

Configure DMVPN for SD-Routing Devices

What is Cisco DMVPN

Cisco DMVPN (Dynamic Multipoint VPN) is a routing technique to build a VPN network with multiple sites without having to statically configure all devices. This technique uses tunnelling protocols and encrypted security measures to create virtual connections, or tunnels, between sites. These tunnels are dynamically created as needed, making them both efficient and cost-effective.

Components of Cisco DMVPN

Cisco DMVPN consists of four main components:

Component	Purpose
Multipoint GRE (mGRE)	mGRE is a tunneling mechanism used for creating multipoint Virtual Private Networks (VPNs) using GRE encapsulation. Encapsulating data packets from different sources into a single tunnel facilitates scalability and simplifies VPN management.
Next Hop Resolution Protocol (NHRP)	Next Hop Resolution Protocol (NHRP) is a resolution protocol that allows a Next Hop Client (NHC) to dynamically register with Next Hop Servers (NHSs). With the Dynamic Multipoint Virtual Private Network (DMVPN) design, the NHC is the spoke router, and the NHS is the hub router. Once all the clients are registered, spoke routers can discover other spoke routers within the same non-broadcast multiple access (NBMA) network. NHRP enables businesses to have a way for next-hop servers and next-hop clients to communicate with each other directly, bypassing a central hub and preventing potential bottlenecks.
IPSec encryption	IPSec is a group of protocols for securing connections between devices. IPSec helps keep data sent over public networks secure. It is often used to set up VPNs, and it works by encrypting IP packets, along with authenticating the source where the packets come from.

Component	Purpose
<p>Routing protocols such as BGP, EIGRP and OSPF</p>	<ul style="list-style-type: none"> • BGP : Border Gateway Protocol (BGP) is a set of rules that determine the best network routes for data transmission on the internet. BGP is used as the routing protocol to dynamically exchange routing information between DMVPN spokes and hub, allowing for optimal routing in a hub-and-spoke topology. • EIGRP : Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol that is used to find the best path between any two-layer 3 devices to deliver the packet. The algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize. Devices that are not affected by topology changes are not involved in recomputations. • OSPF : OSPF is a link-state routing protocol that sends information about directly connected links to all the routers in the autonomous system network. This protocol has a full picture of the network topology, which is shared with all the routers in an area of the autonomous system to calculate the shortest path to each destination.

Deployment Scenarios

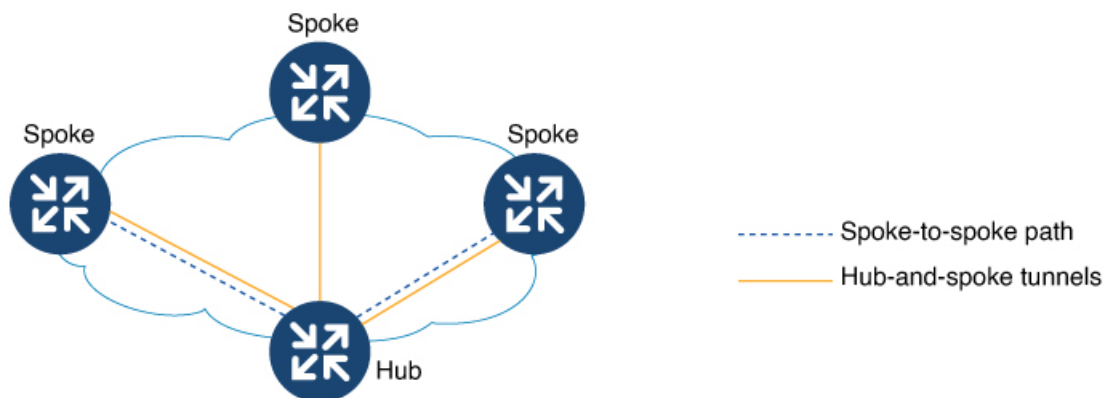
Cisco DMVPN can be deployed in two ways:

Hub and Spoke Deployment Model

In this traditional topology, a central device (Hub) is connected to multiple other devices (Spokes). The primary enterprise resources are located in a large central site, with several smaller sites or branch offices connected directly to the central site over a VPN. Traffic from any remote site to other remote sites passes through the Hub.

This model is best suited for sites requiring lower bandwidth needs.

Figure 1: A DMVPN Solution Deployed in a Hub-Spoke Model

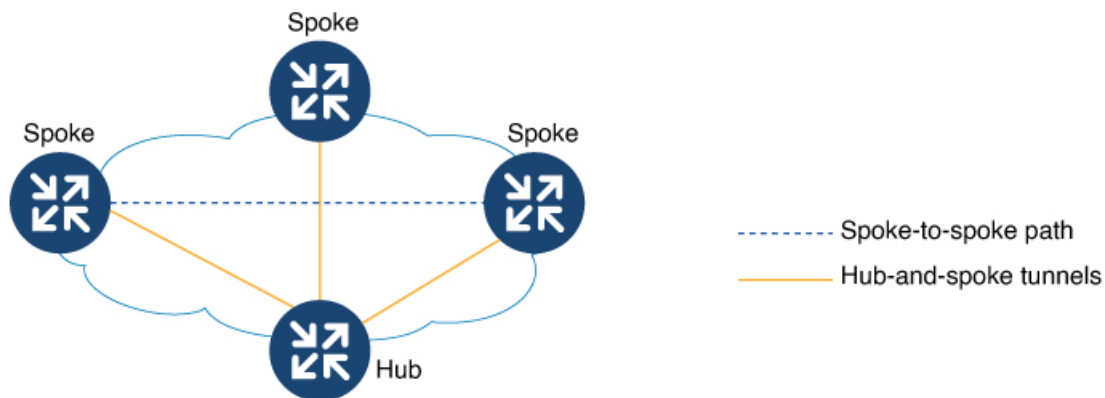


Spoke-to-Spoke Deployment Model

Cisco DMVPN allows the creation of a full-mesh VPN, in which traditional hub-and-spoke connectivity is supplemented by dynamically created IPsec tunnels directly between the spokes. With direct spoke-to-spoke tunnels, traffic between remote sites does not need to go through the Hub.

This eliminates additional delays and conserves WAN bandwidth. This deployment model is best suited for sites requiring higher bandwidth needs.

Figure 2: A DMVPN Solution Deployed in a Spoke-Spoke Model



Configure Cisco DMVPN Using Feature Parcel

This section covers details on how to configure Cisco DMVPN using Feature Parcel for SD-Routing devices.

The following table outlines the various steps involved in creating a DMVPN tunnel using the Feature Parcels in Catalyst SD-WAN Manager.

Steps to Configure a DMVPN Tunnel	To Know More
Configure a VRF in the Service Profile	Configuring a VRF


Steps to Configure a DMVPN Tunnel	To Know More
Configure a DMVPN Tunnel	Step 3 Step 4 Step 5 Step 6 Step 7

Configure a DMVPN Tunnel

This task covers details on configuring a DMVPN tunnel in the Catalyst SD-WAN Manager using Service Profile.

Before you begin

Before you configure a DMVPN tunnel, ensure that you [Configure a VRF in Service Profile](#) .

- Step 1** Go to Cisco Catalyst SD-WAN Manager. Select **Configuration** > **Configuration Groups**. Select Solution as **SD Routing**.
- Step 2** Select the Service Profile created as part of [Configure a VRF](#) task. Select the VRF, click + and select **DMVPN Tunnel**. You can choose an existing DMVPN tunnel from the list or create a new DMVPN tunnel.
- Step 3** Specify a name and description for the DMVPN tunnel. Under the Basic Configuration tab specify the following:
- **Interface Name:** Specify the interface name in the format **dmvpn** <number from 1-255> For example: *dmvpn1*. It is important to ensure that the interface name is unique on the SD-Routing device.
 - **Shutdown :** (Optional) Click the toggle button to turn on the DMVPN tunnel. By default, the DMVPN tunnel is shut.
 - **Description :** (Optional) Specify a description for the interface.
 - **Tunnel Key:** Specify a number from 0 to 4,294,967,295 that identifies the tunnel key. The tunnel key can also be used as a parameter to route different types of traffic through the different tunnels. You can also use the tunnel keys to enforce specific routing policies.
-  The key number must be set to the same value on all hubs and spokes that are in the same DMVPN network.
- Note**
- **IPSec Profile :** (Optional) If you prefer to encrypt the DMVPN tunnel, select an IPSec profile. For steps on creating an IPSec profile, see [Encrypt Data in a DMVPN Tunnel, on page 6](#).

- Step 4** Specify overlay and underlay details.

DMVPN supports IPv4 and IPv6 unicast and multicast transport through the overlay and underlay tunnels.

Overlay

- a) **IPv4 address and IPv4 Subnet Mask :** Specify the IPv4 address and subnet mask.
- b) **IPv6 Prefix :** Specify the prefix for the IPv6 address.

Underlay

Select either **IPv4** or **IPv6** address for underlay transport.

- **Tunnel Source** : Specify a valid interface name for a tunnel interface.
- **VRF** : From the drop-down list, select the VRF that is configured for the **Tunnel Source** interface.
- **Global VRF** : Select the global VRF for forwarding tunnel packets.

Step 5 Configure NHRP

DMVPN Role

- Hub, Spoke, or Both** : Decide the role of DMVPN in the network – Hub, Spoke or both.
- Network ID** : Specify a globally unique 32-bit network identifier from a non-broadcast multiaccess (NBMA) network to enable NHRP on an interface. The range is from 1 to 4294967295.
- Hold Time** : (Optional) Specify the time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses. The recommended value ranges from 300 seconds to 600 seconds.
- Authentication Key** : (Optional) Specify the authentication string for an interface.



The NHRP authentication string must be set to the same value on all hubs and spokes that are in the same DMVPN network.

Note

- Redirect** : (Optional) This option is enabled when you select the DMVPN role as **Hub** or **Both**. When redirect is enabled, the Hub informs the Spokes of a more efficient and shorter paths to reach a particular destination. This allows the devices to communicate directly with each other without the need for an intermediate hop.
- Shortcut** : (Optional) This option is enabled when you select the DMVPN role as **Spoke** and helps the Spoke to accept redirect messages issued by the Hub.

NHRP Summary Map

IPv4 NHRP Summary Map and IPv6 NHRP Summary Map: The spoke-to-spoke NHRP summary map uses the configured IP address network and subnet mask in the NHRP resolution response instead of the IP address network and subnet mask from RIB. This functionality is useful to reduce the NHRP resolution traffic on the network.

NBMA Summary Map



NBMA Summary Map details are only required to be entered if you select the **DMVPN Role** as **Spoke** or **Both**.

Note

IPv4 NHS NBMA Summary Map and IPv6 NHS NBMA Summary Map: You can configure a fully qualified domain name (FQDN) for the non-broadcast multiple access network (NBMA) address of the hub (NHS) on the spokes (NHCs). This allows spokes to dynamically locate the IP address of the hub using FQDN.

- **NHS Address** : Specify the IP address of the Spoke. This IP address should match the IP address of the tunnel interface specified in IPv4 overlay for the Hub.
- **NBMA Address** : Specify the address of the source interface of the tunnel on the Hub.
- **Multicast**: Select the toggle button to enable multicast traffic.

Step 6 Configure BFD

Select the toggle button to enable BFD. Enabling BFD provides fast peer failure detection by sending rapid failure detection notices to the control protocols and reducing overall network convergence time.

- **Transmit Interval (Milliseconds)**: (optional) The minimum interval for transmitting single-hop BFD control packets.
- **Minimum Receive Interval (Milliseconds)**: (optional) The minimum interval for receiving BFD control packets.

- **Multiplier:** (optional) The multiplier specifies the minimum number of consecutive packets that can be missed before a session is declared down.

Step 7 Configure Advanced Parameters.

- IPv4 MTU and IPv6 MTU :** (Optional) Specify the default maximum transmission unit (MTU) size for frames received and transmitted on all interfaces. The default value is 1400 bytes.
- IPv4 TCP MSS and IPv6 TCP MSS :** (Optional) Specify the maximum segment size for all TCP connections. The default value is 1360 seconds.
- Throughput Delay :** (Optional) Set a delay value for an interface, in tens of microseconds. By default value is 1000 seconds.
- Bandwidth :** (Optional) Specify the intended bandwidth, in kilobytes per second (kbps). The default value is 1400 Kbps.

For more information on each of the parameters used in the Feature Profile, see [Security and VPN Configuration Guide](#).

What's next

After configuring a DMVPN tunnel, [Associate and Deploy the Configuration Group to an SD-Routing Device, on page 9](#).

Encrypt Data in a DMVPN Tunnel



Note

Adding IPsec encryption to data helps secure the data in the tunnel while it travels through the network. The IPsec encryption used in Cisco DMVPN is based on IKEv2. Configuring IPsec with IKEv1 is not supported.

This is an optional configuration.

Before you begin

Before you configure **Enterprise CA** as the **IKEv2 Authentication Type** for IPsec encryption, ensure that you have already configured a Trustpoint as part of **SCEP enrollment** in **System Profile > Certificate**.

Step 1 Go to Cisco Catalyst SD-WAN Manager. Select **Configuration > Configuration Groups**. Select solution as **SD Routing**.

Step 2 Select an existing **Service Profile** or create a new one.

Step 3 Select an existing DMVPN tunnel. Click + to create an **IPSec profile**.

Step 4 Specify a name and description to identify the IPsec profile. Enter details to configure the profile.

Authentication

- Local Identity:** Specify the local IKE identity to send in the exchange with the destination peer to establish communication.
- Remote Identity:** Specify the remote IKE identity to exchange with the destination peer to establish communication. You can configure multiple remote identities. The different Identity types are :
 - IPv4
 - IPv6 prefix
 - FQDN
 - Email

KeyID

IKEv2 Authentication Type: IKEv2 is a tunneling protocol that provides a secure VPN communication channel between peer VPN devices and defines negotiation and authentication for IPSec security associations (SAs) in a protected manner.

- a) **Groups PSK:** Select this option to configure a common pre-shared key for all remote access clients connecting to a device. Choose **Global** from the drop-down list and specify the key to be used as an authentication key.
- b) **Peer-peer PSK:** Select this option to configure a common pre-shared key to be shared with peers in the network.

Peer name : Specify a name for the peer.

Pre-shared Key: Specify a key.

Peer Address Type : Select between IPv4 address or IPv6 prefix.

- c) **Enterprise CA :** Select this option to get the certificate signed by the internal Root CA.

PKI Trustpoint Name : Choose a Trustpoint from the drop-down list.

Signature Type : Choose **Global** from the drop-down list. Select the signature type for authentication. The default signature is RSA.

IKEv2 Settings

- a) **DPD keepalive Interval:** Specify the keepalive interval for IKE peers. DPD is a method used by devices to verify the current existence and availability of IPSec peers. By default, it is 10 seconds.
- b) **DPD Retry Interval:** Specify the retry interval for IKE peers. Retry interval indicates the number of seconds between DPD retry messages if the DPD retry message is missed by the peer; the range is from 2 to 60 seconds. By default it is 3 seconds .
- c) **IKE SA Lifetime:** Specify the length of time that a negotiated IKE SA (Security Association) key is effective. By default the lifetime is 86400 seconds.

IPSec Settings

- a) **Security Association (SA) Lifetime (Seconds):**Specify the number of seconds a security association will live before expiring.
- b) **Anti Replay Window Size :**Specify the packet size. This option when set prevents duplication of encrypted packets by assigning a unique sequence number to each encrypted packet.
- c) **Perfect Forward Secrecy(PFS) :**Toggle the button to enable PFS. Enabling PFS ensures that the same key will not be generated again, so this option forces a new Diffie-hellman key exchange. PFS adds another level of security because if one key is ever cracked by an attacker, only the data sent with that key is compromised.
- d) **PFS Group :** Specify the Diffie-Hellman groups. The Internet Key Exchange (IKE) protocol uses Diffie-Hellman to derive key material for both the IKE and IPSec security associations (SA).

Step 5 Click **Save** .

Configure Cisco DMVPN Using Commands

In addition to the features configured using Feature Profile, you can use IOS XE commands in Cisco SD-WAN Manager and configure any additional features.

Use IOS XE CLI commands to add configurations to your device that are not available through Feature Parcels.



Note

The IOS XE commands operate together with the configurations provided through Feature Parcels. However, commands configured either using **CLI Add-on Profile** or **CLI Config Group** override the configurations specified by the corresponding Feature Parcel.

Configuring Cisco DMVPN Using CLI Add-on Profile

Before you begin

- You should have an understanding of the features you want to provision in your setup. Guidance for the different features and their configuration commands are available in [Security and VPN Configuration Guide](#).
- You must onboard the autonomous routing device to the Catalyst Cisco SD-WAN Manager and the status of the devices should be **In Sync**. Check the status of the device using **Configuration > WAN Edges**.

- Step 1** Go to Cisco Catalyst SD-WAN Manager. Select **Configuration > Configuration Groups**. Select Solution as **SD Routing**.
- Step 2** Select an existing Configuration Group or create a new one. Select the configuration group, click + **Add Profile** to add a **CLI Add-on Profile**.
- Step 3** To create a new profile, select + **Create New**. Specify name and description. If you have an existing CLI Add-on profile, select the profile, click **Edit**.
- Step 4** In the **Config Preview** pane, enter the commands required for configuring features. Click **Save** and then **Done**.
- Step 5** [Associate and Deploy the Configuration Group to an SD-Routing Device, on page 9](#). Click **Next**.
- Step 6** In the Summary window, select **Preview CLI**. The old and new configuration is displayed. Review the changes. Click **Cancel** to go back to Configuration Groups.

Configuring Cisco DMVPN Using CLI Config Group

Before you begin

- You should have an understanding of the features you want to have in your setup. Guidance for the features and their configuration commands are available in https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-conn-dmvpn-dmvpn-0.html
- You must onboard the autonomous routing device to the Cisco SD-WAN Manager and the status of the devices should be **In Sync**. Check the status of the device using **Configuration > WAN Edges**.

- Step 1** Go to Cisco Catalyst SD-WAN Manager. Select **Configuration > Configuration Groups**. Select Solution as **SD Routing**.
- Step 2** Select an existing CLI Config group from the list or select **Create Configuration Group** to create a new configuration group.
- Step 3** Specify a name, description. Select the **CLI Configuration Group** checkbox.
- Step 4** Select a device to load the configuration from. In the **Config Preview** pane, review the configuration and enter the commands required for configuring additional features. Click **Save** and **Done**.
- Step 5** [Associate and Deploy the Configuration Group to an SD-Routing Device, on page 9](#). Click **Next**.
- Step 6** In the Summary window, select **Preview CLI**. The old and new configuration is displayed. Click **Cancel** to go back to Configuration Groups.

Associate and Deploy the Configuration Group to an SD-Routing Device

This task involves associating the configured profile to a Configuration Group and provisioning the changes to one or more SD-Routing devices.

Before you begin

Ensure that the Configuration Group you select is created for SD-Routing devices.

- Step 1** On Cisco SD-WAN Manager, select the **Configuration Group** created earlier.
- Step 2** Click + **Add** and select the devices from the list. Click **Save** to attach the configuration group to the selected devices.
- Step 3** To provision the configuration changes, click **Deploy**.
- Select the device on which you want to provision the configuration changes. Click **Next**.
 - For each device, review or update the IP address, hostname. Specify the password to access these devices. Click **Next**.
 - If you want to review the configuration changes, click **Preview CLI**. Select the device to view the configuration changes either inline or side by side. The configurations that are removed are highlighted in red and the new configuration is highlighted in green. To remove or add any device from the list of selected devices, **click Edit Device List**
 - Click **Deploy** to provision the configuration changes on the devices.

Monitor Cisco DMVPN

This section provides details on how to monitor Cisco DMVPN using commands.

Monitor Cisco DMVPN Sessions Using Commands

Use these commands to monitor the DMVPN tunnels and view session information. These commands can be executed using **Tools > SSH terminal** in Cisco Catalyst SD-WAN Manager.

Use command	To
show dmvpn	display DMVPN session information.
show dmvpn detail	display detail DMVPN information for each session, including Next Hop Server (NHS) and NHS status, crypto session information, and socket details.
show crypto session	display status information for active crypto sessions.
show ip nhrp traffic	display statistics of NHRP traffic.
show ip nhrp summary	display the mapping of all the overlay entries.