



Site-to-Site VPN Configuration

A Virtual Private Network (VPN) is an encrypted network connection between devices on a network and provides the same network connectivity for remote users over a public infrastructure as they would have over a private network. Site-to-site VPNs securely connect multiple fixed sites over a public network using IPsec technology.

CVDM-VPNSM allows you to manage and configure site-to-site VPNs on your device, which includes configuring crypto connections and GRE tunnels.

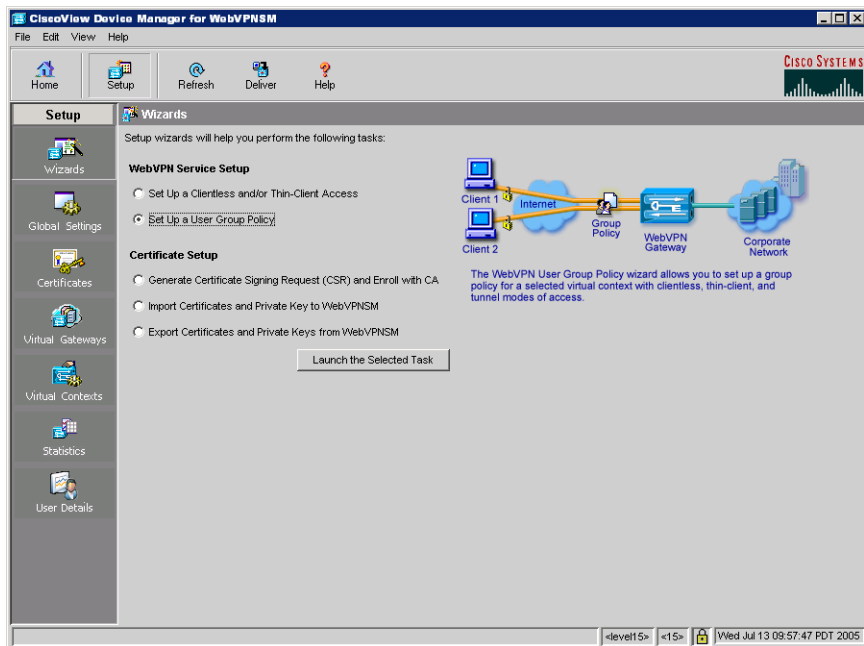
This chapter contains the following topics:

- [Configuring Site-to-Site VPNs, page 3-1](#)
- [Configuring Crypto Connections, page 3-2](#)
- [Configuring GRE Tunnels, page 3-19](#)

Configuring Site-to-Site VPNs

To view information about the site-to-site VPNs configured on the device, click **Setup** at the top of the window and click **Site-to-Site** from the left-most pane to display the main Site-to-Site VPN page (see [Figure 3-1](#)). This page displays all site-to-site crypto connections with and without crypto maps.

Figure 3-1 Site-to-Site VPN page



Configuring Crypto Connections

Click **Setup** at the top of the window, click **Site-to-Site** from the left-most pane, and select **Crypto Connections** from the selector to display the main Crypto Connections page.



Note

If there are multiple VPN modules in the chassis, the available VPN modules are displayed as objects in the selector. You can select a VPN module to display crypto connection information for only that module.

The upper portion of the Crypto Connections page contains a graphical display of the crypto connection configured on the device. The lower portion of the page shows the following information.

GUI Element	Description
VPN Crypto Connections table	
Inside column	Contains the following subcolumns: <ul style="list-style-type: none"> • VLAN ID—VLAN on the inside port; the inside port handles all the traffic going to and coming from the switch inside port. • IP Address/Mask—IP address and subnet mask configured on the inside VLAN. • Crypto Map—Name of crypto map configured on the inside VLAN. • Status—Administrative status of the inside VLAN.
Outside column	Contains the following subcolumns: <ul style="list-style-type: none"> • Routed Port—The routed port crypto-connected to the inside VLAN. • VLAN ID—VLAN ID of the outside VLAN. <p>Note Either the Routed Port column or the VLAN ID column is displayed.</p> <ul style="list-style-type: none"> • Access ports—Access ports attached to the VLAN. • Trunk ports—Trunk ports attached to the VLAN.

From this page, you can access functions to do the following:

- Add a crypto connection. See [Adding Crypto Connections, page 3-4](#).
- Edit a crypto connection. See [Editing Crypto Connections, page 3-15](#).
- Delete a crypto connection. See [Deleting Crypto Connections, page 3-19](#).

Adding Crypto Connections

You can create crypto connections between the inside VLAN and the outside port on this site-to-site VPN.



Note

You can also configure a site-to-site VPN connection using the Site-to-Site VPN Connection Setup wizard. For more information, see [Using the Site-to-Site VPN Connection Setup Wizard, page 2-2](#).

-
- Step 1** Click **Setup** at the top of the window, click **Site-to-Site** from the left-most pane, and select Crypto Connections from the [selector](#).
- Step 2** Click **Add...** The Add Crypto Connection dialog box appears.
- Step 3** Edit the appropriate values.

GUI Element	Description
Crypto Connection tab: VPN Inside Interface pane	
Interface VLAN field	<p>Specify the interface VLAN, which is the Layer 3 VLAN that contains only the VPN module inside port.</p> <p>Before a router can forward the packets using the correct routing table entries, the router needs to know which interface that a packet was received on. For each port VLAN, you need to create another VLAN so that the packets from every switch outside port are presented to the router with the corresponding VLAN number.</p> <p>Note The interface VLAN is removed from all trunk ports on the switch.</p> <p>You can create a VLAN or select from an available VLAN.</p> <p>Click <input type="button" value="v..."/> and do one of the following:</p> <ul style="list-style-type: none"> • Select Select VLAN to open the VLAN Selector dialog box. See VLAN Selector, page 3-9 for more information. • Select Create VLAN to open the Create VLAN dialog box. See Create VLAN Dialog Box, page 3-9 for more information. <p>You can select Clear VLAN to clear the VLAN that is specified in this field.</p>
IP Address field	Enter the IP address of the interface VLAN.
Mask list	Select the subnet mask of the interface VLAN from the list or enter it in the field.
Crypto Map field	<p>Specify the crypto map attached to the interface VLAN. Click <input type="button" value="v..."/> and select Select Crypto Map to open the Select Crypto Map dialog box. See Select Crypto Map Dialog Box, page 3-11 for more information.</p> <p>You can also clear the crypto map entry by clicking <input type="button" value="v..."/> and selecting Clear Selection.</p> <p>Note If HSRP is configured on the VLAN, you cannot assign the same crypto map to multiple VLANs.</p>

GUI Element	Description
Crypto Connection tab: VPN Outside Interface pane	
Connection Mode radio button	<p>Specify the connection mode; you can select the Access/Trunk radio button to specify an access port or trunk port as the outside port, or you can select the Routed Port radio button to specify a routed port as the outside port.</p> <p>If you select the Access/Trunk radio button, do the following:</p> <ul style="list-style-type: none"> • Specify an outside VLAN. You can create a VLAN or choose an available VLAN. From the Outside VLAN field, click <input type="button" value="▽..."/> and do one of the following: <ul style="list-style-type: none"> – Select Select VLAN to open the VLAN Selector dialog box. See VLAN Selector, page 3-9 for more information. – Select Create VLAN to open the Create VLAN dialog box. See Create VLAN Dialog Box, page 3-9 for more information. <p>You can select Clear VLAN to clear the VLAN that is specified in this field.</p> • Optionally, specify or edit access ports assigned to the VLAN. From the Access Ports field, click <input type="button" value="..."/> to open the Port Selector dialog box. For more information, see Port Selector, page 3-9. • Optionally specify or edit the trunk ports assigned to the VLAN. From the Trunk Ports field, click <input type="button" value="..."/> to open the Port Selector dialog box. For more information, see Port Selector, page 3-9. <p>If you select the Routed Port radio button, you must select a routed port. From the Routed Port field, click <input type="button" value="..."/> to open the Select Routed Ports dialog box. For more information, see Select Routed Port Dialog Box, page 3-12.</p>

GUI Element	Description
HSRP tab	
Standby Group Name field	<p>Specify the Hot Standby Routing Protocol (HSRP) standby group name. Click <input type="button" value="v..."/> and select Select Standby Group to display the Select HSRP dialog box. For more information, see Select HSRP Group Dialog Box, page 3-12.</p> <p>An HSRP group is a set of routers that work together as a single virtual router to the hosts on the network. The group name should be unique for all VLANs.</p>
Standby IP Address field	Specify the IP address (instead of the VLAN IP address) that is used for the VPN connection.
Priority field	<p>Enter the HSRP priority value. The default value is 100. The range of values you can use is 0 to 255.</p> <p>The router with the highest priority immediately becomes the active router. Priority is determined first by the configured priority value, and then by the IP address. In each case, a higher value is of greater priority.</p>
Preempt pane	
Preempt check box	<p>Select this check box to enable HSRP preemption; this allows the device with highest priority to immediately become the active router. Priority is determined first by the HSRP priority value, then by IP address.</p> <p>Next, do the following:</p> <ul style="list-style-type: none"> • In the Delay (Sec) field, enter the minimum amount of time, in seconds, for which HSRP preemption is delayed. The range of values you can use is 0 to 3600. • In the Synch Delay (Sec) field, enter the maximum amount of time, in seconds, for which an HSRP group waits to synchronize with IP redundancy clients. The range of values you can use is 0 to 3600.

GUI Element	Description
Standby Delay pane	
Minimum (Sec) field	<p>Enter the time, in seconds, to postpone the local router from taking over the active role.</p> <p>The default value is 1. The range of values you can use is 0 to 10000.</p>
Reload (Sec) field	<p>Enter the time, in seconds, to postpone the local router from taking over the active role after the router has reloaded. This delay value applies to the first interface-up event after the router has reloaded.</p> <p>The default value is 5. The range of values you can use is 0 to 10000.</p>
Standby Timers pane	
Hello Interval (Sec) field	<p>Enter the time, in seconds, between hello packets before other devices declare the active router to be down.</p> <p>The default value is 3. The range of values you can use is 1 to 254.</p> <p>You can select the Millisecond check box to enter the hello interval in milliseconds. The range of values you can use is 15 to 254000.</p>
Hold Time (Sec) field	<p>Enter the hold time, in seconds, before other devices declare the active router to be down.</p> <p>The default value is 10. The range of values you can use is 1 to 256.</p> <p>You can select the Millisecond check box to enter the hold time in milliseconds. The range of values you can use is 50 to 256000.</p>
Track Interfaces table	<p>You can add interfaces and VLANs to track. Interface tracking allows you to specify another interface on the device for the HSRP process to monitor and to alter the HSRP priority for a given group. If the line protocol of the specified interface goes down, the HSRP priority of this device is reduced, allowing another HSRP device with higher priority to become active.</p> <p>You can do the following:</p> <ul style="list-style-type: none"> • To add an interface to track, click Add..., then select Interfaces.... The Select Interfaces to Track dialog box appears. See Select Interfaces to Track Dialog Box, page 3-13 for more information. • To add a VLAN to track Click Add..., then select VLANs. • To remove an interface, select the entry from the table and click Remove.

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device](#), page 1-22.

VLAN Selector

This dialog box displays the available VLANs that you can select from. Select a VLAN from the table and click **OK**.

Column	Description
VLAN ID	Number (ID) of the VLAN.
Name	Name of the VLAN.
Access Ports	Access ports assigned to the VLAN.
Trunk Ports	Trunk ports assigned to the VLAN.
Services	Services associated to the VLAN.

Create VLAN Dialog Box

This dialog box allows you to create a new VLAN. Enter the following information and click **OK**.

GUI Field	Action/Description
VLAN ID	Enter the ID number of the VLAN.
VLAN Name	Enter the name of the VLAN.
Media Type	Type of VLAN.

Port Selector

The Port Selector allows the user to browse and select ports for configuration. The following table describes how to use the Port Selector.

GUI Element	Action/Description
Available Ports column	<p>The table in the Available Ports column displays all physical ports that are available and supported on this switch. It displays ports that are associated with the selected port connection mode.</p> <p>From the table, select the port you want to configure. To select multiple ports, press the Ctrl key as you select random ports or press the Shift key as you select contiguous ports to configure.</p> <p>Note If the destination port mode is Routed, then you can move only one port at a time to the Selected Port(s) column.</p> <p>Depending on what type of port you select, the table in the Available Ports column may contain the following columns:</p> <ul style="list-style-type: none"> • Name—Indicates the name assigned to a port. • Type—Indicates the hardware type of a port. • VLAN—Indicates the VLAN with which a port is associated. This field is displayed only when the Access port connection mode is selected. • Allowed VLANs—Indicates the range of valid VLAN values for a port. This field is displayed only when the Trunk port connection mode is selected. • IP Address—Indicates the IP address of a port. This field is displayed only when the Routed port connection mode is selected.
Add>> button	With ports selected in the Available Ports column , click to add selected ports to the Selected Port(s) column .
<<Remove button	With ports selected in the Selected Port(s) table, click to remove selected ports from that table.

GUI Element	Action/Description
Clear All button	Click to remove all ports listed in the Selected Port(s) table and put them back in the Available Ports table.
Selected Port(s) column	<p>Displays all selected ports. With either Access or Trunk port mode selected, the ports listed here are assigned to the VLAN specified in the VLAN field.</p> <p>The Name field indicates the name of a selected port.</p> <p>Note IP address and network mask values can be seen when you mouseover the port.</p>

Select Crypto Map Dialog Box

This dialog box is launched from several pages; use this dialog box to select a crypto map.

GUI Element	Action/Description
Crypto Map Sets pane	
Name column	<p>Name of the crypto map.</p> <p>Note When you select a crypto map in this table, corresponding data for its crypto map entries is show in the table in the lower pane.</p>
Type column	Type (static or dynamic) of crypto map.
Used by column	Interfaces on which the crypto map is applied.
Crypto Map: X pane	
Seq. No. column	<p>Sequence number of the crypto map entry.</p> <p>Note This table shows the crypto map entries for the crypto map that you selected in the table in the upper pane.</p>
Peers column	IP addresses of the peers using this crypto map entry.
Transform Sets columns	Names of the transform sets applied to this crypto map entry.

GUI Element	Action/Description
IPSec Rule column	Names of the IPSec rules applied to this crypto map entry.
Dynamic Map column	Name of the dynamic crypto map attached to this crypto map entry (if it is static).

Select Routed Port Dialog Box

Use this dialog box to select a routed port.

GUI Element	Action/Description
Routed Ports row	Select the routed port.

Select HSRP Group Dialog Box

This dialog box appears when you are specifying an HSRP standby group. This dialog box contains a table that displays the following information:

Column	Description
Name	Name of the HSRP router.
Group	Name of the HSRP group to which the router belongs.
Priority	HSRP priority value. The router with the highest priority immediately becomes the active router. Priority is determined first by the configured priority value, and then by the IP address. In each case, a higher value is of greater priority.

Column	Description
IP Address	IP address of the standby device.
Tracked Interfaces	Interfaces tracked on the HSRP group. Interface tracking allows you to specify another interface on the device for the HSRP process to monitor and alter the HSRP priority for a given group. If the line protocol of the specified interface goes down, the HSRP priority of this device is reduced, allowing another HSRP device with higher priority to become active.

Select Interfaces to Track Dialog Box

This dialog box appears when you add an interface to track for HSRP.



GUI Element	Action/Description
Interfaces column	<p>The table in the Interfaces column, displays all interfaces and VLANs on the device.</p> <p>From the table, select the interface you want to configure. To select multiple interfaces, press the Ctrl key as you select random interfaces or press the Shift key as you select contiguous interfaces to configure.</p> <p>When you select an interface to track, the table displays the following columns:</p> <ul style="list-style-type: none"> • Name—Indicates the name assigned to an interface. • Type—Indicates the hardware type of an interface. • Mode—Indicates the mode of an interface. <p>When you select a VLAN to track, the table displays the following column:</p> <ul style="list-style-type: none"> • Name—Indicates the name of the VLAN.
Add>> button	With interfaces selected in the Interfaces column, click to add selected interfaces to the Tracked Interfaces table .
<<Remove button	With interfaces selected, click to remove selected interfaces from that table.

GUI Element	Action/Description
Clear All button	Click to remove all interfaces listed in the Tracked Interfaces table and put them back in the Available Ports table.
Tracked Interfaces table	<p>Displays all selected interfaces to track. The Name column indicates the name of a selected interface.</p> <p>Interface tracking allows you to specify another interface on the device for the HSRP process to monitor and alter the HSRP priority for a given group. If the line protocol of the specified interface goes down, the HSRP priority of this device is reduced, allowing another HSRP device with higher priority to become active.</p>

Editing Crypto Connections

You can edit crypto connections between the inside VLAN and the outside port on this site-to-site VPN.

-
- Step 1** Click **Setup** at the top of the window, click **Site-to-Site** from the left-most pane, and select Crypto Connections from the [selector](#).
 - Step 2** Click **Edit...** The Edit Crypto Connection dialog box appears.
 - Step 3** Edit the appropriate values.

GUI Element	Description
VPN Inside Interface pane	
Interface VLAN field	Interface VLAN ID. You cannot edit this field.
IP Address field	Enter the IP address of the interface VLAN.
Mask list	Select the subnet mask of the interface VLAN from the list or enter it in the field.
Crypto Map field	<p>Specify the crypto map attached to the interface VLAN. Click  and select Select Crypto Map to open the Select Crypto Map dialog box. See Select Crypto Map Dialog Box, page 3-11 for more information.</p> <p>You can also clear the crypto map entry by clicking  and selecting Clear Selection.</p> <p>Note If HSRP is configured on the VLAN, you cannot assign the same crypto map to multiple VLANs.</p>

GUI Element	Description
VPN Outside Interface pane	
Connection Mode radio button	<p>Specify the connection mode; you can select the Access/Trunk radio button to specify an access port or trunk port as the outside port, or you can select the Routed Port radio button to specify a routed port as the outside port.</p> <p>If you select the Access/Trunk radio button, do the following:</p> <ul style="list-style-type: none"> • Specify an outside VLAN. You can create a VLAN or choose an available VLAN. From the Outside VLAN field, click <input type="button" value="▽..."/> and do one of the following: <ul style="list-style-type: none"> – Select Select VLAN to open the VLAN Selector dialog box. See VLAN Selector, page 3-9 for more information. – Select Create VLAN to open the Create VLAN dialog box. See Create VLAN Dialog Box, page 3-9 for more information. <p>You can select Clear VLAN to clear the VLAN that is specified in this field.</p> • Optionally, specify or edit access ports assigned to the VLAN. From the Access Ports field, click <input type="button" value="..."/> to open the Port Selector dialog box. For more information, see Port Selector, page 3-9. • Optionally specify or edit the trunk ports assigned to the VLAN. From the Trunk Ports field, click <input type="button" value="..."/> to open the Port Selector dialog box. For more information, see Port Selector, page 3-9. <p>If you select the Routed Port radio button, you must select a routed port. From the Routed Port field, click <input type="button" value="..."/> to open the Select Routed Ports dialog box. For more information, see Select Routed Port Dialog Box, page 3-12.</p>

GUI Element	Description
HSRP tab	
Standby Group Name field	<p>Specify the Hot Standby Routing Protocol (HSRP) standby group name. Click <input type="button" value="▽..."/> and select Select Standby Group to display the Select HSRP dialog box. For more information, see Select HSRP Group Dialog Box, page 3-12.</p> <p>An HSRP group is a set of routers that work together as a single virtual router to the hosts on the network. The group name should be unique for all VLANs.</p>
Standby IP Address field	Specify the IP address (instead of the VLAN IP address) that is used for the VPN connection.
Priority field	<p>Enter the HSRP priority value. The default value is 100. The range of values you can use is 0 to 255.</p> <p>The router with the highest priority immediately becomes the active router. Priority is determined first by the configured priority value, and then by the IP address. In each case, a higher value is of greater priority.</p>
Preempt pane	
Preempt check box	<p>Select this check box to enable HSRP preemption; this allows the device with highest priority to immediately become the active router. Priority is determined first by the HSRP priority value, then by IP address.</p> <p>Next, do the following:</p> <ul style="list-style-type: none"> • In the Delay (Sec) field, enter the minimum amount of time, in seconds, for which HSRP preemption is delayed. The range of values you can use is 0 to 3600. • In the Synch Delay (Sec) field, enter the maximum amount of time, in seconds, for which an HSRP group waits to synchronize with IP redundancy clients. The range of values you can use is 0 to 3600.

GUI Element	Description
Standby Delay pane	
Minimum (Sec) field	<p>Enter the time, in seconds, to postpone the local router from taking over the active role.</p> <p>The default value is 1. The range of values you can use is 0 to 10000.</p>
Reload (Sec) field	<p>Enter the time, in seconds, to postpone the local router from taking over the active role after the router has reloaded. This delay value applies to the first interface-up event after the router has reloaded.</p> <p>The default value is 5. The range of values you can use is 0 to 10000.</p>
Standby Timers pane	
Hello Interval (Sec) field	<p>Enter the time, in seconds, between hello packets before other devices declare the active router to be down.</p> <p>The default value is 3. The range of values you can use is 1 to 254.</p> <p>You can select the Millisecond check box to enter the hello interval in milliseconds. The range of values you can use is 15 to 254000.</p>
Hold Time (Sec) field	<p>Enter the hold time, in seconds, before other devices declare the active router to be down.</p> <p>The default value is 10. The range of values you can use is 1 to 256.</p> <p>You can select the Millisecond check box to enter the hold time in milliseconds. The range of values you can use is 50 to 256000.</p>
Track Interfaces table	<p>You can add interfaces and VLANs to track. Interface tracking allows you to specify another interface on the device for the HSRP process to monitor and to alter the HSRP priority for a given group. If the line protocol of the specified interface goes down, the HSRP priority of this device is reduced, allowing another HSRP device with higher priority to become active.</p> <p>You can do the following:</p> <ul style="list-style-type: none"> • To add an interface to track, click Add..., then select Interfaces.... The Select Interfaces to Track dialog box appears. See Select Interfaces to Track Dialog Box, page 3-13 for more information. • To add a VLAN to track Click Add..., then select VLANs. • To remove an interface, select the entry from the table and click Remove.

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device](#), page 1-22.
-

Deleting Crypto Connections

- Step 1** Click **Setup** at the top of the window, click **Site-to-Site** from the left-most pane, and select Crypto Connections from the [selector](#).
- Step 2** From the table, select the connection you want to delete.
- Step 3** Click **Delete**.
-

Configuring GRE Tunnels

A tunnel is an encapsulated traffic flow. Generic routing encapsulation (GRE) is a tunneling protocol that can encapsulate different protocol packet types inside encrypted IP packets.

You configure GRE tunnels using CVDM-VPNSM for traffic flow on your site-to-site VPNs.

Click **Setup** at the top of the window, click **Site-to-Site** from the left-most pane, and select **GRE** from the [selector](#).

The GRE Tunnels page is displayed and shows the following information.

GUI Element	Description
Tunnel Interfaces table	
Tunnel Name column	Name of the tunnel interface.
IP Address/Mask column	IP address and subnet mask address of the tunnel interface.
Encapsulation column	Algorithm used for protecting traffic on the tunnel.
Source column	Inside VLAN on the tunnel interface.
Destination column	Destination IP address of the tunnel.
Admin. Status column	Administrative status (up or down) of the tunnel interface.
Oper. Status column	Operational status (up or down) of the tunnel interface.
Details pane	
Destination IP Address/Mask	IP address and subnet mask of the destination network of the static route going through the tunnel.
Next Hop	IP address of the next hop device on the static route.
Metric	Metric value of the route. The router chooses the path with the lowest metric through which to send packets to the destination.

From this page, you can access functions to do the following:

- Add a GRE tunnel. See [Adding GRE Tunnels](#), page 3-21.
- Edit a GRE tunnel. See [Editing GRE Tunnels](#), page 3-23.
- Delete a GRE tunnel. See [Deleting GRE Tunnels](#), page 3-26.
- Reset the interface. See [Resetting the Tunnel Interface](#), page 3-26.

Adding GRE Tunnels


Note

CVDM-VPNSM supports the creation of single-point GREs only.


Note

You can also configure GRE tunnels using the Secure GRE Tunnel Setup wizard. For more information, see [Using the Secure GRE Tunnel Setup Wizard, page 2-12](#).

- Step 1** Click **Setup** at the top of the window, click **Site-to-Site** from the left-most pane, and select **GRE** from the [selector](#).
- Step 2** Click **Add...** The Add GRE Tunnel dialog box appears.
- Step 3** Edit the appropriate values.

GUI Element	Action/Description
Tunnel Interface field	Name of the tunnel interface. This field cannot be edited.
IP Address field	Enter the IP address of the tunnel interface.
Mask list	Enter the subnet mask address. of the tunnel interface.
Keepalive field	Enter the tunnel keepalive value, in seconds; this is the number of seconds that the device waits between sending keepalive packets on the tunnel. The default value is 10. The range of values you can use is 0 to 32767.
MTU field	Enter the maximum transmission unit (MTU) value, in kilobytes, of the data packets that can be sent on the tunnel. The default value is 1514. The range of values you can use is 256 to 1000000.
Destination IP Address field	Specify the IP address of the destination on the GRE tunnel.

GUI Element	Action/Description
Source VLAN field	Specify the source VLAN. Click <input type="text" value="..."/> to open the Inside VLANs dialog box. Select a VLAN, then click OK .
Routes table	Contains the following columns: <ul style="list-style-type: none"> • Destination IP Address/Mask—IP address and subnet mask address of the destination of the route on the GRE tunnel. • Next Hop—Next hop device on the route. • Metric—Metric value of the route. The router chooses the path with the lowest metric through which to send packets to the destination. From this table, you can do the following: <ul style="list-style-type: none"> • To add a static route to the GRE tunnel, click Add... The Add Static Route dialog box appears. For more information, see Add Static Route Dialog Box, page 3-22. • To edit a static route, select the static route from the table and click Edit... The Edit Static Route dialog box appears. For more information, see Edit Static Route Dialog Box, page 3-23.

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Add Static Route Dialog Box

This dialog box appears when you add a static route to a GRE tunnel.

GUI Element	Action/Description
Route through field	Tunnel through which the static route flows. You cannot change this value.
Destination IP address field	Enter the IP address of the destination of the static route.
Mask list	Select, from the list, the subnet mask address of the destination of the static route.
Metric Value field	Enter the metric value of the route. The router chooses the path with the lowest metric through which to send packets to the destination.

Edit Static Route Dialog Box

This dialog box appears when you edit a static route on a GRE tunnel.

GUI Element	Action/Description
Route through field	Tunnel through which the static route flows. You cannot change this value.
Destination IP address field	Enter the IP address of the destination of the static route.
Mask list	Select, from the list, the subnet mask address of the destination of the static route.
Metric Value field	Enter the metric value of the route. The router chooses the path with the lowest metric through which to send packets to the destination.

Editing GRE Tunnels

- Step 1** Click **Setup** at the top of the window, click **Site-to-Site** from the left-most pane, and select **GRE** from the [selector](#).
- Step 2** Click **Edit...** The Edit GRE Tunnel dialog box appears.
- Step 3** Edit the appropriate values.

GUI Element	Action/Description
Tunnel Interface field	Name of the tunnel interface. This field cannot be edited.
IP Address field	Enter the IP address of the tunnel interface.
Mask list	Enter the subnet mask address. of the tunnel interface.
Keepalive field	Enter the tunnel keepalive value, in seconds; this is the number of seconds that the device waits between sending keepalive packets on the tunnel. The default value is 10. The range of values you can use is 0 to 32767.
MTU field	Enter the maximum transmission unit (MTU) value, in kilobytes, of the data packets that can be sent on the tunnel. The default value is 1514. The range of values you can use is 256 to 1000000.
Destination IP Address field	Specify the IP address of the destination on the GRE tunnel.

GUI Element	Action/Description
Source VLAN field	<p>Specify the source VLAN.</p> <p>Click <input type="text" value="..."/> to open the Inside VLANs dialog box. Select a VLAN, then click OK.</p>
Routes table	<p>Contains the following columns:</p> <ul style="list-style-type: none"> • Destination IP Address/Mask—IP address and subnet mask address of the destination of the route on the GRE tunnel. • Next Hop—Next hop device on the route. • Metric—Metric value of the route. The router chooses the path with the lowest metric through which to send packets to the destination. <p>From this table, you can do the following:</p> <ul style="list-style-type: none"> • To add a static route to the GRE tunnel, click Add... The Add Static Route dialog box appears. For more information, see Add Static Route Dialog Box, page 3-22. • To edit a static route, select the static route from the table and click Edit... The Edit Static Route dialog box appears. For more information, see Edit Static Route Dialog Box, page 3-23.

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Deleting GRE Tunnels

-
- Step 1** Click **Setup** at the top of the window, click **Site-to-Site** from the left-most pane, and select **GRE** from the [selector](#).
- Step 2** From the table, select the tunnel you want to delete.
- Step 3** Click **Delete**.
-

Resetting the Tunnel Interface

You can shut down a tunnel interface and then restart it.

CVDM-VPNSM issues a shutdown command (`# shutdown`), followed by a no shutdown command (`# no shutdown`). CVDM-VPNSM then refreshes and updates the Admin and Oper Status values.

**Note**

Deliver any pending CLI commands to the device before you reset the interface.
