Topology

Topology

Table 1: Feature History

Feature Name	Release Information	Description
Topology	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature allows you to provision a **Mesh** or a **Hub and Spoke** topology policy which is applied to Cisco Catalyst SD-WAN Controllers. This allows exchange of data traffic between two or more Cisco IOS XE Catalyst SD-WAN devices.
Region Support for Topology	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Apply advanced and custom topologies to a specific MRF region or a group of MRF regions. Create match conditions within custom topologies to match them with MRF region(s).
Support for Topology Tagging	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	With this feature you can add devices to a topology using tags.

Topology

A topology is used to define the network structure. It defines the way different sites in the network are interconnected, as well as how the data flows.

You can create the following types of topology and customize them:

- **Hub and Spoke**
- **Mesh**
- **Custom**

Prerequisites for Topology

Before you begin configuring policy groups, ensure that the following requirements are met:

- Minimum software version for Cisco IOS XE Catalyst SD-WAN devices: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a
- Ensure that granular RBAC for topology groups is specified by expanding it. With specific permissions to the usergroup, ensure that you are able to access policy groups from **Configuration** > **Topology**.
  1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** > **User Groups**.
  2. Click **Add User Group**.
  3. Enter **User Group Name**.
  4. Select the **Read** or **Write** check box against the topology group and device feature that you want to assign to a user group.
  5. Click **Add**.

Create Topology

To create a topology, click **Create Topology** and provide a name, and description and click **Create**. To edit an existing topology, click the ellipsis icon to the right of the topology under **Action** and click **Edit**. When you have created a topology, click **Add Topology** and select from the following options:

- **Hub and Spoke**
- **Mesh**
- **Custom**

Hub and Spoke

In a hub and spoke configuration, devices at the branches and remote offices connect directly to specific devices and will not create tunnels to other devices. Communication is available through the configured VPN hubs.

Table 2: Hub and Spoke

Field	Description
Name	Enter a name for the Hub and Spoke topology. This field is mandatory.
VPN	Select a value for the VPN from the drop-down list. This field is mandatory.
Hub Sites	Click **+ Add Sites** to select hub sites to add to the topology.
Spoke Sites	Click **Add Spoke Group** to select spoke sites to add to the topology. To add a spoke site, at least one hub site must be added. You can use the same site for both hub and spoke.

Mesh

In a mesh configuration, devices at the branch or remote office are configured to connect directly to other devices in the organization that are also in mesh mode along with spoke devices that are configured to use as a hub.

Table 3: Mesh

Field	Description
Name	Enter a name for the Mesh topology.
VPN	Select a value for the VPN from the drop-down list.
Sites	[Optional] Click **Add sites** to add sites to the mesh topology.

Once you have created either a Hub and Spoke or Mesh topology, you can customize the topology by clicking **Customize Topology**. This migrates your current hub and spoke or mesh topology policy to a platform where you can customize the policy.

Custom Topology

This option allows you to configure Routes or TLOC policies, where you can specify the policy rules and match–action pairings to perform when a match occurs.

Table 4: Topology Attributes

Policy Type	Usage
Name	Name of the custom topology.
VPNs	The Used by data-policy and app-route-policy to list the VPNs for which the policy is applicable.

Policy Type	Usage
Level	Starting from Cisco Catalyst SD-WAN Manager Release 20.15.1, you can choose a **Level** for your topology and choose between **Sites** and **Regions**.
InBound Sites	Specify the route advertisements that the Cisco Catalyst SD-WAN Controller receives from the devices.
OutBound Sites	Specify the route advertisements that the Cisco Catalyst SD-WAN Controller sends to the devices.
Inbound Regions	When you choose **Level** as **Regions**, choose an inbound region from the list of regions.
Outbound Regions	When you choose **Level** as **Regions**, choose an outbound region from the list of regions.
Role	Choose between **Border** and **Edge** as a role for the router.

Click **Add Rules** to configure Route or TLOC policy match–action pairings that are numbered and are examined in sequential order. When a match occurs, the action is performed, and the policy analysis on that route or packet terminates. Some types of policy definitions apply only to specific VPNs.

You can configure more sequence rules, as needed and drag and drop to re-order them.

Table 5: Match

Match Condition	Description
Color	One or more colors. The available colors are: 3G, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, LTE, metro-ethernet, MPLS, private1 through private6, public-internet, red, and silver.
Community	Specify communities and community numbers.

Match Condition	Description
Expanded Community	List of one or more BGP communities. In the **Community List** field, you can specify the following: • **aa:nn**: AS number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **internet**: Routes in this community are advertised to the internet community. This community comprises all BGP-speaking networking devices. • **local-as**: Routes in this community are not advertised outside the local AS. • **no-advertise**: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.
OMP Tag	Tag value that is associated with the route or prefix in the routing database on the device. The range is 0 through 4294967295.
Origin	Protocol from which the route was learned.
Originator	IP address from which the route was learned.
Path Type	In a Hierarchical Cisco Catalyst SD-WAN architecture, match a route by its path type, which can be one of the following: • **Hierarchical Path**: 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. • **Direct Path**: A direct path route from one edge router to another edge router. • **Transport Gateway Path**: A route that is reoriginated by a router that has transport gateway functionality enabled.

Match Condition	Description
Preference	The preference value that the route or prefix has in the local site, that is, in the routing database on the device. A higher preference value is more preferred. The range is 0 through 255.
Prefix List	One or more prefixes. Specifies the name of a prefix list.
Region	Starting from Cisco Catalyst SD-WAN Manager Release 20.15.1, one or more region identifiers.
Site	One or more overlay network site identifiers.
TLOC	Individual TLOC address.
VPN	Individual VPN identifier. The range is 0 through 65535.

The **Reject** option is selected by default.

Table 6: Action

Match Condition	Description
Affinity	Specify the
Community	Specify communities and community numbers.
Export To	Select a VPN list, or create a new one.
OMP Tag	Enter the OMP route tag. The range is 0 through 4294967295.
Preference	Enter the preference number for the route, a number between 0-4294967295.

Match Condition	Description
Service	Enter the following information: **Type**: Select a service type from the following options: • **Firewall** • **Intrusion Detection Prevention** • **Intrusion Detection System** • **Net Service 1** • **Net Service 2** **VPN**: Enter the number of the Service VPN. **TLOC IP**: Enter the IP address of the Service TLOC. **Color**: Select a color type from the drop-down list. **Encapsulation**: Select **IPSEC** or **GRE** as the encapsulation type. **TLOC List**: Select a service TLOC list from the drop-down list, or create a new one.
TLOC	Individual TLOC address.

Match Condition	Description
TLOC Action	Select an action from the following option in the drop-down list: • **Strict**: Direct matching traffic only to the intermediate destination. With this action, if the intermediate destination is down, no traffic reaches the final destination. If you do not configure a set tloc-action action in a centralized control policy, strict is the default behavior. • **Primary**: First direct matching traffic to the intermediate destination. If that driver is not reachable, then direct it to the final destination. With this action, if the intermediate destination is down, all traffic reaches the final destination. • **Backup**: First direct matching traffic to the final destination. If that driver is not reachable, then direct it to the intermediate destination. With this action, if the source is unable to reach the final destination directly, it is possible for all traffic to reach the final destination via the intermediate destination. • **Equal Cost Multi-path**: Equally direct matching control traffic between the intermediate destination and the ultimate destination. With this action, if the intermediate destination is down, all traffic reaches the ultimate destination.

Click **Save Match and Actions** to commit your changes and click **Save** to add the customization.

Activate the Topology

When you have created a topology, you must activate the topology for it to take effect. By activating the topology, you create the new network structure, and as a result also deactivate any existing topology. .

1. To activate the topology, click the ellipsis icon to the right of the topology and click **Activate**
2. Click **Preview CLI** and select a device from the left pane to view the configuration difference.
3. Click **Deploy** to deploy the topology group to the Cisco SD-WAN Control Components.

To deactivate the topology, click the ellipsis icon next to the topology and click **Deactivate** and **Deploy**.

Note After you deploy a topology group, any change to the topology group is deployed to the Cisco SD-WAN Controller.