes

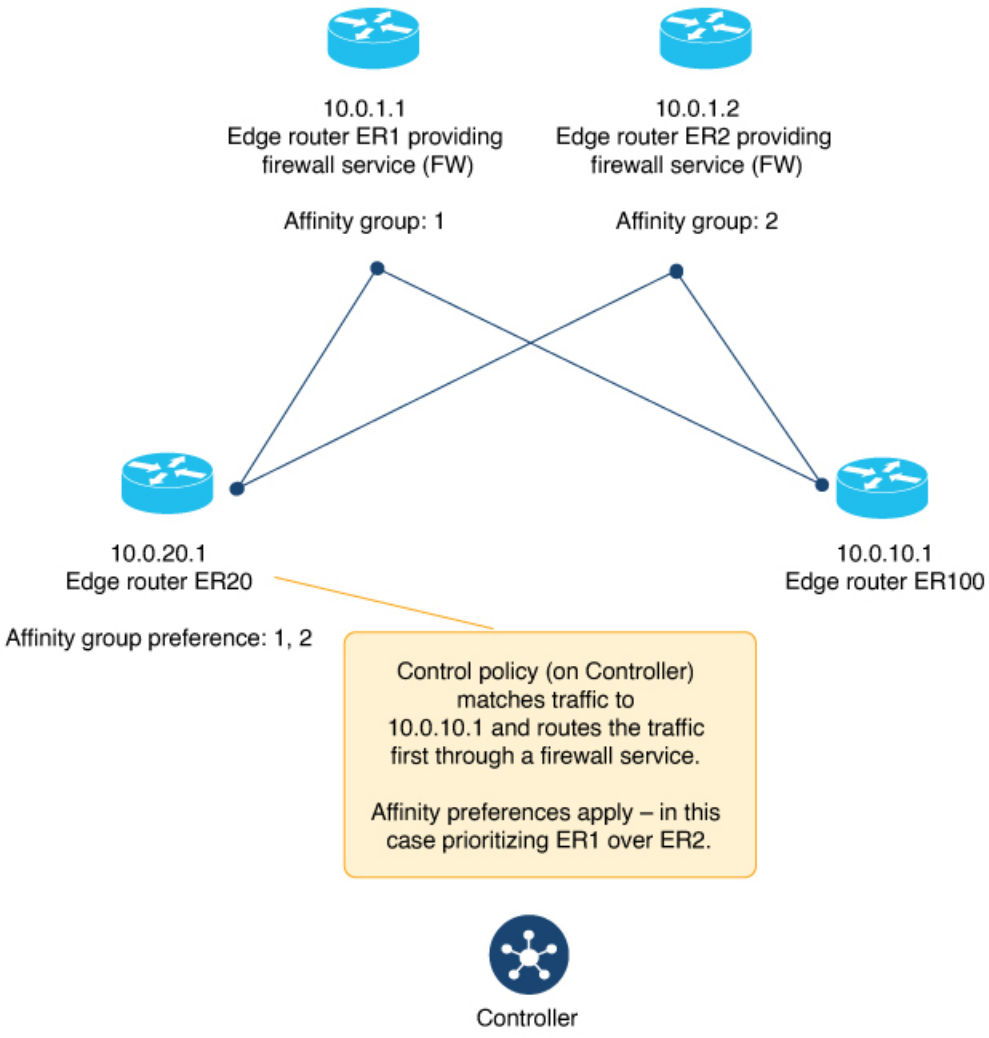
One useful application for affinity groups with service routes is configuring a control policy that directs traffic to a network service.

Routers in a network can advertise network services, such as firewalls, that operate on network traffic. To direct specific types of traffic to the service, create a control policy that matches the specific traffic and redirects the traffic to one or more routers providing the service, as the next hop, before the traffic continues to its destination. When more than one router provides the same network service, such as a firewall, a router in the network can direct traffic to any of the routers providing the service.

For example, if a control policy redirects traffic from router A to a firewall service, and two routers, B and C, provide the firewall service, then router A can send the traffic to either B or C. The affinity group preference list of router A, together with the affinity group assignments B and C, determine whether the traffic uses B or C as the next hop.

In the following illustration, a network has two dedicated routers providing a firewall service. A control policy can match traffic destined to router ER100 (10.0.10.1) and set the service to FW for the matched traffic. The effect is that the Cisco SD-WAN Controller redirects the traffic to ER1 or ER2 as the next hop before the traffic proceeds to its destination. In the example, affinity group preferences prioritize ER1 or ER2 as the firewall service to use.

Figure 14: Affinity Groups and Service Routes



For an overview of configuring control policy, refer to the policy overview section of the *Cisco Catalyst SD-WAN Policies Configuration Guide*. For information about configuring matching parameters and action parameters for control policy, refer to the centralized policy section.

Affinity Groups and TLOC Routes

A useful application of affinity groups with TLOC routes is configuring a control policy that directs traffic to a list of TLOCs. TLOCs inherit the affinity group assignment of their router.

If a control policy redirects traffic from router A to a list of TLOCs, the affinity group preference list of router A, together with the affinity group assignments of each TLOC, determine which TLOC the traffic uses for its next hop.

Supported Devices for Router Affinity Groups

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

- Cisco IOS XE Catalyst SD-WAN devices
- Cisco vEdge devices

Supported Platforms for Setting an Affinity Group by Control Policy

Minimum releases: Cisco Catalyst SD-WAN Control Components Release 20.11.1, Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

Cisco IOS XE Catalyst SD-WAN devices

Supported Devices for Support for Affinity Groups with Service Routes and TLOC Routes

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, Cisco Catalyst SD-WAN Control Components Release 20.11.1

Cisco IOS XE Catalyst SD-WAN devices

Prerequisites for Support for Affinity Groups with Service Routes and TLOC Routes

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, Cisco Catalyst SD-WAN Control Components Release 20.11.1

Support for affinity groups is automatic, without specific prerequisites.

The following prerequisites apply to the common use case of incorporating affinity group functionality when configuring control policy that redirects traffic to a network service:

- Configure one or more routers to operate a network service, such as a firewall. To view the services advertised in a network use the **show sdwan omp services** command on a router in the network. The **SERVICE** column shows the advertised services and the **ORIGINATOR** column shows the routers advertising the services. The **AFFINITY GROUP NUMBER** column shows the affinity group of the router providing the service.
- Configure an affinity preference list on the routers originating traffic that will flow to the network service.
- Configure affinity groups for the routers providing the network service.

Restrictions for Router Affinity Groups

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

The affinity group range is limited to 1 to 63.

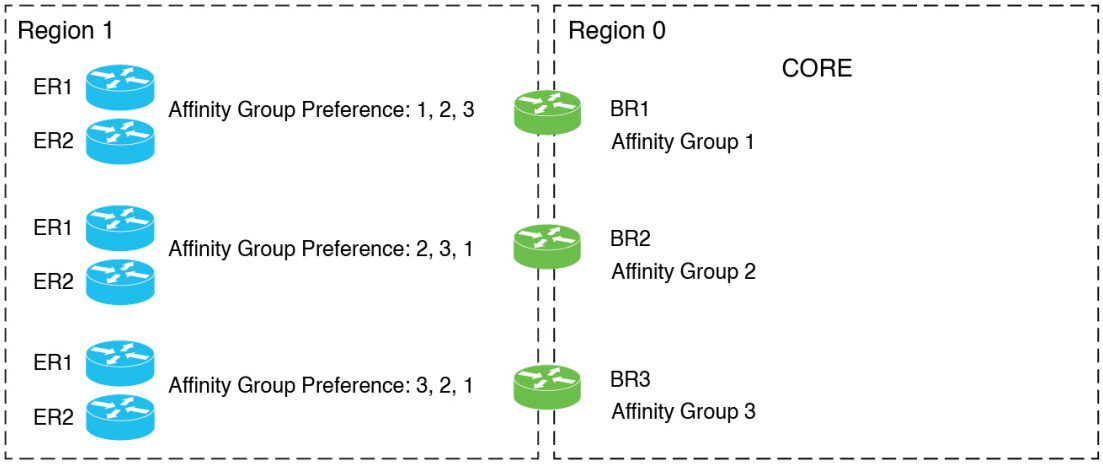
Use Cases for Router Affinity Groups

Use Case 1: Load Balancing for Access Region Traffic to Border Routers

In a scenario in which an access region has six edge routers (ER1 to ER6) and three border routers (BR1, BR2, and BR3), you can use affinity groups to load balance, as follows:

Devices	Configuration	Result
BR1	Assign affinity group 1.	
BR2	Assign affinity group 2.	
BR3	Assign affinity group 3.	
ER1 and ER2	Assign an affinity group preference order of 1, 2, 3.	These two edge routers preferentially direct traffic to BR1 for the next hop, but if BR1 is not available, they attempt to use BR2. If BR2 is not available, they attempt to use BR3.
ER3 and ER4	Assign an affinity group preference order of 2, 3, 1.	These two edge routers preferentially direct traffic to BR2 for the next hop, but if BR2 is not available, they attempt to use BR3. If BR3 is not available, they attempt to use BR1.
ER5 and ER6	Assign an affinity group preference order of 3, 1, 2.	These two edge routers preferentially direct traffic to BR3 for the next hop, but if BR3 is not available, they attempt to use BR1. If BR1 is not available, they attempt to use BR2.

Figure 15: Use Case 1: Load Balancing for Access Region Traffic to Border Routers

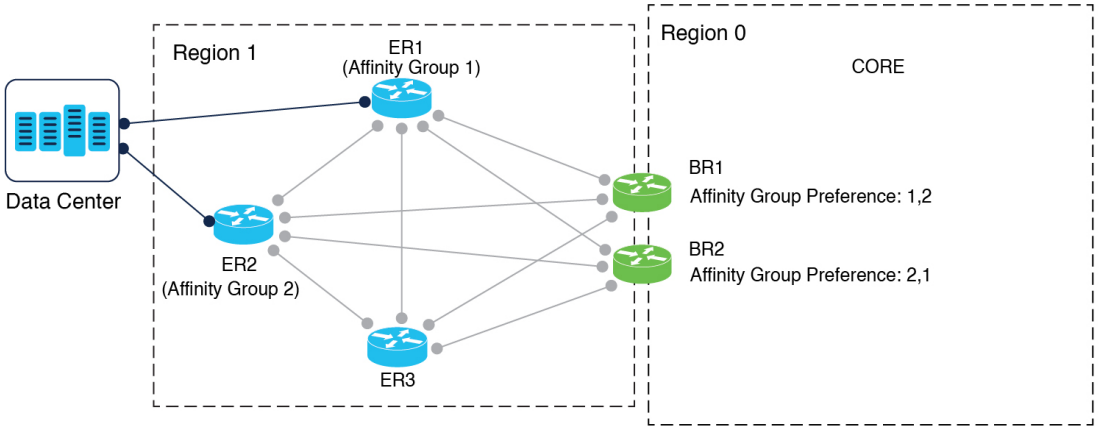


Use Case 2: Load Balancing for Access Region Traffic to Edge Routers

In a scenario in which an access region has two edge routers (ER1 and ER2) serving a high-volume data center, and two border routers (BR1 and BR2), you can use affinity groups to load balance, as follows:

Devices	Configuration	Result
ER1	Assign affinity group 1.	
ER2	Assign affinity group 2.	
BR1	Assign an affinity group preference order of 1, 2.	This border router preferentially directs data center traffic to ER1, but if ER1 is not available, it can use ER2.
BR2	Assign an affinity group preference order of 2, 1.	This border router preferentially directs data center traffic to ER2, but if ER2 is not available, it can use ER1.

Figure 16: Use Case 2: Load Balancing for Access Region Traffic to Edge Routers

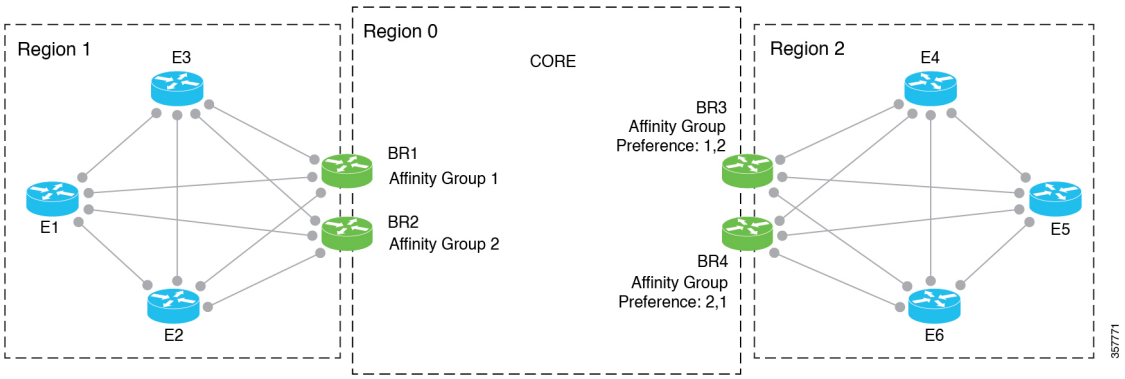


Use Case 3: Load Balancing for Core Region Traffic

In a scenario in which a high-volume access region (Region 1) has two border routers (BR1 and BR2), and receives a lot of traffic from another access region (Region 2), which has two border routers (BR3 and BR4), you can use affinity groups to load balance, as follows:

Devices	Configuration	Result
BR1 (Region 1)	Assign affinity group 1.	
BR2 (Region 1)	Assign affinity group 2.	
BR3 (Region 2)	Assign an affinity group preference order of 1, 2.	When directing traffic to region 1, this border router preferentially directs the traffic to BR1, but if BR1 is not available, it can use BR2.
BR4 (Region 2)	Assign an affinity group preference order of 2, 1.	When directing traffic to region 1, this border router preferentially directs the traffic to BR2, but if BR2 is not available, it can use BR1.

Figure 17: Use Case 3: Load Balancing for Core Region Traffic



Use Cases for Setting an Affinity Group by Control Policy

Minimum releases: Cisco Catalyst SD-WAN Control Components Release 20.11.1, Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

An organization using Multi-Region Fabric has two data centers, each with a hub router in access region 1. Originally, the hub routers had affinity groups defined as shown in the illustration, and the border routers had affinity group preferences defined as shown in the illustration. The result was helpful in allowing BR1 to prefer ER1 and in allowing BR2 to prefer ER2.

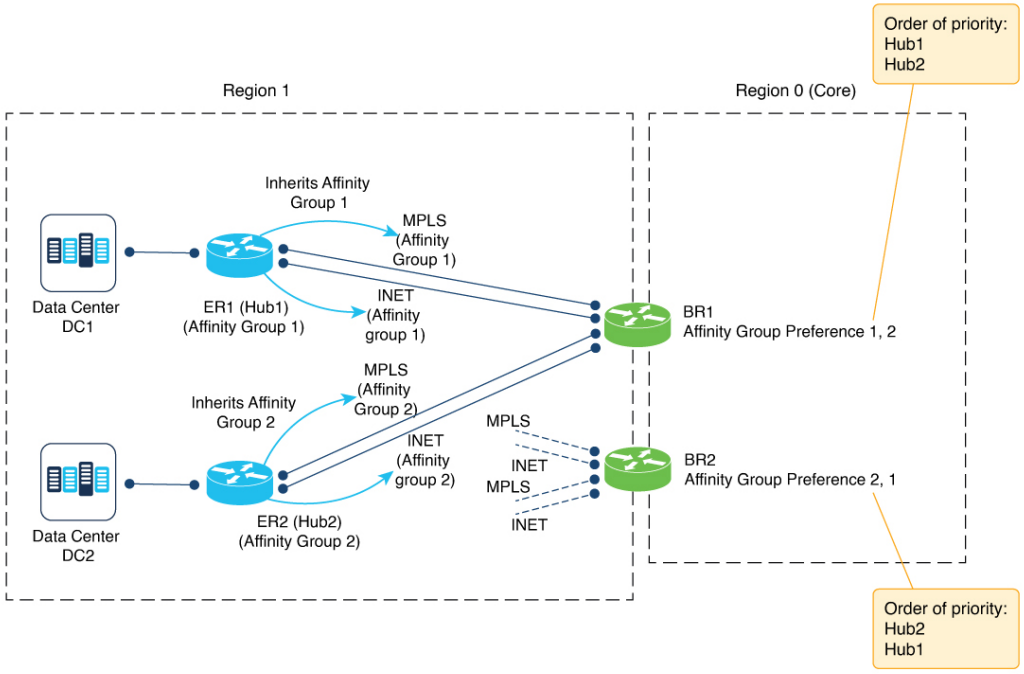
- BR1 route preferences (from higher priority to lower):

  1. Hub1, connecting to data center DC1, using either MPLS or INET connections.

2. Hub2, connecting to data center DC2, using either MPLS or INET connections.

- BR2 route preferences (from higher priority to lower):
  1. Hub2, connecting to data center DC2, using either MPLS or INET connections.
  2. Hub1, connecting to data center DC1, using either MPLS or INET connections.

Figure 18: Before Assigning Affinity Groups Using Control Policy



However, the organization wants to prioritize MPLS connections over internet (INET) connections between hubs and data centers. To accomplish this, they use control policies to set affinity groups for specific types of connections, giving them more granular control of routing. The control policies do the following:

- Match INET routes from Hub1 and assign affinity group 3
- Match INET routes from Hub2 and assign affinity group 4

The resulting preferences are as follows:

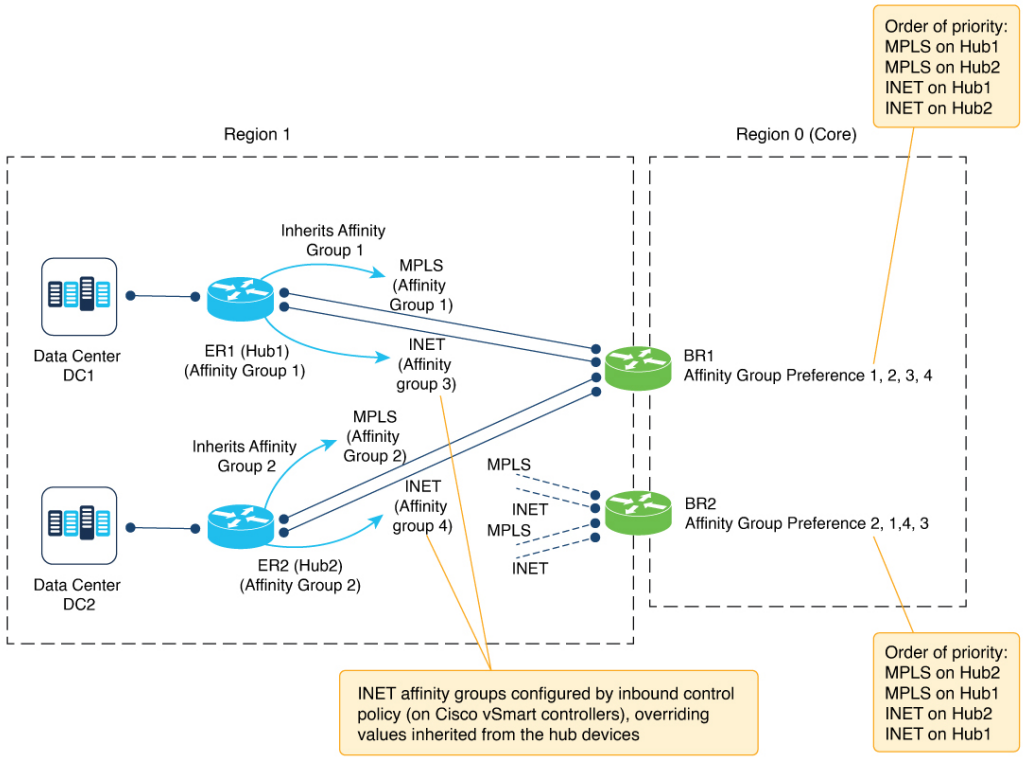
- BR1 route preferences (from higher priority to lower):
  1. Hub1, connecting to data center DC1, using an MPLS connection.
  2. Hub2, connecting to data center DC2, using an MPLS connection.
  3. Hub1, connecting to data center DC1, using an INET connection.
  4. Hub2, connecting to data center DC2, using an INET connection.

- BR2 route preferences (from higher priority to lower):
  1. Hub2, connecting to data center DC2, using an MPLS connection.

2. Hub1, connecting to data center DC1, using an MPLS connection.
3. Hub2, connecting to data center DC2, using an INET connection.
4. Hub1, connecting to data center DC1, using an INET connection.

The following illustration shows the effect of the control policy on the affinity groups of the MPLS and INET connections, and the resulting order of priority for BR1 and BR2:

Figure 19: Assigning Affinity Groups Using Control Policy, Offering More Granular Control



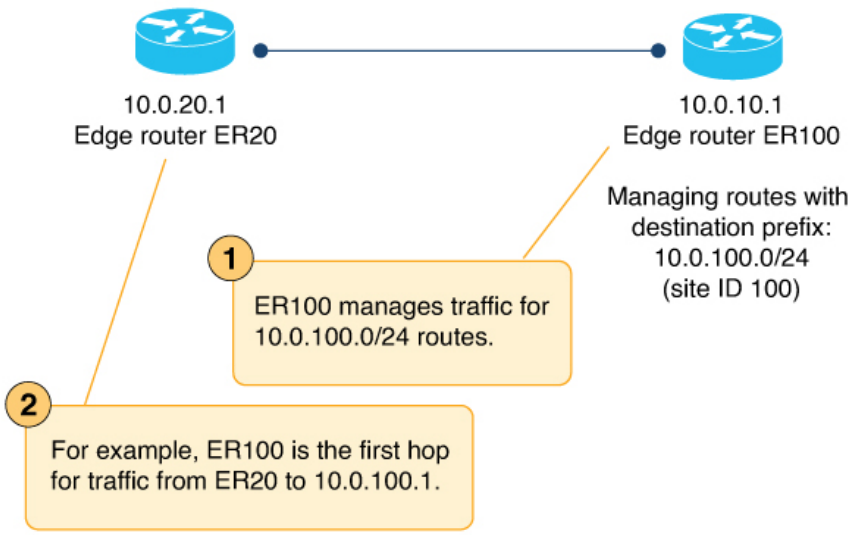
Use Cases Support for Affinity Groups with Service Routes and TLOC Routes

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, Cisco Catalyst SD-WAN Control Components Release 20.11.1

Use Case: Network Services and Control Policy

An organization’s headquarters site has a router ER100, which manages routes defined by the prefix 10.0.100.1/24. The routers in the 10.0.100.1/24 range have a site ID of 100.

Figure 20: Organization Site



Separately, the organization has two dedicated routers, ER1 (with affinity group 1) and ER2 (with affinity group 2), providing firewall services (advertised as FW) for the headquarters.

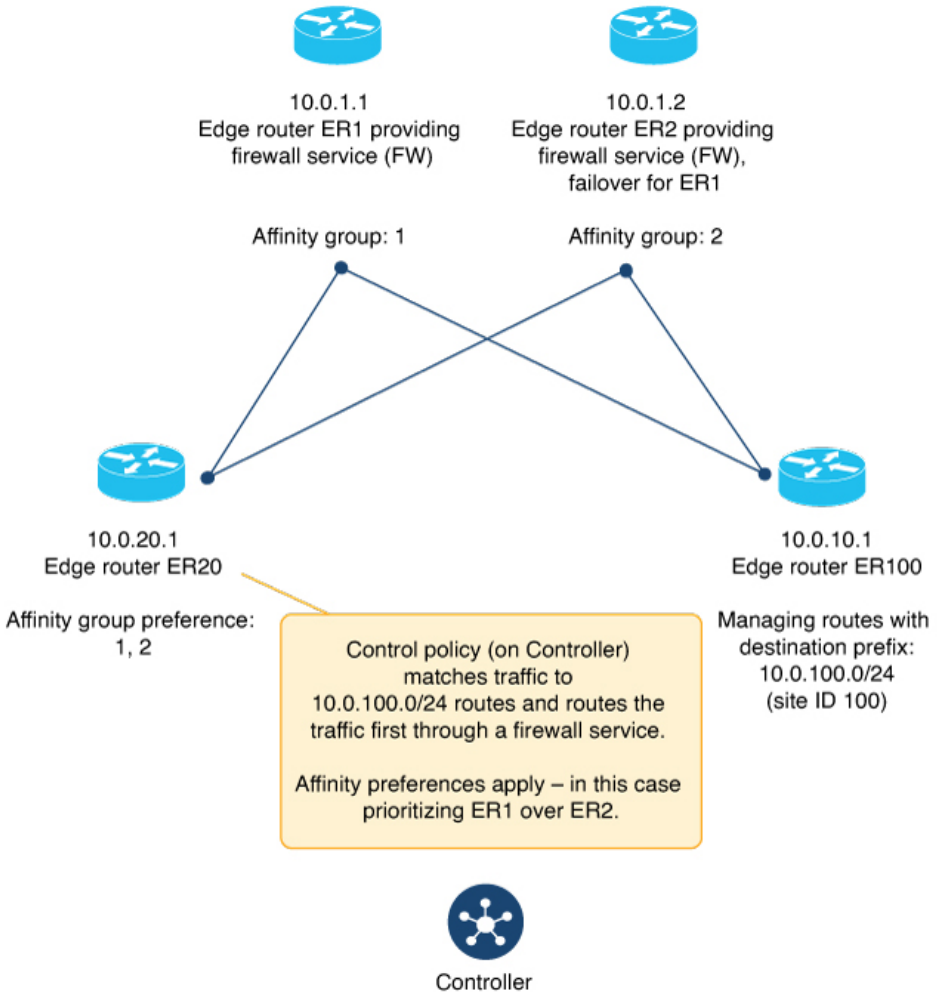
The organization's network administrators decide to route all traffic for devices at site 100 (the range 10.0.100.1/24) first to the dedicated firewall device. This requires redirecting all incoming traffic for site 100 to the firewall services. They configure a control policy to match all site 100 routes and set the service to FW. The effect is that the traffic goes first to one of the firewall servers, then proceeds to its original destination in site 100. Affinity group preferences prioritize ER1 or ER2 as the firewall service to use.

On the Cisco SD-WAN Controllers serving site 100, they add a control policy as follows:

```
policy
 control-policy control1
  sequence 1
   match route
    site-id 100
   !
  action accept
   set
    service FW
   !
  !
 !
 default-action accept
 !
!
```

The following illustration shows how traffic reaches ER100 through one of the two routers providing firewall services, ER1 or ER2.

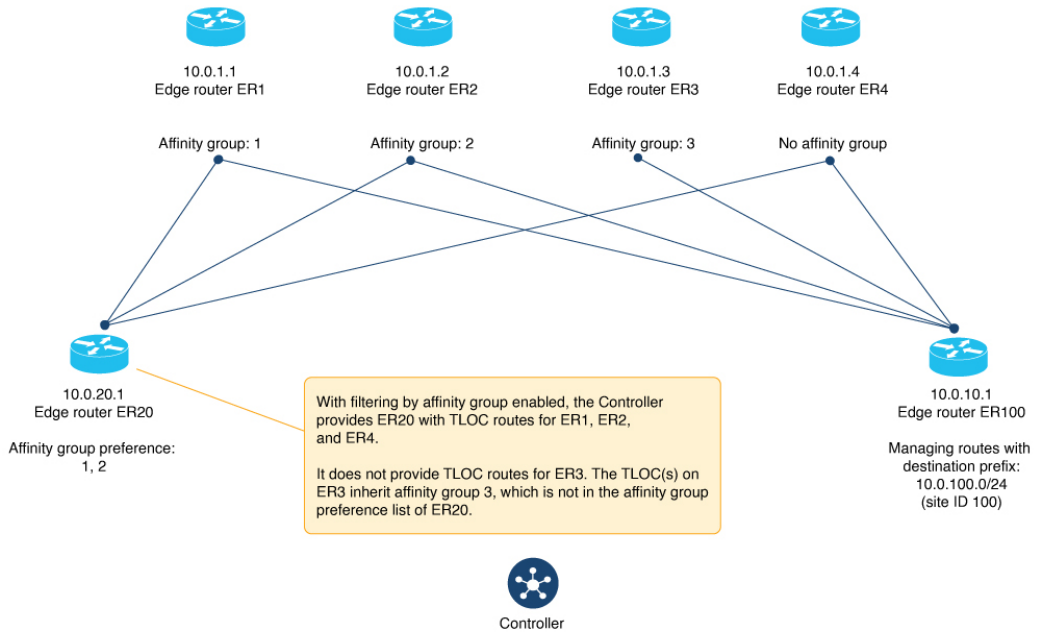
Figure 21: Organization Site with Firewall Service



Use Case: TLOC Route Filtering by Affinity Group

An organization’s headquarters site has a device ER20 with no direct route to ER100. Each of the routers ER1, ER2, ER3, and ER4 can provide a path to ER100. To reduce resource demands on Cisco SD-WAN Controllers and on ER20, the organization's network administrators configure ER20 with an affinity group preference list of 1, 2. This causes the Cisco SD-WAN Controllers to filter out TLOC routes from router ER3, which has an affinity group of 3.

Figure 22: Organization Site



The example is simplified, with only a small number of TLOC routes, but in a network with hundreds of available TLOC routes, this mechanism can significantly reduce resource demands.

Configure Router Affinity Groups Using Cisco SD-WAN Manager

Configure an Affinity Group or Affinity Group Preference on a Device, Using Cisco SD-WAN Manager

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create a system template for the device.
   - In the table, locate the existing system template for the device. In the row for the template, click **…** and choose **Edit**.
4. To assign an affinity group to a border router, in the **Advanced** section, in the **Affinity Group** field, change the mode to **Global** and enter an affinity group number, in the range 1 to 63.

   If an affinity group has been configured previously on the device, the new value replaces the previous.

5. To configure an affinity group preference order for a border router or an edge router, in the **Advanced** section, in the **Affinity Group Preference** field, change the mode to **Global** and enter a comma-separated list of affinity group numbers. This determines the order of preference for connecting to border routers. The affinity groups are in the range 1 to 63.

   Example: 10, 11, 1, 5

Note If you configure a Cisco SD-WAN Controller to filter out routes that are not in the affinity group preference list, then the device can only connect to routers in the affinity group. See Configure a Cisco SD-WAN Controller to Provide Only Paths in the Affinity Preference List, Using Cisco SD-WAN Manager, on page 117.

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

Configure a Cisco SD-WAN Controller to Provide Only Paths in the Affinity Preference List, Using Cisco SD-WAN Manager

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

Before You Begin

The last step of this procedure requires logging in to the Cisco SD-WAN Controllers that serve the regions where you are configuring this, to execute a command using the CLI.

Configure a Cisco SD-WAN Controller to Provide Only Paths in the Affinity Preference List

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create an OMP template for a Cisco SD-WAN Controller.
   - In the table, locate the existing OMP template for the Cisco SD-WAN Controller. In the row for the template, click **…** and choose **Edit**.
4. In the **Best Path** section, in the **Enable Filtering Route Updates Based on Affinity** field, choose **Global** mode and choose **On**.
5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the Cisco SD-WAN Controllers using the template.
6. Connect to each Cisco SD-WAN Controller and clear OMP routes to ensure that only the paths in the affinity group preference list are used.

```
Controller#config terminal
Controller(config)#omp
Controller(config-omp)#filter-route outbound affinity-group-preference
Controller(config-filter-route)#exit
Controller(config-omp)#exit
```

```
Controller(config)#exit
Controller#clear omp all
```

Configure Affinity Group by Control Policy Using Cisco SD-WAN Manager

Minimum releases: Cisco Catalyst SD-WAN Control Components Release 20.11.1, Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policy**.
3. Click **Add Policy**.
4. Click **Next** to show the page for configuring topology.
5. Click the **Add Topology** drop-down menu and choose the **Custom Control** option.
6. Click **Sequence Type** and choose either the **Route** or **TLOC** option.
7. Click **Sequence Rule** to add a sequence rule.
8. Click **Match** and define a match condition.

   The details depend on your objectives. For example, to match TLOCs using MPLS, do the following:

   a. Click **TLOC**.

   b. In the **Match Conditions** area, in the **Color** field, choose **mpls**.
9. Click **Actions** in the new rule to define the action for the rule.
10. Click **Accept** to specify that the rule applies when its match condition is met.
11. Click **Affinity**.
12. In the **Affinity** field, enter a number for the affinity value to assign to the matched route or TLOC.
13. Click **Save Control Policy**.

Configure Router Affinity Groups Using the CLI

Configure an Affinity Group on a Router Using the CLI

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

1. Enter configuration mode.

   ```
   Device#config-transaction
   ```
2. Enter system configuration mode.

   ```
   Device(config)#system
   ```
3. Configure an affinity group ID in the range 1 to 63.

If an affinity group has been configured previously on the device, the new value replaces the previous.

```
Device(config-system)#affinity-group group-id
```

Example

```
Device#config-transaction
Device(config)#system
Device(config-system)#affinity-group 10
```

Configure Affinity Group Preference on a Router Using the CLI

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

1. Enter configuration mode.

   ```
   Device#config-transaction
   ```

2. Enter system configuration mode.

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

3. Enter a list of group IDs, each in the range 1 to 63, to indicate the affinity group preference order, from highest priority to lowest priority. Separate group IDs with spaces.

   ```
   Device(config-system)#affinity-group preference group-id [group-id ...]
   ```

Example

```
Device(config-system)#affinity-group preference 10 11 1 5
```

Configure a Cisco SD-WAN Controller to Provide Only Paths in an Affinity Group Preference List Using a CLI Template

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

For more information about using CLI templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*. By default, CLI templates execute commands in global configuration mode.

1. Enter system OMP configuration mode.

   ```
   omp
     no shutdown
   ```

2. Configure the Cisco SD-WAN Controller to provide each router only paths to routers in its affinity group preference list.

   The effect is to limit routers to connecting only to routers on their affinity group preference lists.

   ```
   filter-route
     outbound affinity-group-preference
   ```



Note You can use the **no** form of the command to disable this configuration. By default, it is disabled.

3. Connect to the Cisco SD-WAN Controller and clear OMP routes to ensure that only the paths in the affinity group preference list are used.

```
Controller#config terminal
Controller(config)#omp
Controller(config-omp)#filter-route outbound affinity-group-preference
Controller(config-filter-route)#exit
Controller(config-omp)#exit
Controller(config)#exit
Controller#clear omp all
```

Example

Add the following to a CLI template:

```
omp
  no shutdown
  filter-route
    outbound affinity-group preference
  exit
```

Enter the following on the Cisco SD-WAN Controller:

```
Controller#config terminal
Controller(config)#omp
Controller(config-omp)#filter-route outbound affinity-group-preference
Controller(config-filter-route)#exit
Controller(config-omp)#exit
Controller(config)#exit
Controller#clear omp all
```

Configure Affinity Group by Control Policy Using a CLI Template

Minimum releases: Cisco Catalyst SD-WAN Control Components Release 20.11.1, Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

For more information about using CLI templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*. By default, CLI templates execute commands in global configuration mode.

1. In a control policy, create a sequence.

```
policy
 control-policy policy-name
  sequence sequence-number
```

2. Create a match condition for either routes or TLOCs.

```
match {route | tloc}
For example, you can match routes from all devices at a site 100 using:
match route
 site-id 100
```

3. Create an action of type accept.

```
action accept
```

4. Set the affinity group number to assign to the matching routes or TLOCs.

```
set
affinity-group-number affinity-group-number
```

Example

This example creates a sequence that matches routes from devices at site 100 and assigns them the affinity group 5.

```
policy
 control-policy policy-1
  sequence 1
   match route
    site-id 100
  !
  action accept
   set
    affinity-group-number 5
   !
  !
 !
!
```

Example

This example does the following:

- Matches routes from site 100 and assigns them affinity group 2
- Matches TLOCs with the system IP address 10.0.0.1, of color lte and encapsulation IPsec, and assigns them affinity group 5

```
show running-config policy
policy
 control-policy policy-1
  sequence 1
   match route
    site-id 100
   !
   action accept
    set
     affinity-group-number 2
    !
   !
  !
  sequence 2
   match tloc
    tloc 10.0.0.1 color lte encap ipsec
   !
   action accept
    set
     affinity-group-number 5
    !
   !
  !
  default-action reject
 !
!
```

Verify an Affinity Group and Affinity Group Preference Using Cisco SD-WAN Manager

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

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

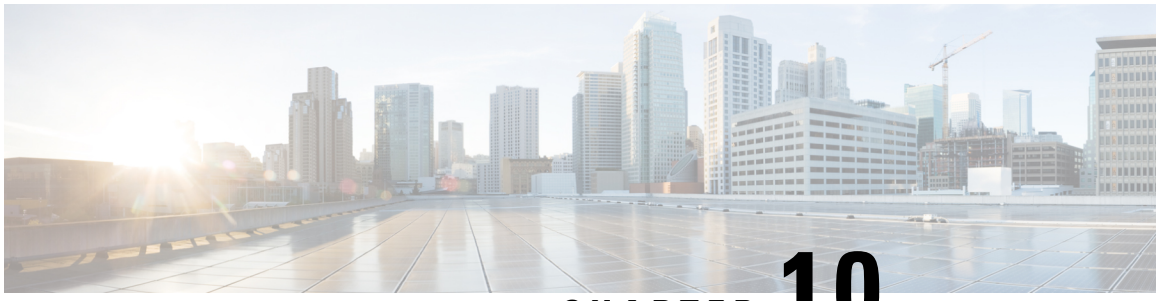
   See the **Affinity Group Number** and **Affinity Group Preference** fields.

Verify the Affinity Group and Affinity Group Preference Using the CLI

Use the **show sdwan running-config system** command to view the affinity group and affinity group preference on a device. The **affinity-group preference** field shows the preference list.

Example

```
Device#show sdwan running-config system
system
 system-ip          192.168.0.1
 domain-id          1
 site-id            1100
 affinity-group 10
 affinity-group preference 15 16
...
```



CHAPTER 10

Multi-Region Fabric Subregions

- Multi-Region Fabric Subregions, on page 123
- Information About Subregions, on page 124
- Supported Devices for Subregions, on page 127
- Restrictions for Subregions, on page 127
- Use Cases for Subregions, on page 128
- Configure and Use Subregions, on page 131

Multi-Region Fabric Subregions

Note Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1 are the last releases to support these features:

- Secondary regions
- Subregions
- Management regions

From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1, configuration of secondary regions and subregions is possible only by API. Because later releases do not support these features, we advise you to update your network design and configuration to use alternative solutions where possible. Refer to End of support for three types of regions, on page 177.

Table 18: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric Subregions	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	You can create subregions within an access region. Subregions enable you to separate edge routers into multiple distinct domains.

Information About Subregions

Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

Within an access region, you can create up to 63 subregions, with ID numbers in the range 1 to 63. Creating subregions within access regions enables you to separate edge routers into multiple distinct domains.

To define a subregion, configure a subregion for edge routers and for border routers. After you configure a subregion for a device, the device advertises its subregion attribute to its overlay management protocol (OMP) peers. Within OMP, a subregion is identified by the tuple of access region number and subregion ID, so you can reuse the same subregion numbers in different access regions—for example, subregion 1 of region 1 is distinct from subregion 1 of region 2.

Terminology

- Parent region: An access region is called the parent region of any subregions that you configure within it.
- Shared: In a Multi-Region Fabric topology that includes subregions, a border or edge router without a subregion assignment is called shared.
- Dedicated: In a Multi-Region Fabric topology that includes subregions, a border or edge router with a subregion assignment is called dedicated.

Connectivity

Default connectivity is as follows:

- Edge routers assigned to an access region, and not assigned to a subregion, form bidirectional forwarding detection (BFD) connectivity to all devices in the region, and to the border routers serving the access region.
- Edge routers assigned to a subregion form BFD connectivity to all other devices in the subregion, and to the border routers serving the subregion and parent region. By default, they do not form BFD connectivity to edge routers outside of the subregion.
- Border routers assigned to a region form BFD connectivity to all edge devices in the region. This is true even if a border router is also assigned to a subregion. Assigning a border router to a subregion causes it to preferentially operate as the border router for devices in the subregion, but it can also serve all devices in the parent region. This means that any border router serving a region can provide failover backup for other border routers serving the region, regardless of whether the border routers have been assigned to subregions.

Configure a Subregion

To configure a subregion, it is sufficient to assign one or more edge routers to a subregion. You do not need to assign a border router to the subregion. The border routers assigned to the parent region are shared by all the edges in that region.

Assigning an edge router to a subregion has the following effects:

- The edge router advertises its subregion to the Cisco SD-WAN Controllers managing its region. This indicates its subregion to all of its OMP peers.

For information about assigning a subregion to an edge router, see Assign a Region ID to an Edge Router TLOCs Using a CLI Template, on page 30.

- The edge router can have full-mesh connectivity only with (a) devices in its subregion, and (b) edge routers that are part of the same parent region but not in any subregion.

Assigning a border router to a subregion has the following effects:

- The border router primarily serves the edge routers in the subregion.
- The border router can also act as a backup border router for edge routers in other subregions within the same parent region.

For information about assigning a subregion to a border router, see Assign a Region ID to a Border Router TLOCs Using a CLI Template, on page 31.

Configure a Transport Gateway to a Subregion

If you assign a device serving as a transport gateway (such as a border router) to a subregion, the transport gateway can serve only devices in that subregion.

Configure Policy

For information about configuring a policy to use subregions, see the following:

- In region lists, you can include a subregion or subregion range for each region that you specify in the list. See Create a Region List Using a CLI Template, on page 159.
- You can apply the policies to specific subregions within a region. See Apply a Policy Using a CLI Template, on page 162.
- Control policy: You can match by subregion. See Configure a Control Policy to Match Region and Role Using a CLI Template, on page 161.
- For information about how subregions affect the prioritization of policies, see Prioritization of Policy, on page 149.

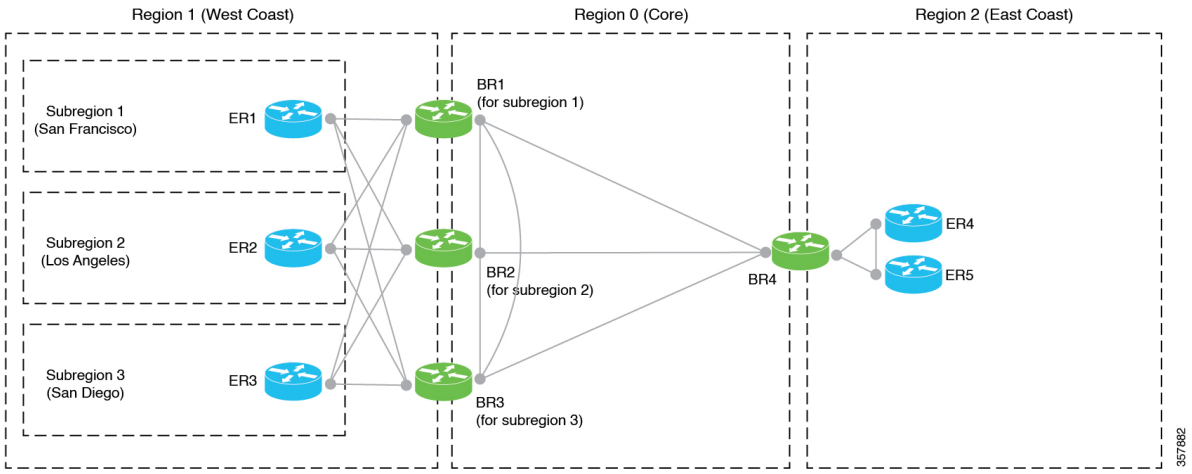
Border Router Preference

With the introduction of subregions, border routers add a new attribute, called br-preference, to routes that they re-originate to the core region. The br-preference attribute ensures that border routers in the core region choose the optimal path to devices in subregions when more than one path is available.

For example, in the following illustration, if BR4 is choosing a path to ER1, which is in subregion 1, the optimal path uses BR1, which serves that subregion. This is true even though BR2 and BR3 can also provide connectivity to ER1. In this example, routes for subregion 1 that BR1 re-originates have the highest br-preference value, so to reach subregion 1, BR4 chooses a path using BR1.

If BR1 becomes unavailable, then BR4 can reach subregion 1 through BR2 or BR3. BR2 and BR3 provide lower br-preference values for routes to subregion 1, but they can serve as failover border routers for subregion 1.

Figure 23: Subregion Scenario



To explain in more detail, when a border router receives a route from an edge router in its access region (across all subregions), it does the following:

1. Determines a br-preference value for the route, as described in the table that follows.
2. Attaches the value to the route, as the br-preference attribute, when re-originating the route to the core region.

Border routers of other regions use this attribute to determine which routes to prefer for a particular destination.

The following table describes how a border router determines the br-preference value when re-originating a route.

Table 19: br-preference

Conditions	br-preference Value for a Route
The route has a subregion ID, and the border router has the same subregion ID. **Note** In the preceding illustration, this would apply to a route from ER1, re-advertised to the core region by BR1.	100
The border router has no subregion ID.	75
The route has a subregion ID, and the border router has a different subregion ID. or The route does not have a subregion ID, and the border router does have a subregion ID. **Note** In the preceding illustration, this would apply to a route from ER1, re-advertised to the core region by BR2.	50

When choosing a route to a destination, border routers prioritize routes with a higher br-preference value.

Secondary Regions

Assigning devices to subregions does not interfere with configuring secondary regions. A device can have a subregion assignment and be part of a secondary region.

Benefits of Subregions

Creating subregions has the following benefits:

- In network topologies that have access regions with a small number of edge routers, it may not be cost-effective to dedicate border routers to each access region. Sharing a set of border routers among multiple access regions addresses this.
- You can enable the border router of one subregion to serve as a failover border router for a different subregion within the same parent region.

Supported Devices for Subregions

Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

You can configure subregions only on Cisco IOS XE Catalyst SD-WAN devices.

Restrictions for Subregions

Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

Restriction	Description
CLI template or CLI add-on template	You must use a CLI template or add-on CLI template to configure a subregion for a device. Furthermore, if you are configuring a subregion for a device, you must also use a CLI template to configure the region. This is because a subregion is configured together with a region, in the following format: **system** **region** *region-id* **subregion** *subregion-id* Using a CLI template to configure the region and subregion for Multi-Region Fabric does not prevent you from using a system template to configure other features for a device. You can use a system template to configure features unrelated to Multi-Region Fabric, and simultaneously use a CLI add-on template to configure the region and subregion.

Restriction	Description
Upgrading routers to Cisco IOS XE Release 17.12.1 or later	When using subregions, if you plan to upgrade routers in the Cisco Catalyst SD-WAN overlay network to Cisco IOS XE Release 17.12.1 or later, first ensure that any routers in the network that are operating as transport gateways are using Cisco IOS XE Release 17.12.1 or later.

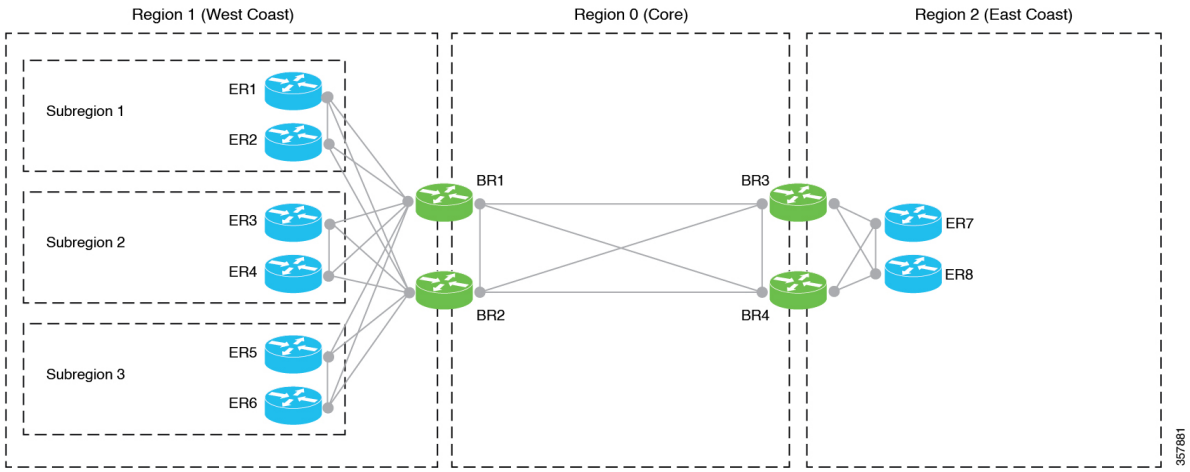
Use Cases for Subregions

Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

The following use cases describe some of the benefits of subregions.

Use Case: Sharing Border Routers

Figure 24: Sharing Border Routers



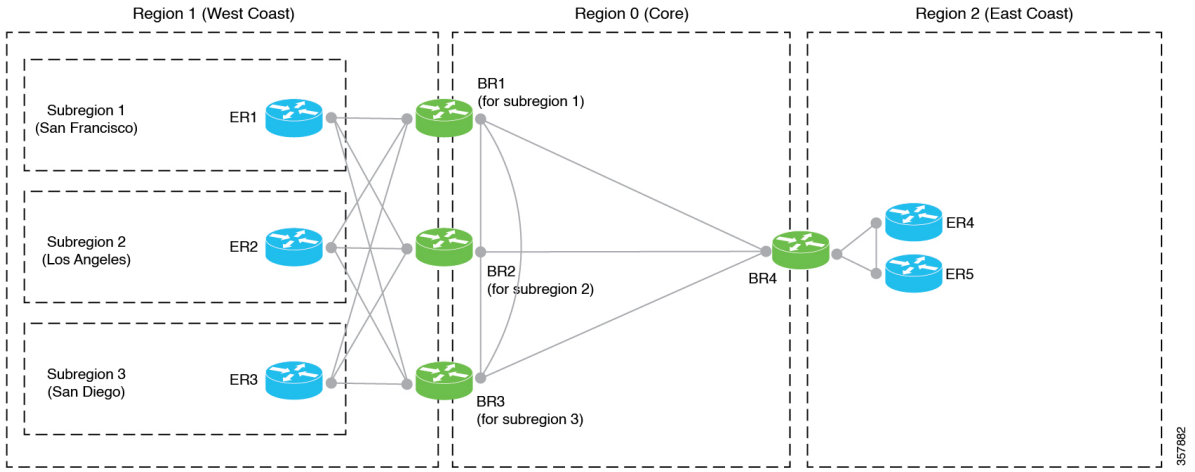
In this use case, an organization needs to have the six edge routers on the West Coast operate in three distinct domains. In addition, the organization needs at least two border routers for each access region, to provide a failover option if one border router becomes inoperative.

One option would be to create three regions for the West Coast and place the edge routers in those distinct regions. But each access region would need two or more border routers, and it may not be cost-effective to dedicate border routers for each of the three separate access regions.

An effective strategy is to create a single access region (region 1) for the West Coast, and to divide region 1 into subregions. This provides three domains for the routers on the West Coast. The entire region can use two shared border routers. The border routers are assigned to region 1, but are not assigned to any subregion. They can service edge routers in any subregion of region 1, without preference.

Use Case: Border Router Failover

Figure 25: Border Router Failover

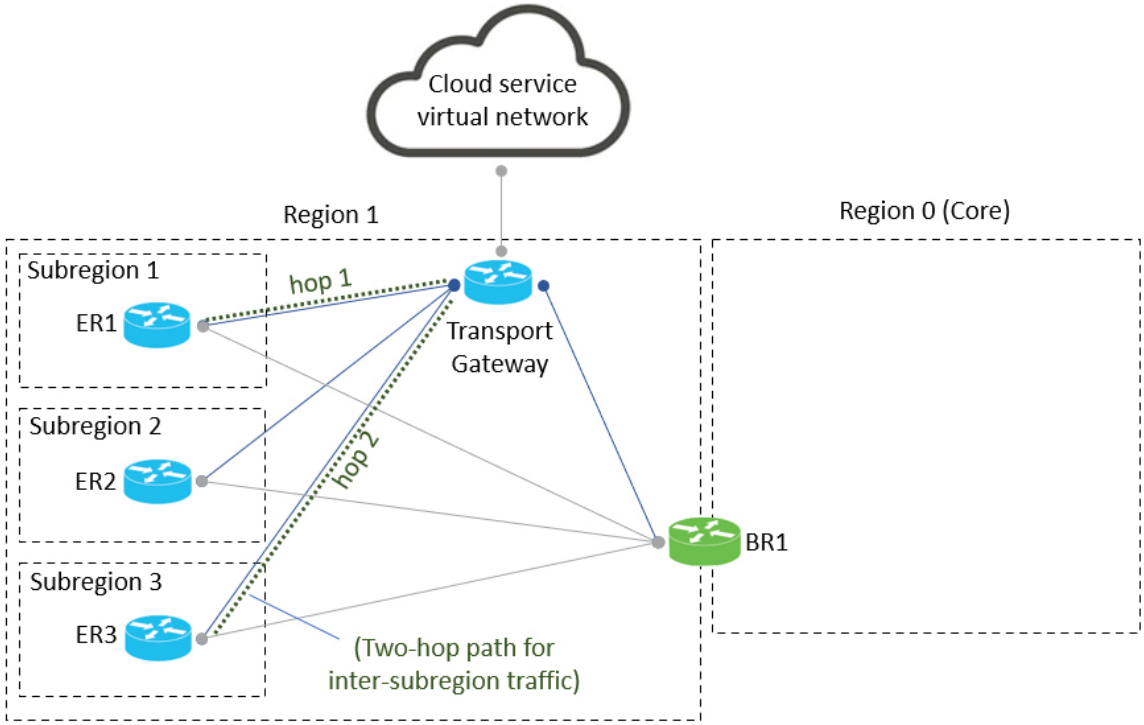


In this use case, access region 1 serves the West Coast. Within region 1, there are three separate subregions serving different cities on the West Coast. There is a separate dedicated border router for each of the three subregions. For each subregion, the border router is located in the city whose subregion it serves, to optimize performance.

Although each border router is dedicated to a specific subregion (by being assigned to that subregion), it has BFD connectivity with the edge routers throughout the entire parent region, meaning throughout the West Coast. This enables any of the border routers serving region 1 to provide failover backup for all of the border routers in the entire parent region. It is advantageous to fail over to border routers that are geographically adjacent, such as in another city on the West Coast, rather than failing over to a border router in a distant geographical region.

Use Case: Sharing Transport Gateways Across Subregions

Figure 26: Sharing a Transport Gateway

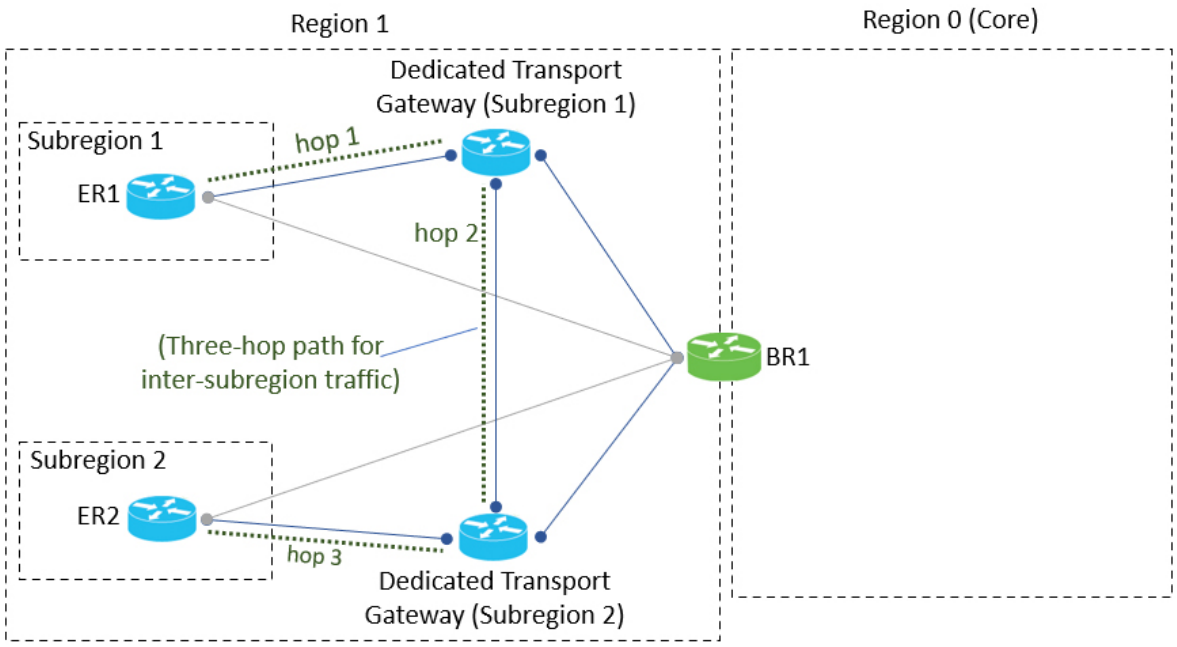


In this use case, an organization has divided access region 1 into three subregions. The organization has configured a single transport gateway to handle a specific class of traffic for the access region. Specifically, the transport gateway handles all traffic between region 1 and a virtual network hosted by a public cloud service, such as Azure.

The scale of the region 1 does not require more than one transport gateway, even though there are three separate subregions. Because the transport gateway has connectivity to all routers in the access region, regardless of the subregion, traffic between subregions flows through the transport gateway. This is similar to a scenario described previously, in which border routers provide connectivity to routers in different subregions, for traffic between subregions within the same parent access region.

Use Case: Dedicated Transport Gateways

Figure 27: Dedicated Transport Gateways



In this use case, an organization has divided access region 1 into two subregions. Each subregion has a dedicated transport gateway to handle a specific class of traffic. Although the illustration shows only a single edge router in each subregion, this use case applies to scenarios in which a large number of routers in each subregion justify a dedicated transport gateway for each subregion, for load balancing among numerous transport gateways.

The transport gateways are connected to each other. A router in one subregion can connect to a router in a different subregion using a three-hop path through their respective transport gateways.

Configure and Use Subregions

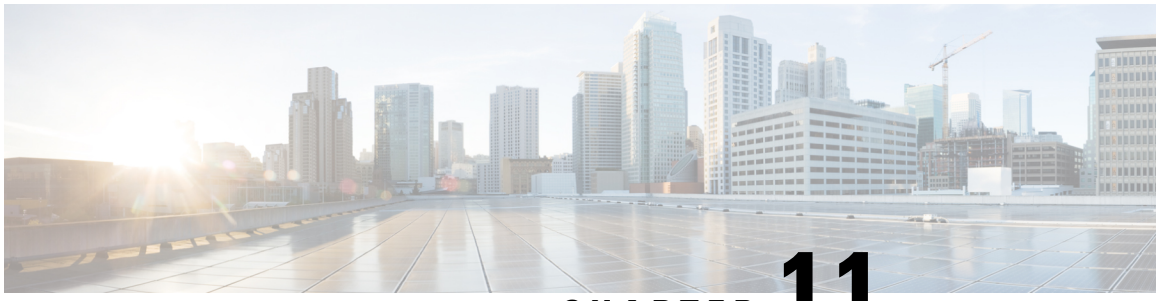
Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

The following table indicates where to find information about configuring subregions for devices and using subregions in policy.

Table 20: Configuring and Using Subregions

Topic	Reference
Assign a subregion to border router.	Assign a Region ID to a Border Router TLOCs Using a CLI Template, on page 31
Assign a subregion to an edge router.	Assign a Region ID to an Edge Router TLOCs Using a CLI Template, on page 30

Topic	Reference
Create a region list, including subregions.	Create a Region List Using a CLI Template, on page 159
Configure a control policy to match by subregion.	Configure a Control Policy to Match Region and Role Using a CLI Template, on page 161
Apply a policy, specifying devices by region and subregion.	Apply a Policy Using a CLI Template, on page 162



CHAPTER 11

Multi-Region Fabric Using Multicloud and SDCI

- Multi-Region Fabric Using Multicloud and SDCI, on page 133
- Information About Multi-Region Fabric Using Multicloud and SDCI, on page 133
- Supported Devices for Multi-Region Fabric Using Multicloud and SDCI, on page 135
- Prerequisites for Multi-Region Fabric Using Multicloud and SDCI, on page 135
- Restrictions for Multi-Region Fabric Using Multicloud and SDCI, on page 135
- Use Cases for Multi-Region Fabric Using Multicloud and SDCI, on page 135
- Workflow for Configuring Multi-Region Fabric with a Cloud Service Core Region, on page 138

Multi-Region Fabric Using Multicloud and SDCI

Table 21: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric Using Multicloud and SDCI	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	This feature enables you to configure a cloud backbone or a Software-Defined Cloud Interconnect (SDCI) provider backbone as core region (region 0), and cloud gateways or interconnect gateways as border routers. You can thus easily establish site-to-site connectivity in multiple cloud regions and cloud networks.

Information About Multi-Region Fabric Using Multicloud and SDCI

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

Cisco Catalyst SD-WAN includes a technology called Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud, for integrating public cloud infrastructure into the Cisco Catalyst SD-WAN fabric. For a network using Multi-Region Fabric, you can establish site-to-site connectivity in multiple cloud regions and cloud networks by using a cloud backbone or a Software-Defined Cloud Interconnect (SDCI) provider backbone as core region (region 0). In this configuration, one or more cloud regions are configured as separate Multi-Region Fabric regions. Cloud gateways or interconnect gateways are configured as border routers, and full-mesh

connectivity between gateways in different Multi-Region Fabric regions is set up to carry site-to-site traffic over the cloud backbone or the SDCI provider backbone.

The following cloud services support a cloud-based core region:

- Microsoft Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

The following SDCI provider supports an interconnect gateway-based core region:

- Megaport



Note

- In case of AWS, when site-to-site connectivity is enabled at the global setting level, each cloud gateway must be configured as a border router.
- In case of GCP, when site-to-site connectivity is enabled at the global setting level, only border routers that have site-to-site connectivity participate in core routing.
- The Megaport fabric supports private site-to-site connectivity. Therefore, it is not always necessary to have a full mesh of site-to-site connectivity when SDCI routers are configured as border routers. Routers that have direct connectivity with each other can create a full-mesh network among the connected sites. However, if the SDCI routers are in partial-mesh connectivity, it is still possible to establish full-mesh connectivity using the BFD tunnels. The routing protocol helps in advertising the connected links between the sites that do not have direct connectivity, and thus a full logical mesh of BFD tunnels over private links between the connected sites is created.

  For example, Site A is connected to Site B through a Virtual Cross Connect (VXC). Similarly, Site C is connected to Site B through another VXC. However, there is no direct connection between Site A and Site C. In this scenario, Site A can connect to Site C by using the VXC between Site B and Site C. The connectivity between Site A and Site C is discovered through the standard routing protocol in underlay, and thus BFD tunnels are formed between Site A and Site C.

Benefits of Multi-Region Fabric Using Multicloud and SDCI

- Multi-Region Fabric provides fully automated path compute for site-to-site traffic across a provider (cloud or SDCI) backbone. There are no manual hop-by-hop route policies needed, thereby providing you significant operational simplification.
- The network automatically routes around traffic routing failures, providing resiliency.
- In a deployment scenario with thousands of branches, using a cloud service or SDCI for the core region can be an easier option than configuring a complex control policy.

Supported Devices for Multi-Region Fabric Using Multicloud and SDCI

This feature is supported only on Cisco IOS XE Catalyst SD-WAN devices. Minimum supported release for the devices is Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.

Prerequisites for Multi-Region Fabric Using Multicloud and SDCI

- You must have a cloud or SDCI account.
- Cloud gateways or interconnect gateways for regions that need to exchange traffic must be reachable to each other in the underlay routing.
- When using AWS, enable full-mesh connectivity between transit virtual path connections (TVPCs) of cloud gateways in different regions to carry site-to-site traffic.

Restrictions for Multi-Region Fabric Using Multicloud and SDCI

- After you enable the **Multi-Region Fabric** option in Cisco SD-WAN Manager, you cannot set it to disabled again.
- If you choose to assign a device to a different Multi-Region Fabric region, then assign all devices belonging to a cloud gateway or an interconnect gateway to the same Multi-Region Fabric region because there is no check to prevent a region mismatch.
- The Equinix SDCI is supported from Cisco Catalyst SD-WAN Control Components Release 20.12.1.

Use Cases for Multi-Region Fabric Using Multicloud and SDCI

Use Case 1: Multi-Region Fabric Deployment with Cloud Service Provider as Backbone

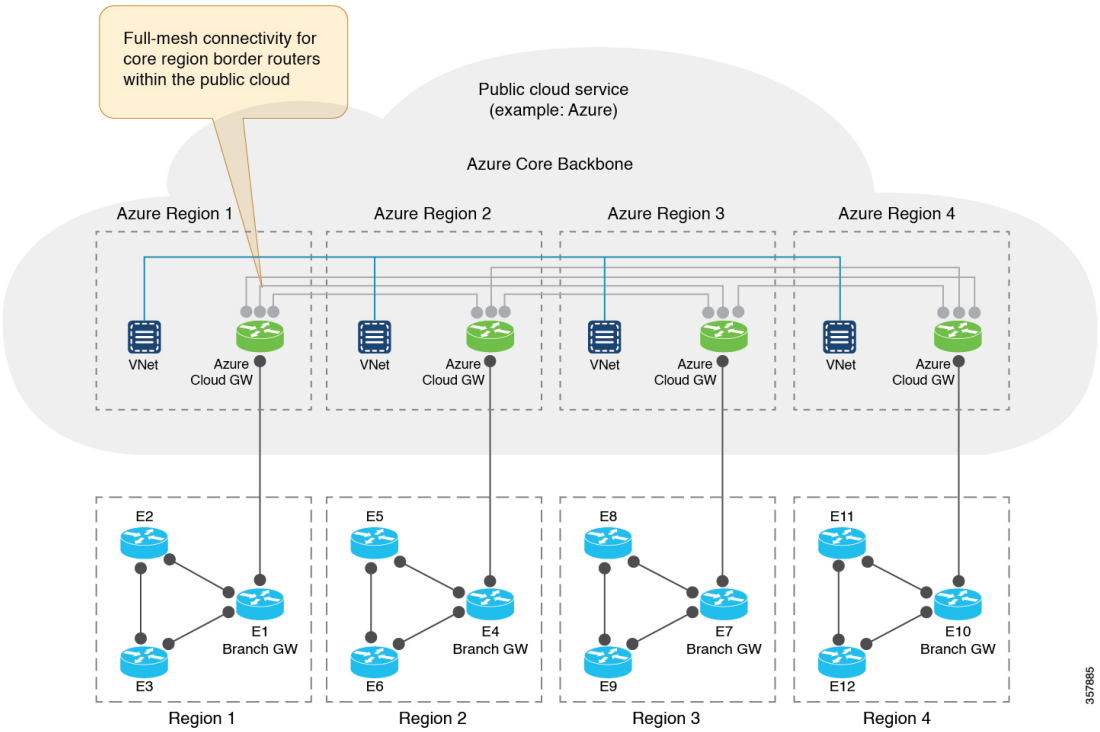
An organization has a large number of branch offices, and is using Multi-Region Fabric. They choose to use a public cloud service—Microsoft Azure—for the core region to simplify configuration and to enable rapid deployment of additional border routers when needed.

The organization configures four Azure cloud regions as Multi-Region Fabric regions: Azure Region 1, Azure Region 2, Azure Region 3, and Azure Region 4. In each region, a cloud gateway is brought up and configured as a border router. The border routers form the core region and have full-mesh connectivity.

Within each access region, edge routers connect to a cloud gateway that serves as the border router for the region.

An edge router in region 2 can connect to an edge router in region 3 by traversing the core overlay network. For example, E5 can connect to E9 by traversing the core overlay network.

Figure 28: Multi-Region Fabric Deployment with Cloud Service Provider as Backbone



Use Case 2: Multi-Region Fabric Deployment with SDCI as Backbone: Edge-Cloud Topology

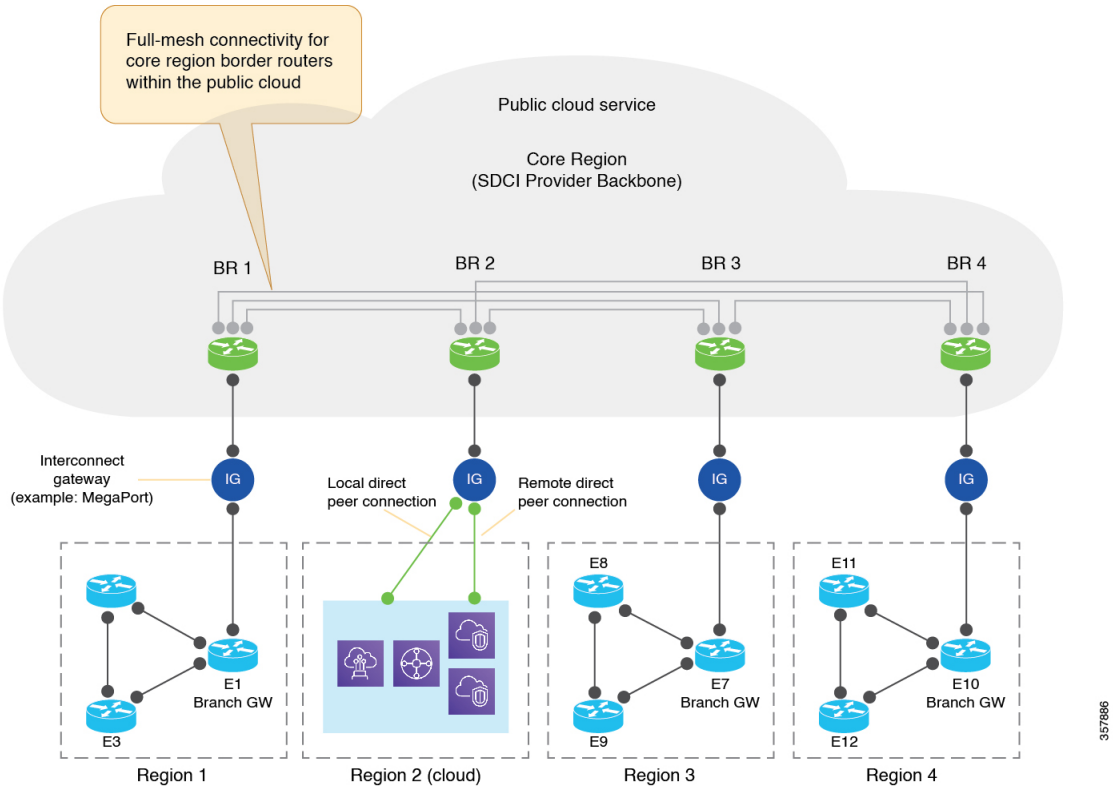
An organization has a large number of branch offices, and is using Multi-Region Fabric. They choose to use a cloud interconnect service—Megaport—for the core region to simplify configuration and to provide cost-effective, reliable connectivity between access regions and border routers.

The organization configures three cloud regions as Multi-Region Fabric regions: Region 1, Region 3, and Region 4. In addition, there is one cloud region that has not been configured as Multi-Region Fabric region: cloud region 2. In each region, an interconnect gateway is brought up and configured as a border router. The border routers form the core region and have full-mesh connectivity.

An edge router in region 1 can connect to an edge router in region 4 by traversing the core overlay network. For example, E3 can connect to E11 by traversing the core overlay network.

In addition, in this deployment, an edge router in region 1, region 3, or region 4 can directly connect to a cloud resource in cloud region 2 without the presence of a router in the cloud region itself.

Figure 29: Multi-Region Fabric Deployment with SDCI as Backbone: Edge-Cloud Topology



Use Case 3: Multi-Region Fabric Hybrid Deployment with SDCI as Backbone and Cloud Gateway as Edge Router

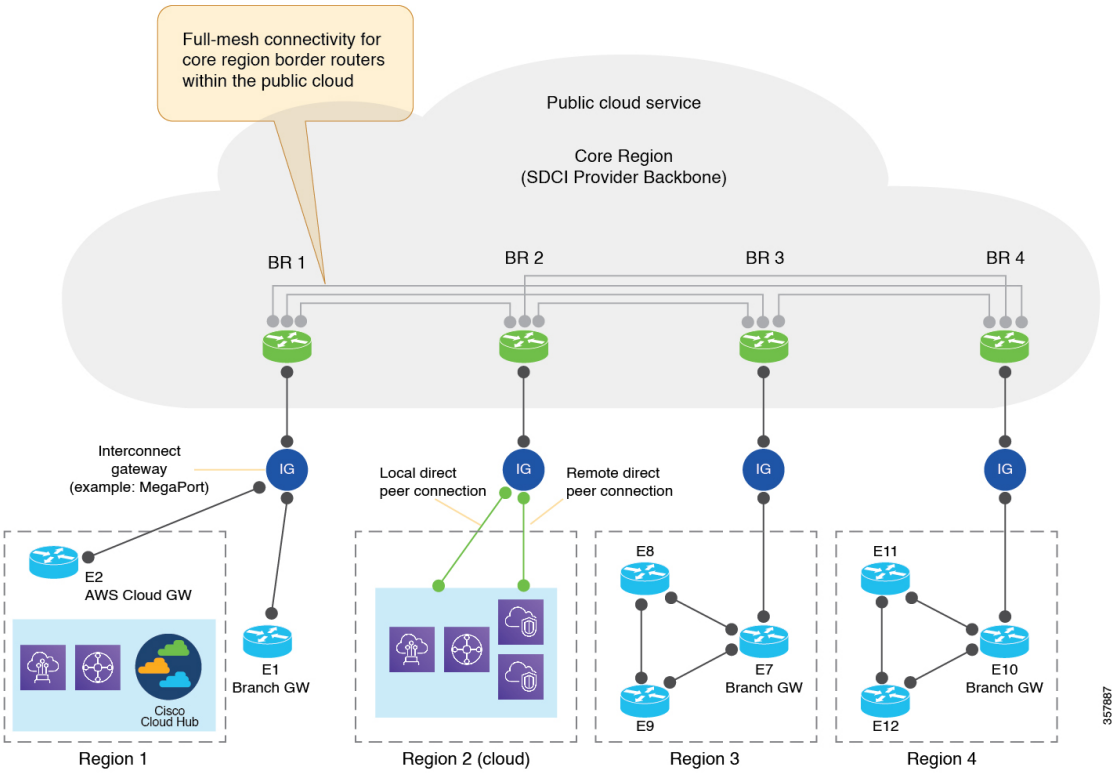
An organization has a large number of branch offices, and is using Multi-Region Fabric. They choose to use a cloud interconnect service—Megaport—for the core region to simplify configuration and to provide cost-effective, reliable connectivity between access regions and border routers.

The organization configures two cloud regions as Multi-Region Fabric regions: region 3 and region 4. In addition, there are two cloud regions that have not been configured as Multi-Region Fabric regions: cloud region 1 and cloud region 2. In each region, an interconnect gateway is brought up and configured as a border router. The border routers form the core region and have full-mesh connectivity.

An edge router in region 3 can connect to an edge router in region 4 by traversing the core overlay network. For example, E8 can connect to E11 by traversing the core overlay network.

In addition, in this deployment, cloud region 1 has a cloud gateway that acts as an edge router. It can connect to other edge routers within region 1 and also connect to the interconnect gateway or the border router that is assigned to the region.

Figure 30: Multi-Region Fabric Hybrid Deployment with SDCI as Backbone and Cloud Gateway as Edge Router



Workflow for Configuring Multi-Region Fabric with a Cloud Service Core Region

1. Enable Multi-Region Fabric, on page 16.
2. Create a region in a network hierarchy.
3. Create a site in a network hierarchy.
4. Attach devices to a site.

   In this procedure, when specifying the site ID for a device, you can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.
5. Assign regions to a Cisco Catalyst SD-WAN Controller using templates, on page 28.
6. Create a cloud gateway border router.

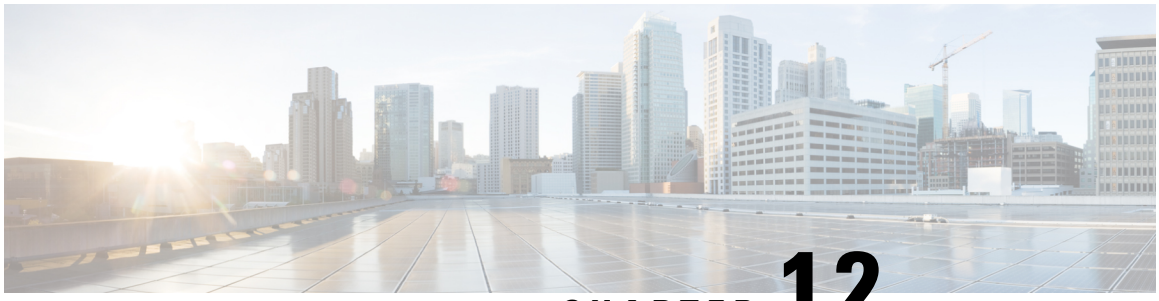
   Using Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud, create a cloud gateway in a public cloud service, and configure the **MRF Role** as **Border** router. For information about creating a cloud gateway in one of the supported public cloud services, such as AWS, Azure, or GCP, refer to the *Cisco Catalyst SD-WAN Cloud OnRamp Configuration Guide*.

7. If your topology includes Megaport, create an interconnect gateway at a Megaport location.

   Configure the **MRF Role** as **Border** router. For more information about creating an interconnect gateway at a Megaport location, refer to the *Cisco Catalyst SD-WAN Cloud OnRamp Configuration Guide*.



Note After creating a cloud gateway or an interconnect gateway, if you move a site from one region to another, it creates a mismatch between the current region and the configured region. This notification is generated on the **Configuration** > **Cloud onRamp for Multicloud** > **Gateway Management** page. To ensure that the current region and the configured region are the same, click **…** adjacent to the gateway name and choose **Push Configuration**.



CHAPTER 12

Multi-Region Fabric Policy

- Multi-Region Fabric Policy, on page 141
- Information About Configuring Policies for Multi-Region Fabric, on page 142
- Supported Devices for Multi-Region Fabric Policy Options, on page 149
- Restrictions for Multi-Region Fabric Policy Options, on page 149
- Multi-Region Fabric Use Cases, on page 150
- Configure Multi-Region Fabric Policy Using Cisco SD-WAN Manager, on page 151
- Configure Multi-Region Fabric Policy Using the CLI, on page 158

Multi-Region Fabric Policy

Table 22: Feature History

Feature Name	Release Information	Description
Match Traffic by Destination: Access Region, Core Region, or Service VPN	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can apply a policy to traffic whose destination is any one of the following—access region, core region, service VPN. Use this match condition for data policy or application route policy on a border router.
Match Routes According to Path Type	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	When configuring a control policy for a Multi-Region Fabric architecture, you can match routes according to whether the route uses a hierarchical path, a direct path, or a transport gateway path.
Match Routes by Region and Role in a Control Policy	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco Catalyst SD-WAN Control Components Release 20.8.1	In a control policy, you can match routes according to the region of the device originating the route, or the role (edge router or border router) of the device originating the route.

Feature Name	Release Information	Description
Match Traffic by Destination Region	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	When creating an application route policy or data policy, you can match traffic according to its destination region. The destination may be a device in the same primary region, the same secondary region, or neither of these.
Specify Path Type Preference	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco Catalyst SD-WAN Control Components Release 20.9.1	When configuring a centralized policy, you can create a preferred color group list, which specifies three levels of route preference, called primary, secondary and tertiary. The route preferences are based on TLOC color and, optionally, on the path type—direct tunnel, multi-hop path, or all paths. Path type is relevant to networks using Multi-Region Fabric.
Subregions in Policy	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Subregions are defined domains within access regions. You can specify subregions when creating region lists, configuring policies, and applying policies.
Enhancements to Match Conditions	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	When configuring match conditions for a policy, you can specify to match to all access regions, or to match according to a subregion.
Specify Path Type Preference with Restrict Mode	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Control Components Release 20.13.1	With this feature, the preferred color group action in app-route and data-policy has additional color-restrict option to restrict traffic to configured colors. With this option, if multitiered preferred colors are not available, the traffic is dropped.

Information About Configuring Policies for Multi-Region Fabric

Matching Routes by Path Type, Region, or Role

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

Path Type

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

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

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

- Direct path: Match direct paths (direct routes) from one edge router to another edge router. You can enable a direct path between edge routers in different access regions by configuring a secondary region, and adding the two edge routers to the secondary region. See Information About Secondary Regions, on page 68.

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

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

  For information about transport gateways, see Information About Transport Gateways, on page 91.

Region and Role

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

Matching Traffic-To

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

Background

In a flat, non-Multi-Region Fabric architecture, each edge router handles traffic flowing in one of the following ways:

- From a service VPN to the overlay network
- From a service VPN to a service VPN
- From the overlay network to a service VPN
- From the overlay network to the same overlay network

To target a traffic policy to one or the other of these types of traffic, you can use the **apply-policy** keyword when applying the traffic policy, as follows:

Table 23: Using apply-policy

Traffic Type	Use This Command
From a service VPN to the overlay network and From a service VPN to a service VPN	**apply-policy from-service**
From the overlay network to a service VPN and From the overlay network to the same overlay network	**apply-policy from-tunnel**

Multi-Region Fabric: Multiple Overlay Networks

With the introduction of the Multi-Region Fabric architecture and the border router role, a border router can handle traffic flowing from one overlay network to a different overlay network (access region to core region, or core region to access region). Border routers can handle traffic flowing in one of the following ways:

- From the access region to one of the following:
  - Access region
  - Core region
  - Service VPN
- From the core region to one of the following:
  - Access region
  - Core region
  - Service VPN
- From the service VPN to one of the following:
  - Access region
  - Core region
  - Service VPN

With more directions of traffic flows on a border router, the **apply-policy** options do not offer sufficient granularity. The **traffic-to** match criteria address this, enabling you to specify each of these types of traffic flow.

Match Criteria: Traffic-To

When creating a data policy or app-route policy for a border router, you can use the following match criteria to match traffic flowing to the access region, the core region, or a service VPN.

- **traffic-to access**: Matches all traffic flowing in one of the following ways:
  - From a service VPN to the access region
  - From the core region to the access region
  - From the access region to the access region
- **traffic-to core**: Matches all traffic flowing in one the following ways:
  - From a service VPN to the core region
  - From the access region to the core region
  - From the core region to the core region
- **traffic-to service**: Matches all traffic flowing in one the following ways:
  - From the access region to the service VPN

- From the core region to a service VPN
- From one service VPN to another service VPN

You can use these match conditions together with other match conditions that are not specific to Multi-Region Fabric, such as **prefix-list**, **site-list**, and so on.

Combining Match Conditions with the Apply-Policy Keyword

When applying the policy, you can use these match conditions, and use the **apply-policy** keyword when applying the policy to traffic as described in the following table.

Table 24: Traffic-To and Apply-Policy

Match Condition	apply-policy Keyword	Effect: The Policy Acts on the Following Traffic
match traffic-to access	**from-tunnel** (includes traffic from access and core regions)	From the access region to the access region and From the core region to the access region
	from-service (includes traffic from service VPN tunnels)	From a service VPN to the access region
	all (includes traffic from access and core regions, and from service VPN tunnels)	From the access region to the access region and From the core region to the access region and From a service VPN to the access region

Match Condition	apply-policy Keyword	Effect: The Policy Acts on the Following Traffic
match traffic-to core	**from-tunnel** (includes traffic from access and core regions)	From the core region to the core region and From the access region to the core region
	from-service (includes traffic from service VPN tunnels)	From a service VPN to the core region
	all (includes traffic from access and core regions, and from service VPN tunnels)	From the core region to the core region and From the access region to the core region and From a service VPN to the core region
match traffic-to service	**from-tunnel** (includes traffic from access and core regions)	From the core region to a service VPN and From the access region to a service VPN
	from-service (includes traffic from service VPN tunnels)	From a service VPN to a service VPN
	all (includes traffic from access and core regions, and from service VPN tunnels)	From the core region to a service VPN and From the access region to a service VPN and From one service VPN to another service VPN

Matching by Region and Role

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

When configuring a control policy, you can match routes and TLOCs according to the region of the device originating the route, or the role (edge router or border router) of the device originating the route. The originating device can be either an edge router or border router.



Note Only Cisco IOS XE Catalyst SD-WAN devices support the border router role.

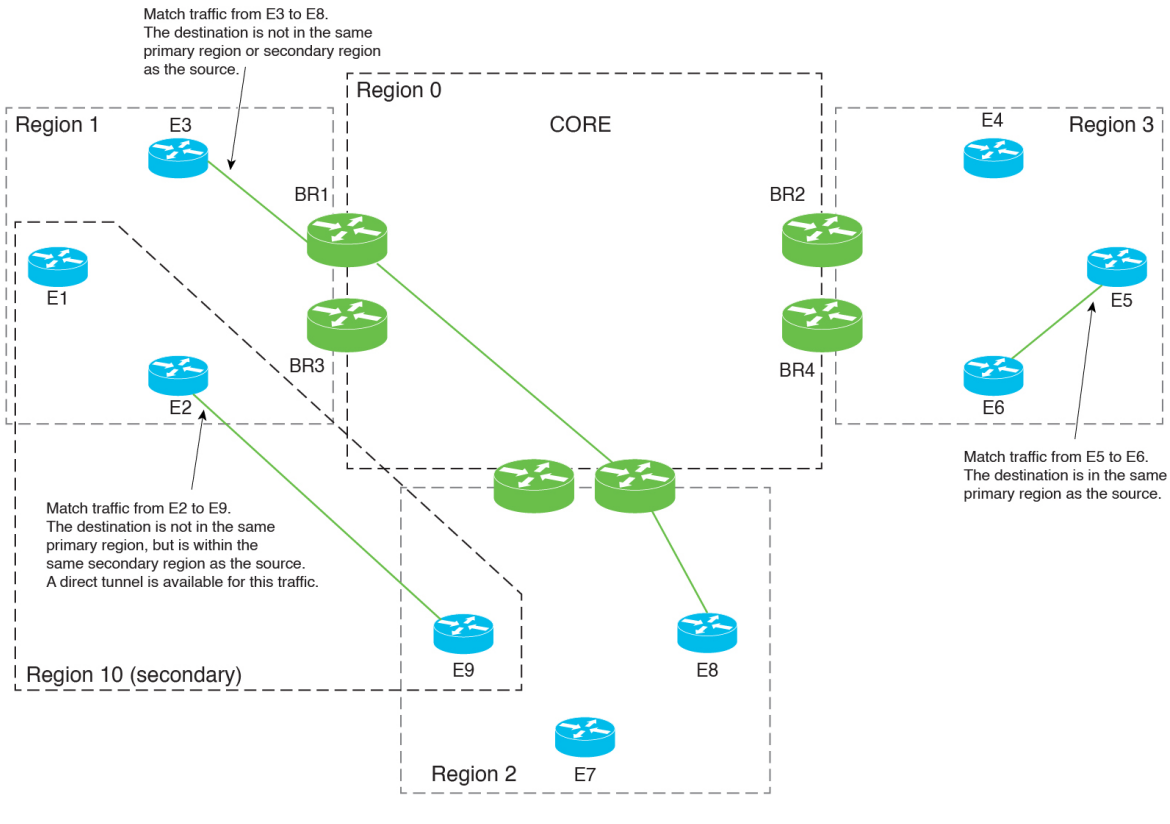
Information About Matching Traffic According to the Destination Region

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

When creating an application route policy or data policy, you can match traffic according to the region of the traffic's destination, with the following options:

- **Primary**: Match traffic if the destination device is in the same primary region (also called access region) as the source. This traffic reaches the destination using the access region bi-directional forwarding detection (BFD).
- **Secondary**: Match traffic if the destination device is not in the same primary region as the source but is within the same secondary region as the source. This traffic can reach the destination using a direct tunnel, as described for secondary regions.
- **Other**: Match traffic if the destination device is not in the same primary region or secondary region as the source. This traffic requires a multi-hop path from the source to the destination.

Figure 31: Match Traffic by Destination



Information About Configuring Path Preference

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

When configuring a centralized policy, you can create a preferred color group list, which specifies three levels of route preferences, called primary, secondary and tertiary. The route preferences are based on either or both of the following:

- TLOC color
- Path type (direct tunnel, multi-hop path, or all paths), which is relevant to networks using Multi-Region Fabric

When you configure an application-aware routing (AAR) policy or a traffic data policy, you can use the preferred color group list in the action portion of a sequence to specify how to route the matched traffic.

For complete information about configuring a policy list preference, refer to the information about configuring centralized policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

Sequence of Steps

1. Create a preferred color group list.
2. In the preferred color group list, specify the path preference—direct tunnel or multi-hop path.

3. Use the preferred color group list in an AAR policy or traffic data policy.

The result is that the policy applies the path preferences that you have configured in the preferred color group list.

Prioritization of Policy

When more than one policy applies to the same traffic, Cisco Catalyst SD-WAN prioritizes the policies as follows, beginning with the highest priority:

1. Policy that matches by a site list
2. Policy that matches by region and subregion
3. Policy that matches by a region list that includes a subregion
4. Policy that matches by a region that does not include a subregion
5. Policy that matches by a region list that does not include a subregion

Supported Devices for Multi-Region Fabric Policy Options

- Policy match conditions:
  - Match traffic-to: Cisco IOS XE Catalyst SD-WAN devices only
  - Match region: Cisco IOS XE Catalyst SD-WAN device and Cisco vEdge devices
  - Match role: Cisco IOS XE Catalyst SD-WAN device and Cisco vEdge device
  - Match by destination region: Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices

    (Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco SD-WAN Release 20.9.1
- Policy actions:
  - Path preference: Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices

    (Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco SD-WAN Release 20.9.1

Restrictions for Multi-Region Fabric Policy Options

- Match traffic-to: Use this match condition only on policies applied to border routers. Applying such a policy to an edge router has no effect.
- Path preference: When creating a policy for a network that does not use Multi-Region Fabric, either do not define a path preference, or choose the option to use all paths, which is equivalent to not defining a path preference.

Multi-Region Fabric Use Cases

The following are use cases for Multi-Region Fabric policy features.

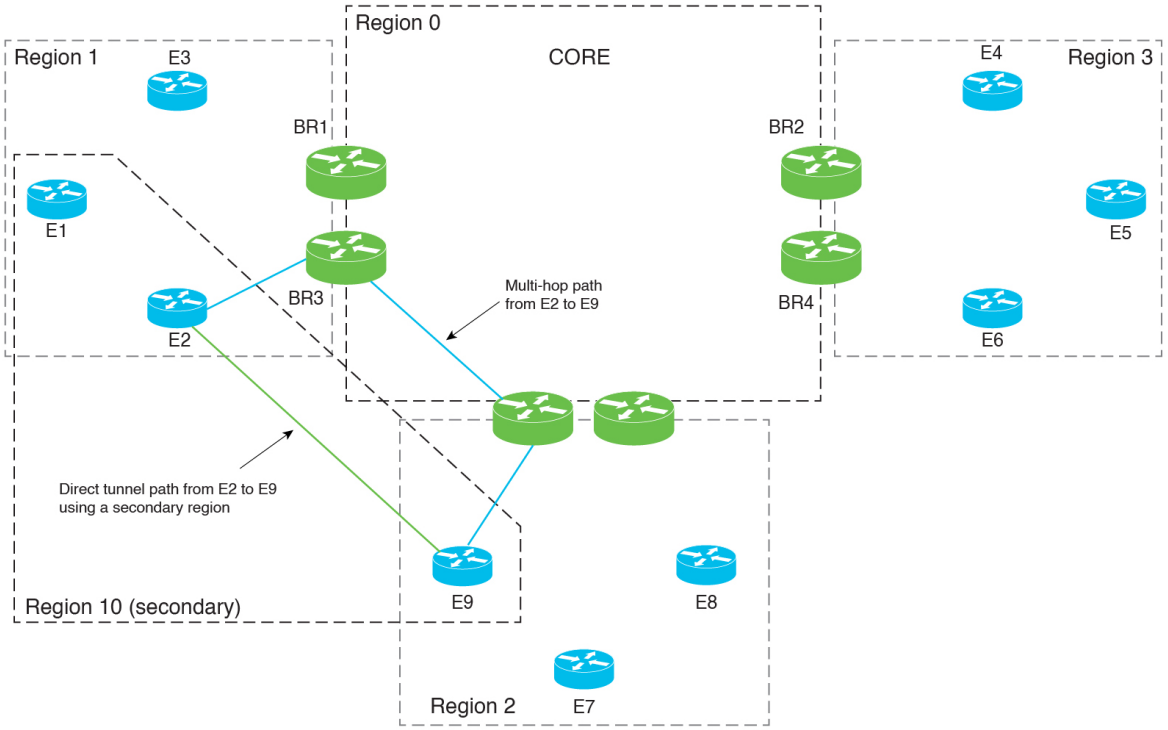
Use Cases for Configuring Path Preference

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

An organization using a Multi-Region Fabric network has configured a secondary region to enable a direct tunnel path between two edge routers in different primary regions.

Traffic between the two edge routers can use the multi-hop path through the core region, or use the direct tunnel path that is made possible by the secondary region. The direct path is intended for critical traffic. It uses a premium carrier, and there is a charge based on traffic volume over this path.

Figure 32: Multi-Hop Path and Direct Tunnel Path



To create a policy that preferentially routes only critical traffic through the direct path, the network administrator creates two preferred color group lists, A and B:

- Preferred color group list A is intended for non-critical traffic. It specifies a primary preference for the multi-hop path. Its secondary preference specifies the direct tunnel path. Including the secondary preference provides a backup path in case the multi-hop path is not available.
- Preferred color group list B is intended for critical traffic. It specifies a primary preference for the direct tunnel path, the premium link that incurs a toll. Its secondary preference specifies the multi-hop path. This provides a backup path in case the direct tunnel path is not available.

The network administrator creates an application routing policy with two sequences:

- Sequence 1 matches the non-critical traffic, and for its action, applies preferred color group list A.
- Sequence 2 matches the critical traffic, and for its action, applies preferred color group list B.

Configure Multi-Region Fabric Policy Using Cisco SD-WAN Manager

Configure a Data Policy or Application Route Policy to Match Traffic-To Using Cisco SD-WAN Manager

Before You Begin

Configure a VPN list to use when applying the policy.

Configure a Data Policy or Application Route Policy to Match Traffic-To

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policies**.
3. Do one of the following:
   - To create a new policy, click **Add Policy**.
   - To edit an existing policy, click **…** in the row of the policy and click **Edit Policy**.
4. Click **Next**.
5. Click **Next**.
6. Click one of the following to create a traffic policy:
   - **Application Aware Routing**
   - **Traffic Data**
7. Click **Add Policy** and choose **Create New**.

Note To reuse an existing policy, you can choose **Import Existing**.

8. Enter a name and description for the new policy.
9. Click **Sequence Type** and choose **Custom**.
10. Click **Sequence Rule**.
11. Click **Match** (selected by default) and click **Traffic To**.

12. In the **Match Conditions** area, in the **Traffic To** field, choose one of the following:
    - **Access**
    - **Core**
    - **Service**
13. Choose an action for the sequence and complete the configuration of the policy.

    For information about creating traffic policies in general, refer to the *Cisco Catalyst SD-WAN Policies Configuration Guide*.
14. To save the policy, click **Save Application Aware Routing Policy** or **Save Data Policy**, depending on the type of policy that you are creating. A table shows the new policy.
15. Click **Next**.
16. At the **Apply Policies to Sites and VPNs** step, enter the name of the policy to apply.
17. Click one of the following, depending on the type of policy that you are creating and applying:
    - **Application-Aware Routing**
    - **Traffic Data**
18. Click **New Site/Region List and VPN List**.
19. If you are configuring a traffic data policy, choose one of the following options:
    - **From Service**
    - **From Tunnel**
    - **All**
20. Choose one of the following options to configure the sites or Multi-Region Fabric regions to which to apply the policy:
    - **Site List**: Enter a site list.
    - **Region**: Enter a Multi-Region Fabric region ID or select a region list.
21. If you are configuring a data policy, do the following:
    a. In the **Select VPN List** field, choose a VPN list.
    b. Click **Add**.
22. Click **Role Mapping for Regions**.
23. For each region ID or region list, in the **Role** column, choose a role of **Edge** or **Border**. If you do not choose a role, Cisco SD-WAN Manager applies the policy to all routers in the region.



Note For policies that match by Traffic-To, choose **Border**. This match condition has no effect on edge routers.

24. Click **Save Policy**. A table shows the new policy. Optionally, to view the details of the policy, in the row of the policy, click **…** and choose **Preview**.

Configure a Control Policy to Match Region and Role Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policies**.
3. Do one of the following:
   - To create a new policy, click **Add Policy**.
   - To edit an existing policy, click **…** in the row of the policy and click **Edit Policy**.
4. Click **Next**.
5. In the **Configure Topology and VPN Membership** step, click **Add Topology** and choose **Custom Control (Route & TLOC)**.
6. Enter a name and description for the new policy.
7. Click **Sequence Rule**.
8. Click **Match** (selected by default) and click **Region**.
9. In the **Match Conditions** area, do one of the following:
   - In the **Region List** field, enter a preconfigured region list name.



Note You can click the field and choose **New Region List** to define a list.

   - In the **Region ID** field, enter a single region ID.
10. (Optional) To specify a router type within the configured regions, click **Role** and choose **Border** or **Edge**.
11. Choose an action for the sequence and complete the configuration of the policy.

    For information about creating traffic policies in general, refer to the *Cisco Catalyst SD-WAN Policies Configuration Guide*.
12. To save the policy, click **Save Control Policy**. A table shows the new policy.
13. Click **Next**.
14. At the **Apply Policies to Sites and VPNs** step, enter the name of the policy to apply
15. Click **Topology**.
16. Click **New Site/Region List**.

17. Choose one of the following options to configure the sites or Multi-Region Fabric regions to which to apply the policy:
    - **Site List**: Enter a site list.
    - **Region**: Enter a Multi-Region Fabric region ID or select a region list.
18. Click **Role Mapping for Regions**.
19. For each region ID or region list, in the **Role** column, choose a role of **Edge** or **Border**. If you do not choose a role, Cisco SD-WAN Manager applies the policy to all routers in the region.



Note For policies that match by Traffic-To, choose **Border**. This match condition has no effect on edge routers.

20. Click **Save Policy**. A table shows the new policy. Optionally, to view the details of the policy, in the row of the policy, click **…** and choose **Preview**.

Match Traffic According to the Destination Region Using Cisco SD-WAN Manager

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

For complete information about configuring an application-aware routing (AAR) policy or traffic data policy, refer to the information about configuring centralized policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide*. The information here only addresses how to use the **Destination Region** match condition.

Use the following procedure for an application-aware policy or a traffic data policy.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Choose **Centralized Policy**, which is selected by default.
3. Click **Add Policy**.
4. Optionally, you can click a list type and define a list.
5. Click **Next**.
6. Optionally, add a topology.
7. Click **Next**.
8. Do one of the following:
    - For an AAR policy, click **Application Aware Routing**, which is selected by default.
    - For a traffic data policy, click **Traffic Data**.
9. Click **Add Policy** and select **Create New**.
10. Do one of the following:
    - For an AAR policy, click **Sequence Type** to create a sequence that matches traffic by destination.

- For a traffic data policy, click **Sequence Type** and choose **Custom** to create a sequence that matches traffic by destination.

11. Click **Sequence Rule** to create a new rule for the sequence.
12. With the **Match** option selected, click **Destination Region** to add this option to the match conditions area of the sequence rule.
13. In the **Match Conditions** area, click the **Destination Region** field and choose one of the following:
    - **Primary**: Match traffic if the destination device is in the same primary region (also called access region) as the source. This traffic reaches the destination using the access-region bidirectional forwarding detection (BFD).
    - **Secondary**: Match traffic if the destination device is not in the same primary region as the source but is within the same secondary region as the source. This traffic can reach the destination using a direct tunnel, as described for secondary regions.
    - **Other**: Match traffic if the destination device is not in the same primary region or secondary region as the source. This traffic requires a multi-hop path from the source to the destination.
14. Continue to configure the policy as described in the instructions for configuring centralized policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

Configure the Path Preference for a Preferred Color Group List Using Cisco SD-WAN Manager

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

For complete information about configuring an application-aware routing (AAR) policy, refer to the information about configuring centralized policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide*. The information here only addresses how to configure a path preference as part of a preferred color group.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**, and choose **Centralized Policy**.
2. Click **Add Policy**.
3. Click **Application List**, which is selected by default.
4. Click **Preferred Color Group**.
5. Click **New Preferred Color Group**.
6. Configure the following fields:

Field	Description
Preferred Color Group Name	Enter a name for the color group.
Primary Colors: **Color Preference**	Click the field and select one or more colors for the primary preference.

Field	Description
Primary Colors: **Path Preference**	Click the drop-down list and choose one of the following for the primary preference: • **Direct Path**: Use only a direct path between the source and the destination devices. **Note** Do not use this option in a non-Multi-Region Fabric network. • **Multi Hop Path**: In a Multi-Region Fabric network, use a multi-hop path, which includes the core region, between the source and destination devices, even if a direct path is available. • **All Paths**: Use any path between the source and destination devices. **Note** This option is equivalent to not configuring path preference at all. If you are applying the policy to a non-Multi-Region Fabric network, use this option.
Secondary Colors: **Color Preference** **Path Preference**	Configure the secondary preference using the same method as for the **Primary Colors** options.
Tertiary Colors: **Color Preference** **Path Preference**	Configure the tertiary preference using the same method as for the **Primary Colors** options.

Use a Preferred Color Group in a Policy

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

For complete information about configuring policies, refer to the information about configuring centralized policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide*. The information here only addresses how to use the **Preferred Color Group** action, which incorporates path preference.

Use the following procedure for an application-aware policy or a traffic data policy.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Add Policy**.
3. Choose **Centralized Policy**, which is selected by default.

4. Click **Add Policy**.
5. Optionally, you can click a list type and define a list.
6. Click **Next**.
7. Optionally, add a topology.
8. Click **Next**.
9. Do one of the following:
   - For an AAR policy, click **Application Aware Routing**, which is selected by default.
   - For a traffic data policy, click **Traffic Data**.
10. Click **Add Policy** and select **Create New**.
11. Do one of the following:
    - For an AAR policy, click **Sequence Type** to create a sequence that matches traffic by destination.
    - For a traffic data policy, click **Sequence Type** and choose **Custom** to create a sequence that matches traffic by destination.
12. Click **Sequence Rule** to create a new rule for the sequence.
13. Click **Actions**.
14. For an AAR policy, do one of the following:
    a. Click **SLA Class List**.
    b. Click the **Preferred Color** and choose a preferred color.

    Or

    a. Click **SLA Class List**.
    b. Click the **Preferred Color Group** and choose a preferred color group.
    c. The **Restrict to Preferred Color Group** option is available from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a. Enable **Restrict to Preferred Color Group** option to drop the traffic if none of the color in **Preferred Color Group** is available. If a restriction is configured in both data policy and application-route policy, then data policy has higher priority compared to application route policy.



Note **Preferred Color** and **Preferred Color Group** options are mutually exclusive. The **Restrict to Preferred Color Group** field is available only for the **Preferred Color Group** option.

15. For an traffic control policy, do the following:
    a. Click **Accept**.
    b. Click **Preferred Color Group**.
    c. Click the **Preferred Color Group** field and choose a preferred color group.

Configure Multi-Region Fabric Policy Using the CLI

Match Routes According to Path Type Using the CLI

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

Before You Begin

This procedure applies to a Multi-Region Fabric architecture.

For background information about matching by path type, refer to Matching Routes by Path Type, Region, or Role, on page 71.

For general information about using matching parameters in control policies, refer to the information about matching parameters in a control policy in *Cisco Catalyst SD-WAN Policies Configuration Guide*.

Match Routes According to Path Type

In a control policy, use **path-type** to match routes according to the path type.

```
match route path-type {hierarchical-path | direct-path | transport-gateway-path}
```

Example

This example contains two control policy sequences that do the following:

- Sequence 1 matches routes that use a hierarchical path from one edge router to another edge router. It configures a policy action of **accept**, a preference value for the routes, and an omp tag of 100.
- Sequence 2 matches routes that use a direct path from one edge router to another edge router. It configures a policy action of **accept** and an omp tag of 200.

```
policy
 control-policy control_policy_A
   sequence 1
    match route
     path-type hierarchical-path
    !
    action accept
     set
      preference 200
      omp-tag 100
     !
    !
   !
sequence 2
    match route
     path-type direct-path
    !
    action accept
     set
      omp-tag 200
    !
   !
  !
  default-action reject
```

```
 !
!
```

Match Routes According to Region and Role Using the CLI

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

Before You Begin

This procedure applies to a Multi-Region Fabric architecture.

For background information about matching by path type, see Matching Routes by Path Type, Region, or Role, on page 71.

For general information about using matching parameters in control policies, refer to the information about matching parameters in a control policy in *Cisco Catalyst SD-WAN Policies Configuration Guide*.

Match Routes According to Region and Role

In a control policy, use **region** to match routes that are originated by a device that is in a specific region. Optionally, you can include the **role** keyword to match according to the role of the originating device.

match route region {*region-id* | *region-list*} [**role** {**border-router** | **edge-router**}]

Example

The following **match** statement matches routes that originate from edge routers in region 1.

```
match route region 1 role edge-router
```

Create a Region List Using a CLI Template

For more information about using CLI templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*. By default, CLI templates execute commands in global configuration mode.

1. On a Cisco SD-WAN Controller, create the region list.

   policy lists region-list *region-list-name*

2. Repeat the following command for each region that you want to add to the region list.

   The **subregion** option is available from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Subregions are applicable only to access regions, not the core region (region 0).

   region-id *region-id* [**subregion-id** *subregion-id*]

Examples

The following example creates a region list called region_list_a that includes regions 1, 2, and 3.

```
policy
 lists
  region-list region_list_a
   region-id 1
   region-id 2
   region-id 3
  !
```

```
 !
!
```

The following example creates a region list called region_list_b that includes the following:

- Devices in regions 1 to 3
- Devices in subregions 1 to 4 of region 10
- Devices in subregions 1 to 5 of regions 4 to 6

```
policy
 lists
  region-list region_list_b
   region-id 1-3
   region-id 10 subregion-id 1-4
   region-id 4-6 subregion-id 1-5
  !
 !
!
```

Configure a Data Policy or Application Route Policy to Match Traffic-To Using a CLI Template

For more information about using CLI templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*. By default, CLI templates execute commands in global configuration mode.

Before You Begin

Creating a policy is not specific to Multi-Region Fabric, but the **match traffic-to** condition is specifically a Multi-Region Fabric feature. Use **match traffic-to** only for policies applied to border routers.

For complete information about policies, refer to the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

Configure a Data Policy or Application Route Policy to Match Traffic-To

When configuring a data policy or application route policy, configure the match condition.

policy {**app-route-policy** | **data-policy** } *policy-name* **vpn-list** *vpn-list-name* **sequence** *sequence-number* **match traffic-to** {**access** | **core** | **service**}

Example 1

The following example creates a data policy that matches traffic flows to the access region, and applies the policy to region 1 border routers. The example includes the **apply-policy** command, and the **from-tunnel** keyword refines the target of the policy to address traffic flowing in either of the following ways:

- The access region to the access region
- The core region to the access region

```
policy data-policy data_policy_a vpn-list vpn1 sequence 1 match traffic-to access
apply-policy region 1 role border-router data-policy data_policy_a from-tunnel
```

Configure a Control Policy to Match Region and Role Using a CLI Template

For more information about using CLI templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*. By default, CLI templates execute commands in global configuration mode.

Before You Begin

- This procedure configures a control policy that matches routes or TLOCs according to region, and optionally according to role (border router or edge router) also. If you do not specify a role, the policy applies to routers of both roles.

  For example, you can create a policy that matches all the TLOCs of edge routers in region 1.

- The **region** and **role** match conditions are specific to Multi-Region Fabric architectures, but the policy can include match conditions that are not related to Multi-Region Fabric.

- To use the **region-list** option, create a region list first. For information about creating a region list, see Create a Region List Using a CLI Template, on page 159.

Configure a Control Policy to Match Region and Role

Configure the control policy on a Cisco SD-WAN Controller. When configuring a control policy, match specific regions, and optionally the device role.

The **subregion** and **region-enhanced** options are available from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Subregions are applicable only to access regions, not the core region (region 0).

```
policy control-policy policy-name sequence sequence-number match {route | tloc} {region
region-id | region-list region-list-name} [role {border-router | edge-router}]
```

Examples

The following example applies the policy_a control policy to region_list_a.

```
policy
 control-policy policy_a
  sequence 1
   match route
    region-list region_list_a
    role border-router
   !
  !
!
```

The following example defines the policy_cp control policy for the core region (region 0). Note that subregions are not relevant to the core region.

```
policy
 control-policy policy_cp
  sequence 1
   match route
    region-enhanced region core
   !
   action reject
   !
  !
  default-action accept
 !
!
```

The following example defines the policy_cp control policy for subregion 1 of all access regions.

```
policy
 control-policy policy_cp
  sequence 1
   match route
    region-enhanced region any-access
    region-enhanced subregion 1
   !
   action reject
   !
  !
  default-action reject
 !
!
```

The following example defines the policy_cp control policy for region 5, subregion 2.

```
policy
 control-policy policy_cp
  sequence 1
   match route
    region-enhanced region 5
    region-enhanced subregion 2
   !
   action reject
   !
  !
  default-action reject
 !
!
```

Apply a Policy Using a CLI Template

For more information about using CLI templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*. By default, CLI templates execute commands in global configuration mode.

After configuring a policy, use the **apply-policy** command to apply the policy to devices. There are several options that relate to Multi-Region Fabric, including the ability to specify a region, subregion, region list, and role (border router or edge router).

For complete information about policies, refer to the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

The **subregion** option is available from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.

Note The **role** keyword can also specify an edge-router, but use **match traffic-to** only for policies applied to border routers.

Apply a Policy

Use the **apply-policy** command to apply a policy.

```
apply-policy {region region-id [subregion subregion-id] | region-list | site-list}
 [role {border-router | edge-router}] [data-policy policy-name {from-tunnel |
 from-service | all}
```

Example 1

The following example applies a data policy called data_policy_a to region 1 border routers. The **from-tunnel** keyword refines the target of the policy to address traffic flowing in either of the following ways:

- The access region to the access region
- The core region to the access region

```
apply-policy
 region 1
 role border-router
 data-policy data_policy_a
 from-tunnel
```

Example 2

The following example applies a data policy to region 1, subregion 1.

```
apply-policy
 region 1
  subregion 1
  data-policy data_policy_s from-tunnel
 !
!
```

Match Traffic According to the Destination Region Using the CLI

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

Within an application route policy or data policy, use the **destination-region** keyword to match traffic according to its destination region.

1. Create an application route policy or data policy.

   app-route-policy *policy-name*

   or

   data-policy *policy-name*

2. Specify a VPN or VPN list.

   vpn *vpn-id*

   or

   vpn-list *vpn-list-name*

3. Create a sequence.

   sequence *sequence-number*

4. Within the sequence, create a match condition.

   match

5. Enter the details of the match condition.

   dscp *dscp-id*
   destination-region {**primary** | **secondary** | **other**}

The following is a sample application route policy that includes sequences for each of three different **destination-region** types: **primary**, **secondary**, and **other**.

```
app-route-policy SAMPLE_HSDWAN_AAR
 vpn-list ONE
  sequence 10
   match
    dscp 46
    destination-region primary
   !
   action
    sla VOICE_SLA strict preferred-color-group GROUP2_COLORS
   !
  !
  sequence 20
   match
    dscp 46
    destination-region secondary
   !
   action
    sla VOICE_SLA preferred-color-group GROUP1_COLORS
   !
  !
  sequence 30
   match
    dscp 46
    destination-region other
   !
   action
    sla VOICE_SLA preferred-color-group GROUP1_COLORS
   !
  !
 !
!
```

The following is a sample data policy that includes sequences for each of three different **destination-region** types: **primary**, **secondary**, and **other**.

```
data-policy SAMPLE_HSDWAN_DATA
 vpn-list ONE
  sequence 10
   match
    dscp 46
    destination-region primary
   !
   action
    set
     preferred-color-group GROUP2_COLORS
   !
  !
  sequence 20
   match
    dscp 46
    destination-region secondary
   !
   action
    set
     preferred-color-group GROUP1_COLORS
   !
  !
  sequence 30
   match
    dscp 46
    destination-region other
```

```
    !
    action
     set
      preferred-color-group GROUP1_COLORS
    !
   !
  !
!
```

Configure the Path Preference for a Preferred Color Group List Using the CLI

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

1. Configure a new policy list.

   policy
   lists

2. Create a preferred color group list.

   preferred-color-group *group-name*

3. Configure the primary preferences.



Note There are primary, secondary, and tertiary preferences.

   primary-preference

4. Configure the color preference for the primary preference.



Note For a complete list of color options, see the Cisco Catalyst SD-WAN documentation. Options include default, 3g, biz-internet, blue, bronze, custom1, custom2, custom3, gold, green, lte, metro-ethernet, mpls, private1, private2, private3, private4, private5, private6, public-internet, red, and silver.

   color-preference *color-option*

5. Configure the path preference for the primary preference.

   path-preference {**direct-path** | **multi-hop-path** | **all-paths**}

6. Exit the primary-preference configuration.

   exit

7. Repeat steps 3 to 6 for the secondary-preference and tertiary-preference, using **secondary-preference** and **tertiary-preference**.

Example: Configure the Path Preference in a Preferred Color Group

In the following preferred color group configuration, the GROUP1_COLORS color group has a primary preference that specifies **direct-tunnel**. The secondary preference specifies **multi-hop-path**. When you use GROUP1_COLORS in a policy, the policy will favor a direct tunnel path over a multi-hop path.

```
policy
 lists
  preferred-color-group GROUP1_COLORS
   primary-preference
    color-preference internet
    path-preference direct-tunnel
   !
   secondary-preference
    color-preference mpls
    path-preference multi-hop-path
   !
   tertiary-preference
    color-preference lte
   !
  !
  preferred-color-group GROUP2_COLORS
   primary-preference
    color-preference mpls
   !
   secondary-preference
    color-preference internet
   !
   !
   preferred-color-group GROUP3_COLORS
   primary-preference
    color-preference mpls internet lte
   !
    !
    !
```

Example: Use the Path Preference in an AAR Policy

The following AAR policy uses the preceding preferred color group configuration. For each of the three sequences, the action specifies a preferred color group, such as GROUP1_COLORS, GROUP2_COLORS, or GROUP3_COLORS. For example, sequence 20 applies the GROUP1_COLORS color group, which has a primary preference for a direct tunnel and a secondary preference for a multi-hop path. The color-restrict option example is shown for sequence 30.

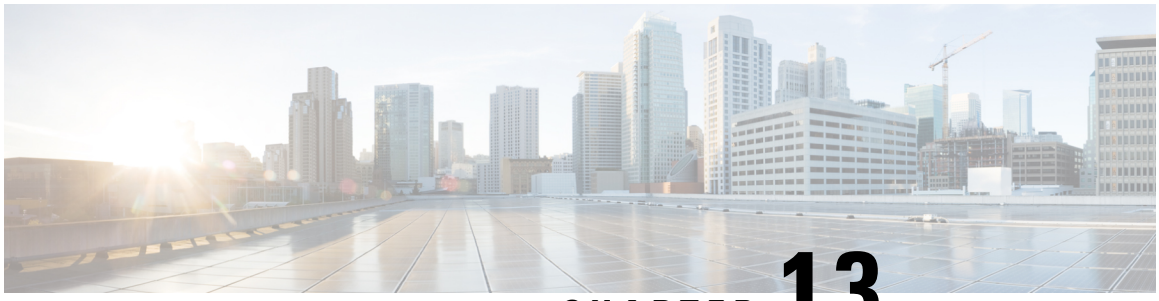
```
app-route-policy SAMPLE_HSDWAN_AAR
 vpn-list ONE
  sequence 10
   match
    dscp 46
   !
   action
    sla VOICE_SLA strict preferred-color-group GROUP2_COLORS
   !
  !
  sequence 20
   match
    dscp 34
   !
   action
    sla VOICE_SLA preferred-color-group GROUP1_COLORS
   !
  !
app-route-policy Rank-Color-Restrict-AARP
vpn-list VPN-1
sequence 30
match
dscp 28
destination-ip 192.168.255.254/32
!
```

```
action
sla-class Default preferred-color-group PCG1
sla-class Default preferred-color-group-options color-restrict
!
!
```

Example: Use the Path Preference in a Traffic Data Policy

The following data policy uses the same preferred color group configuration described earlier in this section. As with the application route policy above, sequence 20 in this data policy applies the GROUP1_COLORS color group, which has a primary preference for a direct tunnel and a secondary preference for a multi-hop path. The color-restrict option example is shown for sequence 30.

```
data-policy SAMPLE_HSDWAN_DATA
 vpn-list ONE
  sequence 10
   match
    dscp 46
   !
   action
    set
     preferred-color-group GROUP2_COLORS
   !
  !
  sequence 20
   match
    dscp 34
   !
   action
    set
     preferred-color-group GROUP1_COLORS
   !
  !
  sequence 30
   match
    dscp 28
   !
   action
    set
     preferred-color-group GROUP3_COLORS
     preferred-color-group-options color-restrict
   !
  !
 !
!
```



CHAPTER 13

Route Aggregation on Border Routers and Transport Gateways

- Route Aggregation on Border Routers and Transport Gateways, on page 169
- Information About Route Aggregation on Border Routers and Transport Gateways, on page 169
- Supported Platforms for Route Aggregation on Border Routers and Transport Gateways, on page 172
- Use Cases for Route Aggregation on Border Routers and Transport Gateways, on page 173
- Configure Route Aggregation on Border Routers and Transport Gateways Using Cisco SD-WAN Manager, on page 173
- Configure Route Aggregation on Border Routers and Transport Gateways Using a CLI Template, on page 175

Route Aggregation on Border Routers and Transport Gateways

Table 25: Feature History

Feature Name	Release Information	Description
Route Aggregation on Border Routers and Transport Gateways	Cisco Catalyst SD-WAN Control Components Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This feature enables you to configure route aggregation on border routers and transport gateways in a Multi-Region Fabric network environment. For a border router, you can specify whether the route aggregation operates only for the core region, the router's access region, or both.

Information About Route Aggregation on Border Routers and Transport Gateways

Minimum releases: Cisco Catalyst SD-WAN Control Components Release 20.11.x, Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

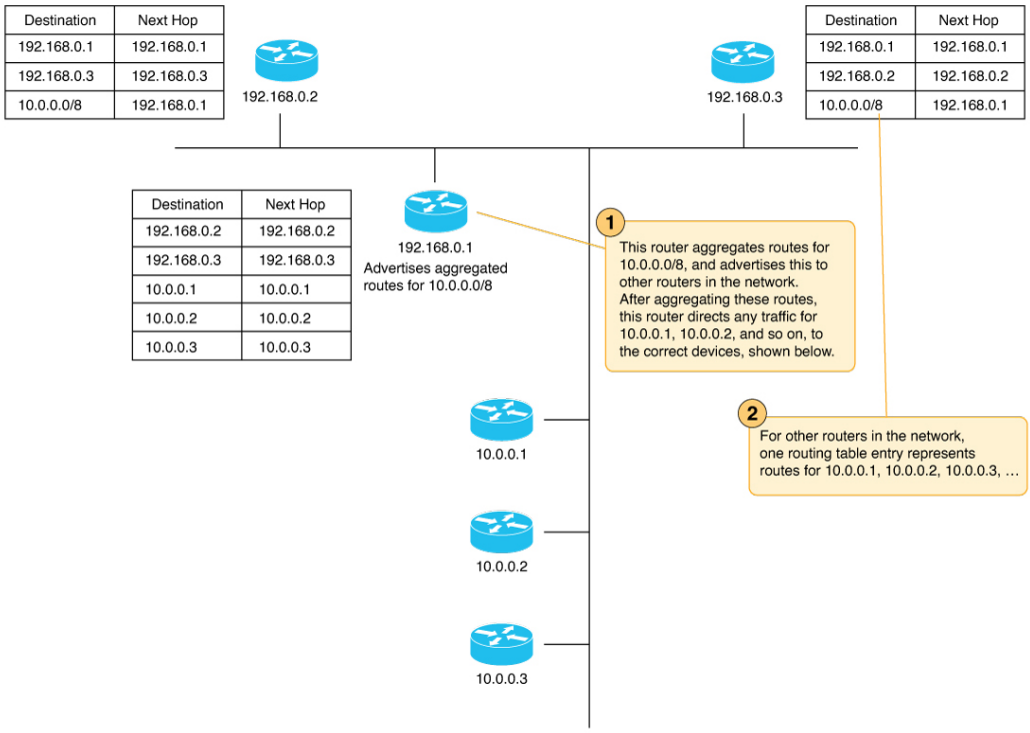
Route aggregation is a method for reducing the number of entries that routers in a network must maintain in routing tables, for better scaling. In some enterprise settings, the number of routes available to a device might reach the thousands. Storing this number of entries in the routing tables of devices in the network may require excessive resources on each device, and can reduce network performance.

To reduce the demand on router resources, and improve network performance, you can configure a router in the network to manage a range of IP addresses using a networking method called route aggregation, which works as follows:

- Configure a router to advertise to the network a single prefix that represents a range of IP addresses. Provide the prefix in classless inter-domain routing (CIDR) notation. For example, 10.0.0.0/8 includes all addresses from 10.0.0.1 to 10.255.255.254.
- Other routers in the network only require a single routing table entry for this prefix, which aggregates a range of IP addresses.
- When a router in the network receives traffic for a route represented by an IP address in the aggregated range, the router directs the traffic to the device handling that range of addresses.

In this manner, route aggregation can significantly reduce the size of routing tables on devices in the network.

Figure 33: Route Aggregation



Note the following behaviors regarding route aggregation:

- An aggregating device advertises the aggregate prefix only if a component route within the prefix range is available.
- By default, an aggregating router advertises each individual route and the summary prefix. You can use an aggregate-only option to advertise only the summary prefix and not each individual route.

Route Aggregation with Multi-Region Fabric and Transport Gateways

Releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.11.1a support configuring aggregation for OMP routes. This includes configuring aggregation for edge routers in access regions of a network using Multi-Region Fabric. Cisco IOS XE Catalyst SD-WAN Release 17.11.1a adds support for using route route aggregation with border routers (with the option to advertise routes to either the access region or core region) and transport gateways.

When you configure route aggregation on a border router or transport gateway, the aggregation includes even routes that the device reoriginates. For example, if you configure a border router to aggregate routes defined by the prefix 10.0.0.0/8, the aggregation applies to the route 10.0.0.20, even if that is a route that the border router is reoriginating.

For more information about route aggregation, refer to the information about configuring OMP in the *Cisco Catalyst SD-WAN Routing Configuration Guide*.

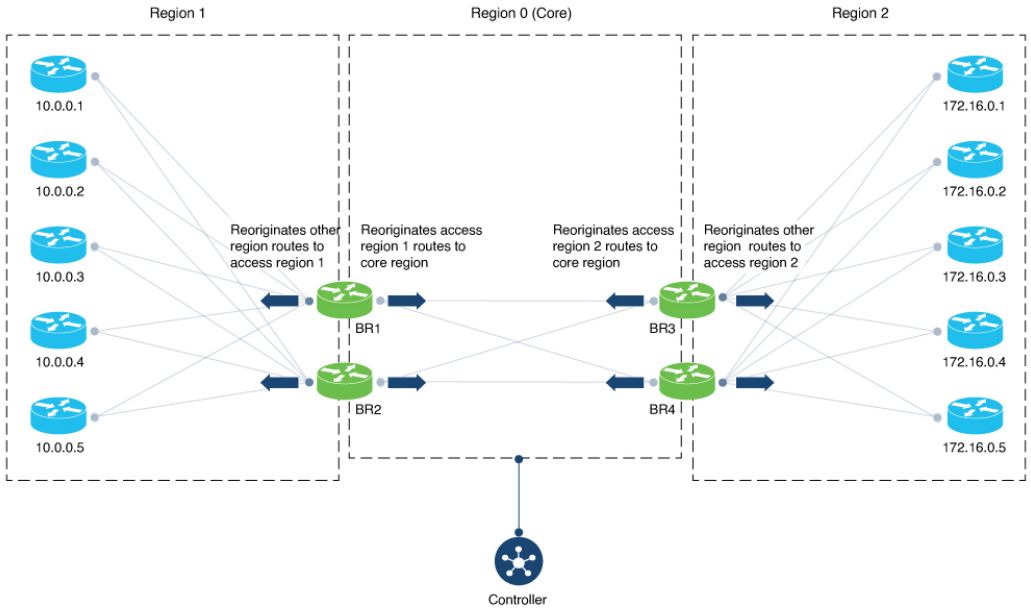
Reorigination of Routes by a Border Router

By the nature of the Multi-Region Fabric network topology, a border router functions as a gateway to routers in the access region that it serves to reach other Multi-Region Fabric regions. To do this, the border router reoriginates routes of devices in its access region to the core region, and similarly reoriginates routes from the core region to the access region. As the number of routers in the access or core region grows, the number of routes that the border router reoriginates grows too.

Each route that a border router reoriginates to the core region creates an additional resource demand on all of the border routers in the core region. The following simplified illustration shows a few important points:

- As the number of routes in an access region grows, the number of routes that the border router for that region readvertises grows.
- Each border router for a region reoriginates the same set of routes as other border routers in the region, so the number of readvertised routes multiplies with each new border router.
- As the number of readvertised routes grows, the resource demands grow for the Cisco SD-WAN Controllers serving the core region.

Figure 34: Reorigination of Routes in a Multi-Region Fabric Network



IPv6 Support

Route aggregation supports IPv4 and IPv6 addresses.

Benefits of Route Aggregation on Border Routers and Transport Gateways

Configuring a border router to perform route aggregation reduces the need to readvertise all routes individually in the core region. Reoriginating fewer individual routes alleviates resource demands on border routers and Cisco SD-WAN Controllers.

Similarly, you can configure route aggregation for an edge router operating as a transport gateway. The benefits do not apply specifically to the core region, but as with all route aggregation, the result is to reduce demands on router resources by minimizing the size of routing tables.

Supported Platforms for Route Aggregation on Border Routers and Transport Gateways

Minimum releases: Cisco Catalyst SD-WAN Control Components Release 20.11.x, Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

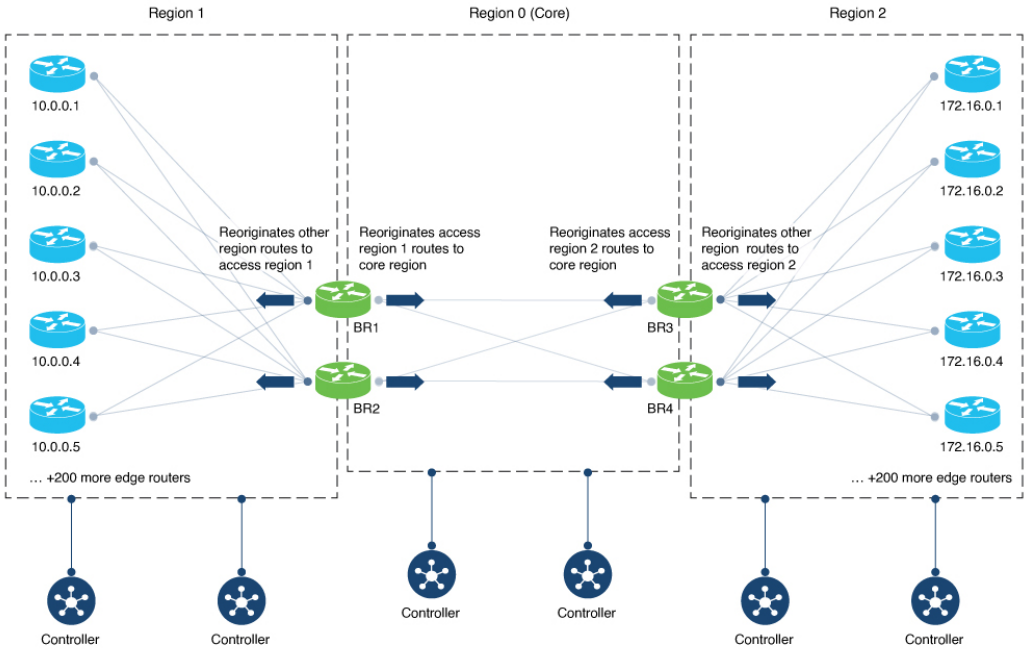
Cisco IOS XE Catalyst SD-WAN devices

Use Cases for Route Aggregation on Border Routers and Transport Gateways

Minimum releases: Cisco Catalyst SD-WAN Control Components Release 20.11.x, Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

An organization using Multi-Region Fabric has a large number of edge routers in two access regions, with two Cisco SD-WAN Controllers managing each access region and the core region. The large number of routes reoriginated by each of two border routers for each access region strain the resources of the Cisco SD-WAN Controllers for the core region.

Figure 35: Route Aggregation on Border Routers



To reduce the number of routes reoriginated in the core region, configure border routers BR1 and BR2 to aggregate the routes for the 200+ edge routers in region 1. Configure the border routers BR3 and BR4 to aggregate the routes for the 200+ edge routers in region 2.

Configure Route Aggregation on Border Routers and Transport Gateways Using Cisco SD-WAN Manager

Minimum releases: Cisco Catalyst SD-WAN Control Components Release 20.11.x, Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

Before You Begin

When configuring route aggregation for a border router, ensure that the VPN template in the procedure that follows is attached to the device template of a border router. If not, the **core** and **access** options that occur in the procedure are not available.

For information about configuring a device as a border router, see Assign a Role and Region to a Device Using Cisco SD-WAN Manager, on page 24.

Configure Route Aggregation on Border Routers and Transport Gateways

1. If you do not have a VPN template attached to the device template of the border router that you are configuring, do the following to create a VPN template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**.
   c. Click **Add Template**.
   d. Choose the device type of the border router.
   e. Choose the VPN template.
   f. In the **Template Name** and **Description** fields, enter a name and description for the template.
   g. Click **Save** to save the template.
   h. Attach the VPN template to the border router device template for the border router you are configuring, or to the device template of the transport gateway router you are configuring.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
3. Click **Feature Templates**.
4. Locate the VPN template that is attached to the border router you are configuring. Adjacent to the VPN template, click **…** and choose **Edit**.
5. In the **Advertise OMP** section of the template, click **New Advertise OMP**.
6. In the **Protocol** field, choose **Aggregate**.
7. Click **Add**.
8. Click **New Aggregate**.
9. In the **Prefix** field, enter the prefix, in CIDR notation, for the range of IP addresses corresponding to routes to aggregate. Example: 10.0.0.0/8
10. (This step applies only for a border router. It does not apply to a transport gateway edge router.) In the **Region** field, choose **Core** or **Access** to indicate whether the router advertises the prefix of aggregated routes to the core region or the access region that it serves.
11. Click **Add**.
12. Click **Save** to save the template.

Configure Route Aggregation on Border Routers and Transport Gateways Using a CLI Template

Minimum releases: Cisco Catalyst SD-WAN Control Components Release 20.11.x, Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

For more information about using CLI templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*. By default, CLI templates execute commands in global configuration mode.

Note By default, CLI templates execute commands in global config mode.

For a border router performing route aggregation, we recommend configuring either **region core** or **region access**.

1. Enter OMP configuration mode.

   sdwan omp

2. Enter VRF configuration mode.

   address-family {**ipv4** | **ipv6**} **vrf** *vrf-id*

3. Configure aggregation of routes of a specific IP range, using a prefix in CIDR notation. If you are configuring a border router, you can optionally specify whether the border router advertises the aggregated routes to the core region or its access region. If you do not specify one, the border router applies the aggregation to both the access region that it serves and the core region.

   Use **aggregate-only** to advertise only the aggregate prefix and not the component routes included within the range of the prefix.

   - Border router, which may or may not also be configured as a transport gateway

   Note If you omit **region** {**core** | **access**}, the border router advertises the routes to both its access region and the core region.

   advertise aggregate *prefix* [**aggregate-only**] [**region** {**core** | **access**}]

   - Transport gateway edge router

     advertise aggregate *prefix* [**aggregate-only**]

Examples

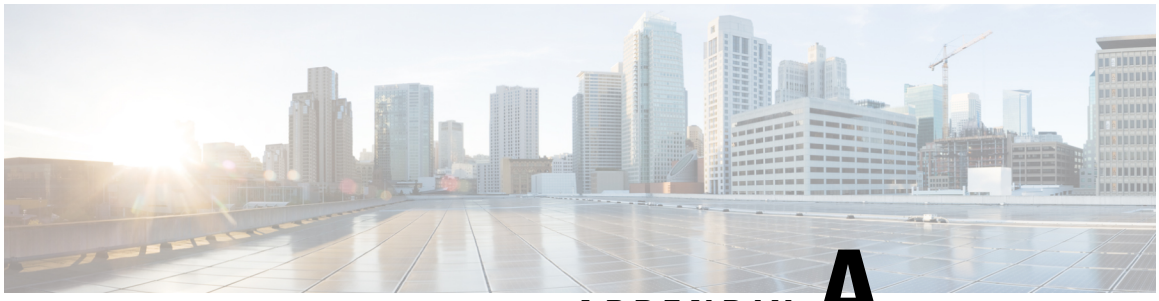
The following example configures route aggregation on a border router, advertising the aggregated routes only to the core region:

```
sdwan omp
  address-family ipv4 vrf 1
    advertise aggregate 10.0.0.0/8 aggregate-only region core
```

```
    !
  !
```

The following example configures route aggregation on a transport gateway:

```
sdwan omp
  address-family ipv4 vrf 1
    advertise aggregate 10.0.0.0/8 aggregate-only
    !
  !
```



APPENDIX A

End of support for three types of regions

- Overview of end of support for three types of regions, on page 177
- Secondary regions, on page 177
- Subregions, on page 178
- Management regions, on page 180

Overview of end of support for three types of regions

To streamline Multi-Region Fabric (MRF) architecture and simplify operations, Cisco Catalyst SD-WAN is phasing out three features. From Cisco Catalyst SD-WAN Release 20.15.1 and Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, these MRF features are being phased out:

- Secondary Regions
- Subregions
- Management regions

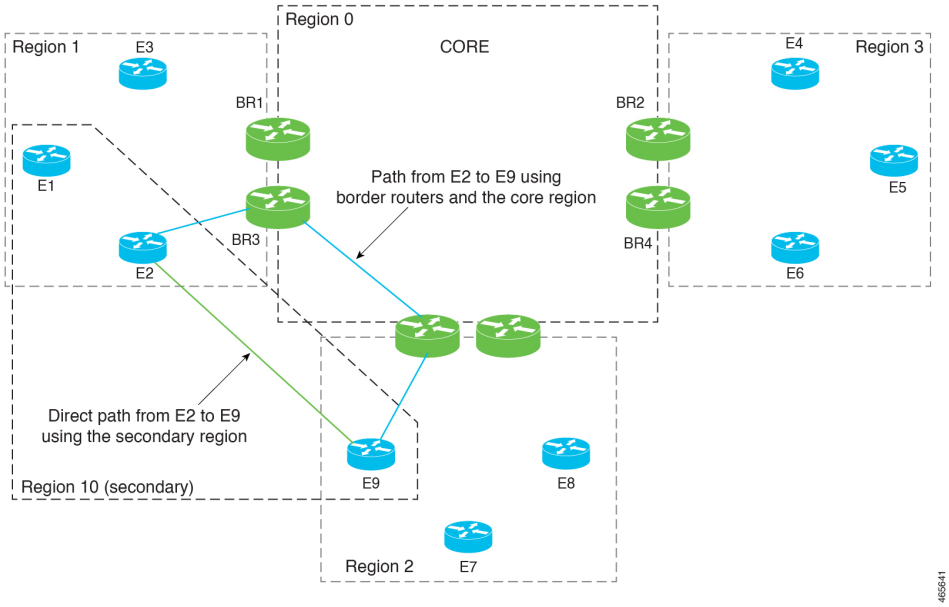
From Cisco Catalyst SD-WAN Release 20.15.1, we do not recommend using these features. If necessary, you can configure them by API. Later releases discontinue support for the features.

If your network uses any of these features, see the recommendations described here for the steps to take.

Secondary regions

In the most basic Multi-Region Fabric (MRF) architecture, each device belongs to a single region. Secondary regions were introduced to provide another facet to MRF architecture, enabling direct tunnel connections between edge routers in different primary regions. Defining a secondary region means that devices operate in two regions simultaneously, with different paths available through the device's primary and secondary regions. Devices establish tunnels with peers in both the primary access region and the secondary region.

Figure 36: Comparison of a Direct Path Using a Secondary Region and a Multi-Hop Path Using Primary Regions and the Core Region



Ending support for secondary regions

Secondary regions can lead to networks that mix two types of environments:

- A hierarchical network design regionalized, with isolated per-region control-planes, which is simple to manage, and is optimized for scale and fault-tolerance
- A flat, non-hierarchical secondary region network without the safeguards of network hierarchy, control-plane isolation, and fault-tolerance

This can create numerous traffic forwarding paths and adds complexity to network operations. For this reason, secondary regions are not recommended from Cisco Catalyst SD-WAN Release 20.15.1, and support ends in a later release.

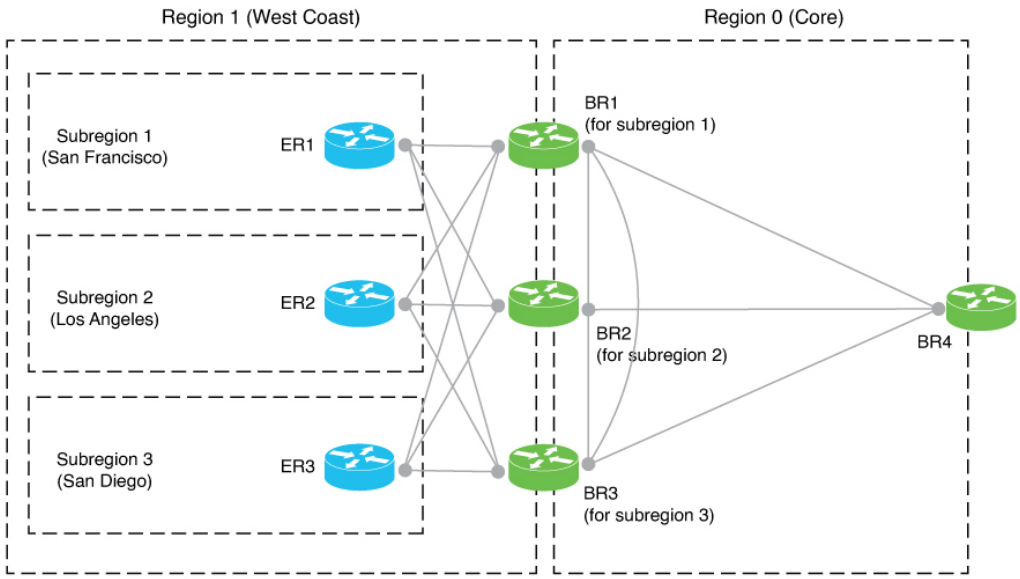
What to do next

For simple, optimized, scaled and fault-tolerant hierarchical network design, with the benefits of isolated per-region control and data planes, continue to use MRF. If you do not require a hierarchical network design, explore flat (non-MRF) network designs. If your network uses secondary regions, reconfigure to eliminate secondary regions.

Subregions

Subregions were introduced to enable subdividing access regions to separate edge routers into multiple distinct domains within a region. Devices in a subregion can have full-mesh connectivity to subregion peers without requiring full-mesh connectivity to all devices in the access region.

Figure 37: Subregion Scenario



Alternative: tunnel groups and affinity groups

You can achieve a similar subdivision of access regions using tunnel groups or affinity groups.

- Tunnel groups: You can constrain tunnel connectivity by configuring tunnel groups, per TLOC. Devices establish Cisco Catalyst SD-WAN tunnels only with TLOCs that (a) have a matching tunnel group ID, or (b) do not have a tunnel group ID configured. Tunnel groups scale to 62 per WAN access region. When you reuse a tunnel group ID in different regions, the ID operates independently within each separate region.
- Affinity groups (AG) and affinity group preference (AGP): You can use affinity groups and affinity group preference with or without tunnel groups to designate path preferences among distinct groups of devices within an access region. With affinity groups, you can configure Cisco SD-WAN Control Components to restrict TLOC and route advertisement according to affinity group. For example, you can use an affinity group to restrict route advertisement to devices within the same site.

Ending support for subregions

Subregion and affinity group configurations apply at the device level, encompassing all TLOCs on a device. By contrast, tunnel group configurations operate per TLOC.

Because the functionality is similar, and because tunnel groups and affinity groups offer simplicity, subregions are not recommended from Cisco Catalyst SD-WAN Release 20.15, and support ends in a later release.

What to do next

Replace subregion configurations with tunnel groups.

Replace Subregion Configurations with Tunnel Groups

Cisco Catalyst SD-WAN Release 17.15.x and Cisco Catalyst SD-WAN Control Components Release 20.15.x are the last releases to support subregions. If your network uses subregions, we recommend replacing them with tunnel groups.

Note This procedure triggers a reset of control connections, which can cause a small amount of packet loss. Perform the procedure during a maintenance window.

Procedure

Step 1 For each configured subregion, choose a tunnel group ID to apply to each device in the subregion. The range of tunnel group IDs is 0 to 61.

Step 2 Remove the subregion ID configuration from the devices.

Step 3 Apply the tunnel group ID configuration to the devices.

Step 4 After the configuration takes effect, verify that devices form tunnels based on the new tunnel groups tunnel group IDs, and the affinity groups and affinity group preference configuration.

Management regions

Management regions were introduced to provide a distinct means, separate from individual access regions, for connecting to management gateways. Management gateways are devices that can carry device management traffic, such as simple network management protocol (SNMP), system logs, Cisco NetFlow data, and so on. Connectivity between devices and management gateways is by a hub-and-spoke architecture.

Ending support for a management region

To simplify MRF network configuration, management regions are not recommended from Cisco Catalyst SD-WAN Release 20.15.1, and support ends in a later release.

What to do next

Instead of management regions, we recommend using a management VRF to carry device management traffic.