Cisco Catalyst SD-WAN Network Topology, Releases 26.x and Later

Cisco SD-WAN
Updated September 28, 2026

Topics included

1 Topology....4
Feature history for topology....5
Topologies....5
Configure user group permissions for topology groups....6
Create Topology....6
Activate the topology....14

2 Hub-and-Spoke....16
Feature history for Hub-and-Spoke....17
Hub-and-Spoke configuration....17
Benefits of Hub-and-Spoke....18
Restrictions for Hub-and-Spoke....19
Hub-and-Spoke connectivity example....19
Device0 (Hub) connectivity before and after....21
Device1 (Spoke1) connectivity before and after....24
Device2 (Spoke2) connectivity before and after....26
Hub-and-Spoke use cases....28
Configure a Hub-and-Spoke topology....29
Configure a Cisco Catalyst SD-WAN Controller to enable Hub-and-Spoke using Cisco SD-WAN Manager....30
Configure a Cisco SD-WAN Controller to enable Hub-and-Spoke using a CLI template....30
Configure a router as a transport gateway using Cisco SD-WAN Manager....31
Configure a router as a transport gateway using a CLI template....32
Configure the site type for a router using Cisco SD-WAN Manager....32
Configure the site type for a router using a CLI template....32
Hub-and-Spoke configuration verification....33

1 Topology

Topics:

- Feature history for topology
- Topologies
- Configure user group permissions for topology groups
- Create Topology
- Activate the topology

Provides a minimal reference for the topology concept in this content set. Use this topic to identify that a topology definition exists when no additional descriptive details are supplied.

Feature history for topology

Provides information about topology policies on Cisco IOS XE Catalyst SD-WAN devices, summarizing feature history, Mesh and Hub and Spoke options, region-specific application of advanced or custom topologies, and tag-based device assignment, with associated cEdge and vManage release references.

Feature history
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.

Topologies

Describes topologies as network structures that define how sites interconnect and how data flows, with configurable types such as Hub and Spoke, Mesh, and Custom. Explains tag-based device association in supported releases and the need to reactivate to apply changes.

A topology is a network structure that

- defines how different sites in a network are interconnected
- defines how data flows, and
- supports **Hub and Spoke**, **Mesh**, and **Custom** types

You can create and customize **Hub and Spoke**, **Mesh**, and **Custom** topologies.

Topology tags

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

In Cisco Catalyst SD-WAN Manager Release 20.16.1 and earlier releases, you can choose devices for each topology and activate the topology.

From Cisco Catalyst SD-WAN Manager Release 20.18.1, you can add devices to a topology using tags. You can specify the tag rule in the topology. When devices are assigned a matching tag, they are automatically associated to the topology. You must reactivate the topology to apply the changes.

Configure user group permissions for topology groups

Configure RBAC by creating a user group with read or write permissions for topology groups so users can access policy groups in vManage. This procedure is performed after verifying the minimum supported software version for IOS SD-WAN devices.

Before you begin

Before you begin configuring policy groups, ensure that these 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**.

Procedure

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

Information about creating a topology policy.

Procedure

1. To create a topology, click **Create Topology** and enter a name and description.
   a) Click **Create**. When you have created a topology, click **Add Topology**.
   b) To edit an existing topology, click the ellipsis icon to the right of the topology under **Action** and click **Edit**.
2. Select from the following options:
   - Hub and Spoke

     n 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. From Cisco Catalyst SD-WAN Manager Release 20.18.1 , choose **By Tag Rules** to select sites and devices which are tagged. For more information about device tagging, see Add Tags to Devices Using Cisco SD-WAN Manager From, SD-WAN Manager 26.1.1.1 , Click **Manage rule** . You can select **Modify rules** or **Remove rules** . For Cisco Catalyst SD-WAN Manager Release 20.18.1 , click **Add and Edit Rules** . The **Automated Rules** window is displayed. In the **Rules** section, choose values for the following options: • (From, SD-WAN Manager 26.1.1.1) **Rule name:** Enter a unique name for the rule. Rule names cannot be duplicated once you create it. • **Rule Conditions** : Choose one of the following conditions: **Match All** or **Match Any** . • **Device Attribute** : Choose **Tags** . • **Condition** : Choose one of the following operators: **Equals** , **Contains** , **Not Contains** , **Not Equals** , **Starts with** , **Ends with** . • **Select Value** : Select a tag from the list of available tags. If you edit the hub site, you must update the spoke group preferences accordingly.

Field	Description
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. From Cisco Catalyst SD-WAN Manager Release 20.18.1 , choose **By Tag Rules** to select sites and devices which are tagged. For more information about device tagging, see Add Tags to Devices Using Cisco SD-WAN Manager From, SD-WAN Manager 26.1.1.1 , Click **Manage rule** . You can select **Modify rules** or **Remove rules** . For Cisco Catalyst SD-WAN Manager Release 20.18.1 , click **Add and Edit Rules** . The **Automated Rules** window is displayed. In the **Rules** section, choose values for the following options: • (From, SD-WAN Manager 26.1.1.1) **Rule name:** Enter a unique name for the rule. Rule names cannot be duplicated once you create it. • **Rule Conditions** : Choose one of the following conditions: **Match All** or **Match Any** . • **Device Attribute** : Choose **Tags** . • **Condition** : Choose one of the following operators: **Equals** , **Contains** , **Not Contains** , **Not Equals** , **Starts with** , **Ends with** . • **Select Value** : Select a tag from the list of available tags. Select the **Hub Preference** from the **Priority** drop-down list. You can add multiple priorities using the plus sign.

- 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.

Field	Description
Sites	[Optional] Click **Add sites** to add sites to the mesh topology. From Cisco Catalyst SD-WAN Manager Release 20.18.1 , choose **By Tag Rules** to select sites and devices which are tagged. For more information about device tagging, see Add Tags to Devices Using Cisco SD-WAN Manager From, SD-WAN Manager 26.1.1.1 , Click **Manage rule** . You can select **Modify rules** or **Remove rules** . For Cisco Catalyst SD-WAN Manager Release 20.18.1 , click **Add and Edit Rules** . The **Automated Rules** window is displayed. In the **Rules** section, choose values for the following options: • (From, SD-WAN Manager 26.1.1.1) **Rule name:** Enter a unique name for the rule. Rule names cannot be duplicated once you create it. • **Rule Conditions** : Choose one of the following conditions: **Match All** or **Match Any** . • **Device Attribute** : Choose **Tags** . • **Condition** : Choose one of the following operators: **Equals** , **Contains** , **Not Contains** , **Not Equals** , **Starts with** , **Ends with** . • **Select Value** : Select a tag from the list of available tags.

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

  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.
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** .

Policy Type	Usage
InBound Sites	Specify the route advertisements that the Cisco Catalyst SD-WAN Controller receives from the devices. From Cisco Catalyst SD-WAN Manager Release 20.18.1 , choose **By Tag Rules** to select sites and devices which are tagged. For more information about device tagging, see Add Tags to Devices Using Cisco SD-WAN Manager From, SD-WAN Manager 26.1.1.1 , Click **Manage rule** . You can select **Modify rules** or **Remove rules** . For Cisco Catalyst SD-WAN Manager Release 20.18.1 , click **Add and Edit Rules** . The **Automated Rules** window is displayed. In the **Rules** section, choose values for the following options: • (From, SD-WAN Manager 26.1.1.1) **Rule name:** Enter a unique name for the rule. Rule names cannot be duplicated once you create it. • **Rule Conditions** : Choose one of the following conditions: **Match All** or **Match Any** . • **Device Attribute** : Choose **Tags** . • **Condition** : Choose one of the following operators: **Equals** , **Contains** , **Not Contains** , **Not equals** , **Starts with** , **Ends with** . • **Select Value** : Select a tag from the list of available tags.

Policy Type	Usage
OutBound Sites	Specify the route advertisements that the Cisco Catalyst SD-WAN Controller sends to the devices. From Cisco Catalyst SD-WAN Manager Release 20.18.1 , choose **By Tag Rules** to select sites and devices which are tagged. For more information about device tagging, see Add Tags to Devices Using Cisco SD-WAN Manager From, SD-WAN Manager 26.1.1.1 , Click **Manage rule** . You can select **Modify rules** or **Remove rules** . For Cisco Catalyst SD-WAN Manager Release 20.18.1 , click **Add and Edit Rules** . The **Automated Rules** window is displayed. In the **Rules** section, choose values for the following options: • (From, SD-WAN Manager 26.1.1.1) **Rule name:** Enter a unique name for the rule. Rule names cannot be duplicated once you create it. • **Rule Conditions** : Choose one of the following conditions: **Match All** or **Match Any** . • **Device Attribute** : Choose **Tags** . • **Condition** : Choose one of the following operators: **Equals** , **Contains** , **Not Contains** , **Not Equals** , **Starts with** , **Ends with** . • **Select Value** : Select a tag from the list of available tags.
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.

3. 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.

Match Condition	Description
Community	Specify communities and community numbers.
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.
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.

Match Condition	Description
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. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.

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.
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.

Note

Starting from Cisco IOS XE Catalyst SD-WAN Release 26.1.1 , export and import of topology is not supported because the sites can be added with site ID and tag rules.

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

Activate the topology

Configure topology activation to apply a newly created network topology, optionally preview configuration differences, and deploy changes to controllers; this process replaces any existing topology with the new structure.

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.

Procedure

1. Activate the topology.

To activate the topology, click the ellipsis icon to the right of the topology and click **Activate**.

2. Preview configuration differences.

   Click **Preview CLI** and select a device from the left pane to view the configuration difference.

3. Deploy the topology group.

   Click **Deploy** to deploy the topology group to the Cisco SD-WAN Control Components.

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

What to do next

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

2 Hub-and-Spoke

Topics:

- Feature history for Hub-and-Spoke
- Hub-and-Spoke configuration
- Hub-and-Spoke connectivity example
- Hub-and-Spoke use cases
- Configure a Hub-and-Spoke topology
- Hub-and-Spoke configuration verification

Provides details about designating routers as hubs or spokes to optimize resource demands and enforce centralized security services across all logical segments. Understanding this centralized model enables you to simplify network management while maintaining robust connectivity between branch and headquarters sites.

Hub-and-spoke topology configuration refers to a simplified method for setting up a hub-and-spoke network, particularly within a Cisco Catalyst SD-WAN. This configuration approach streamlines the process by eliminating the need for complex centralized control policies, which were traditionally required and often lengthy.

Feature history for Hub-and-Spoke

Lists the development milestones and release information for Hub-and-Spoke, including feature description.

This table describes the developments of this feature, by release.

Table 7: Feature history

Feature Name	Release Information	Description
Hub-and-Spoke configuration method	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	Hub-and-spoke configuration simplifies the process of configuring a hub-and-spoke topology. This approach makes complex centralized control policy unnecessary. The configuration requires only a few simple configurations: a single command each on: • The Cisco Catalyst SD-WAN Controllers serving a network • A router that serves as a hub • The routers that operate as spokes.

Hub-and-Spoke configuration

Explains the simplified method for building a centralized architecture using transport gateway functionality and site-type attributes. Understanding this mechanism allows you to implement a hub-and-spoke topology that automatically filters route information to spokes, ensuring all inter-spoke traffic flows through a designated hub.

Hub-and-spoke configuration is a method that simplifies the process of establishing a hub-and-spoke topology. Historically, this topology required complex expertise and lengthy centralized control policies in a Cisco Catalyst SD-WAN environment. This new configuration method, available from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, eliminates the need for complex control policy, making configuration faster.

This method involves configuring the Cisco Catalyst SD-WAN Controller that serve the network to enable hub-and-spoke and configuring transport gateway functionality on a router that will serve as a hub.

> **Note**
>
> The resulting hub-and-spoke topology applies to all VRFs.

Configuration overview

Hub-and-spoke configuration for Cisco Catalyst SD-WAN has three parts, as described in the following table:

Intent	Devices or Controllers to Configure	Configuration
1. Enable a hub-and-spoke topology in the network.	Cisco SD-WAN Controllers that serve the network	Enable hub-and-spoke configuration in the network. See the following: • Configure a Cisco Catalyst SD-WAN Controller to Enable Hub-and-Spoke Using Cisco SD-WAN Manager. • Configure a Cisco SD-WAN Controller to Enable Hub-and-Spoke Using a CLI Template. The CLI template method uses the **topology hub-and-spoke enable** command.
2. Configure a router as a transport gateway to function as a hub.	Router designated as hub	Enable transport gateway functionality on the router. See *Configure a router as a transport gateway using a CLI template*. The CLI template method uses the **transport-gateway enable** command.
3. Configure routers to function as spokes.	Routers designated as spokes	Configure the device site type as spoke. See *Configure the site type for a router using a CLI template*. The CLI template method uses the **site-type** command.

Result of configuration

This configuration results in the following network behavior:

- Cisco Catalyst SD-WAN Controllers in the network filter the TLOC and route information that they advertise to each router in the network.
  - Routers operating as hubs (transport gateways) receive all TLOC and route information.
  - Routers operating as spokes receive TLOC and route information for the hubs (transport gateways) in the network. They do not receive TLOCs or routes for other spokes. Consequently, there are no bidirectional forwarding detection (BFD) sessions between spoke devices.
- All spoke-to-spoke traffic flows through the transport gateway, which re-originates routes for each spoke.

Taken together, the result is a hub-and-spoke topology. Routers operating as spokes receive TLOC and route information for the hubs (transport gateways) in the network. They do not receive TLOCs or routes for other spokes. Consequently, there are no bidirectional forwarding detection (BFD) sessions between spoke devices. `

If there are non-spoke sites in the network, spoke sites continue to receive TLOCs or routes from such sites and BFD is established from spoke sites to the non-spoke sites. In this case, it is not a true hub-and-spoke topology.

Benefits of Hub-and-Spoke

Provides details about the operational advantages of using a centralized topology, such as improved network isolation and reduced resource demands on edge devices. Understanding these benefits helps you optimize your architecture to support centralized network services like firewall policies for all inter-branch traffic.

A hub-and-spoke topology offers several applications and benefits, including the following:

- Operating each spoke network with a degree of isolation allows for applying different policies, transport mechanisms, and other configurations to each discrete spoke.
- Decreasing the number of peers for the edge routers serving each spoke reduces the resource demands on those edge routers.
- Routing all inter-spoke traffic through a hub enables the application of network services, such as firewall policy, to all inter-spoke traffic.
- The described configuration process simplifies the setup of a hub-and-spoke topology, avoiding the need for complex centralized control policy.

Restrictions for Hub-and-Spoke

Provides details about the limitations and usage constraints of the simplified centralized configuration method. Reviewing these restrictions, such as the lack of support for on-demand tunnels and specific site-type requirements, helps you avoid misconfigurations and ensure a successful topology deployment.

When implementing a hub-and-spoke topology, adhere to the following restrictions to ensure proper functionality and avoid misconfigurations.

Key restrictions for hub-and-spoke configurations include:

- Transport gateway site type: When using a transport gateway as a hub, do not configure its site type as spoke.
- On-demand tunnels: In a hub-and-spoke topology, on-demand tunnels are not supported. This is because spoke-to-spoke direct tunnels are not supported in the hub-and-spoke topology.
- Migration: There is no automatic procedure for migrating from a hub-and-spoke topology defined by control policy to the hub-and-spoke configuration method described here.

Hub-and-Spoke connectivity example

Provides details about the changes in network connectivity when converting a full-mesh environment into a centralized architecture. Reviewing this scenario helps you visualize how BFD sessions and route advertisements are modified to ensure that spokes communicate exclusively through the designated hub router.

This section provides a detailed example demonstrating how network connectivity changes when a full-mesh network is converted to a hub-and-spoke topology.

The following table details the devices, their intended roles, IP addresses, interfaces, and prefixes used in this example, along with their corresponding color coding for illustrations.

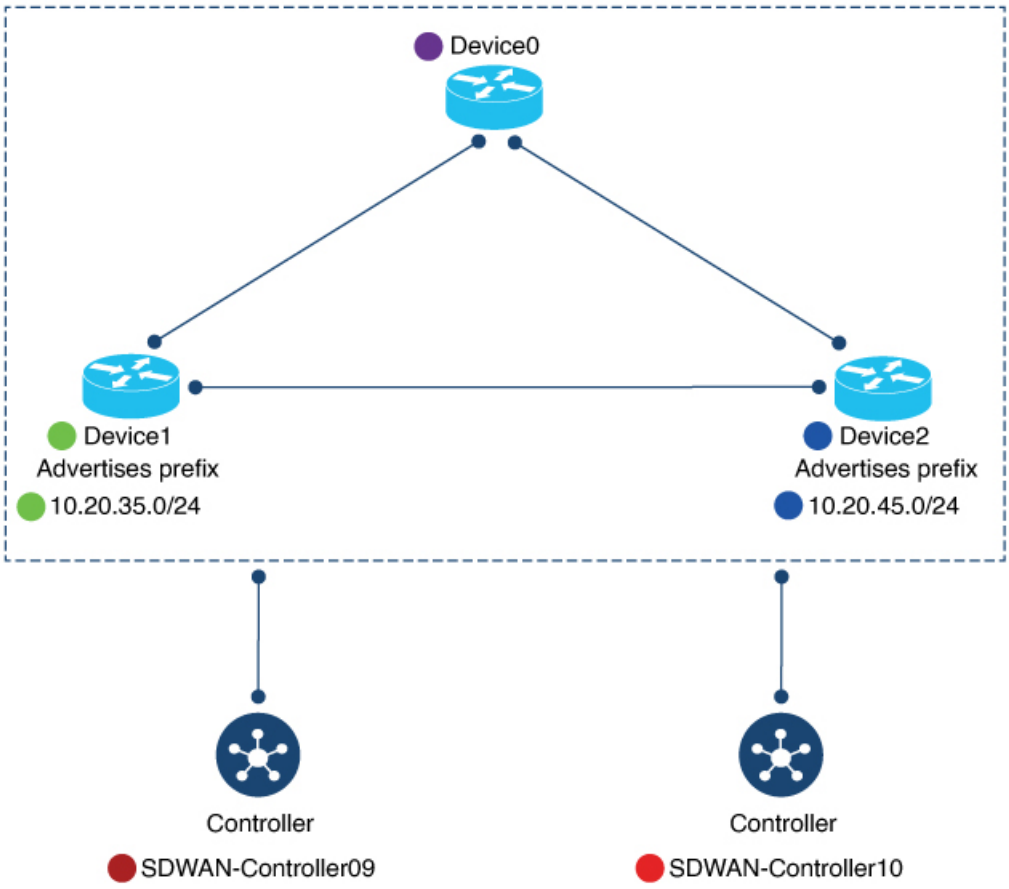
Table 8: Devices, IP Addresses, Roles, Interfaces, and Prefixes

Device	Intended Role	Interfaces	Prefixes
Device0 172.16.255.15 Color in illustration: Purple	Hub	10.0.20.15 (3g) 10.1.15.15 (LTE)	None
Device1 172.16.255.35 Color in illustration: Green	Spoke1	10.5.1.35 (LTE)	10.20.35.0/24 Color in illustration: Green highlight

Device	Intended Role	Interfaces	Prefixes
Device2 172.16.255.45 Color in illustration: Blue	Spoke2	10.0.6.45 (LTE)	10.20.45.0/24 Color in illustration: Blue highlight
SDWAN-Controller09 172.16.255.19 Color in illustration: Dark red	Cisco SD-WAN Controller	Not applicable	Not applicable
SDWAN-Controller10 172.16.255.20 Color in illustration: Red	Cisco SD-WAN Controller	Not applicable	Not applicable

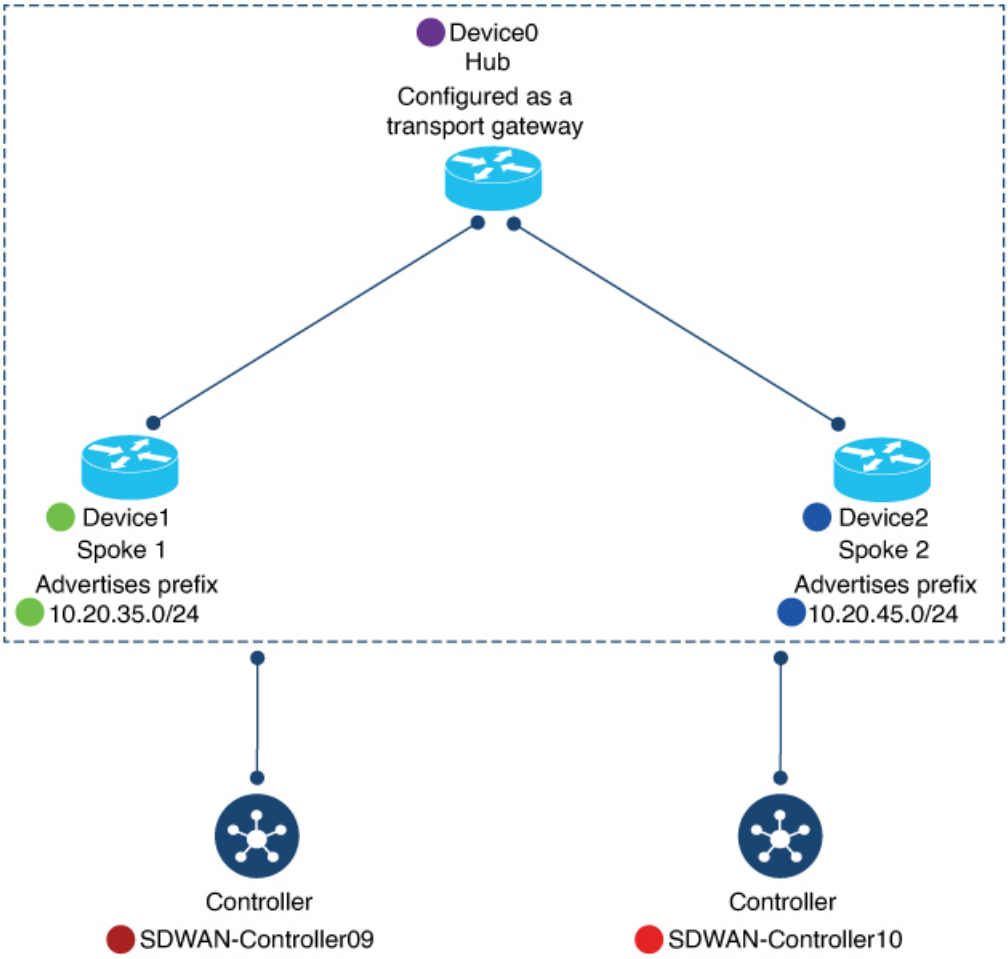
The following figure shows the initial state of the network, with full-mesh connectivity before configuring hub-and-spoke.

Figure 1: Network Connectivity Before Hub-and-Spoke Configuration



The following figure shows the network connectivity after configuring hub-and-spoke.

Figure 2: Network Connectivity After Hub-and-Spoke Configuration



Device0 (Hub) connectivity before and after

Provides details about the state of BFD sessions and OMP routes on the designated hub router during topology conversion. Comparing these states helps you verify that the hub correctly maintains sessions with all spokes and re-originates prefixes to facilitate centralized traffic flow.

This section details the observed connectivity for Device0, which functions as the hub, both before and after the hub-and-spoke configuration. It includes information regarding BFD sessions, OMP routes, and IP routes.

BFD Sessions on Device0 (Hub)

The following describes the state of BFD sessions on Device0.

- Before Configuration: The **show sdwan bfd sessions** command shows that it has BFD sessions with both Device1 (Spoke1) and Device2 (Spoke1).
- After configuration: Device0 retains the same BFD sessions with both Device1 (Spoke1) and Device2 (Spoke2).

Figure 3: Hub: BFD Sessions Before and After

Before

```
Device0-future-hub#show sdwan bfd sessions
                                       SOURCE TLOC  REMOTE TLOC                 DST PUBLIC
SYSTEM IP        SITE ID   STATE        COLOR        COLOR       SOURCE IP
-------------------------------------------------------------------------------------------
172.16.255.45    2500      up           3g           lte         10.0.20.15
172.16.255.35    1500      up           3g           lte         10.0.20.15
172.16.255.45    2500      up           lte          lte         10.1.15.15
172.16.255.35    1500      up           lte          lte         10.1.15.15
```

BFD sessions with Device1 (green) and Device2 (blue)

After

```
Device0-Hub#show sdwan bfd sessions
                                       SOURCE TLOC  REMOTE TLOC                 DST PUBLIC
SYSTEM IP        SITE ID   STATE        COLOR        COLOR       SOURCE IP
-------------------------------------------------------------------------------------------
172.16.255.45    2500      up           3g           lte         10.0.20.15
172.16.255.35    1500      up           3g           lte         10.0.20.15
172.16.255.45    2500      up           lte          lte         10.1.15.15
172.16.255.35    1500      up           lte          lte         10.1.15.15
```

BFD sessions with Device1 (green) and Device2 (blue)

OMP Routes on Device0 (Hub)

The following describes the state of OMP routes on Device0.

- Before Configuration: The **show sdwan omp route vpn 1** command shows that the prefixes advertised by Device1 (Spoke1) and Device2 (Spoke2) are reachable only through Device1 (Spoke1) and Device2 (Spoke2), respectively.
- After configuration: The Device1 (Spoke1) prefix and the Device2 (Spoke2) prefix are reachable through the hub itself (indicated by 0.0.0.0 in the FROM PEER column).

Figure 4: Hub: OMP Routes Before and After

Before

```
Device0-future-hub#show sdwan omp route vpn 1

                                                                PATH                                ATTRIBUTE
TENANT     VPN     PREFIX            FROM PEER                  ID      LABEL     STATUS          TYPE        TLO
-------------------------------------------------------------------------------------------------------------------
0          1       10.20.35.0/24     172.16.255.19              13      1003      C,I,R           installed   172
                                     172.16.255.20              21      1003      C,R             installed   172
0          1       10.20.45.0/24     172.16.255.19              46      1003      C,I,R           installed   172
                                     172.16.255.20              17      1003      C,R             installed   172
```

Device1 prefix

Device2 prefix

via Device

After

```
Device0-hub#show sdwan omp route vpn 1

                                                                PATH                                ATTRIBUTE
TENANT     VPN     PREFIX            FROM PEER                  ID      LABEL     STATUS          TYPE        TLO
-------------------------------------------------------------------------------------------------------------------
0          1       10.20.35.0/24     0.0.0.0                    10737   1003      C,Red,R,        installed   172
                                                                41894             TGW-R
                                     0.0.0.0                    10737   1003      C,Red,R,        installed   172
                                                                41895             TGW-R
                                     172.16.255.19              8       1003      C,I,R           installed   172
                                     172.16.255.20              8       1003      C,R             installed   172
0          1       10.20.45.0/24     0.0.0.0                    10737   1003      C,Red,R,        installed   172
                                                                41894             TGW-R
                                     0.0.0.0                    10737   1003      C,Red,R,        installed   172
                                                                41895             TGW-R
                                     172.16.255.19              9       1003      C,I,R           installed   172
                                     172.16.255.20              9       1003      C,R             installed   172
```

Device1 prefix

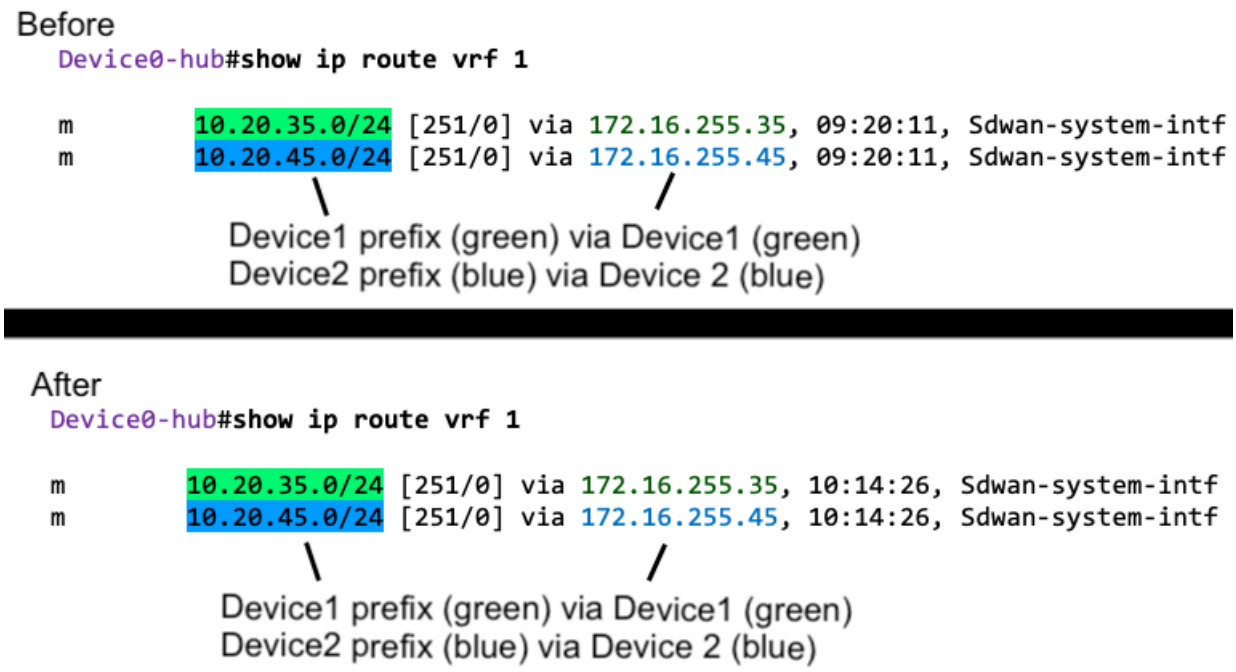
Device2 prefix

IP Routes on Device0 (Hub)

The following describes the state of IP routes on Device0.

- Before Configuration: The **show ip route vrf 1** command shows that the prefixes advertised by Device1 (Spoke1) and Device2 (Spoke2) are reachable through Device1 (Spoke1) and Device2 (Spoke2), respectively.
- After configuration: This connectivity remains unchanged for Device0.

Figure 5: Hub: IP Routes Before and After



Device1 (Spoke1) connectivity before and after

Provides details about the connectivity changes for a spoke router when transitioning to a centralized model. Reviewing these observations helps you confirm that direct sessions with other spokes are removed and that all remote prefixes are now reachable only through the hub.

This section details the observed connectivity for Device1, which functions as Spoke1, both before and after the hub-and-spoke configuration. It includes information regarding BFD sessions, OMP routes, and IP routes.

BFD Sessions on Device1 (Spoke1)

The following describes the state of BFD sessions on Device1.

- Before Configuration: The **show sdwan bfd sessions** command shows BFD sessions with both Device0 (future hub) and Device2 (future Spoke2).
- After configuration: Device1 only has BFD sessions with the hub; there are no BFD sessions with other spokes (for example, Spoke2).

Figure 6: Spoke1: BFD Sessions Before and After

Before

```
Device1-future-spoke1#show sdwan bfd sessions
                                       SOURCE TLOC  REMOTE TLOC             DST PUBLIC
SYSTEM IP       SITE ID   STATE        COLOR        COLOR       SOURCE IP       IP
-------------------------------------------------------------------------------------------
172.16.255.45   2500      up           lte          lte         10.5.1.35       10.0.6.45
172.16.255.15   500       up           lte          3g          10.5.1.35       10.0.20.15
172.16.255.15   500       up           lte          lte         10.5.1.35       10.1.15.15
```

BFD sessions with Device2 (blue) and Hub (purple)

After

```
Device1-spoke1#show sdwan bfd sessions
                                       SOURCE TLOC  REMOTE TLOC             DST PUBLIC
SYSTEM IP       SITE ID   STATE        COLOR        COLOR       SOURCE IP       IP
-------------------------------------------------------------------------------------------
172.16.255.15   500       up           lte          3g          10.5.1.35       10.0.20.15
172.16.255.15   500       up           lte          lte         10.5.1.35       10.1.15.15
```

BFD sessions only with Hub (purple)

OMP Routes on Device1 (Spoke1)

The following describes the state of OMP routes on Device1.

- Before Configuration: The **show sdwan omp route vpn 1** command shows that it can reach the Device2 (Spoke2) prefix directly through Device2. This is evident because the TLOC IP column shows the system IP of Device2.
- After configuration: Device1 can reach the Device2 (Spoke2) prefix only through the hub.

Figure 7: Spoke1: OMP Routes Before and After

Before

```
Device1-future-spoke1#show sdwan omp route vpn 1

                                                  PATH                ATTRIBUTE
TENANT   VPN   PREFIX          FROM PEER         ID    LABEL  STATUS   TYPE       TLOC IP         COLOR
-------------------------------------------------------------------------------------------------------
0        1     10.20.45.0/24   172.16.255.19     43    1003   C,I,R    installed  172.16.255.45   lte
               172.16.255.20     21    1003   C,R      installed  172.16.255.45   lte
```

Device2 prefix

via Device2

After

```
Device1-spoke1#show sdwan omp route vpn 1

                                                  PATH                ATTRIBUTE
TENANT   VPN   PREFIX          FROM PEER         ID    LABEL  STATUS   TYPE       TLOC IP         COLOR
-------------------------------------------------------------------------------------------------------
0        1     10.20.45.0/24   172.16.255.19     10    1003   C,I,R    installed  172.16.255.15   lte
               172.16.255.19     11    1003   C,I,R    installed  172.16.255.15   3g
               172.16.255.20     10    1003   C,R      installed  172.16.255.15   lte
               172.16.255.20     11    1003   C,R      installed  172.16.255.15   3g
```

Device2 prefix

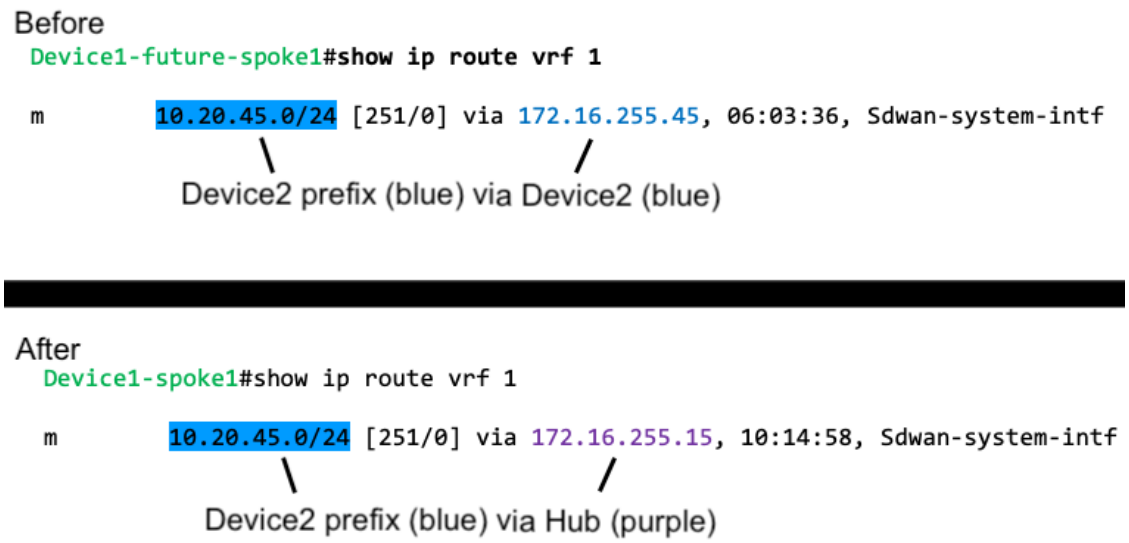
via Hub

IP Routes on Device1 (Spoke1)

The following describes the state of IP routes on Device1.

- Before Configuration: The **show ip route vrf 1** command shows Device1 could reach the Device2 prefix directly through Device2.
- After configuration: Device1 (Spoke1) can reach the Device2 (Spoke2) prefix only through the hub..

Figure 8: Spoke1: IP Routes Before and After



Device2 (Spoke2) connectivity before and after

Provides details about the observed routing and session modifications for a secondary spoke router. Comparing these results ensures that the centralized topology is applied consistently across multiple spoke sites, with all inter-spoke communication correctly redirected through the transport gateway.

This section details the observed connectivity for Device2, which functions as Spoke2, both before and after the hub-and-spoke configuration, mirroring the changes observed for Device1. It includes information regarding BFD sessions, OMP routes, and IP routes.

BFD Sessions on Device2 (Spoke2)

The following describes the state of BFD sessions on Device2.

- Before Configuration: The **show sdwan bfd sessions** command shows Device2 had BFD sessions with both Device0 (future hub) and Device1 (future Spoke1).
- After configuration: Device2 only has BFD sessions with the hub; there are no BFD sessions with other spokes (for example, Spoke1).

Figure 9: Spoke2: BFD Sessions Before and After

Before

```
Device2-future-spoke2#show sdwan bfd sessions
                                       SOURCE TLOC  REMOTE TLOC              DST PUBLIC
SYSTEM IP        SITE ID   STATE       COLOR        COLOR       SOURCE IP                IP
-------------------------------------------------------------------------------------------------
172.16.255.35    1500      up          lte          lte         10.0.6.45                10.5.1.35
172.16.255.15    500       up          lte          3g          10.0.6.45                10.0.20.15
172.16.255.15    500       up          lte          lte         10.0.6.45                10.1.15.15
```

BFD sessions with Device1 (green) and Hub (purple)

After

```
Device2-spoke2#show sdwan bfd sessions
                                       SOURCE TLOC  REMOTE TLOC              DST PUBLIC
SYSTEM IP        SITE ID   STATE       COLOR        COLOR       SOURCE IP                IP
-------------------------------------------------------------------------------------------------
172.16.255.15    500       up          lte          3g          10.0.6.45                10.0.20.15
172.16.255.15    500       up          lte          lte         10.0.6.45                10.1.15.15
```

BFD sessions only with Hub (purple)

OMP Routes on Device2 (Spoke2)

The following describes the state of OMP routes on Device2.

- Before Configuration: The **show sdwan omp route vpn 1** command shows that Device2 could reach the Device1 (Spoke1) prefix directly through Device1 (TLOC IP column shows the system IP of Device1).
- After configuration: Device2 can reach the Device1 (Spoke1) prefix only through the hub.

Figure 10: Spoke2: OMP Routes Before and After

Before

```
Device2-future-spoke2#show sdwan omp route vpn 1

                                                  PATH                    ATTRIBUTE
TENANT    VPN    PREFIX           FROM PEER       ID     LABEL    STATUS  TYPE       TLOC IP          COLOR
-----------------------------------------------------------------------------------------------------------
0         1      10.20.35.0/24    172.16.255.19   17     1003     C,I,R   installed  172.16.255.35    lte
                                  172.16.255.20   23     1003     C,R     installed  172.16.255.35    lte
```

Device1 prefix

via Device1

After

```
Device2-spoke2#show sdwan omp route vpn 1
                                                  PATH                    ATTRIBUTE
TENANT    VPN    PREFIX           FROM PEER       ID     LABEL    STATUS  TYPE       TLOC IP          COLOR
-----------------------------------------------------------------------------------------------------------
0         1      10.20.35.0/24    172.16.255.19   11     1003     C,I,R   installed  172.16.255.15    lte
                                  172.16.255.19   12     1003     C,I,R   installed  172.16.255.15    3g
                                  172.16.255.20   11     1003     C,R     installed  172.16.255.15    lte
                                  172.16.255.20   12     1003     C,R     installed  172.16.255.15    3g
```

Device1 prefix

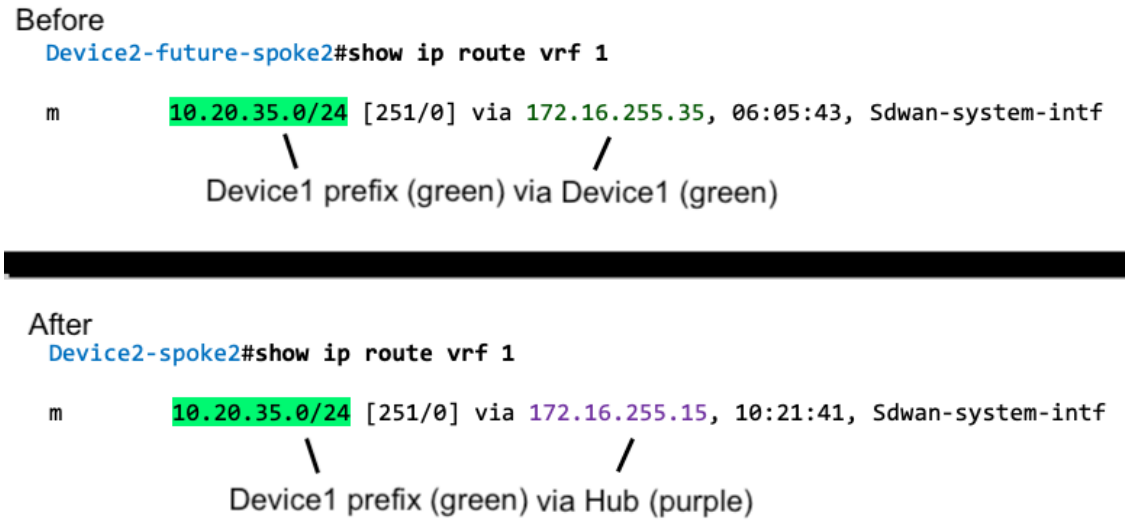
via Hub

IP Routes on Device2 (Spoke2)

The following describes the state of IP routes on Device2.

- Before Configuration: The **show ip route vrf 1** command shows that Device2 could reach the Device1 prefix directly through Device1.
- After configuration: Device2 can reach the Device1 (Spoke1) prefix only through the hub.

Figure 11: Spoke2: IP Routes Before and After



Hub-and-Spoke use cases

Provides details about practical scenarios where a centralized architecture meets specific organizational needs. Reviewing these examples, such as implementing centralized firewall services for branch traffic, helps you identify opportunities to enhance security and policy enforcement across your network locations.

Hub-and-spoke use cases describe practical scenarios where this network topology is effectively applied to meet specific organizational needs and leverage its benefits.

Example (Centralized Network Services)

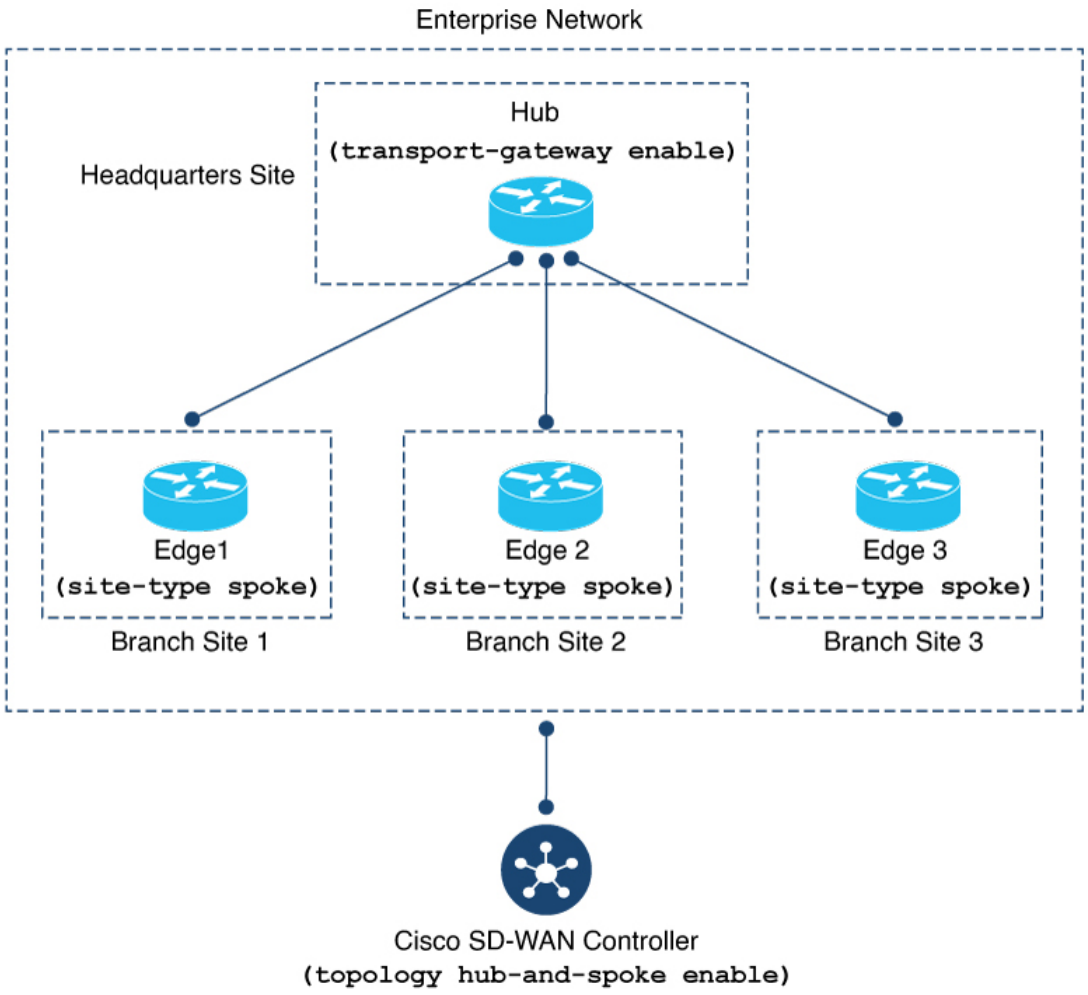
Consider an organization's network with the following characteristics:

- Headquarters Site: Features a single device designated as a hub, running numerous network services such as an enterprise firewall.
- Branch Sites: Consists of three branch locations, each equipped with an edge router.

Network administrators choose to implement a hub-and-spoke topology to route all traffic between branch sites through the headquarters hub. This strategic decision allows for the consistent application of centralized network services to all inter-branch traffic, enhancing security and policy enforcement.

The following illustration depicts the configured hub-and-spoke topology for this use case.

Figure 12: Hub-and-Spoke Topology



Configure a Hub-and-Spoke topology

Explains how to implement a centralized network model by enabling specific controller settings and assigning router roles. This task guides you through configuring transport gateways and defining site types to achieve an organized topology that simplifies management and reduces peer requirements.

To provide a high-level overview and guide users through the complete process of setting up a hub-and-spoke topology using simplified configuration methods.

Before you begin

Follow these steps to configure a hub-and-spoke topology:

Procedure

1. Configure a Cisco SD-WAN Controller to enable Hub-and-Spoke using Cisco SD-WAN Manager. For more information, see Configure a Cisco Catalyst SD-WAN Controller to enable Hub-and-Spoke using Cisco SD-WAN Manager on page 30.
2. Configure a Cisco SD-WAN Controller to enable Hub-and-Spoke using a CLI Template. For more information, see Configure a Cisco SD-WAN Controller to enable Hub-and-Spoke using a CLI template on page 30.
3. Configure a Router as a Transport Gateway, for Hub-and-Spoke. Hub-and-spoke configuration makes use of site types and transport gateways. See the following procedures in the transport gateway documentation:

Configure a router as a transport gateway using Cisco SD-WAN Manager on page 31
Configure a router as a transport gateway using a CLI template on page 32

4. Configure the Site Type for a Router, for Hub-and-Spoke. Hub-and-spoke configuration makes use of site types and transport gateways. See the following procedures in the transport gateway documentation:

   Configure the site type for a router using Cisco SD-WAN Manager on page 32
   Configure the site type for a router using a CLI template on page 32

Configure a Cisco Catalyst SD-WAN Controller to enable Hub-and-Spoke using Cisco SD-WAN Manager

Explains how to activate centralized topology filtering through the management interface. This task enables the controller to restrict route advertisements to spoke sites, ensuring that all remote connectivity is directed through a designated hub to simplify your network architecture.

Use this procedure to enable the simplified hub-and-spoke topology configuration method on your Cisco SD-WAN Controller via the Cisco SD-WAN Manager graphical user interface.

This configuration is a foundational step for implementing the simplified hub-and-spoke topology in your Cisco Catalyst SD-WAN environment. It prepares the controllers to filter and advertise TLOC and route information appropriately for hub and spoke devices.

Before you begin

Follow these steps to enable hub-and-spoke configuration on your Cisco SD-WAN Controller:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   a) To create a new System template for Cisco SD-WAN Controllers, click **Add Template**, choose **Controller**, and click **System**.
   b) To edit an existing Cisco SD-WAN Controller System template, locate a template of type **Controller System** in the table of existing feature templates, click **...** adjacent to the template, and choose **Edit**.
4. In the **Topology** field, choose **Hub and Spoke**.
5. Click **Save** if creating a new template, or **Update** if editing an existing template.

The Cisco SD-WAN Controller is now configured to enable the hub-and-spoke topology, allowing for the simplified configuration of hub and spoke routers in the network.

Configure a Cisco SD-WAN Controller to enable Hub-and-Spoke using a CLI template

Explains how to enable centralized topology logic by applying specific command-line parameters to your controller configuration. This task allows you to automate the deployment of hub-and-spoke filtering across multiple controllers, ensuring consistent route management and reduced manual intervention in the overlay.

Use this procedure to enable the simplified hub-and-spoke topology configuration method on your Cisco SD-WAN Controllers by applying a CLI template.

This method provides an alternative to using Cisco SD-WAN Manager for enabling hub-and-spoke functionality on controllers. It is suitable for automated deployments or when direct CLI configuration is preferred. 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

Follow these steps to enable hub-and-spoke configuration on your Cisco SD-WAN Controller using a CLI template:

Procedure

1. Enter system configuration mode.

```
system
```

2. Enable a hub-and-spoke topology.

```
topology hub-and-spoke enable
```

> **Note**
>
> To disable hub-and-spoke functionality, use the **no** form of the command.

Example

The following example shows how to enable the hub-and-spoke topology:

```
system
topology hub-and-spoke enable
```

The Cisco SD-WAN Controller is now configured to enable the hub-and-spoke topology via the CLI template, allowing for the simplified configuration of hub and spoke routers in the network.

Configure a router as a transport gateway using Cisco SD-WAN Manager

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - To create a new System template, click **Add Template**, choose a device type, and click **Cisco System**.
   - To edit an existing System template, locate a System template in the table of existing feature templates, click **...** adjacent to the template, and choose **Edit**.
4. In **Basic Configuration**, in the **Transport Gateway** field, choose **On**.
5. Click **Save** if creating a new template, or **Update** if editing an existing template.

Configure a router as a transport gateway using a CLI template

Before you begin

By default, CLI templates execute commands in global configuration mode.

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Procedure

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.

```
system
  transport-gateway enable
```

Configure the site type for a router using Cisco SD-WAN Manager

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - To create a new System template, click **Add Template**, choose a device type, and click **Cisco System**.
   - To edit an existing System template, locate a System template in the table of existing feature templates, click **...** adjacent to the template, and choose **Edit**.
4. In **Basic Configuration**, click **Site Type** and choose a type from the drop-down list .
5. Click **Save** if creating a new template, or **Update** if editing an existing template.

Configure the site type for a router using a CLI template

Before you begin

By default, CLI templates execute commands in global configuration mode.

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Procedure

1. Enter system configuration mode.

   ```
   system
   ```

2. Configure up to four site types for the router. Possible values are br, branch, cloud, spoke, type-1, type-2, and type-3.

   ```
   site-type site-type
   ```

   Note

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

   Example

   The following example configures a router site type as cloud:

   ```
   system
     site-type cloud
   ```

   The following example configure a router with site types cloud and branch:

   ```
   system
     site-type cloud branch
   ```

Hub-and-Spoke configuration verification

Explains how to confirm that your centralized topology is operational and follows expected network behavior. This task involves using specific show commands to examine BFD sessions and OMP routes, ensuring that traffic is correctly following the designated hub-and-spoke paths.

Hub-and-spoke configuration verification involves confirming the correct setup and operational status of a hub-and-spoke topology within a Cisco Catalyst SD-WAN environment. This includes examining configurations on Cisco SD-WAN Controllers, individual hub and spoke routers, and observing expected network behavior.

Methods for Verifying Cisco SD-WAN Controller Configuration

Hub-and-spoke configuration makes use of transport gateways and the site type parameter, which are described in the *transport gateway documentation*.

- For information about verifying a transport gateway configuration, see *Verify a transport gateway configuration using the CLI*.
- For information about verifying the site type, see *Verify the site type of a router using the CLI*.
- For information about verifying BFD sessions, OMP routes, and IP routes on the devices in the network after configuring hub-and-spoke, see the example in the introduction to this feature, here: Hub-and-Spoke connectivity example on page 19.

To verify that a Cisco SD-WAN Controller configuration includes the topology hub-and-spoke enable command, use the show running-config command.

In the following example, the Cisco SD-WAN Controller is configured to enable a hub-and-spoke topology.

```
sdwanController# show running-config
...
system
 topology hub-and-spoke
  enable

To verify that the topology hub-and-spoke enable command has taken effect, use
 the show omp summary command. The output indicates the topology. In the
following example, the topology is hub-and-spoke.

sdwanController# show omp summary
per-state UP
admin-state UP
...
topology hub-and-spoke
```