



Configuring VPN Settings

VPN settings provide a framework for network behavior and policy implementation.

Settings are defined under **Configuration>Settings** and include the following:

- General VPN settings, in which you define failover and routing and fragmentation policies. See [Working With General VPN Settings, page 1-2](#).
- General firewall settings, in which you define the parameters required for implementing CBAC and for defining access rules, such as fragmentation, timeouts, half open connections, logging, and ACL ranges. See [Defining General Firewall Settings, page 1-2](#).
- Hub settings, in which you define the inside interfaces and internal networks on the hub side of the VPN tunnel, and the parameters required for HA (High Availability) and VPN Services Module support. See [Working with Hub Settings, page 1-19](#).
- Spoke settings, in which you define the inside interfaces, internal networks, and VPN interface on the spoke side of the VPN tunnel, hub assignment for spokes, and the parameters required for NAT traversal support. See [Working with Spoke Settings, page 1-31](#).
- Configuration additions, in which you can manually add CLI commands to the beginning and/or end of a device's configuration. See [Entering Additional CLI Commands \(Beginning and Ending Commands\), page 1-46](#).

Working With General VPN Settings

General VPN settings apply to both hubs and spokes, unlike hub settings, which are specific to hubs, and spoke settings, which are specific to spokes.

Access general VPN settings by selecting **Configuration > Settings > General VPN**.

General VPN settings include:

- Failover and routing settings, where you select either IKE keepalive for failover, or Generic Routing Encapsulation (GRE) for failover and routing. See [Understanding Failover and Routing, page 1-2](#) and [Configuring Failover and Routing Policies, page 1-8](#).
- Fragmentation settings, where you define maximum transmission unit (MTU) handling parameters. See [Understanding Packet Fragmentation, page 1-17](#).

Understanding Failover and Routing

IPSec failover provides VPN tunnel resiliency by rolling tunnel connections seamlessly to a failover (backup) hub if the active hub in a hub-and-spoke configuration becomes unavailable for any reason.

For failover and routing in your VPN hierarchy, you can use either IKE keepalive or IPSec with GRE. You also have the option to configure Dynamic Multipoint VPN (DMVPN) and GRE for devices with dynamic IP addresses.



Note

IKE keepalive is the default failover and routing policy defined on the Global object.

You can define multiple failover and routing policies within your Router MC object hierarchy, but only one failover and routing policy applies per device. For example, you could define IKE keepalive for failover on Global, and GRE on a specific device group. The GRE policy would override the IKE keepalive policy for that device group and all its descendants.

If you create, update, or remove a failover and routing policy, all the devices configured with that failover and routing policy must be deployed together.

**Note**

A hub and its associated spokes must use the same failover and routing policy. It is important to remember this when moving devices within the device hierarchy.

The following topics provide information about each failover and routing method:

- [Understanding IKE Keepalive, page 1-3](#)
- [Understanding GRE, page 1-4](#)
- [How Does Router MC Implement GRE?, page 1-5](#)
- [Prerequisites for Configuring and Deploying GRE, page 1-9](#)
- [Important Notes about Configuring GRE, page 1-10](#)
- [Understanding GRE with DMVPN, page 1-6](#)
- [Understanding GRE Configuration for Dynamically Addressed Spokes, page 1-8](#)

For procedures for configuring failover and routing policies, see [Configuring Failover and Routing Policies, page 1-8](#).

Understanding IKE Keepalive

With IKE keepalive, the tunnel peers exchange messages that demonstrate they are available to send and receive data in the tunnel. Keepalive messages transmit at set intervals, and any disruption in that interval results in the creation of a new tunnel, using a backup device.

Devices that rely on IKE keepalive for resiliency transmit their keepalive messages regardless of whether they are exchanging other types of information. These keepalive messages can therefore create a small but additional demand on your network.

A variation on IKE keepalive called keepalive dead-peer detection (DPD) sends keepalive messages only between peer devices that are not already exchanging other types of data. DPD is used on devices that support it.

See [Configuring IKE Keepalive, page 1-8](#) for the procedure for configuring IKE keepalive.

Understanding GRE

GRE is a tunneling protocol that can encapsulate different protocol packet types (such as AppleTalk, IPX, or multicast/broadcast) inside encrypted IP packets, allowing IPsec security to apply in non-IP environments.

For VPN resilience, a spoke must be configured with two GRE tunnels, one to the primary hub and the other to the backup hub. Both GRE tunnels are secured with IPsec: each one has its own IKE SA and a pair of IPsec SAs. An associated routing protocol, either EIGRP or OSPF, automates the failover mechanism, transferring to the backup tunnel if virtual link loss is detected.

Advantages of IPsec Tunneling with GRE

The main advantages of IPsec tunneling with GRE are:

- GRE uses a routing protocol by which every IPsec peer knows the status of every other peer at all times. You must specify the routing protocol you prefer: EIGRP or OSPF.
- GRE provides higher resiliency than IKE keepalive.
- Spoke-to-spoke connectivity is supported when you use GRE.
- GRE supports multicast and broadcast transmissions.

Disadvantages of IPsec Tunneling with GRE

GRE does not support the use of dynamic cryptographic tunnels.

Using GRE With Frame Relay

Most of the same advantages and disadvantages apply to generic routing encapsulation (GRE) over frame relay as apply to GRE without frame relay.

Router MC supports a frame relay topology in which each hub acts only as a VPN endpoint, and each spoke acts as both a VPN endpoint and a frame relay endpoint. There must be a device in the hub subnet that acts as the second frame relay endpoint and is positioned before the VPN endpoint at the hub.

See [Configuring GRE, page 1-11](#) for the procedure for configuring GRE.

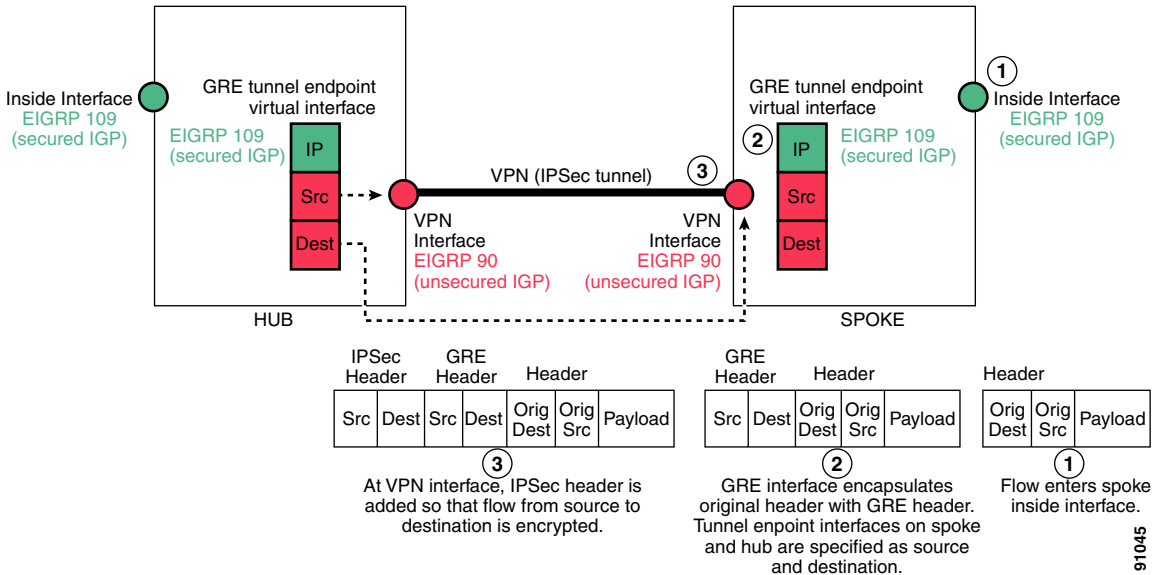
How Does Router MC Implement GRE?

Router MC implements a double Interior Gateway Protocol (IGP) solution for GRE. An IGP refers to a group of devices that receive routing updates from one another by means of a routing protocol, either EIGRP or OSPF. Each “routing group” is identified by a logical number. For general routing purposes, the interfaces on the routers in your networks belong to an IGP. Router MC does not manage this existing IGP. Rather, it adds an additional IGP that is dedicated for IPsec and GRE secured communication. This additional IGP is known as the secured IGP. The existing IGP (unsecured IGP), is used for routing traffic that does not require encryption.

When a GRE tunnel is established, a virtual interface is configured on each peering device. These virtual interfaces are the endpoints of the GRE tunnel. Each virtual interface is unique and is assigned with its own crypto map. The GRE tunnel interface has an IP address (inside tunnel IP address) which is taken from a loopback interface that Router MC creates specifically for this purpose. The GRE tunnel points to the source and destination IP addresses of the physical VPN interfaces on the hub and spoke. The GRE virtual interfaces on the hub and its assigned spokes belong to the secured IGP, as do the inside interfaces you defined for the hub and spoke. Routing updates within the secured IGP are GRE encapsulated and IPsec is applied. A flow whose destination is a secured interface (according to the routing updates of the secured IGP) is directed through the GRE interface where it is GRE encapsulated and then evaluated against the crypto ACL. If it matches the crypto ACL, it is routed through the GRE and VPN tunnels.

The Router MC implementation of GRE is illustrated in [Figure 1-1](#).

Figure 1-1 Router MC Implementation of GRE



See [Configuring GRE, page 1-11](#) for the procedure for configuring GRE.

Understanding GRE with DMVPN

The Dynamic Multipoint VPN (DMVPN) feature allows for better scaling of large and small IPSec Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IPsec (IPSec) encryption, and Next Hop Resolution Protocol (NHRP).



Note

DMVPN configuration is supported on devices with IOS 12.2(13)T and higher. If your device IOS does not support DMVPN, use GRE dynamic IP to configure GRE for dynamically addressed spokes. See [Understanding GRE Configuration for Dynamically Addressed Spokes, page 1-8](#).

In Router MC, using DMVPN with GRE provides the following advantages:

- **Support for dynamically addressed spokes**

When using GRE, the physical interface IP address of the spoke routers must be known when configuring the hub router because this IP address must be configured as the GRE tunnel destination address. DMVPN allows spoke routers to have dynamic external interface IP addresses, and provides robust configuration that does not have to be redeployed to the device even if the external interface IP address changes.

- **Dynamic tunnel creation for direct spoke-to-spoke communication**

NHRP provides the capability for the spoke routers to dynamically learn the external interface IP address of the routers in the VPN network. This enables the dynamic creation of an IPsec+GRE tunnel directly between spoke routers, without having to go through a hub router, thus reducing the delay of multiple encryption and decryption actions on the hub.

- **Simplified GRE configuration on the hub**

With GRE, a tunnel is configured on the hub for each connected spoke. With GRE + DMVPN, only one tunnel is configured for all the connected spokes.

Router MC uses the Auto Update Server (AUS) to retrieve information from dynamically addressed devices. Therefore, to use the DMVPN feature, you must have the AUS installed. In the Admin tab, you must provide Router MC with the information necessary to communicate with AUS. See [Defining Configuration Support Settings, page 1-3](#).

In addition, to successfully configure DMVPN on your devices using Router MC, certain prerequisites must be met. See [Prerequisites for Working With Dynamically Addressed Devices, page A-10](#) for more information.

**Note**

DMVPN is not supported on Catalyst VPN Services Module devices or on High Availability (HA) groups.

See [Configuring DMVPN, page 1-12](#) for the procedure for configuring DMVPN.

Understanding GRE Configuration for Dynamically Addressed Spokes

When a spoke has a dynamic IP address, there is no fixed GRE tunnel source address (to be used by the GRE tunnel on the spoke side) or destination address (to be used by the GRE tunnel on the hub side). Therefore, Router MC creates additional loopback interfaces on the hub and the spoke, to be used as the GRE tunnel endpoints. You must specify a subnet from which Router MC can allocate an IP address for the loopback interfaces.

Router MC uses the Auto Update Server (AUS) to retrieve information from dynamically addressed devices. Therefore, to use this feature, you must have the AUS installed. In the Admin tab, you must provide Router MC with the information necessary to communicate with AUS. See [Defining Configuration Support Settings, page 1-3](#).

In addition, certain prerequisites must be met before configuring dynamically addressed devices with Router MC. See [Prerequisites for Working With Dynamically Addressed Devices, page A-10](#) for more information.

Configuring Failover and Routing Policies

The following topics provide information about configuring different types of failover and routing policies:

- [Configuring IKE Keepalive, page 1-8](#)
- [Prerequisites for Configuring and Deploying GRE, page 1-9](#)
- [Important Notes about Configuring GRE, page 1-10](#)
- [Configuring GRE, page 1-11](#)
- [Configuring DMVPN, page 1-12](#)
- [Configuring GRE for Spokes With Dynamic IP Addresses, page 1-12](#)

Configuring IKE Keepalive

Follow the procedure below to define IKE keepalive settings.

Before you Begin

- If workflow mode is enabled, make sure that you are working within the context of an open activity.

Procedure

- Step 1** Select **Configuration > Settings**.
 - Step 2** Select **General VPN > Failover and Routing** in the TOC. The Failover and Routing page appears. [Table 1-1 on page 1-14](#) describes the elements displayed in the Failover and Routing page.
 - Step 3** Select **IKE Keepalive** in the Policy Type list box.
 - Step 4** Specify the keepalive interval in seconds.
 - Step 5** Click **Apply**.
-

Prerequisites for Configuring and Deploying GRE

Consider the following prerequisites before using GRE in your network:

- To use GRE, you must identify the inside interfaces on your devices and specify these in the Router MC Settings configuration area. Inside interfaces are the physical interfaces on the device that connect the device to its internal subnets and networks.
- In Router MC, you must select a routing protocol whenever you enable GRE. The available routing protocols in Router MC are EIGRP and OSPF:
 - Enhanced Interior Gateway Routing Protocol (EIGRP) allows the exchange of routing information within an autonomous system and addresses some of the more difficult issues associated with routing in large, heterogeneous networks. Compared to other protocols, EIGRP provides superior convergence properties and operating efficiency. EIGRP combines the advantages of several different protocols.
 - Open Shortest Path First (OSPF) is a link-state, hierarchical protocol that features least-cost routing, multipath routing, and load balancing.
- In Router MC, you must specify an Interior Gateway Protocol (IGP) process number. This number identifies the IGP. When GRE is implemented, this IGP will be the secured IGP. See [How Does Router MC Implement GRE?](#), [page 1-5](#) for more information about IGP. For secure communication, the inside interfaces on peering devices in your VPN must belong to the same IGP. The IGP process number must be within the range specified in the configuration support settings under the Admin tab. If you have an existing

IGP on the device that is within this range, but is different from the IGP process number specified in your GRE settings, Router MC will remove the existing IGP. If the existing IGP process number matches the one specified in your GRE settings, any networks included in the existing IGP process that do not match the specified inside interfaces, will be removed.

- If the inside interfaces on your devices are configured to use an IGP other than the IGP specified in your GRE settings (meaning that the interfaces belong to an unsecured IGP):
 - For spokes: Manually remove the inside interfaces from the unsecured IGP by means of the device CLI before configuring GRE with Router MC.
 - For hubs: If the hub inside interface is used as a network access point for Router MC, then on deployment, the interface will be published in both secured and unsecured IGPs. To ensure that the spoke peers use only the secured IGP, manually add the auto-summary command for the unsecured IGP or remove the unsecured IGP for that inside interface.
- In Router MC, you must provide a subnet that is unique and not globally-routable for loopback. This subnet must only be used to support the implementation of loopback for GRE. The loopback interfaces are created, maintained, and used only by Router MC. You should not use them for any other purpose.
- If you are using static routes instead of unsecured IGP, make sure you configure static routes on the spokes through to the hub inside interfaces.
- **For 7100 and 7400 devices:**

In general, it is recommended that Router MC has its own network access interface, separate from the inside interfaces on the device. However, if a device does not have interfaces that can be reserved for management only, and the external interface on the device is an Ethernet interface, Router MC can be connected to the network by means of an additional Ethernet hub that is attached to the hub's external Ethernet interface.

Important Notes about Configuring GRE

- You can define GRE on the Global object or on any device group (with the exception of a High Availability (HA) group).

- You can define different GRE policies for different groups of devices within your hierarchy. If you define GRE on Global, the GRE settings will be inherited by all device groups and devices in the hierarchy. You can override the Global GRE policy by defining a different GRE policy on one or more device groups.
- Peering devices must be configured with the same failover and routing policy. Therefore, if you define a specific GRE policy on a device group, both the hub and the spoke must be descendants of that device group and there must be no overriding policy on a lower level that changes the GRE policy on either the peering hub or spoke.
- **Switching from IKE keepalive to GRE**—If you previously used IKE keepalive for failover, and you later switch to GRE, everything outside your attached networks will no longer be a part of your VPN. Attached networks include only those networks that are directly connected to the router's inside interfaces.

Configuring GRE

Follow the procedure below to configure GRE.

Before you Begin

- Please read the following topics:
 - [Prerequisites for Configuring and Deploying GRE, page 1-9](#)
 - [Important Notes about Configuring GRE, page 1-10](#)
- If workflow mode is enabled, make sure that you are working within the context of an open activity.

Procedure

-
- Step 1** Select **Configuration>Settings**.
 - Step 2** Select **General VPN>Failover and Routing** in the TOC. The Failover and Routing page appears. [Table 1-1 on page 1-14](#) describes the elements in the Failover and Routing page.
 - Step 3** Select **GRE** in the Policy Type list box. The page refreshes to display only the fields that are relevant for GRE configuration.

- Step 4** Enter information in the displayed GRE fields, as required. Click **Advanced** to display additional GRE fields (optional). See [Table 1-1 on page 1-14](#) for a description of each field.
- Step 5** Click **Apply**.
-

Configuring DMVPN

Follow the procedure below to configure DMVPN.

Before you Begin

- Please read [Understanding GRE with DMVPN, page 1-6](#).
- If workflow mode is enabled, make sure that you are working within the context of an open activity.

Procedure

- Step 1** Select **Configuration>Settings**.
- Step 2** Select **General VPN>Failover and Routing** in the TOC. The Failover and Routing page appears. [Table 1-1 on page 1-14](#) describes the elements in the Failover and Routing page.
- Step 3** Select **DMVPN** in the Policy Type list box. The page refreshes to display only the fields that are relevant for DMVPN configuration.
- Step 4** Enter information in the displayed fields, as required. Click **Advanced** to display additional fields (optional). See [Table 1-1 on page 1-14](#) for a description of each field.
- Step 5** Click **Apply**.
-

Configuring GRE for Spokes With Dynamic IP Addresses

Follow the procedure below to configure GRE for spokes with dynamic IP addresses.

Before you Begin

- Please read [Understanding GRE Configuration for Dynamically Addressed Spokes, page 1-8](#)
- When using the GRE Dynamic IP option, you must define a group preshared key on the hub because the IP address of the assigned spokes is dynamic. See [Creating Group Preshared Keys, page 1-23](#) for more information.
- If workflow mode is enabled, make sure that you are working within the context of an open activity.

Procedure

- Step 1** Select **Configuration>Settings**.
- Step 2** Select **General VPN>Failover and Routing** in the TOC. The Failover and Routing page appears. [Table 1-1 on page 1-14](#) describes the elements in the Failover and Routing page.
- Step 3** Select **GRE Dynamic IP** in the Policy Type list box.
The page refreshes to display only the fields that are relevant for GRE Dynamic IP configuration.
- Step 4** Enter information in the displayed fields, as required.
Click **Advanced** to display additional fields (optional).
See [Table 1-1 on page 1-14](#) for a description of each field.
- Step 5** Click **Apply**.
-

Table 1-1 describes the elements in the Failover and Routing page.

Table 1-1 Failover and Routing: GUI Reference

GUI Element	Description
Policy Type list box	<p>Select the type of failover method you want to use. The page will refresh to display only the fields relevant for your selection.</p> <p>The following policy types are available:</p> <ul style="list-style-type: none"> • IKE Keepalive. See Understanding IKE Keepalive, page 1-3 for more information. • GRE. See Understanding GRE, page 1-4 for more information. • GRE Dynamic IP. See Understanding GRE Configuration for Dynamically Addressed Spokes, page 1-8 for more information. • DMVPN. See Understanding GRE with DMVPN, page 1-6 for more information.
IKE Keepalive Elements	
Keepalive Interval field	Enter the required keepalive interval in seconds. This value defines the interval between the keepalive signals that peers exchange. The default value is 10 seconds.
GRE Elements	
Routing Protocol list box	Select either EIGRP or OSPF as the routing protocol. See Prerequisites for Configuring and Deploying GRE, page 1-9 for more information.
Tunnel Interface IP field	Enter a private IP address, including the subnet mask in bits, which defines a subnet in your enterprise to be used to support the implementation of loopback for GRE. For example, 192.10.9.1/255.255.255.0. Router MC creates a loopback interface on the peering devices, with an IP address from this subnet. The loopback interfaces serve as the GRE tunnel endpoints.
Tunnel Source IP field	<p>For GRE Dynamic IP only. Enter a private IP address, including the subnet mask in bits.</p> <p>Note To provide robust, stable tunnels, Router MC creates a static IP route using this IP address. If you change this IP address or you change the failover and routing policy, Router MC does not remove the static route from the device configuration. Please consider this if you have a problem with unstable GRE tunnels.</p>

Table 1-1 Failover and Routing: GUI Reference (continued)

GUI Element	Description
Enable IP Multicast check box	<p>Select this check box to enable multicast transmissions across your GRE tunnels. IP multicast delivers application source traffic to multiple receivers without burdening the source or the receivers, while using a minimum of network bandwidth.</p> <p>When IP Multicast is enabled, you must specify a rendezvous point that acts as the meeting place for sources and receivers of multicast data.</p>
Rendezvous Point field	<p>This field is only editable when the IP Multicast check box is selected.</p> <p>Enter the IP address of the interface that will serve as the rendezvous point (RP) for multicast transmission. Sources send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree.</p>
Allow direct spoke to spoke tunnels check box	<p>For DMVPN only. Select this check box to enable direct communication between spokes, without going through the hub.</p> <p>Note With direct spoke-to-spoke communication, you must use the Main Mode Address option for preshared key negotiation. See Defining Preshared Key Parameters, page 1-17 for more information.</p>
Advanced or Basic button	<p>Click the Advanced button to display additional fields for optional advanced configuration. Router MC provides default values for all the advanced options. You can change these default values if required.</p> <p>When the advanced fields are displayed, click the Basic button to display only the basic configuration fields and hide the advanced fields.</p>
Process Number field	<p>Router MC adds an additional Interior Gateway Protocol (IGP) that is dedicated for IPsec and GRE secured communication. An IGP refers to a group of devices that receive routing updates from one another by means of a routing protocol, either EIGRP or OSPF. Each “routing group” is identified by a logical number, the process number.</p> <p>Enter a routing process number that will be used to identify the secured IGP that Router MC adds when configuring GRE. See How Does Router MC Implement GRE?, page 1-5 for more information.</p> <p>The number that you provide must be within the range specified next to the field name. The default is the lowest value in the range. This range can be changed in the Configuration Support Settings page in the Admin tab. See Defining Configuration Support Settings, page 1-3 for more information.</p>

Table 1-1 Failover and Routing: GUI Reference (continued)

GUI Element	Description
Delay	Specify the throughput delay for the interface, in seconds.
Hello Interval EIGRP	Specify the interval between hello packets sent on the interface, from 1 to 65535 seconds. The default is 5 seconds.
Hold Time EIGRP	Specify the number of seconds the router will wait to receive a hello message before invalidating the connection. The default hold time is 15 seconds (three times the hello interval).
Tunnel Key field	For DMVPN only. Enter a number that identifies the tunnel key. The tunnel key differentiates between different multipoint GRE (mGRE) tunnel Non Broadcast Multiple Access (NBMA) networks. All mGRE interfaces in the same NBMA network must use the same tunnel key value. If there are two mGRE interfaces on the same router, they must have different tunnel key values.
Network ID (NHRP) field	For DMVPN only. All NHRP stations within one logical NBMA network must be configured with the same network identifier. Enter a globally unique, 32-bit network identifier within the range of 1 to 4294967295.
Hold Time (NHRP) field	For DMVPN only. Enter the time in seconds that routers will keep information provided in authoritative Next Hop Resolution Protocol (NHRP) responses. The cached IP-to-NBMA (non-broadcast multi-access) address mapping entries are discarded after the hold time expires. The default is 600 seconds.
Authentication (NHRP) field	For DMVPN only. Enter an authentication string that controls whether the source and destination NHRP stations allow intercommunication. All routers within the same network using NHRP must share the same authentication string. The string can be up to eight characters long.
Apply button	Click to apply your definitions.
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

Understanding Packet Fragmentation

Fragmentation is the process of breaking a packet into smaller units when it is transmitted over a physical interface that cannot support the original size of the packet. Fragmentation is the best mechanism available for minimizing packet loss in a VPN tunnel, because it permits the transmission of secured packets that might otherwise be too large to transmit successfully. This benefit is particularly relevant when using GRE, because any packet of more than 1420 bytes will not have enough room in its header for the additional 80 bytes that the combined use of IPSec and GRE adds to the packet payload.

The transmission setting for an interface is called the maximum transmission unit (MTU), and it specifies the maximum packet size, in bytes, that the particular interface can handle. If a packet exceeds the MTU, it is either fragmented or dropped (if the DF bit is set). If the DF bit is not set and the packet is fragmented, fragmentation typically takes place after encryption. Because reassembly of an encrypted packet is more difficult, fragmentation can degrade network performance. To prevent these network performance problems, fragmentation settings in Router MC configure the device so that fragmentation occurs before encryption.

Router MC can instruct the device to handle packets that are larger than the MTU either with end-to-end MTU discovery or by setting the MTU locally on the device.

- **MTU Discovery:** End-to-end MTU discovery uses Internet Control Message Protocol (ICMP) messages to determine the maximum MTU that a host can use to send a packet through the VPN tunnel without causing fragmentation. The MTU setting for each link in a transmission path is checked to ensure that no transmitted packet exceeds the smallest MTU in that path. The discovered MTU is used to decide whether fragmentation is necessary.
- **Local MTU handling:** Typically used when ICMP is blocked. The default MTU size is 1420 bytes, however you can define a different MTU size, if required.



Tip

The recommended best practice is to use end-to-end MTU discovery.

Defining Fragmentation Settings (VPN)

Configuring fragmentation involves specifying how the maximum transmission unit (MTU) will be defined: either by discovery, using ICMP messages, or by setting it locally on the device.

Before you Begin

- If workflow mode is enabled, make sure that you are working within the context of an open activity.

Procedure

-
- Step 1** Select **Configuration > Settings**.
- Step 2** Select **General VPN > Fragmentation** in the TOC. The Fragmentation page appears. See [Table 1-2 on page 1-18](#) for a description of the elements displayed in the Fragmentation page.
- Step 3** Choose one of the fragmentation options:
- To use ICMP messages to determine MTU size along the transmission path, select **End-to-End MTU discovery**.
 - To set the MTU locally on the device, select **Local MTU handling**.
- Step 4** Click **Apply**.
-

[Table 1-2](#) describes the elements in the Fragmentation page.

Table 1-2 Fragmentation: GUI Reference

GUI Element	Description
End-to-End MTU discovery radio button	Select to use ICMP messages for the discovery of MTU.
Local MTU handling radio button	Select to set the MTU locally on the devices. Enter the MTU size in bytes in the field provided. The MTU can be between 68 and 1500 bytes. The default is 1420 bytes.
Apply button	Click to apply your definitions.

Table 1-2 Fragmentation: GUI Reference (continued)

GUI Element	Description
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

Working with Hub Settings

Hub settings specify the inside interfaces and internal networks on the hubs in your VPN. Hub settings also include parameters for High Availability (HA) groups.

Access hub settings by selecting **Configuration>Settings>Hub Settings**.

Hub settings include:

- Inside interfaces, where you specify the physical interfaces or subinterfaces on the hub that connect the hub with all of the hub side networks (both attached and internal networks). See [Specifying a Hub's Inside Interfaces, page 1-20](#).
- Networks, where you specify the group of subnets that reside behind the hub but are not directly connected to its inside interfaces. See [Specifying a Hub's Internal Networks, page 1-24](#).
- HA Settings, where you define the parameters of HA groups that use HSRP to provide high availability. See [Defining HA Group Settings, page 1-25](#).
- Catalyst VPN Services Module Settings, where you define the parameters of the Catalyst 6500 devices installed with the VPN Services Module, that can serve as hubs in your VPN. See [Defining Catalyst VPN Services Module Settings, page 1-28](#).

Specifying a Hub's Inside Interfaces

A hub's inside interfaces are physical interfaces or subinterfaces on the hub that connect the hub with the hub side networks. The subnets that are directly connected to the hub's inside interfaces, with no intermediary network device, are known as "attached networks." The subnets located beyond the attached networks, that are connected to the attached networks through an intermediary router, are known as "internal networks." See [Specifying a Hub's Internal Networks](#), page 1-24.

You choose which of the hub's interfaces will function as the inside interfaces.



Note

You cannot choose an inside interface that has already been assigned to a spoke as the tunnel endpoint interface.

Your inside interface definitions have the following purposes in Router MC:

- Inside interfaces can be included in your tunnel policy filter definition to specify what traffic to secure in the IPsec tunnel. For example, you can secure all traffic between the inside interfaces on the hub and the inside interfaces on the spoke. Router MC uses your inside interface specifications to create the required ACLs for the tunnel policy filter options that include inside interfaces. See [Defining a Traffic Filter](#), page 1-10 for more information.
- When GRE is enabled, your inside interface definitions specify what traffic will be secured in the GRE tunnels. Only traffic from the networks directly attached to the inside interfaces is included in the tunnels. See [Understanding GRE](#), page 1-4 for more information.



Note

If you intend to use GRE and the inside interfaces that you specify are configured with a different IGP process than the IGP process specified in your GRE settings, then you must either manually configure the auto-summary command for the IGP or remove the unsecured IGP from the interface. See [Prerequisites for Configuring and Deploying GRE](#), page 1-9 for more information.

Follow the procedure below to define hub inside interfaces.

Before you Begin

- If workflow mode is enabled, make sure that you are working within the context of an open activity.

Procedure

-
- Step 1** Select **Configuration > Settings**.
- Step 2** Select **Hub > Inside Interfaces** in the TOC. The Hub Inside Interfaces page appears. See [Table 1-3 on page 1-21](#) for a description of the elements in the Hub Inside Interfaces page.
- Step 3** Specify the interface type, port and slot in the relevant fields and click the >> button to add it to the list.

or

Click **Show Interfaces**.

The Show Interfaces dialog box appears, and lists the interfaces on the devices in the selected object that are available for selection. See [Table 1-4 on page 1-22](#) for a description of the elements displayed in the Show Interfaces dialog box.

- Step 4** Select the check box next to the interface(s) to be specified as inside interfaces.
- Step 5** Click **Select** to confirm your choices and close the Show Interfaces dialog box.
- Step 6** Optionally, specify a subinterface in the Subinterface field that will function as the inside interface for the hub.
- Step 7** Click **Apply**.
-

[Table 1-3](#) describes the elements in the Hub Inside Interfaces page.

Table 1-3 *Hub Inside Interfaces: GUI Reference*

GUI Element	Description
Type list box	Select the physical interface on the device. You must use a different interface from the one that is defined as the VPN interface.
Slot list box	Select the slot on which the interface is located.

Table 1-3 Hub Inside Interfaces: GUI Reference (continued)

GUI Element	Description
Port list box	Select the interface's physical port. If you do not select a port, Router MC will include all the interfaces of the specified type in the inside interfaces. For example, if you select Ethernet in the Type list box and do not select a port, the selected interface will be Ethernet *, where * indicates that any Ethernet interface will be included.
Subinterface field	Optionally, specify a subinterface that will function as the inside interface.
Show Interfaces button	Click to open the Show Interfaces dialog box, in which you can select from a list of available interfaces. See Table 1-4 on page 1-22 for a description of elements displayed in the Show Interfaces dialog box.
>> button; << button	Click >> to add your selections to the list of selected interfaces. Click << to remove your selections from the list of selected interfaces.
Apply button	Click to apply your definitions.
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

[Table 1-4](#) describes the elements in the Show Interfaces dialog box.

Table 1-4 Show Interfaces: GUI Reference

GUI Element	Description
Check box or radio button column	Enables you to select an interface.
Interface column	Shows the interfaces available on the selected device or on the devices in the selected device group. Note If an interface has already been defined as the inside interface or the VPN interface on a device group, it will not appear in the list of available interfaces. To override this setting on a specific device in the group, close the Show Interfaces dialog box and select the required interface type, slot and port.

Table 1-4 Show Interfaces: GUI Reference (continued)

GUI Element	Description
Supported By column	Indicates the number of devices that support the interface out of the total number of devices in the selected device group.
Rows per page list box	Enables you to change the number of interfaces displayed in the list.
<< link; >> link	Click the << link, when it is available, to return to the previous page in the Available Interfaces table. Click the >> link, when it is available, to advance to the next page in the Available Interfaces table.
Select button	Click to save your selections and return to the Interface Assignment or Inside Interface Definition page. The interfaces you selected are placed in the selected interfaces list. Click Apply to apply your interface definitions.
Cancel button	Click to exit without saving your selections.

Specifying a Hub's Internal Networks

A hub's internal networks are a group of subnets that reside behind the hub but are not directly connected to the inside interfaces on that hub. This means that there is an intermediary router located between the internal networks and the networks directly attached to the hub inside interfaces (attached networks).

Internal networks can be included in your tunnel policy filter definition to specify what traffic to secure in the IPSec tunnel. For example, you can secure all traffic between the internal networks on the hub and the internal networks on the spoke. Router MC uses your internal network specifications to create the required ACLs for the tunnel policy filter options that include the internal networks.

Procedure

Step 1 Select **Configuration > Settings**.

Step 2 Select **Hub > Networks** in the TOC.

The Hub Side Networks page appears. See [Table 1-5 on page 1-25](#) for a description of the elements displayed in the Hub Side Networks page.

Step 3 You have the following options for specifying internal networks:

- To add a specific subnet to the hub side networks, enter its IP address and subnet mask in the Add a Host/Network field, then click >>.
- To add a specific host to the hub side networks, enter its IP address or host name in the Add a Host/Network field, then click >>.
- To add an existing network group to the hub side networks, select it from the Add Network Groups list, then click >>. See [Working with Network Groups, page 1-13](#) for more information.

Step 4 Click **Apply**.

[Table 1-5](#) describes the elements in the Hub Side Networks page.

Table 1-5 Hub Side Networks: GUI Reference

GUI Element	Description
Add a Host Network field	To add a subnet to the hub side networks, enter the IP address and subnet mask, for example, 192.10.9.0/255.255.255.0. To add a host to the hub side networks, enter the IP address or host name.
Add Network Groups list box	Hub side networks can contain other network groups. Select an existing network group from the list and click >> to add it to the hub side networks. See Working with Network Groups, page 1-13 for more information.
>> button; << button	Click >> to add the specified network/host/network group to the hub side networks. Click << to remove the specified network/host/network group from the hub side networks.
Apply button	Click to apply your definitions and override the values inherited from a higher level object.
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

Defining HA Group Settings

A High Availability (HA) group is made up of two or more hub devices that use Hot Standby Routing Protocol (HSRP) to provide transparent, automatic router failover. By sharing a virtual IP address, the hubs in the HA group present the appearance of a single virtual router or default gateway to the hosts on a LAN. One of the hubs in the HA group is always active and assumes the virtual IP address, while the others are standby hubs. The hubs in the group watch for hello packets from the active and the standby routers. If the active router becomes unavailable for any reason, a standby hub seamlessly assumes the virtual IP address and the functionality.

To enable this functionality, Router MC associates the inside and outside interfaces on the HA devices with a virtual standby group. Inside interfaces belong to standby group #4, while outside interfaces belong to standby group #3.

If you have existing HSRP configurations on some of your devices and you want Router MC to use the same identifying numbers for the standby groups, you can specify these numbers in the Configuration Support Settings page under the Admin tab. If you do not specify different standby group numbers, Router MC will disregard your existing standby group numbers and will add standby groups 3 and 4 as usual. See [Defining Configuration Support Settings, page 1-3](#) for information about changing standby group numbers.

**Note**

You cannot set the priority of the hubs in the HA group using Router MC. The device with the lowest IP address on the internal or external subnet has the highest priority.

See [Working with HA Groups, page 1-9](#) for more information about HA groups.

To use HSRP in Router MC, the hubs in the HA group must have one interface that matches the internal virtual IP subnet and one interface that matches the external virtual IP subnet. Router MC uses this information to determine which hub interface will be the inside interface and which will be the outside interface. The shared virtual IP address must be from this subnet, but must not be identical to the IP address of the interfaces of any of the hubs in the group.

**Note**

GRE cannot be configured on an HA group.

In Router MC, for each HA group, you must provide the following information:

- The virtual IP address and subnet mask that will be shared by the outside interfaces on the hubs in the group. This virtual IP address will serve as the VPN interface for the tunnel, when a spoke is assigned to the HA group.
- The virtual IP address that will be shared by the inside interfaces on the hubs in the group.
- The interval between hello packets sent between the hubs to indicate status and priority.
- The duration in seconds that a router waits before it declares the active router to be down.

See [Table 1-6 on page 1-28](#) for a description of the HA Settings page, in which you can provide this information.



Note Router MC creates two standby groups on each device, one on the inside interface and one on the external interface.

Enabling Stateful Failover

You can enable stateful failover for your HA groups. With stateful failover, State Synchronization Protocol (SSP) is used to ensure that state information is shared between the HSRP routers in the HA group. In the event of router failure, the shared state information enables the standby router to maintain IPSec sessions without having to re-establish the tunnel or renegotiate the security associations.

Consider the following before enabling stateful failover:

- Stateful failover cannot be used when RSA Signature is the IKE authentication method.
- An HA group configured with stateful failover cannot contain more than two hubs.

Procedure

- Step 1** Select the required HA group in the Object Selector.
- Step 2** Select **Configuration > Settings**.
- Step 3** Select **Hub > HA Settings** in the TOC.
- The HA Settings page appears. See [Table 1-6 on page 1-28](#) for a description of the elements displayed in the HA Settings page.
- Step 4** Enter the virtual IP addresses and masks that will represent the inside interface and the VPN interface of the HA group, in the relevant fields. Also enter the hello interval and hold time in seconds.
- Step 5** If required, select the Use Stateful Failover check box to enable stateful failover for the HA group.
- Step 6** Click **Apply**.
-

[Table 1-6](#) describes the elements in the HA Settings page.

Table 1-6 HA Settings: GUI Reference

GUI Element	Description
Inside Virtual IP field	Enter the IP address that will be shared by the hubs in the HA group and will represent the inside interface of the HA group. The virtual IP address must be on the same subnet as the inside interfaces of the hubs in the HA group, but must not be identical to the IP address of any of these interfaces. Note If there is an existing standby group on the device, make sure that the IP address you provide is different from the virtual IP address already configured on the device.
Inside Mask field	Enter the subnet mask for the inside virtual IP address.
VPN Virtual IP field	Enter the IP address that will be shared by the hubs in the HA group and will represent the VPN interface of the HA group. This IP address will serve as the hub endpoint of the VPN tunnel. Note If there is an existing standby group on the device, make sure that the IP address you provide is different from the virtual IP address already configured on the device.
VPN Mask field	Enter the subnet mask for the inside virtual IP address.
Hello Interval field	Enter the duration in seconds between each hello message sent by a hub to the other hubs in the group to indicate status and priority.
Hold Time field	Enter the duration in seconds that a standby hub will wait to receive a hello message from the active hub before concluding that the active hub is down.
Use Stateful Failover check box	Select to enable the use of SSP for stateful failover. To use stateful failover, the HA group cannot contain more than two hubs. This check box is disabled if the HA group contains more than two hubs. See Enabling Stateful Failover, page 1-27 for more information.
Apply button	Click to apply your definitions
Clear button	Click to remove your current definitions.

Defining Catalyst VPN Services Module Settings

Router MC supports Catalyst 6500 devices fitted with the IPSec VPN Services Module. This device can be a hub in the VPN managed by Router MC.

When you import the Catalyst 6500 device, Router MC detects the configuration of its ports (routed, access, or trunk). When generating CLI commands for VPN policy, Router MC creates an inside VLAN on the inside trunk interface of the VPN Services Module to which it attaches the required crypto maps. This VLAN serves as the inside interface to the VPN Services Module and is also the hub endpoint of the VPN tunnel. In the VPN Services Module settings, you must provide the IP address for this inside VLAN. The IP address must be on the same subnet as the next hop device after the Catalyst device.

Router MC connects the inside VLAN with the Catalyst's external port according to the external port configuration:

- **Routed:** The inside VLAN is connected directly to the physical external port on the Catalyst.
- **Access:** The inside VLAN is connected to the access VLAN with which the Catalyst's external port is associated.
- **Trunk:** Since the external port is associated with more than one VLAN, you must identify which VLAN should be connected to the inside VLAN. Router MC only provides encryption for the VLAN you specify, not for all the VLANs on the trunk port.

**Note**

A Catalyst VPN Services Module device can only serve as a hub. If its role is specified as 'spoke' in the device settings, Router MC will automatically change its role to hub.

Before You Begin

Select the required Catalyst device in the Object Selector.

Procedure

Step 1 Select **Configuration > Settings**.

Step 2 Select **Hub > Catalyst VPN Services Module** in the TOC.

The VPN Services Module page appears. See [Table 1-7 on page 1-30](#) for a description of the elements displayed in the VPN Services Module page.

Step 3 Enter the IP address that Router MC should use to create the inside VLAN.

Step 4 For trunk external port configuration only, specify the number of the VLAN to be connected with the inside VLAN.

Step 5 Click **Apply**.

[Table 1-7](#) describes the elements in the VPN Services Module page.

Table 1-7 VPN Services Module: GUI Reference

GUI Element	Description
Inside VLAN IP field	<p>Enter the IP address and subnet mask that Router MC should use to create the inside VLAN on the VPN Services Module. This inside VLAN will serve as the hub tunnel endpoint interface. The IP address should be on the same subnet as the next hop device after the Catalyst.</p> <p>Note Make sure that the IP address you provide is published in your routing protocol tables. You must do this on the device itself, not through Router MC.</p>
External VLAN Number for Trunk Port field	<p>Relevant only for trunk external port configuration, meaning when hub assignment is to a trunk port. Enter the number of the external VLAN that will be connected to the inside VLAN and therefore used for the encrypted IPsec flow. The external VLAN number cannot be within the range defined for the inside VLAN.</p> <p>Note Router MC only provides encryption for the specified VLAN, not for all the VLANs on the trunk port.</p>
Inside VLAN Min Value field	The starting point of the range within which the inside VLAN number must be included.
Inside VLAN Max Value field	The ending point of the range within which the inside VLAN number must be included.
Apply button	Click to apply your definitions.
Clear button	Click to remove your current definitions.

Working with Spoke Settings

Spoke settings allow you to specify a spoke's inside interfaces and internal networks, set a spoke's VPN interface, and establish a spoke's hub assignment. They also enable you to define NAT traversal parameters.

Access spoke settings by selecting **Configuration > Settings > Spoke Settings**.

Spoke settings include:

- Inside interfaces, where you specify the physical interfaces or subinterfaces on the spoke that connect the spoke with all of the spoke side networks (both attached and internal networks). See [Specifying a Spoke's Inside Interfaces, page 1-31](#).
- Networks, where you specify the group of subnets that reside behind the spoke but are not directly connected to its inside interfaces. See [Specifying a Spoke's Internal Networks, page 1-34](#).
- VPN Interface, where you specify the tunnel endpoint interface on the spoke. See [Specifying a Spoke's VPN Interface, page 1-35](#).
- Hub Assignment, where you specify the hub with which the spoke will be communicating and the VPN (tunnel endpoint) interface on the hub. See [Specifying a Spoke's Hub Assignment, page 1-40](#).
- NAT Traversal, where you define the parameters required to implement NAT traversal. See [Defining NAT Traversal Settings, page 1-41](#).
- Dial Backup, where you define the parameters that enable a secondary gateway to be used if the primary gateway is down. See [Configuring Dial Backup, page 1-43](#).

Specifying a Spoke's Inside Interfaces

A spoke's inside interfaces are physical interfaces or subinterfaces on the spoke that connect the spoke with all the spoke side networks (both attached and internal networks). The subnets that are directly connected to the spoke's inside interfaces, with no intermediary network device, are known as "attached networks." The subnets located beyond the attached networks, that are connected to the attached networks through an intermediary router, are known as "internal networks." See [Specifying a Spoke's Internal Networks, page 1-34](#).

You choose the interfaces on the spoke that will serve as inside interfaces.

**Note**

You cannot choose an inside interface that has already been defined as a VPN interface.

Your inside interface definitions have the following purposes in Router MC:

- Inside interfaces can be included in your tunnel policy filter definition to specify what traffic to secure in the IPsec tunnel. For example, you can secure all traffic between the inside interfaces on the hub and the inside interfaces on the spoke. Router MC uses your inside interface specifications to create the required ACLs for the filter options that include inside interfaces. See [Defining a Traffic Filter, page 1-10](#) for more information.
- When GRE is enabled, your inside interface definitions specify what traffic will be secured in the GRE tunnels. Only traffic from the networks attached to the inside interfaces is included in the tunnels. See [Understanding Failover and Routing, page 1-2](#) for more information.

**Note**

For GRE, make sure that the inside interfaces that you specify are not included in any IGP process other than the IGP process specified in your GRE settings. Otherwise, the traffic on this interface might be transmitted unsecured. See [Prerequisites for Configuring and Deploying GRE, page 1-9](#) for more information.

- For NAT, Router MC marks the specified inside interfaces as NAT inside interfaces. This means that only packets arriving on these interfaces will be subject to translation. See [Chapter 1, “Configuring Translation Rules”](#) for more information.

Procedure

- Step 1** Select **Configuration > Settings**.
- Step 2** Select **Spoke > Inside Interfaces** from the TOC. The Spoke Inside Interfaces page appears. See [Table 1-8 on page 1-33](#) for a description of the elements in the Spoke Inside Interfaces page.
- Step 3** Click **Show Interfaces**.

The Available Interfaces dialog box appears, and lists the interfaces on the devices in the selected object that are available for selection. See [Table 1-4 on page 1-22](#) for a description of the elements displayed in the Show Interfaces dialog box.

- Step 4** Select the check box next to one or more of the listed interface options to select it.
- Step 5** Click **Select** to confirm your choices and close the Available Interfaces dialog box.
- Step 6** Optionally, specify a subinterface in the Subinterface field that will function as the inside interface for the spoke.
- Step 7** Click **Apply**.

[Table 1-8](#) describes the elements in the Spoke Inside Interfaces page.

Table 1-8 Spoke Inside Interfaces: GUI Reference

GUI Element	Description
Type list box	Select the physical interface on the device.
Slot list box	Select the slot on which the interface is located.
Port list box	Select the interface's physical port. If you do not select a port, Router MC will include all the interfaces of the specified type in the inside interfaces. For example, if you select Ethernet in the Type list box and do not select a port, the selected interface will be Ethernet *, where * indicates that any Ethernet interface will be included.
Subinterface field	Optionally, specify a subinterface that should function as the inside interface.
Show Interfaces button	Opens the Available Interfaces dialog box. See Table 1-4 on page 1-22 for a description of elements displayed in the Available Interfaces dialog.
>> button; << button	Click >> to copy your selections to the list of selected interfaces. Or, click << to remove your selections from the list of selected interfaces.
Apply button	Click to apply your definitions.

Table 1-8 Spoke Inside Interfaces: GUI Reference (continued)

GUI Element	Description
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

Specifying a Spoke's Internal Networks

A spoke's internal networks are a group of subnets that reside behind the spoke but are not directly connected to the spoke's inside interfaces. This means that there is an intermediary router located between the internal networks and the networks directly attached to the hub's inside interfaces (attached networks).

Internal networks can be included in your tunnel policy filter definition to specify what traffic to secure in the IPsec tunnel. For example, you can secure all traffic between the internal networks on the hub and the internal networks on the spoke. Router MC uses your internal network specifications to create the required ACLs for the filter options that include the internal networks.

Procedure

-
- Step 1** Select **Configuration > Settings**.
- Step 2** Select **Spoke > Networks** from the TOC. The Spoke Side Networks page appears. See [Table 1-9 on page 1-35](#) for a description of the elements in the Spoke Side Networks page.
- Step 3** Choose from among the following options:
- To add a specific subnet to the spoke side networks, enter its IP address and subnet mask in the Add a Host/Network field and click >>.
 - To add a specific host to the spoke side networks, enter its IP address or host name in the Add a Host/Network field and click >>.
 - To add an existing network group to the spoke side networks, select it from the Add Network Groups list and click >>. See [Working with Network Groups, page 1-13](#) for more information.

Step 4 Click **Apply**.

[Table 1-9](#) describes the elements displayed in the Spoke Side Networks page.

Table 1-9 Spoke Side Networks: GUI Reference

GUI Element	Description
Add a Host/Network field	To add a subnet to the spoke side network, enter the IP address and subnet mask, for example, 192.10.9.0/255.255.255.0. To add a host to the spoke side networks, enter the IP address or host name.
Add Network Groups field	Spoke side networks can contain other network groups. Select an existing network group from the list and click >> to add it to the spoke side networks. See Working with Network Groups, page 1-13 for more information.
>> button; << button	Click >> to add the specified network/host/network group to the spoke side networks. Click << to remove the specified network/host/network group from the spoke side networks.
Apply button	Click to apply your definitions.
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

Specifying a Spoke's VPN Interface

A spoke's VPN interface is the physical interface through which communication occurs in the IPsec tunnel. You choose which of the spoke's interfaces to use as the VPN interface.



Note

You cannot choose a VPN interface that has already been defined as an inside interface.

The VPN interface must have a globally routable IP address (unless it is a Frame Relay interface and you are using GRE, or unless the interface has a dynamic IP address, either dynamic or DHCP).

An interface with a negotiated IP address (e.g., a Dialer interface) or a dynamic IP address from a DHCP server, can be used as the VPN interface. Router MC identifies the interface's IP address as negotiated or from a DHCP server, and you must provide the IP address.

Specifications for VPN Interface When Using GRE over Frame Relay

If you are using GRE over a Frame Relay configuration, the VPN interface must comply with the following:

- Serial interface with Frame Relay encapsulation.
- Subinterfaces must be point-to-point and they must all get their IP address from the same loopback interface.
- All subinterfaces must have data link connection identifier (DLCI) configuration.

Using the Same Interface VPN Feature

In cases where a single external interface is used to both receive traffic and to distribute it after encryption, Router MC uses the loopback0 interface on the device as the VPN interface.

This feature can be enabled by selecting the Same Interface VPN check box in the Spoke VPN Interface page.



Note

To use this feature, the device must be configured with a loopback0 interface.



Note

If NAT is configured on the external interface, NAT will be applied to the flow that matches the NAT filter, and this flow will also be IPsec encapsulated.

Procedure

- Step 1** Select **Configuration > Settings**.
- Step 2** Select **Spoke > VPN Interface** from the TOC. The Spoke VPN Interface page appears. See [Table 1-10 on page 1-38](#) for a description of the elements in the Spoke VPN Interface page.
- Step 3** If you have an individual spoke selected in the Object Selector, select your desired interface in the Select Interface list box and click **Apply** to confirm your selection.

Otherwise, if you have selected Global or selected a device group in the Object Selector, do as follows.

- Step 4** Click **Show Interfaces**.

The Show Interfaces dialog box appears, and lists the interfaces on the device(s) in the selected object that are available for selection. See [Table 1-4 on page 1-22](#) for a description of the elements displayed in the Show Interfaces dialog box.



Note An interface that has already been defined as the inside interface will not appear in the list of available interfaces because you cannot use the same interface for both inside interface and VPN interface.

- Step 5** Select the check box next to one or more of the listed interface options to select it.
- Step 6** Click **Select** to confirm your choices and close the Show Interfaces dialog box.
See [Table 1-4 on page 1-22](#) for a description of elements in the Show Interfaces dialog box.
- Step 7** Click **Validate** to open the Validate Interface dialog box and validate your interface selection.

For example, if you selected Ethernet 1/0, the Validate Interface dialog box will indicate how many of the devices in your selected object have this interface available. If the selected interface is not available on any of the devices, you must either choose another interface that is on at least one of the devices, or select a different interface on the individual devices that are not covered.
- Step 8** Click **Close** to return to the Spoke VPN Interface page.
- Step 9** Optionally, specify a subinterface in the Subinterface field that should function as the VPN interface for the spoke.

Step 10 Click **Apply** to apply your selections.

[Table 1-10](#) describes the elements displayed in the Spoke VPN Interface page.



Note

If you have selected a spoke in the Object Selector, the Spoke VPN Interface page displays only the Select Interface list box, the Enable Same Interface VPN check box, the Apply button, and the Defaults button. If you have selected a device group, the Spoke VPN Interface page contains the elements listed in the following table.

Table 1-10 Spoke VPN Interface: GUI Reference

GUI Element	Description
Select Interface list box	This list box appears only if you have an individual spoke selected in the Object Selector. Select the desired VPN interface on that spoke.
Negotiated IP for Interface field	Only appears when a spoke with a Dialer or Serial interface is selected in the Object Selector, and the interface has a negotiated IP address. Enter the negotiated IP address. Enter only the IP address, without a subnet.
Interface Type list box	Select the physical interface on the device.
Slot list box	Select the slot on which the interface is located.
Port list box	Select the interface's physical port.
Channel field	If the spoke has a controller, you can specify the channel you want to serve as the VPN interface. This field is filled in automatically if you select an interface with a channel in the Show Interfaces dialog box.
Subinterface field	Optionally, specify a subinterface as the VPN interface.
Validate button	Opens the Validate Interface dialog box that indicates how many of the devices in the selected object contain that interface. See Table 1-11 on page 1-39 for a description of the elements in the Validate Interface dialog box.
Show Interfaces button	Opens the Show Interfaces dialog box. See Table 1-4 on page 1-22 for descriptions of the elements in the Show Interfaces dialog box.

Table 1-10 Spoke VPN Interface: GUI Reference (continued)

GUI Element	Description
Enable Same Interface VPN	Select this check box to indicate that a single interface is being used for incoming and outgoing traffic on the device. See Using the Same Interface VPN Feature, page 1-36 for more information.
Apply button	Click to apply your definitions.
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

[Table 1-11](#) describes the elements displayed in the Validate Interface dialog box.

Table 1-11 Validate Interface: GUI Reference

GUI Element	Description
Device column	Displays the device name.
Supported column	Indicates whether or not the specified interface is supported on the device.
Rows per page list box	Enables you to change the number of interfaces displayed in the list.
<< link; >> link	Click the << link, when it is available, to return to the previous screen in the Validate Interface table. Click the >> link, when it is available, to advance to the next screen in the Validate Interface table.
Close button	Click to close the Validate Interface dialog box and return to your work in the Interface Assignment or Spoke VPN Interface page.

Specifying a Spoke's Hub Assignment

You must specify which hub will serve as the IPsec peer for each of your spokes, and the interface on the hub that will be the tunnel endpoint interface. This interface must have a globally routable IP address. You can also assign a failover hub to your spokes, to be used if the primary hub fails.

**Note**

You can only assign a hub to a spoke if both the hub and the spoke use the same failover and routing policy. See [Understanding Failover and Routing, page 1-2](#) for more information.

An HA (High Availability) group can be assigned to a spoke as the primary or secondary hub. See [Working with HA Groups, page 1-9](#) and [Defining HA Group Settings, page 1-25](#) for information about HA groups.

Hub assignment can be defined on a group of spokes simultaneously, or on individual spokes.

When you create a tunnel policy on a spoke, Router MC writes the appropriate commands to the tunnel endpoint interface on the spoke and to the hub interface assigned to that spoke. This enables the setup and proper functioning of the IPsec tunnel between the spoke and its assigned hub.

**Note**

You cannot assign a spoke to an interface on the hub that has already been defined as an inside interface.

Procedure

- Step 1** Select **Configuration > Settings**.
- Step 2** Select **Spoke > Hub Assignment** from the TOC. The Hub Assignment page appears.
- Step 3** Select your primary hub from the Primary Hub list box.
- Step 4** Select an interface from the Primary Interface list box.
- Step 5** Select your failover hub from the Failover Hub list box.
- Step 6** Select an interface from the Failover Interface list box.

Step 7 Click **Apply**.

Table 1-12 describes the elements in the Hub Assignment page.

Table 1-12 Hub Assignment: GUI Reference

GUI Element	Description
Primary Hub list box	Select a hub or HA group that will serve as the primary hub.
Primary Interface list box	Select the interface on the primary hub that will be the tunnel endpoint interface. Note If more than one spoke is assigned to the same Catalyst VPN Services Module device, you must select the same interface for all the spokes. This is due to a hardware limitation in which the VPN Services Module does not support multiple external interfaces. This is also relevant when selecting the interface for the failover hub.
Failover Hub list box	Select a hub or HA group that will serve as the failover hub.
Failover Interface list box	Select the interface on the primary hub that will be the tunnel endpoint interface.
Apply button	Click to apply your definitions.
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

Defining NAT Traversal Settings

NAT traversal is required when there is a device (for example, a PIX device) located between a VPN-connected hub and spoke, that performs Network Address Translation (NAT) on the IPsec flow. This device will be referred to as the middle device.

If the IP address of the VPN interface on the spoke is non-globally routable, the NAT on the middle device replaces it with a new globally routable IP address. Since this change is made in the IPSec header, it violates the checksum of the spoke causing a mismatch with the hub's checksum calculation. This results in loss of connectivity between the hub and the spoke.

With NAT traversal, the spoke adds a UDP header to the payload. The NAT on the middle device changes the IP address in the UDP header, leaving the IPSec header and the checksum intact.

If the middle device uses static NAT, you must provide Router MC with the static NAT IP address (globally routable) on the inside interface of the middle device, that will be provided for all flows through that interface that require NAT.

However, if the middle device uses dynamic NAT where the NAT IP address is unknown, you must define dynamic crypto on the hub to serve any connection request from the spoke. Router MC will generate the required tunnel configuration for the spoke. See [Working with Dynamic Crypto Policies, page 1-21](#) for information about defining dynamic crypto on the hub.

**Note**

NAT traversal is supported on routers running IOS 12.2(12.10)T1 and higher.

Procedure

-
- Step 1** Select **Configuration>Settings**.
 - Step 2** Select **Spoke>NAT Traversal** from the TOC. The NAT Traversal page appears.
 - Step 3** Specify the static NAT IP address to be provided for flows requiring NAT, and specify the interval between keepalive signals. See [Table 1-13 on page 1-43](#) for a description of the elements in the NAT Traversal page.
 - Step 4** Click **Apply**.
-

[Table 1-13](#) describes the elements in the Nat Traversal page.

Table 1-13 NAT Traversal: GUI Reference

GUI Element	Description
Keepalive field	Specify the interval, in seconds, between the keepalive signals sent between the spoke and the middle device to indicate that the session is active.
NAT IP address check box	Select this check box if the middle device uses static NAT. In this case, you must provide Router MC with the static NAT IP address (globally routable) on the inside interface of the middle device, that will be provided for all flows through that interface that require NAT.
Inside Global IP Address field	Specify the globally routable IP address to be provided for flows passing through the inside interface on the middle device, in the format a.b.c.d. See Defining NAT Traversal Settings, page 1-41 for information about the NAT traversal topology.
Apply button	Click to apply your definitions.
Clear button	Click to remove your current definitions.

Configuring Dial Backup

Dial backup is supported on IOS versions 12.3.2XE and higher.

Dial backup can be used to provide a fallback link for a primary, direct connection when the primary link becomes unavailable. The Router MC implementation of the dial backup feature is based on the assumption that two static routes exist:

- A primary route through a primary gateway, which has highest priority.
- A secondary route through a secondary gateway, which has lower priority and only appears in the routing table when the primary gateway is down.

Router MC configures a logical dialer interface on the spoke. The dialer interface is associated with a physical backup interface. When the primary route is down, the dialer interface is activated and traffic is redirected through this backup interface, along the secondary route. To ensure that the spoke-hub traffic is encrypted, Router MC applies a crypto map to the dialer interface. This crypto map is identical to the crypto map on the VPN interface (the primary route interface).

The IOS technology, Service Assurance Agent (SAA), is used to detect loss of network performance on the primary route. SAA was previously known as Response Time Reporter (RTR). RTR is still used in the CLI commands for this technology.

Follow the procedure below to configure dial backup on your spokes.

Before you Begin

- Make sure that the primary route is functioning.
- Dial backup cannot be configured on its own. You must configure the basic settings and policies that allow a VPN tunnel to be created, such as VPN interfaces, hub assignment, tunnel policy, and IKE policy.

Procedure

-
- Step 1** Select **Configuration > Settings**.
- Step 2** Select **Spoke > Dial Backup** from the TOC. The Dial Backup page appears.
- Step 3** Enter information in the fields provided to configure dial backup on the spokes. See [Table 1-14 on page 1-44](#) for a description of the elements in the Dial Backup page.
- Step 4** Click **Apply**.
-

[Table 1-14](#) describes the elements in the Dial Backup page.

Table 1-14 Dial Backup: GUI Reference

GUI Element	Description
Physical Interface list box	Select the physical interface through which the secondary route traffic will be directed when the logical dialer interface is activated. This can be a Serial, Async or BRI interface. The list displays all the interfaces of these types on the devices.
ISDN Switch Type list box	Only relevant when the physical interface is a BRI interface. Select the ISDN service provider switch type.
Primary Route Destination IP field	Enter the IP address of the next hop device in the primary route.

Table 1-14 Dial Backup: GUI Reference (continued)

GUI Element	Description
Secondary Route Destination IP field	Enter the IP address of the next hop device in the secondary route.
Disable Negotiated IP check box	Only available when a single spoke is selected in the Object Selector. Select this check box if you want to provide a specific IP address for the logical dialer interface on the spoke, rather than using the negotiated IP address. When this check box is selected, the IP Address field appears. Note If you are using GRE for failover and routing, you must disable negotiated IP and specify a fixed IP address.
IP Address field	Only present when the Disable Negotiated IP check box is selected. Enter the fixed IP address you want to assign to the dialer interface.
Dialer Interface area	Allows you to define the settings required to set up the dialer interface communication path.
Remote Device Name field	Enter the host name of the next hop device in the secondary route.
Telephone Number field	Enter the telephone number of the remote device, including the international calling code (if required), and the local area code.
RTR area	Allows you to define the settings for the Service Assurance Agent Response Time Reporter (RTR) operations.
ICMP Target Device field	Enter the IP address or host name of the destination device to which connectivity must be maintained. This is the device that is pinged by the Service Assurance Agent through the primary route to track connectivity.
Timeout field	Specify the number of milliseconds the Service Assurance Agent operation waits to receive a response from the destination device. The default is 5000 ms.
Threshold field	Specify the rising threshold in milliseconds that generates a reaction event and stores history information for the Service Assurance Agent operation.
Frequency field	Specify in seconds how often the Service Assurance Agent operation should be performed. The default is every 60 seconds.
Apply button	Click to apply your definitions.

Table 1-14 Dial Backup: GUI Reference (continued)

GUI Element	Description
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

Entering Additional CLI Commands (Beginning and Ending Commands)

Router MC enables you to manually enter additional CLI commands and deploy them to the devices in the job. You can add these commands to the beginning or the end of the configurations generated by Router MC for the devices.

When deploying to a file, the beginning and ending commands are shown in the full configuration. When deploying to a live device, Router MC reads the configuration on the device and incorporates the beginning and ending commands into this configuration. Before deploying beginning and ending commands to your devices, you are recommended to view the generated configurations to make sure they meet your requirements. See [Viewing Device Configurations, page 1-30](#) for more information.



Note

Router MC does not manipulate or validate your beginning and ending commands; it simply deploys them to the devices. Therefore, ensure that your commands do not conflict in any way with the VPN or firewall configuration on the devices.



Note

If there is more than one set of commands for an interface, only the last set of commands will be deployed. Therefore, it is not recommended to use beginning and ending commands to configure interfaces.

Procedure

-
- Step 1** Select **Configuration > Settings**.
- Step 2** Select **Config Additions > Beginning and Ending Commands** from the TOC. The Beginning and Ending Commands page appears.
- Step 3** Enter beginning or ending commands in the relevant fields. See [Table 1-15 on page 1-47](#) for a description of the Beginning and Ending Commands page, and for more details about entering beginning and ending commands.
-

[Table 1-15](#) describes each element in the Beginning and Ending Commands page.

Table 1-15 Beginning and Ending Commands—GUI Reference

UI Element	Description
Enter Beginning Commands field	<p>Enter the commands you want to add before the Router MC generated configuration on the device. You do not need to enter configuration mode before you enter the beginning commands.</p> <p>If you have chosen to generate the full TFTP configuration (in the deployment options), beginning commands will be placed before the start of the interface configurations.</p> <p>For incremental configurations, beginning commands are placed immediately after the config terminal command.</p>
Enter Ending Commands field	<p>Enter the commands you want to add after the Router MC generated configuration on the device. Do not exit configuration mode after entering ending commands.</p> <p>If you have chosen to generate the full TFTP configuration (in the deployment options), ending commands will be placed immediately after the interface configurations.</p> <p>For incremental configurations, ending commands are placed just before the exit command.</p>
Apply button	Click to apply your definitions.
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.

Table 1-15 *Beginning and Ending Commands—GUI Reference (continued)*

UI Element	Description
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.