Multi-Region Fabric Policy

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.

Multi-Region Fabric Policy

Table 1: 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.

Feature Name	Release Information	Description
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.
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.

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

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

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

Region and Role

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

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 2: 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 3: 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 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 Condition	apply-policy Keyword	Effect: The Policy Acts on the Following Traffic
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

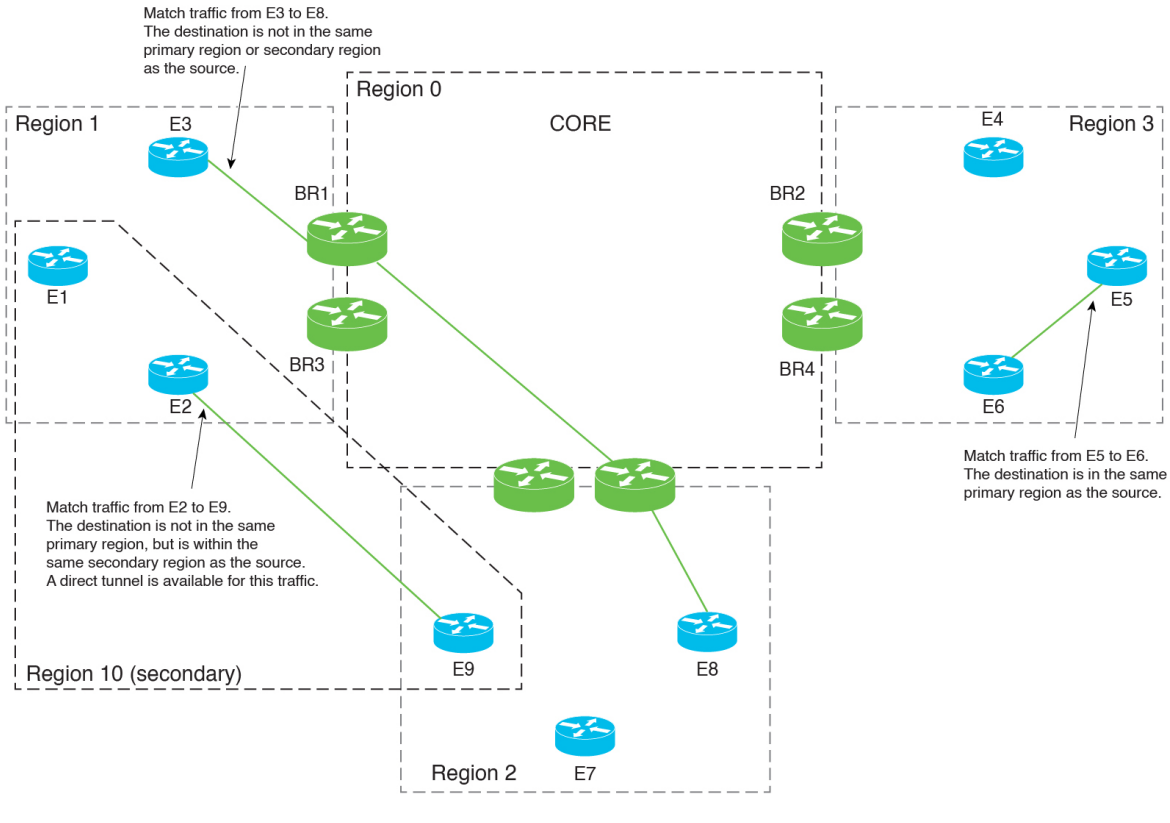
Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

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 1: 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, see Configure Centralized Policies Using Cisco SD-WAN Manager in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*.

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.

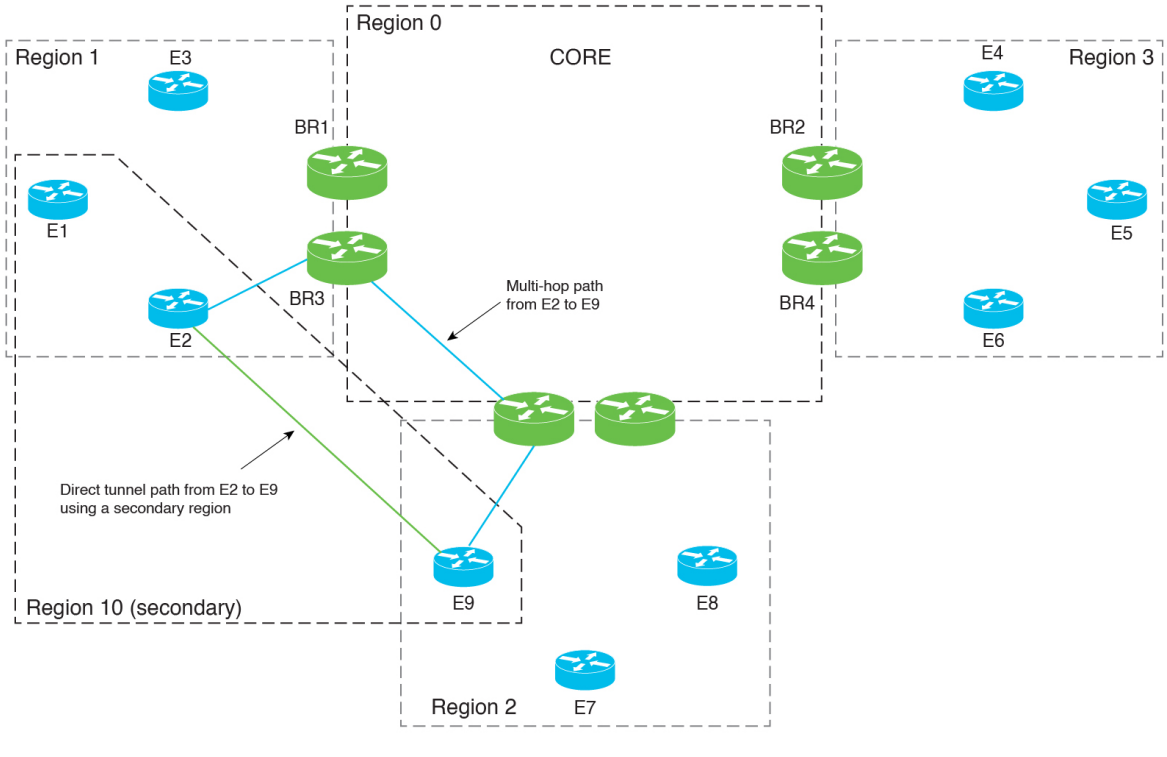
Use Cases for Configuring Path Preference

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 2: 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, see Centralized Policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*.

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, see Centralized Policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*.
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, see Configure Centralized Policies Using Cisco SD-WAN Manager in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*. 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 Configure Centralized Policies Using Cisco SD-WAN Manager, cited earlier in this section.

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, see Configure Centralized Policies Using Cisco SD-WAN Manager in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*. 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, see Configure Centralized Policies Using Cisco SD-WAN Manager in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*. 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, see Matching Routes by Path Type, Region, or Role.

For general information about using matching parameters in control policies, see Match Parameters - Control Policy.

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.

For general information about using matching parameters in control policies, see Match Parameters - Control Policy.

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, see CLI Add-On Feature Templates and CLI Templates. 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, see CLI Add-On Feature Templates and CLI Templates. 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, see the Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x.

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, see CLI Add-On Feature Templates and CLI Templates. 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 20.

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, see CLI Add-On Feature Templates and CLI Templates. 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, see the Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x.

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
   !
  !
 !
!
```