DMVPN

These help topics provide information about Dynamic Multipoint Virtual Private Network (DMVPN) configuration screens.

Dynamic Multipoint VPN

This wizard will help you to configure your router as a Dynamic Multipoint VPN (DMVPN) hub or DMVPN spoke. A typical VPN connection is a point-to-point IPSec tunnel connecting two routers. DMVPN enables you to create a network with a central hub that connects other remote routers, referred to as spokes using a GRE over IPSec tunnel. IPSec traffic is routed through the hub to the spokes in the network. Cisco SDM allows you to configure your router as a primary or a secondary DMVPN hub, or as a spoke router in a DMVPN network.

The following link contains more information about DMVPN (requires CCO login ID).

Multipoint IPSec VPNs

Cisco SDM supports the configuration of a hub-and-spoke DMVPN that uses IPSec profiles to define encryption. You can configure a fully-meshed DMVPN, and use crypto-maps to define encryption in the DMVPN using the CLI. Fully meshed DMVPNs and DMVPN networks using crypto maps are managed and modified using the CLI. Cisco SDM supports the configuration of a DMVPN starting from IOS version 12.2(13)T.

Cisco SDM supports the configuration of a single DMVPN on a router.

In this screen, identify your router as a hub or as a spoke in the DMVPN network.
It is important to configure the hub first because spokes must be configured using information about the hub. If you are configuring a hub, you can use the SpokeConfiguration feature available in the Summary window to generate a procedure that you can send to spoke administrators so that they can configure the spokes with the correct hub information. If you are configuring a spoke, you must obtain the correct information about the hub before you begin.

Create a spoke (client) in Dynamic Multipoint VPN

Select if your router is a spoke in the DMVPN network. Spokes are the logical endpoints in the network. Before starting configuration, you should ping the hub to be sure you have connectivity to it, and have all the necessary information about the hub configuration that you need. This information is listed in Dynamic Multipoint VPN (DMVPN) Spoke Wizard.

Create a hub (server or head-end) in Dynamic Multipoint VPN

Select if your router is a hub in the DMVPN network. The hub is the logical center point in a DMVPN network, and is connected to each spoke router via a point-to-point IPSec connection. The hub can route IPSec traffic between the spoke routers in the network.

Dynamic Multipoint VPN (DMVPN) Hub Wizard

This wizard will help you configure your router as a DMVPN hub. The hub should be configured before the spokes so that you can provide the spoke administrators with the information they need to configure their spoke routers.

The application window explains what you will be configuring. After you have finished, you will need to provide spoke administrators with the following information about the hub:

- The IP address of the hub router’s physical interface.
- The IP address of the hub’s mGRE tunnel interface.
- The dynamic routing protocol to use to send routing updates to the DMVPN, and the autonomous system (AS) number (for EIGRP), or process ID (for OSPF) that should be used.
Cisco SDM’s Configure Spoke feature enables you to create a text file that contains the information that spoke administrators need about the hub’s configuration. This feature is available from the Summary window of this wizard. You also need to tell the spoke administrators which subnet mask to use, and assign each spoke an IP address from the same subnet as the hub so that address conflicts do not occur.

**Type of Hub**

DMVPN networks can be configured with a single hub, or with a primary and a backup hub. Identify the type of hub you are configuring your router as.

**Primary Hub**

Check if the router is the primary hub in the DMVPN network.

**Backup Hub**

Check this button if the router is a backup hub in a full-mesh DMVPN network.

**Configure Pre-Shared Key**

DMVPN peers can use a pre-shared key or digital certificates to authenticate connections from each other. If pre-shared keys are used, each hub router and spoke router in the network must use the same pre-shared key.

Pre-shared keys should be exchanged with the administrator of the remote site through some secure and convenient method, such as an encrypted e-mail message. Question marks (?) and spaces must not be used in the pre-shared key. The pre-shared key can contain a maximum of 128 characters.

**Pre-Shared Key**

Enter the pre-shared key used in the DMVPN network. Question marks (?) and spaces must not be used in the pre-shared key. The pre-shared key can contain a maximum of 128 characters.
Digital Certificates

Select this button if your router uses digital certificates for authentication. Digital certificates are configured under VPN Components>Public Key Infrastructure.

Confirm Pre-Shared Key

Reenter the key for confirmation. If the values in this field and the Pre-Shared Key field do not match, Cisco SDM prompts you to reenter them.

Hub GRE Tunnel Interface Configuration

Multipoint Generic Routing Encapsulation (mGRE) is used in a DMVPN network to allow a single GRE interface on a hub to support an IPSec tunnel to each spoke router. This greatly simplifies DMVPN configuration. GRE allows routing updates to be sent over IPSec connections.

Select the interface that connects to the Internet

Select the router interface that connects to the Internet. The GRE tunnel originates from this interface.

Selecting an interface that uses a dialup connection may cause the connection to be always up. You can examine supported interfaces in Interfaces and Connections to determine if a dialup connection. Typically, interfaces such as ISDN or Asynchronous Serial will be configured for a dialup connection.

IP Address

Enter the IP address for the mGRE interface. This must be a private address and be in the same subnet as the GRE interfaces of the other routers in the network. For example, the GRE interfaces might share the subnet 10.10.6.0, and be given IP addresses in the range 10.10.6.1 through 10.10.6.254.

Subnet Mask

Enter the mask for the subnet that the GRE interfaces are in. For example, the mask for the subnet 10.10.6.0 could be 255.255.255.0. For more information, see IP Addresses and Subnet Masks.
Advanced Button

Cisco SDM provides default values for advanced tunnel settings. However, the hub administrator must decide on the tunnel settings and give them to the personnel administering spoke routers so that they can make matching settings.

Advanced Configuration for the Tunnel Interface

Use this window to configure GRE tunnel parameters. Cisco SDM provides default values, but you must obtain the correct values from the hub administrator and enter them here.

The default values are provided in this help topic. If you change from the default, and need to restore it, consult this help topic.

NHRP Authentication String

Enter the string that DMVPN hubs and spokes must use to authenticate themselves for NHRP transactions. The string can be up to 8 characters long. Special characters such as spaces, question marks (?) are not allowed. All devices in the DMVPN must be configured with the same authentication string.

Cisco SDM Default: DMVPN_NW

NHRP Network ID

Enter the NHRP Network ID. The network ID is a globally unique, 32-bit network identifier for a nonbroadcast, multiaccess (NBMA) network. The range is 1 to 4294967295.

Cisco SDM Default: 100000

NHRP Hold Time

Enter the number of seconds that NHRP network IDs should be advertised as valid.

Cisco SDM Default: 360
Tunnel Key

Enter the key to use for this tunnel. This key should be the same for all mGRE tunnels in the network.
Cisco SDM Default: 100000

Bandwidth

Enter the intended bandwidth, in kilobytes per second (kbps). Default bandwidth values are set during startup; the bandwidth values can be displayed using the show interfaces EXEC command. 1000 is a typical bandwidth setting in DMVPN configurations.
Cisco SDM Default: 1000

MTU

Enter the largest amount of data, in bytes, that should be allowed in a packet travelling through the tunnel.
Cisco SDM Default: 1400

Tunnel Throughput Delay

Set a delay value for an interface, in tens of microseconds.
Cisco SDM Default: 1000

Primary Hub

If the router you are configuring is the backup hub in the DMVPN network, you need to identify the primary hub by providing its public and private IP addresses.

Public IP Address

Enter the IP address of the interface on the primary hub that is used for this tunnel. This should be a static IP address. Obtain this information from the hub administrator.
IP Address of hub’s mGRE tunnel interface

Enter the IP address of the mGRE tunnel interface on the primary hub. Obtain this information from the hub administrator.

Select Routing Protocol

Use this window to specify how other networks behind your router are advertised to the other routers in the network. Select one of the following:

- **EIGRP**—Extended Interior Gateway Routing Protocol.
- **OSPF**—Open Shortest Path First.
- **RIP**—Routing Internet Protocol.
- **Static Routing.** This option is enabled when you are configuring a GRE over IPSec tunnel.

**Note**

RIP is not supported for DMVPN Hub and spoke topology but is available for DMVPN Full Mesh topology.

Routing Information

Use this window to add or edit routing information about networks behind the router that you want to advertise to the other routers in the network. The fields in this window vary according to the routing protocol specified.

For more information on RIP parameters, see Add or Edit an RIP Route.
For more information on EIGRP parameters, see Add or Edit EIGRP Route.
For more information on OSPF parameters, see Add or Edit an OSPF Route.

Please select the version of RIP to enable

Specify RIP version 1 or version 2.
Select an existing OSPF process ID/EIGRP AS number

You can select an existing process ID for OSPF or AS number for EIGRP if one has been previously configured. See Recommendations for Configuring Routing Protocols for DMVPN.

Create a new OSPF process ID/EIGRP AS number

If no process IDs exist, or if you want to use a different one, you can configure a process ID in this field.

OSPF Area ID for tunnel network

Enter a new OSPF area ID for the network. This area ID is for the tunnel network. Cisco SDM automatically adds the tunnel network to this process using this area ID.

Private networks advertised using <protocol-name>

This area shows the networks advertised using the selected routing protocol. If you have already configured the routing protocol you specified in this wizard, the networks that you specified to be advertised will appear in this list.

Add all the private networks that you want to advertise to the DMVPN peers using this routing process. The DMVPN wizard automatically adds the tunnel network to this process.

Network—A network address. You can enter the address of a specific network, and use the wildcard mask to generalize the advertisement.

Wildcard mask—(EIGRP and OSPF protocols) A bit mask that specifies how much of the network address must match the address given in the network column. This mask can be used to have the router advertise networks in a particular range, based on the given address. A 0 bit specifies that the bit in the network address must match the corresponding bit in the given network address.

For example, if the network address were 172.55.10.3, and the wildcard mask was 0.0.255.255, the router would advertise all networks starting with the numbers 172.55, not just the network 172.55.10.3.

Area—Shown when OSPF is selected, the OSPF area number for that network. Each router in a particular OSPF area maintains a topological database for that area.
**Dynamic Multipoint VPN (DMVPN) Spoke Wizard**

This wizard helps you to configure your router as a spoke in a DMVPN network. Before starting the configuration, you should ping the hub to be sure that your router can send traffic to it. Also you should have all the information about the hub you need before you begin. A hub administrator who uses Cisco SDM to configure the hub can generate a text file that contains the hub information spoke administrators need.

You need to obtain the following information before you begin:

- The IP address of the hub’s physical interface.
- The IP address of the hub’s mGRE tunnel interface.
- The IP address and subnet mask the hub administrator tells you to use for your spoke. The hub administrator must assign addresses to each spoke to ensure that all routers in the DMVPN are in the same subnet, and that each is using a unique address.
- The routing protocol to use, and the AS number (EIGRP) or Process ID (OSPF) that is to be used to send routing updates in the DMVPN.

**DMVPN Network Topology**

Select the type of DMVPN network this router is a part of.

**Hub and Spoke Network**

Select this option if you are configuring the router in a network where each spoke router has a point-to-point GRE over IPSec connection to the DMVPN hub, and will send traffic destined for other spokes through the hub. When you select this option, the graphic displays links from the spokes to the hub.
Fully Meshed Network

Select if you are configuring the router as a spoke capable of establishing a direct IPSec tunnel to other spokes in the network. A multipoint GRE tunnel is configured on the spoke to support this functionality. When you select this option, the graphic displays links from the spokes to the hub, and links to each other.

The wizard screen list the IOS images required to support a fully-meshed DMVPN network.

Specify Hub Information

Use this window to provide necessary information about the hub in the DMVPN.

IP Address of Hub’s physical interface

Enter the IP address of the interface on the hub. Obtain this address from the hub administrator. This address will be used as the tunnel destination.

IP Address of hub’s mGRE tunnel interface

Enter the IP address of the mGRE tunnel interface on the hub. The mGRE tunnel addresses for the hub and spokes must be in the same subnet.

Spoke GRE Tunnel Interface Configuration

A point-to-point will be created for this spoke using the information entered in this window.

Select the interface that connects to the Internet

Select the router interface that connects to the Internet. The GRE over IPSec tunnel originates from this interface.

Selecting an interface that uses a dialup connection may cause the connection to be always up. You can examine supported interfaces in Interfaces and Connections to determine if a dialup connection, such as an ISDN or Async connection has been configured for the physical interface you selected.
Re-register with hub when IP address of interface-name changes—This option is available when the interface you selected receives a dynamic IP address via DHCP or IPCP. Specifying this option will allow the spoke to re-register with the hub when it receives a new IP address.

IP Address

Enter the IP address for the GRE interface to this hub. This must be a private address and be in the same subnet as the GRE interfaces of the other routers in the network. For example, the GRE interfaces might share the subnet 10.10.6.0, and be given IP addresses in the range 10.10.6.1 through 10.10.6.254.

If you are configuring a spoke router, you must use the IP address assigned to your router by the hub administrator. Failure to do so may result in address conflicts.

Subnet Mask

Enter the mask for the subnet that the GRE interfaces are in. This mask must be assigned by the hub administrator and be the same for all routers in the DMVPN. For example, the mask for the subnet 10.10.6.0 could be 255.255.255.0. For more information, see IP Addresses and Subnet Masks.

Advanced Button

Click this button to provide NHRP and tunnel parameters for this connection. Cisco SDM provides default values for advanced tunnel settings. However, the hub administrator must decide on the tunnel settings and give them to the personnel administering spoke routers so that they can make matching settings. If you are configuring a spoke router, obtain the tunnel settings from the hub administrator, click this button, and enter them in the dialog box displayed.

Cisco SDM Warning: DMVPN Dependency

This window appears when the interface you have chosen for the DMVPN tunnel source has a configuration that prevents its use for DMVPN. Cisco SDM informs you of the conflict and gives you the option of allowing Cisco SDM to modify the configuration so that the conflict is removed.
Firewall

If a firewall has been applied to the interface that was designated as the tunnel source, Cisco SDM can add access rule entries to the configuration so that GRE, IPSec, and ISAKMP traffic is allowed through the firewall.

View Details

Click this button to view the access control entries that Cisco SDM will add to the access rule if you select Allow GRE, IPSec, and ISAKMP traffic through the firewall.

These entries allow both kinds of ISAKMP traffic, GRE traffic, Encapsulating Security Protocol (ESP), and Authentication Header Protocol (AHP).

Edit Dynamic Multipoint VPN (DMVPN)

This window displays the existing DMVPN tunnel configurations. DMVPN enables you to create a network with a central hub that connects other remote routers, referred to as spokes. Cisco SDM supports hub-and-spoke network topology, in which GRE over IPSec traffic is routed through the hub. Cisco SDM allows you to configure your router as a primary or a secondary DMVPN hub, or as a spoke router in a DMVPN network.

The following link contains more information about DMVPN (requires CCO login ID). Multipoint IPSec VPNs

Cisco SDM supports the configuration of a hub-and-spoke DMVPN that uses IPSec profiles to define encryption. You can configure a fully-meshed DMVPN, and use crypto-maps to define encryption in the DMVPN using the CLI. Fully meshed DMVPN and DMVPN using crypto maps are managed and modified using the CLI.

Cisco SDM supports the configuration of a single DMVPN on a router.

The hub should be configured first, to establish the hub IP addresses and the routing parameters that the spokes must be configured with. For other recommendations on how to configure the routers in a DMVPN, see DMVPN Configuration Recommendations.
Interface

The physical interface from which this tunnel originates.

IPSec Profile

The IPSec profile that the tunnel uses. The IPSec profile defines the transform sets that are used to encrypt traffic on the tunnel. Cisco SDM supports the use of only IPSec profiles to define encryption in a DMVPN. If you want to use crypto-maps, configure the DMVPN using the CLI.

IP Address

The IP address of the GRE tunnel. The GRE tunnel is used to send routing updates to the DMVPN.

Description

A description of this tunnel.

Details panel

The Details panel shows the values for the entire configuration of the DMVPN tunnel.

Why Are some Tunnels Interfaces Shown as Read-Only?

A tunnel interface is shown as read-only if it has already been configured with crypto-map associations and NHRP parameters. You will be able to modify NHRP parameters and routing information from this window, but you must edit the IP address, tunnel source, and tunnel destination from the Interfaces and Connections window.

Add

Click to add a new DMVPN tunnel configuration.

Edit

Click to edit a selected DMVPN tunnel configuration.
Delete

Click to delete a DMVPN tunnel configuration.

General Panel

In this panel add or edit general configuration parameters of the DMVPN tunnel.

IP Address

Enter the IP address of the tunnel. This must be a private address and must be in the same subnet as the other tunnel addresses in the DMVPN. If you are configuring a spoke, you must use the address that the hub administrator has assigned to your router so that no address conflicts occur.

Mask

Enter the subnet mask that the hub administrator has assigned to the DMVPN. For more information, see IP Addresses and Subnet Masks.

Tunnel Source

Select the interface that the tunnel is to use, or enter that interface’s IP address. See Using Interfaces with Dialup Configurations before you select an interface configured for a dialup connection.

Tunnel Destination

Click This is a multipoint GRE tunnel if this is a DMVPN tunnel in a fully-meshed network. Click IP/Hostname and specify an IP address or hostname if this is a hub-and-spoke network.

IPSec Profile

Select a configured IPSec profile for this tunnel. The IPSec profile defines the transform sets that are used to encrypt traffic on this tunnel.
MTU

Enter the largest amount of data, in bytes, that should be allowed in a packet traveling through the tunnel.

Bandwidth

Enter the intended bandwidth, in kilobytes per second (kbps). Default bandwidth values are set during startup; the bandwidth values can be displayed using the show interfaces EXEC command. The value 1000 is a typical bandwidth setting in DMVPN configurations.

Delay

Set a delay value for an interface, in tens of microseconds. The value 1000 is a typical delay setting in DMVPN configurations.

Tunnel Key

Enter the key to use for this tunnel. This key should be the same for all mGRE tunnels in the network.

This is a multipoint GRE Tunnel

Check if this to be an mGRE tunnel interface, an interface capable of maintaining connections to multiple peers. If this router is being configured as a DMVPN hub, you must check this box to allow the hub to establish connections with all spokes. If the router is being configured as a spoke, check this box if you are configuring a fully meshed DMVPN. In this way, a spoke can establish a connection to the hub to send traffic and receive next hop information to directly connect to all other spokes in the DMVPN.

NHRP Panel

Use this panel to provide NHRP configuration parameters.
**Authentication String**

Enter the string that DMVPN hubs and spokes must use to authenticate themselves for NHRP transactions. The string can be up to 8 characters long. All NHRP stations in the DMVPN must be configured with the same authentication string.

**Hold Time**

Enter the number of seconds that NHRP network IDs should be advertised as valid.

**Network ID**

Enter the NHRP Network ID. The network ID is a globally unique, 32-bit network identifier for a nonbroadcast, multiaccess (NBMA) network. The range is 1 to 4294967295. The network ID must be unique for each NHRP station.

**Next Hop Server**

This area lists the IP addresses of the next hop servers that this router can contact. This area must contain the IP address of the primary and secondary hub if this is a spoke router. If this is a hub, this area must contain the IP addresses of the other hub routers in the DMVPN.

Click Add to enter the IP address of a next hop server. Select a server, and click Delete to delete it from the list.

**NHRP Map**

This area lists the available IP-to-NBMA address mappings. Click Add to create a new map. After you create the map, it will be added to this list. Click Edit to modify a selected map. Click Delete to remove a selected map configuration.

**NHRP Map Configuration**

Use this window to create or edit a mapping between IP and NBMA addresses.
Statistically configure the IP-to-NMBA address mapping of IP destinations connected to an NBMA network.

Click this button if you are configuring a spoke in a fully meshed network. Cisco SDM treats backup hubs as spokes to primary hubs, so also click this if you are configuring a backup hub. In this part of the window you are providing the address information that the spoke or backup hub needs to contact the primary hub.

Destination Reachable through NBMA network—Enter the IP address of the mGRE tunnel configured on the primary hub. Spokes and backup hubs use this tunnel information to establish contact with the hub and create an mGRE tunnel to it. Spokes use the tunnel to send encrypted data to the hub and to query the hub for next hop information to other spokes.

NBMA Address directly reachable—Enter the static IP Address of the interface on the primary hub that supports the mGRE tunnel.

Configure NBMA addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network.

Use this area of the window to provide information used by routing protocols.

Dynamically add spokes’ IP addresses to hub’s multicast cache—Configure this option if you are configuring a primary or a backup hub. This option is needed by the hub to send routing updates to all connected DMVPN spokes.

IP address of NBMA address directly reachable—if you are configuring a spoke in a full meshed DMVPN, or a backup hub, check this box, and provide the static IP Address of the interface on the primary hub that supports the mGRE tunnel.

Routing Panel

Use this panel to configure routing information for the DMVPN cloud.

Routing Protocol

Select the dynamic routing protocol that the hub and spoke routers in this DMVPN use to perform routing. Note that all the routers in the DMVPN must be configured for the routing protocol that you select.

- RIP—Routing Internet Protocol
- OSPF—Open Shortest Path First
Chapter 13  DMVPN

Edit Dynamic Multipoint VPN (DMVPN)

- **EIGRP**—Extended Interior Gateway Routing Protocol

**RIP Fields**

If you selected RIP as the dynamic routing protocol, select **Version 1**, **Version 2**, or **Default**. If you select **Version 2**, the router will include the subnet mask in the routing update. If you select **Default**, the router will send out Version 2 updates, but it will be able to receive RIP Version 1 or Version 2 updates.

**Turn off split horizon**—If this is the hub router, check this box to turn off split horizon on the mGRE tunnel interface. Turning off split horizon allows the router to advertise the routes that it has learned from the tunnel interface out the same interface.

**OSPF Fields**

If you selected OSPF, the following fields must be completed:

**OSPF process ID**—Enter the process ID. This value identifies the OSPF process to other routers. See Recommendations for Configuring Routing Protocols for DMVPN.

**OSPF Network Type**—Select point-to-multipoint or broadcast. Point-to-multipoint causes OSPF to add routes to the routing table on spoke routers. If you wish to avoid this, you can select broadcast.

**OSPF Priority**—The OSPF priority identifies this router as a hub or as a spoke. If this is a hub router, enter a priority value of 2. If this is a spoke router, enter a priority value of 0.

**EIGRP Fields**

If you selected EIGRP, the following fields must be completed:

**Autonomous System Number**—Enter the Autonomous System Number for the group of routers using EIGRP. Routers with the same EIGRP autonomous system number maintain a topological database of routers in the region identified by that number. See Recommendations for Configuring Routing Protocols for DMVPN.

**Turn off split horizon**—If this is the hub router, check this box to turn on split horizon on the mGRE tunnel interface. Leave it unchecked to disable split horizon. Turning off split horizon allows the router to advertise the routes that it has learned from the tunnel interface out the same interface.
Use original next hop— If this is a DMVPN hub router, EIGRP will advertise this router as the next hop. Check this box to have EIGRP use the original IP next hop when advertising routes to the DMVPN spoke routers.

How Do I Configure a DMVPN Manually?

You can configure your router as a DMVPN hub or spoke using the VPN Components windows and the Edit Dynamic Multipoint VPN (DMVPN) window. In order to do so you need to complete the following tasks:

- Configure an IPSec profile. You cannot configure a DMVPN connection until you have configured at least one IPSec profile.
- Configure the DMVPN connection.
- Specify the networks you want to advertise to the DMVPN cloud.

Procedures for these tasks are given below:

To configure an IPSec Profile:

You need to configure an IPSec policy, and then configure a DMVPN tunnel.

Step 1 Click **VPN** in the left panel, and then click **VPN Components**.
Step 2 Click the IPSec Profiles branch, and then click **Add** in the IPSec Profiles window.
Step 3 Name the profile, and select the transform sets it is to contain in the Add an IPSec profile window. You can enter a short description if you want to.
Step 4 Click **OK**.

To configure a DMVPN connection:

Step 1 In the VPN tree, click the **Dynamic Multipoint VPN** branch.
Step 2 Click **Edit Dynamic Multipoint VPN (DMVPN)**.
Step 3 Click **Add**.
How Do I Configure a DMVPN Manually?

Step 4 In the DMVPN Tunnel Configuration window, complete the General, NHRP, and Routing tabs to create a DMVPN tunnel. Consult the online help for more information about a particular field.

To specify the networks you want to advertise to the DMVPN:

If there are networks behind your router that you want to advertise to the DMVPN, you can do so by adding the network numbers in the Routing windows.

Step 1 From the left panel, click Routing.

Step 2 In the Routing window, select the routing protocol that you specified in DMVPN configuration, and click Edit.

Step 3 Add the network numbers that you want to advertise.