CHAPTER 5

Edit Interface/Connection

This window displays the router's interfaces and connections. The window also enables you to add, edit, and delete connections, and to enable or disable connections.

Add

When you choose an unconfigured physical interface and click **Add**, the menu contains choices for adding a connection on that interface. Click **Add** to create a new loopback or tunnel interface. If the Cisco IOS image on the router supports Virtual Template Interfaces (VTI), the context menu contains an option to add a VTI. If there are switch ports present on the router, you can add a new VLAN.

If you want to reconfigure an interface, and see no choices except Loopback and Tunnel when you click **Add**, choose the interface and click **Delete**. All the types of connections available for that kind of interface will appear in the Add menu. Click **Available Interface Configurations** to see what configurations are available for an interface.

Edit

When you choose an interface and click **Edit**, a dialog appears. If the interface is a supported and configured interface and is not a switch port, the dialog will have the following tabs:

- Connection
- Association tab
- NAT tab

- Application Service
- General tab

If the interface is not supported, the dialog will *not* have a Connection tab. If you choose a switch port, the Edit Switch Port dialog appears. The Edit button will be disabled if the interface is supported and unconfigured.

Delete

Choosing a connection and clicking **Delete** displays a dialog box informing you of the associations this connection has and asking you if you want to remove the associations along with the connection. You can delete just the connection, or the connection and all of its associations.

Summary

Clicking the Summary button hides the details about the connection, restricting the information to the IP address, Type, Slot, Status, and Description.

Details

Clicking **Details** displays the Details About Interface area, described next. Details about the interface are shown by default.

Enable or Disable

When the chosen interface or connection is down, this appears as the **Enable** button. Click the **Enable** button to bring up the chosen interface or connection. When the chosen interface or connection is up, this appears as the **Disable** button. Click the **Disable** button to administratively shut down the interface or connection. This button cannot be used with an interface whose configuration was not delivered to the router.

Test Connection

Click to test the chosen connection. A dialog appears that enables you to specify a remote host to ping through this connection. The dialog then reports on the success or failure of the test. If the test fails, information about why the test may have failed is given, along with the steps you need to take to correct the problem.

Interface List

The interface list displays the physical interfaces and the logical connections to which they are configured.

Interfaces

This column lists the physical and logical interfaces by name. If a logical interface is configured for a physical interface, the logical interface is shown under the physical interface.

If Cisco SDM is running on a Cisco 7000 family router, you will be able to create a connection only on Ethernet and Fast Ethernet interfaces.

IP Address

This column can contain the following types of IP addresses:

- The configured IP address of the interface.
- DHCP Client—The interface receives an IP address from a Dynamic Host Configuration Protocol (DHCP) server.
- IP address negotiated—The interface receives an IP address through negotiation with the remote device.
- IP unnumbered—The router will use one of a pool of IP addresses supplied by your service provider for your router, and for the devices on the LAN.
- Not Applicable—The interface type cannot be assigned an IP address.

Type

The Type column displays the interface type, such as Ethernet, serial, or ATM.

Slot

The number of the physical slot in the router that the interface is installed in. If Cisco SDM is running on a Cisco 1710 router, the slot field is empty.

Status

This column shows whether this interface is up or down. The green icon with the upward-pointing arrowhead indicates the interface is up. The red icon with the downward-pointing arrowhead indicates that the interface is down.

Description

This column contains any descriptions provided for this connection.

Details About Interface

This area of the window displays association and, if applicable, connection details about the interface chosen in the interface list. Association details include such information as Network Address Translation (NAT), access, and inspection rules, IPsec policies, and Easy VPN configurations. Connection details include IP address, encapsulation type, and DHCP options.

Item Name

The name of the configuration item, such as IP address/Subnet mask, or IPsec policy. The actual items listed in this column depend on the type of interface chosen.

Item Value

If the named item has a configured value, it is displayed in this column.

What do you want to do?

To:	Do This:
Add a new connection.	Click **Add**, and choose a connection from the context menu.
Add a new logical interface.	Click **Add**, and choose a logical interface from the context menu.
Add a new VLAN interface.	Click **Add**, choose **New Logical Interface** from the context menu, and then choose **VLAN** from the submenu.
Edit an existing interface.	Highlight the interface you want to edit, and click **Edit**. **Note** If you are editing a GRE tunnel, the Connection tab will not appear if the GRE tunnel is not configured to use **gre ip** mode.
Reset a physical interface to an unconfigured state.	Choose the physical interface, and click **Reset**.

To:	Do This:
Delete a logical interface.	Choose the interface you want to delete, and click **Delete**.
Find out how to perform related configuration tasks.	See one of the following procedures: • How Do I Configure a Static Route? • How Do I View Activity on My LAN Interface? • How Do I Enable or Disable an Interface? • How Do I View the IOS Commands I Am Sending to the Router? • How Do I Configure an Unsupported WAN Interface? • How Do I View Activity on My WAN Interface? • How Do I Configure NAT on a WAN Interface? • How Do I Configure a Static Route? • How Do I Configure a Dynamic Routing Protocol?

Why Are Some Interfaces or Connections Read-Only?

There are many conditions that can prevent Cisco SDM from modifying a previously configured interface or subinterface.

- For reasons why a previously configured serial interface or subinterface may appear as read-only in the interface list, see the help topic Reasons Why a Serial Interface or Subinterface Configuration May Be Read-Only.
- For reasons why a previously configured ATM interface or subinterface may appear as read-only in the interface list, see the help topic Reasons Why an ATM Interface or Subinterface Configuration May Be Read-Only.
- For reasons why a previously configured Ethernet LAN or WAN interface may appear as read-only in the interface list, see the help topic Reasons Why an Ethernet Interface Configuration May Be Read-Only.
- For reasons why a previously configured ISDN BRI interface may appear as read-only in the interface list, see the help topic Reasons Why an ISDN BRI Interface Configuration May Be Read-Only.

Connection: Ethernet for IRB

This dialog box contains the following fields if you chose **Ethernet for IRB** in the Configure list.

Current Bridge Group/Associated BVI

These read-only fields contain the current bridge group value and the current Bridge-Group Virtual Interface (BVI) name.

Create a new Bridge Group/Join an existing Bridge Group

Choose whether you want to make this interface a member of a new bridge group, or if you want to join an existing bridge group. If you want to create a new bridge group, enter a number in the range 1 to 255. If you want to have the interface join an existing bridge group, choose the BVI interface that is already a member of that group.

IP Address

Enter the IP address and subnet mask in the fields provided.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Ethernet for Routing

This dialog box contains the following fields if you chose **Ethernet for Routing** in the Configure list.

IP Address

Enter an IP address and subnet mask in the IP Address fields. This address will be the source IP address for traffic originating from this interface, and the destination IP address for traffic destined for hosts connected to this interface.

DHCP Relay

Click to enable the router to act as a DHCP relay. A device acting as a DHCP relay forwards DHCP requests to a DHCP server. When a device needs to have an IP address dynamically assigned, it broadcasts a DHCP request. A DHCP server replies to this request with an IP address. You can have a maximum of one DHCP relay or one DHCP server per subnetwork.

Note If the router was configured to be a DHCP relay and to have more than one remote DHCP server IP address, these fields are disabled.

IP Address of Remote DHCP Server

Enter the IP address of the DHCP server that will provide addresses to devices on the LAN.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Existing Dynamic DNS Methods

This window allows you to choose a dynamic DNS method to associate with a WAN interface.

The list of existing dynamic DNS methods shows each method's name and associated parameters. Choose a method from the list, and then click **OK** to associate it to the WAN interface.

To add, edit, or delete dynamic DNS methods, go to **Configure > Additional Tasks > Dynamic DNS Methods**.

Add Dynamic DNS Method

This window allows you to add a dynamic DNS method. Choose the type of method, HTTP or IETF, and configure it.

HTTP

HTTP is a dynamic DNS method that updates a DNS service provider with changes to the associated interface's IP address.

Server

If using HTTP, choose the domain address of the DNS service provider from the drop-down menu.

Username

If using HTTP, enter a username for accessing the DNS service provider.

Password

If using HTTP, enter a password for accessing the DNS service provider.

IETF

IETF is a dynamic DNS method that updates a DNS server with changes to the associated interface's IP address.

DNS Server

If using IETF, and no DNS server is configured for the router in **Configure** > **Additional Tasks** > **DNS**, then enter the IP address of your DNS server.

Hostname

Enter a hostname if one is not configured in **Configure** > **Additional Tasks** > **Router Properties** > **Edit** > **Host**, or if you want to override the configured hostname. When updating the interface IP address, the dynamic DNS method sends the hostname along with the interface's new IP address.

Domain Name

Enter a domain name if one is not configured in **Configure** > **Additional Tasks** > **Router Properties** > **Edit** > **Domain**, or if you want to override the configured domain name. When updating the interface IP address, the dynamic DNS method sends the domain name along with the interface's new IP address.

Wireless

If the router has a wireless interface, you can launch the wireless application from this tab. You can also launch the wireless application from the Tools menu by choosing **Tools** > **Wireless Application**.

Association

Use this window to view, create, edit, or delete associations between interfaces and rules or VPN connections.

Interface

The name of the interface you selected in the Interfaces and Connections window.

Zone

If this interface is a member of a security zone, the name of the zone is displayed in this field. If you want to include this interface in a security zone, click the button to the right of the field, choose **Select a Zone**, and specify the zone in the displayed dialog. If you need to create a new zone, choose **Create a Zone**, enter a name for the zone in the displayed dialog, and click OK. The name of the zone you created appears in the zone field.

Access Rule

The names or numbers of any access rules associated with this interface. Access rules permit or deny traffic that matches the IP address and service criteria specified in the rule.

Inbound

The name or number of an access rule applied to inbound traffic on this interface. If you want to apply a rule, click the **...** button and either choose an existing rule or create a rule and choose it.

When a rule is applied to inbound traffic on an interface, the rule filters traffic before it enters the router. Any packet that the rule does not permit is dropped and will not be routed to another interface. When you apply a rule to the inbound

direction on an interface, you are not only preventing it from entering a trusted network connected to the router, you are also preventing it from being routed anywhere else by the local router.

Outbound

The name or number of an access rule applied to outbound traffic on this interface. If you want to apply a rule, click the **...** button and either choose an existing rule or create a rule and choose it.

When a rule is applied to outbound traffic on an interface, the rule filters traffic after it enters the router and before it exits the interface. Any packet that the rule does not permit is dropped before it leaves the interface.

Inspect Rule

The names of inspection rules associated with this interface. Inspection rules create temporary holes in firewalls so that hosts inside the firewall that started sessions of a certain type can receive return traffic of the same type.

Inbound

The name or number of an inspection rule applied to inbound traffic on this interface. If you want to apply an inbound rule, click the **Inbound** drop-down menu and choose a rule.

Outbound

The name or number of an inspection rule applied to outbound traffic on this interface. If you want to apply an outbound rule, click the **Outbound** drop-down menu and choose a rule.

VPN

VPNs protect traffic that may flow over lines that your organization does not control. You can use the chosen interface in a VPN by associating it with an IPsec policy.

IPsec Policy

The configured IPsec policy associated with this interface. To associate the interface with an IPsec policy, choose the policy from this list.

Note An interface can be associated with only one IPsec policy.

Note To create a GRE-over-IPsec Tunnel, you must first associate the policy with the tunnel interface, and then associate it with the source interface for the tunnel. For example, if you wanted to associate a policy with Tunnel3, whose source interface is Serial0/0, you would first choose Tunnel3 in the Interfaces and Connections window, click **Edit** and associate the policy with it, and then click **OK**. Then you would choose the Serial0/0 interface and associate the same policy with it.

EzVPN

If the interface is used in an Easy VPN connection, the name of the connection is shown here.

Note An interface cannot be used in both a virtual private network (VPN) connection and an Easy VPN connection.

Making Association Changes

When you change the association properties of an interface, the changes are reflected in the lower portion of the Edit Interface/Connection window. For example, if you associate an IPsec policy with the interface, the name of the IPsec policy appears in the lower portion of the window. If you delete an association, the value in the Item Value column changes to <None>.

NAT

If you intend to use this interface in a NAT configuration, you must designate it as either an inside or an outside interface. Choose the traffic direction to which NAT is to be applied. If the interface connects to a LAN that the router serves, choose **Inside**. If it connects to the Internet or to your organization's WAN, choose **Outside**. If you have chosen an interface that cannot be used in a NAT configuration, such as a logical interface, this field is disabled and contains the value Not Supported.

Edit Switch Port

This window lets you edit VLAN information for Ethernet switch ports.

Mode Group

Choose the type of VLAN information you want to be carried across this Ethernet switch port. Choosing **Access** causes the switch port to forward only data destined for the specific VLAN number. Choosing **Trunking** causes the switch port to forward data for all VLANs, including the VLAN data itself. Choose **Trunking** only for "trunking" VLAN ports that connect to other networking devices, such as another switch, that will connect to devices in multiple VLANs.

VLAN

To assign the switch port to a VLAN, enter the VLAN number to which this switch port should belong. If the switch port does not already have a VLAN associated with it, this field will show the default value VLAN 1. To create a new VLAN interface corresponding to a VLAN ID, enter that VLAN ID here and check the **Make VLAN visible to interface list** check box.

Make VLAN visible to interface list Check Box

Check if you want to create a new VLAN with the VLAN ID specified in the VLAN field.

Stacking Partner

Choose a switch module as the stacking partner to use. When a device contains multiple switching modules, these must be stacked before other stacking partners.

Bridge Group Number

If you want this switch port to form part of a bridge to a wireless network, enter the number of an existing bridge group.

Speed

Choose the speed to match the network to which the switch port will be connected. Or choose **auto** to allow for the speed to be automatically set to the optimal value.

Duplex

Choose **full** or **half**, or **auto** to allow for the duplex to be automatically set to match the network to which the switch port will be connected.

If **Speed** is set to **auto**, then **Duplex** is disabled.

Power Inline

The **Power inline** drop-down list appears if the switch port supports an inline power supply. Choose one of the following values:

- **auto**—Automatically detect and power inline devices.
- **never** —Never apply inline power.

Application Service

This window allows you to associate QoS policies and application and protocol monitoring with the chosen interface.

QoS

To associate a QoS policy with the interface in the inbound direction, choose a QoS policy from the **Inbound** drop-down menu.

To associate a QoS policy with the interface in the outbound direction, choose a QoS policy from the **Outbound** drop-down menu.

QoS statistics for the interface can be monitored by going to **Monitor > Traffic Status > QoS**.

Netflow

To associate Netflow statistics monitoring with the interface in the inbound direction, check the **Inbound** check box.

To associate Netflow statistics monitoring with the interface in the outbound direction, check the **Outbound** check box.

Netflow statistics for the interface can be monitored by going to **Monitor > Interface Status**. Netflow top talkers and top protocols can be monitored by going to **Monitor > Traffic Status > Top N Traffic Flows**.

NBAR

To associate Network-based application recognition (NBAR) with the interface, check the **NBAR Protocol** check box.

NBAR statistics for the interface can be monitored by going to **Monitor > Traffic Status > Application/Protocol Traffic**.

General

This window displays general security settings and allows you to enable or disable them by checking or unchecking the check box next to the name and description. If you have allowed the Security Audit feature to disable certain properties and want to reenable them, you can reenable them in this window. The properties listed in this window follow.

Description

In this field you can enter a short description of the interface configuration. This description is visible in the Edit Interfaces and Connections window. A description, such as “Accounting” or “Test Net 5,” can help other Cisco SDM users understand the purpose of the configuration.

IP Directed Broadcasts

An IP directed broadcast is a datagram that is sent to the broadcast address of a subnet to which the sending machine is not directly attached. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, the one that is connected directly to the target subnet, can conclusively identify a directed broadcast. Directed broadcasts are occasionally used for legitimate purposes, but such use is not common outside the financial services industry.

IP directed broadcasts are used in the extremely common and popular “smurf” denial of service attack, and they can also be used in related attacks. In a “smurf” attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send

replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger reply stream, which can completely inundate the host whose address is being falsified.

Disabling IP directed broadcasts drops directed broadcasts that would otherwise be "exploded" into link-layer broadcasts at that interface.

IP Proxy ARP

ARP is used by the network to convert IP addresses into MAC addresses. Normally ARP is confined to a single LAN, and a router can act as a proxy for ARP requests, making ARP queries available across multiple LAN segments. Because it breaks the LAN security barrier, proxy ARP should be used only between two LANs with an equal security level, and only when necessary.

IP Route Cache-Flow

This option enables the Cisco IOS Netflow feature. Using Netflow, you can determine packet distribution, protocol distribution, and current flows of data on the router. This information is useful for certain tasks, such as searching for the source of a spoofed IP address attack.

Note The IP Route Cache-Flow option enables Netflow on both inbound and outbound traffic. To enable Netflow on either inbound traffic *or* outbound traffic, use the Netflow options available on the **Application Service** tab.

IP Redirects

ICMP redirect messages instruct an end node to use a specific router as a part of its path to a particular destination. In a properly functioning IP network, a router sends redirects only to hosts on its own local subnets, no end node will ever send a redirect, and no redirect will ever traverse more than one network hop. However, an attacker may violate these rules. Disabling ICMP redirects has no negative impact on the network and can eliminate redirect attacks.

IP Mask-Reply

ICMP mask reply messages are sent when a network device must know the subnet mask for a particular subnetwork in the internetwork. ICMP mask reply messages are sent to the device requesting the information by devices that have the requested information. These messages can be used by an attacker to gain network mapping information.

IP Unreachables

ICMP host unreachable messages are sent if a router receives a nonbroadcast packet that uses an unknown protocol, or if the router receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address. These messages can be used by an attacker to gain network mapping information.

Select Ethernet Configuration Type

This window is displayed when you click an interface in the Interfaces and Connections window and Cisco SDM cannot determine whether the interface is configured as a LAN interface or as a WAN interface. When you configure an interface using Cisco SDM, you designate it as an inside or outside interface, and Cisco SDM adds a descriptive comment to the configuration file based on your designation. If you configure an interface using the command-line interface (CLI), the configuration will not include this descriptive comment, and Cisco SDM will not have this information.

To Indicate that the Interface is a LAN Interface:

Click **LAN**, and then click **OK**. Cisco SDM adds the comment line $ETH-LAN$ to the interface configuration, and the interface appears in the LAN wizard window with the designation Inside in the Interfaces and Connections window.

To Indicate that the Interface is a WAN Interface:

Click **WAN**, and then click **OK**. Cisco SDM adds the comment line $ETH-WAN$ to the interface configuration, and the interface appears in the WAN wizard window with the designation Outside in the Interfaces and Connections window.

Connection: VLAN

This window lets you configure a VLAN interface.

VLAN ID

Enter the ID number of the new VLAN interface. If you are editing a VLAN interface, you cannot change the VLAN ID.

Native VLAN Check Box

Check if this VLAN is a nontrunking VLAN.

IP Address Fields

IP Address Type

Choose whether this VLAN interface will have a static IP address or no IP address. This field is visible when **VLAN only** is chosen in the Configure As field.

IP Address

Enter the IP address of the VLAN interface.

Subnet Mask

Enter the subnet mask of the VLAN interface, or indicate the number of subnet bits using the scrolling field.

DHCP Relay

Click DHCP Relay for more information.

Subinterfaces List

This window displays the subinterfaces configured for the interface that you chose, and enables you to add, edit, and remove configured subinterfaces. For each configured subinterface, the window displays the Subinterface ID, VLAN ID, IP address and mask, and a description, if one was entered. For example, if the router had the interface FastEthernet1, and the subinterfaces FastEthernet1.3 and FastEthernet1.5 are configured, this window might contain the following display

```
5       56      56.8.1.1/255.255.255.0
3       67      Bridge No. 77
```

In this example, FastEthernet1.5 is configured for routing, and FastEthernet1.3 is configured for IRB.

Note You must choose the physical interface on which the subinterfaces are configured to display this window. For the example described, you would have to choose FastEthernet 1 to display this window. If you chose FastEthernet1.3 or FastEthernet1.5 and clicked edit, you would display the edit dialog with the information for that interface.

Add, Edit, and Delete Buttons

Use these buttons to configure, edit, and remove subinterfaces from the chosen physical interface.

Add or Edit BVI Interface

Add or edit a Bridge Group Virtual Interface (BVI) in this window. If your router has a Dot11Radio interface, a BVI is automatically created when you configure a new bridge group. This is done to support IRB bridging. You can change the IP address and subnet mask in this window.

IP Address/Subnet Mask

Enter the IP address and subnet mask that you want to give the BVI.

Add or Edit Loopback Interface

This window enables you to add a loopback interface to the chosen interface.

IP Address

Choose whether the loopback interface is to have no IP address or a static IP address.

Static IP Address

If you chose **Static IP address**, enter that IP address in this field.

Subnet Mask

Enter the subnet mask in this field, or choose the number of subnet bits from the field on the right. The subnet mask tells the router which bits of the IP address designate the network address and which bits designate the host address.

Connection: Virtual Template Interface

You can add or edit a VTI as part of an 802.1x or VPN configuration. When you are editing a VTI, the fields that you can edit appear in a Connection tab.

Interface Type

Choose either **default** or **tunnel**. If you choose tunnel, you must also select a tunnel mode.

IP Address

Choose **Unnumbered**. The VTI uses the IP address of the physical interface that is chosen in the Unnumbered to field.

Unnumbered to

This field appears when you choose **Unnumbered** in the IP Address field. Choose the interface whose IP address you want this VTI to use.

Tunnel Mode

Choose **IPSec-IPv4**.

Connection: Ethernet LAN

Use this window to configure the IP address and DHCP properties of an Ethernet interface that you want to use as a LAN interface.

IP Address

Enter the IP address for this interface. Obtain the IP address value from your service provider or network administrator. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. Obtain this value from your network administrator. The subnet mask enables the router to determine how much of the IP address is used to define the network and subnet portion of the address.

DHCP Relay

Click to enable the router to act as a DHCP relay. A device acting as a DHCP relay forwards DHCP requests to a DHCP server. When a device needs to have an IP address dynamically assigned, it broadcasts a DHCP request. A DHCP server replies to this request with an IP address. You can have a maximum of 1 DHCP relay or 1 DHCP server per subnetwork.

Note If the router was configured to be a DHCP relay with more than one remote DHCP server IP address, this button will be disabled.

IP Address of Remote DHCP Server

If you clicked **DHCP Relay**, enter the IP address of the DHCP server that will provide addresses to devices on the LAN.

Connection: Ethernet WAN

This window lets you add an Ethernet WAN connection.

Enable PPPoE Encapsulation

Click this option if the connection must use Point-to-Point Protocol over Ethernet (PPPoE) encapsulation. Your service provider can tell you whether the connection uses PPPoE. When you configure a PPPoE connection, a dialer interface is automatically created.

IP Address

Choose one of the following IP address types, and enter the information in the fields displayed. If the Ethernet connection is not using PPPoE, you will see only the Static IP address and Dynamic options.

Static IP Address

If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.

Dynamic (DHCP Client)

If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Enter the name of the DHCP server from which addresses will be leased.

IP Unnumbered

Choose **IP Unnumbered** if you want the interface to share an IP address that is already assigned to another interface. Then choose the interface whose IP address this interface is to share.

Easy IP (IP Negotiated)

Choose Easy IP (IP Negotiated) if the router will obtain an IP address through Point-to-Point Protocol/IP Control Protocol (PPP/IPCP) address negotiation.

Authentication

Click to enter CHAP/PAP authentication password information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Ethernet Properties

This window enables you to configure properties for an Ethernet WAN link.

Enable PPPoE Encapsulation

Click **Enable PPPoE encapsulation** if your service provider requires that you use it. PPPoE specifies Point-to-Point Protocol over Ethernet encapsulation.

IP Address

Static IP Address

Available with PPPoE encapsulation and with no encapsulation. If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.

Dynamic (DHCP Client)

Available with PPPoE encapsulation and with no encapsulation. If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Enter the name of the DHCP server that will assign addresses.

IP Unnumbered

Available with PPPoE encapsulation. Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address this interface is to share.

Easy IP (IP Negotiated)

Available with PPPoE encapsulation. Choose **Easy IP (IP Negotiated)** if the router will obtain an IP address using PPP/IPCP address negotiation.

Authentication

Click to enter CHAP/PAP authentication password information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Ethernet with No Encapsulation

Use this window to configure an Ethernet connection with no encapsulation.

IP Address

Choose how the router will obtain an IP address for this link.

- Static IP address—If you choose **Static IP Address**, enter the IP address and subnet mask or network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
- Dynamic IP address—If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Then enter the name or IP address of the DHCP server.

Hostname

If your service provider inserts a hostname for the router into the DHCP response that contains the dynamic IP address, you can enter that name in this field for informational purposes.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.
- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.
- Create a new dynamic DNS method.

Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: ADSL

This window enables you to specify or edit properties of a PPPoE link supported by an ADSL connection.

Encapsulation

Choose the type of encapsulation that will be used for this link.

- PPPoE specifies Point-to-Point Protocol over Ethernet encapsulation.
- PPPoA specifies Point-to-Point Protocol over ATM encapsulation.
- RFC 1483 Routing (AAL5 SNAP) specifies that each PVC can carry multiple protocols.
- RFC 1483 Routing (AAL5 MUX) specifies that each PVC can carry only one type of protocol.

If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

For more information on these encapsulation types, click Encapsulation.

Virtual Path Identifier

The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Enter the VPI value given to you by your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

Virtual Circuit Identifier

The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that your connection may share with other connections. Enter the VCI value given to you by your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

IP Address

Choose how the router will obtain an IP address for this link.

- Static IP address—If you choose **Static IP Address**, enter the IP address and subnet mask, or network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
- Dynamic IP address—If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Then enter the name or IP address of the DHCP server.
- Unnumbered IP address—Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address this interface is to share.
- IP Negotiated—This interface will obtain an IP address using PPP/IP Control Protocol (IPCP) address negotiation.

Hostname

If your service provider has provided a hostname for DHCP option 12, enter it here.

Operating Mode

Choose one of the following values:

- **auto**—Configure the Asymmetric Digital Subscriber Line (ADSL) after autonegotiating with the digital subscriber access line multiplexer (DSLAM) located at the central office.
- a**nsi-dmt**—Configure the ADSL line to train in the ANSI T1.413 Issue 2 mode.
- **itu-dmt**—Configure the ADSL line to train in the ITU G.992.1 mode.

- **adls2**—Configure the ADSL line to train in the ITU G.992.3 mode. This mode is available for the HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, and HWIC-1ADSLI ADSL network modules.
- **adsl2+**—Configure the ADSL line to train in the ITU G.992.4 mode. This mode is available for the HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, and HWIC-1ADSLI ADSL network modules.
- **splitterless**—Configure the ADSL line to train in the G.Lite mode. This mode is available for older ADSL network modules such as the WIC-1ADSL.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.
- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.
- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Enable Multilink PPP

Check this check box if you want to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.

Connection: ADSL over ISDN

Add or edit an ADSL over ISDN connection in this window.

Encapsulation

Choose the type of encapsulation to use for this link.

- **PPPoE** specifies Point-to-Point Protocol over Ethernet encapsulation.
- **RFC 1483 Routing** (**AAL5 SNAP**) specifies that each PVC can carry multiple protocols.
- **RFC 1483 Routing** (**AAL5 MUX**) specifies that each PVC can carry only one type of protocol.

If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Virtual Path Identifier

The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

Virtual Circuit Identifier

The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that your connection may share with other connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

IP Address

Choose how the router will obtain an IP address for this link.

- Static IP address—If you choose **Static IP Address**, enter the IP address and subnet mask, or network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
- Dynamic IP address—If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Then enter the name or IP address of the DHCP server.
- Unnumbered IP address—Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address this interface is to share.
- IP Negotiated—This interface will obtain an IP address using PPP/IP Control Protocol (IPCP) address negotiation.

Operating Mode

Choose the mode that the ADSL line should use when training.

Note If the Cisco IOS release you are running on the router does not support all five operating modes, you will see options only for the operating modes supported by your Cisco IOS release.

- **annexb**—Standard Annex-B mode of ITU-T G.992.1.
- **annexb-ur2**—ITU-T G.992.1 Annex-B mode.
- **auto**—Configure the Asymmetric Digital Subscriber Line (ADSL) line after autonegotiating with the digital subscriber access line multiplexer (DSLAM) located at the central office.
- **etsi**—European Telecommunications Standards Institute mode.
- **multimode**—Mode chosen by the firmware for the best operating condition on digital subscriber line (DSL). The final mode can be either ETSI mode or standard Annex-B mode depending on the current DSLAM setting.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Enable Multilink PPP

Check this check box if you want to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.

Connection: G.SHDSL

This window enables you to create or edit a G.SHDSL connection.

Note If the connection that you are configuring uses a DSL controller, the Equipment Type and Operating Mode fields do not appear in the dialog.

Encapsulation

Choose the type of encapsulation that will be used for this link.

- **PPPoE** specifies Point-to-Point Protocol over Ethernet encapsulation.
- **PPPoA** specifies Point-to-Point Protocol over ATM encapsulation.
- **RFC 1483 Routing** (**AAL5 SNAP**) specifies that each PVC can carry multiple protocols.
- **RFC 1483 Routing** (**AAL5 MUX**) specifies that each PVC can carry only one type of protocol.

If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

For more information on these encapsulation types, click Encapsulation.

Virtual Path Identifier

The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

Virtual Circuit Identifier

The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that your connection may share with other connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

IP Address

Choose how the router will obtain an IP address for this link. The fields that appear in this area change according to the encapsulation type chosen. Your service provider or network administrator must tell you the method the router should use to obtain an IP address.

Static IP address

If you choose **Static IP Address**, enter the address that the interface will use, and the subnet mask or the network bits. Obtain this information from your service provider or network administrator. For more information, see IP Addresses and Subnet Masks.

Dynamic IP address

If you choose Dynamic IP address, the interface will obtain an IP address from a DHCP server on the network. If the DHCP server uses DHCP option 12, it sends a hostname for the router along with the IP address the router is to use. Check with your service provider or network administrator to determine the hostname sent.

IP Unnumbered

Choose this option if you want the interface to share an IP address with an Ethernet interface on the router. If you choose this option, you must specify from the drop-down list the Ethernet interface whose address you want to use.

IP Address for Remote Connection in Central Office

Enter the IP address of the gateway system to which this link will connect. This IP address is supplied by the service provider or network administrator. The gateway is the system that the router must connect to in order to access the Internet or your organization's WAN.

Equipment Type

Choose one of the values below:

CPE

Customer premises equipment. If the encapsulation type is PPPoE, CPE is automatically chosen and the field is disabled.

CO

Central office.

Operating Mode

Choose one of the values below:

Annex A (U.S.)

Configures the regional operating parameters for North America.

Annex B (Europe)

Configures the regional operating parameters for Europe.

Enable Multilink PPP

Check this check box if you want to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.
- Choose an existing dynamic DNS method from a list.

Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Configure DSL Controller

Cisco SDM supports the configuration of the Cisco WIC-1SHDSL-V2. This WIC supports TI, E1, or a G.SHDSL connection over an ATM interface. Cisco SDM only supports a G.SHDSL connection using the ATM interface. This window lets you set the controller mode on the WIC to ATM, enabling a G.SHDSL connection, and lets you create or edit DSL controller information for the G.SHDSL connection.

Controller Mode

Cisco SDM supports only ATM mode, which provides for a G.SHDSL connection, on this controller. This field will automatically be set to ATM mode when the OK button is clicked.

Equipment Type

Choose whether your connection terminates at the central office (CO) or your customer premises equipment (CPE).

Operating Mode

Choose whether the DSL connection should use Annex A signaling (for DSL connections in the United States) or Annex B signaling (for DSL connections in Europe).

Line Mode

Choose whether this is a 2-wire or 4-wire G.SHDSL connection.

Line Number

Choose the interface number on which the connection will be made.

Line Rate

Choose the DSL line rate for the G.SHDSL port. If you have chosen a 2-wire connection, you can choose either **auto**, which configures the interface to automatically negotiate the line rate between the G.SHDSL port and the DSLAM, or the actual DSL line rate. The supported line rates are 200, 264, 392, 520, 776, 1032, 1160, 1544, 2056, and 2312.

If you have chosen a 4-wire connection, you must choose a fixed line rate. The supported line rates for a 4-wire connection are 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480, and 4608

Note If different DSL line rates are configured at opposite ends of the DSL uplink, the actual DSL line rate is always the lower rate.

Enable Sound to Noise Ratio Margin

The sound-to-noise ratio margin provides a threshold for the DSL modem to determine whether it should reduce or increase its power output depending on the amount of noise on the connection. If you have set the line rate to “auto”, you can enable this feature to maximize the quality of the DSL connection. Note that you cannot use this feature if your line rate is fixed. To enable the sound-to-noise ratio margin, check this check box and choose the ratio margins in the Current and Snext fields. To disable this feature, uncheck this check box.

Current

Choose the sound-to-noise ratio margin in the form of decibels (dB) on the current connection. The lower the ratio chosen here, the more noise will be tolerated on the connection. A lower dB setting will cause the DSL modem to allow more noise on the line, potentially resulting in a connection of lower quality but higher throughput. A higher dB setting causes the modem to restrict noise, potentially resulting in a connection of higher quality but lower throughput.

Snext

Choose the Self near-end crosstalk (Snext) sound-to-noise ratio margin in the form of decibels.

DSL Connections

This field displays all of the G.SHDSL connections currently configured on this controller. To configure a new G.SHDSL connection, click **Add**. This displays the Add a G.SHDSL Connection page, letting you configure the new connection. To edit an existing G.SHDSL connection, choose the connection in this field and click **Edit**. This also will display the Add a G.SHDSL Connection page, letting you edit the connection configuration. To delete a connection, choose the connection in this field, and click **Delete**.

Add a G.SHDSL Connection

This window enables you to create or edit a G.SHDSL connection.

Encapsulation

Select the type of encapsulation that will be used for this link.

- **PPPoE** specifies Point-to-Point Protocol over Ethernet encapsulation.
- **PPPoA** specifies Point-to-Point Protocol over ATM encapsulation.
- **RFC 1483 Routing** (**AAL5 SNAP**) specifies that each PVC can carry multiple protocols.
- **RFC 1483 Routing** (**AAL5 MUX**) specifies that each PVC carry only one type of protocol.

If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection, and recreate it, using the encapsulation type you need.

Virtual Path Identifier

The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and recreate it using the value you need.

Virtual Circuit Identifier

The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that it may share with other connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and recreate it using the value you need.

IP Address

Select how the router will obtain an IP address for this link. The fields that appear in this area change according to the encapsulation type chosen. Your service provider or network administrator must tell you the method the router should use to obtain an IP address.

Static IP address

If you select Static IP address, enter the address that the interface will use, and the subnet mask, or the network bits. Obtain this information from your service provider or network administrator. For more information, refer to IP Addresses and Subnet Masks.

Dynamic IP address

If you select Dynamic IP address, the interface will obtain an IP address from a DHCP server on the network. If the DHCP server uses DHCP option 12, it sends a host name for the router along with the IP address it is to use. Check with your service provider or network administrator to determine the host name sent.

IP Unnumbered

Select this option if you want the interface to share an IP address with an Ethernet interface on the router. If you select this option, you must specify from the drop down list the Ethernet interface whose address you want to use.

Description

Enter a description of this connection that makes it easy to recognize and manage.

Enable Multilink PPP

Check this check box if you want to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to automatically update your DNS servers whenever the WAN interface's IP address changes.

Note This feature appears only if supported by your Cisco server's IOS.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in Configure > Additional Tasks > Dynamic DNS Methods.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose to use an existing method. A window with a list of existing dynamic DNS methods will open. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Serial Interface, Frame Relay Encapsulation

Complete these fields if you are configuring a serial subinterface for Frame Relay encapsulation. If you are editing a connection or creating a connection in the Edit Interfaces and Connections window, the encapsulation is shown but is not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Encapsulation

Frame Relay chosen.

IP Address

Choose either **Static IP address** or **IP unnumbered**.

IP Address

If you chose **Static IP address**, enter the IP address for this interface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

If you chose **Static IP address**, enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the subnet bits. Your network administrator or service provider provides the value of the subnet mask or the network bits.

Subnet Bits

Alternatively, enter the network bits to specify how much of the IP address provides the network address.

IP Unnumbered

If you chose IP unnumbered, the interface will share an IP address that has already been assigned to another interface. Choose the interface whose IP address this interface is to share.

DLCI

Enter the data link connection identifier (DLCI) in this field. This number must be unique among all DLCIs used on this interface. The DLCI provides a unique Frame Relay identifier for this connection.

If you are editing an existing connection, the DLCI field will be disabled. If you need to change the DLCI, delete the connection and create it again.

LMI Type

Ask your service provider which of the following Local Management Interface (LMI) types you should use. The LMI type specifies the protocol used to monitor the connection:

ANSI

Annex D defined by American National Standards Institute (ANSI) standard T1.617.

Cisco

LMI type defined jointly by Cisco and three other companies.

ITU-T Q.933

ITU-T Q.933 Annex A.

Autosense

Default. This setting allows the router to detect which LMI type is used by the switch and then use that type. If autosense fails, the router will use the Cisco LMI type.

Use IETF Frame Relay Encapsulation

Check this check box to use Internet Engineering Task Force (IETF) encapsulation. This option is used to connect with routers not from Cisco. Check this box if you are connecting to a router not from Cisco on this interface.

Clock Settings

In most cases, clock settings should not be changed from the default values. If you know that your requirements are different from the defaults, click and adjust the clock settings in the window displayed.

The Clock Settings button appears only if you are configuring a T1 or E1 serial connection.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Serial Interface, PPP Encapsulation

Complete these fields if you are configuring a serial interface for Point-to-Point Protocol encapsulation. If you are editing a connection or creating a connection in the Edit Interfaces and Connections window, the encapsulation is shown but is not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Encapsulation

PPP chosen.

IP Address

Choose **Static IP Address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **IP Unnumbered**, choose the interface whose IP address this interface is to share. If you choose **IP Negotiated**, the router obtains an IP address from the service provider for this interface. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Clock Settings

In most cases, clock settings should not be changed from the default values. If you know that your requirements are different from the defaults, click and adjust the clock settings in the window displayed.

The Clock Settings button appears only if you are configuring a T1 or E1 serial connection.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Serial Interface, HDLC Encapsulation

Fill out these fields if you are configuring a serial interface for HDLC encapsulation. If you are editing a connection or creating a connection in the Edit Interfaces and Connections window, the encapsulation is shown but is not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Encapsulation

HDLC chosen.

IP Address

Choose either **Static IP address** or **IP Unnumbered**. If you choose **IP Unnumbered**, choose the interface whose IP address this interface is to share. If you choose **Static IP Address**, complete the fields below.

IP Address

Enter the IP address for this interface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, choose the number of bits that specify how much of the IP address provides the network address.

Clock Settings

In most cases, clock settings should not be changed from the default values. If you know that your requirements are different from the defaults, click and adjust the clock settings in the window displayed.

The Clock Settings button appears only if you are configuring a T1 or E1 serial connection.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Add or Edit GRE Tunnel

You can add a GRE tunnel to an interface or edit an existing interface in this window. This window does not appear if the GRE tunnel is not configured using **gre ip** mode.

Tunnel Number

Enter a number for this tunnel.

Tunnel Source

Choose the interface that the tunnel will use. This interface must be reachable from the other end of the tunnel; therefore, it must have a public, routable IP address.

Tunnel Destination

The tunnel destination is the interface on the router at the other end of the tunnel. Choose whether you will specify an IP address or a hostname, and then enter that information. If you chose IP address, provide the IP address and subnet mask in dotted decimal format; for example, 192.168.20.1 and 255.255.255.0.

Make sure that this address or hostname is reachable using the **ping** command; otherwise, the tunnel will not be properly created.

Tunnel IP Address

Enter the IP address of the tunnel in dotted decimal format; for example, 192.168.20.1. For more information, see IP Addresses and Subnet Masks.

GRE Keepalive Check Box

Check if you want the router to send GRE keepalives. Specify the interval, in seconds, that keepalives will be sent, and the waiting period, in seconds, between retries.

Maximum Transmission Unit

Enter the maximum transmission unit (MTU) size. If you want the size adjusted to a lower value when the adjustment would avoid packet fragmentation, click **Adjust MTU to avoid fragmentation**.

Bandwidth

Click to specify the bandwidth for this tunnel in kilobytes.

Connection: ISDN BRI

Complete these fields if you are configuring an ISDN BRI connection. Because Cisco SDM supports only PPP encapsulation over an ISDN BRI connection, the encapsulation shown is not editable.

Encapsulation

PPP chosen.

ISDN Switch Type

Choose the ISDN switch type. Contact your ISDN service provider for the switch type for your connection.

Cisco SDM supports these BRI switch types:

- For North America:
  - basic-5ess—Lucent (AT&T) basic rate 5ESS switch
  - basic-dms100—Northern Telecom DMS-100 basic rate switch
  - basic-ni—National ISDN switches
- For Australia, Europe, and the UK:
  - basic-1tr6—German 1TR6 ISDN switch
  - basic-net3—NET3 ISDN BRI for Norway NET3, Australia NET3, and New Zealand NET3switch types; ETSI-compliant switch types for Euro-ISDN E-DSS1 signaling system
  - vn3—French ISDN BRI switches
- For Japan:
  - ntt—Japanese NTT ISDN switches
- For Voice/PBX systems:
  - basic-qsig—PINX (PBX) switches with QSIG signaling per Q.931 ()

SPIDs

Click if you need to enter service profile ID (SPID) information.

Some service providers use SPIDs to define the services subscribed to by the ISDN device that is accessing the ISDN service provider. The service provider assigns the ISDN device one or more SPIDs when you first subscribe to the service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid, assigned SPID to the service provider when accessing the switch to initialize the connection.

Only the DMS-100 and NI switch types require SPIDs. The Lucent (AT&T) 5ESS switch type may support a SPID, but we recommend that you set up that ISDN service without SPIDs. In addition, SPIDs have significance at the local-access ISDN interface only. Remote routers never receive the SPID.

A SPID is usually a seven-digit telephone number with some optional numbers. However, service providers may use different numbering schemes. For the DMS-100 switch type, two SPIDs are assigned, one for each B channel.

Remote Phone Number

Enter the phone number of the destination of the ISDN connection.

Options

Click if you need to associate ACLs with a dialer list to identify interesting traffic, enter timer settings, or enable or disable multilink PPP.

Identifying interesting traffic will cause the router to dial out and create an active connection only when the router detects interesting traffic.

Timer settings will cause the router to automatically disconnect a call after the line is idle for the specified amount of time.

Multilink PPP can be configured to provide load balancing between ISDN B channels.

IP Address

Choose **Static IP address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Analog Modem

Complete these fields if you are configuring an analog modem connection. Because Cisco SDM supports only PPP encapsulation over an analog modem connection, the encapsulation shown is not editable.

Encapsulation

PPP chosen.

Remote Phone Number

Enter the phone number of the destination of the analog modem connection.

Options

Click if you need to associate ACLs with a dialer list to identify interesting traffic or enter timer settings.

Identifying interesting traffic will cause the router to dial out and create an active connection only when the router detects interesting traffic.

Timer settings will cause the router to automatically disconnect a call after the line is idle for the specified amount of time.

Clear Line

Click to clear the line. You should clear the line after creating an async connection so that interesting traffic triggers the connection.

IP Address

Choose **Static IP address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: (AUX Backup)

Complete these fields if you are configuring an asynchronous dial-up connection using the console port to double as an AUX port on a Cisco 831 or 837 router. Once you enter the information in this window, click **Backup Details** and enter dial-backup information, which is required for this type of connection. Note that because Cisco SDM supports only PPP encapsulation over an analog modem connection, the encapsulation shown is not editable.

The option to configure the AUX port as a dial-up connection appears only for the Cisco 831 and 837 routers. This option will not be available for those routers if any of the following conditions occur:

- Router is not using a Zutswang Cisco IOS release
- Primary WAN interface is not configured
- Asynchronous interface is already configured
- Asynchronous interface is not configurable by Cisco SDM because of the presence of unsupported Cisco IOS commands in the existing configuration

Encapsulation

PPP chosen.

Remote Phone Number

Enter the phone number of the destination of the analog modem connection.

Options

Click if you need to associate ACLs with a dialer list to identify interesting traffic or enter timer settings.

Identifying interesting traffic will cause the router to dial out and create an active connection only when the router detects interesting traffic.

Timer settings will cause the router to automatically disconnect a call after the line is idle for the specified amount of time.

Clear Line

Click to clear the line. You should clear the line after creating an async connection so that interesting traffic triggers the connection.

IP Address

Choose **Static IP address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Backup Details

Click to display the Backup Configuration window, which lets you configure dial-backup information for this connection. This information is mandatory for this type of connection, and an error will be displayed if you try to complete the connection configuration without entering dial-backup configuration information.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Authentication

This page is displayed if you enabled PPP for a serial connection or PPPoE encapsulation for an ATM or Ethernet connection, or you are configuring an ISDN BRI or analog modem connection. Your service provider or network administrator may use a Challenge Handshake Authentication Protocol (CHAP) password or a Password Authentication Protocol (PAP) password to secure the connection between the devices. This password secures both incoming and outgoing access.

CHAP/PAP

Check the box for the type of authentication used by your service provider. If you do not know which type your service provider uses, you can check both boxes: the router will attempt both types of authentication, and one attempt will succeed.

CHAP authentication is more secure than PAP authentication.

Login Name

The login name is given to you by your service provider and is used as the username for CHAP/PAP authentication.

Password

Enter the password exactly as given to you by your service provider. Passwords are case sensitive. For example, the password *test* is not the same as *TEST.*

Reenter Password

Reenter the same password that you entered in the previous box.

SPID Details

Some service providers use service profile ID numbers (SPIDs) to define the services subscribed to by the ISDN device that is accessing the ISDN service provider. The service provider assigns the ISDN device one or more SPIDs when you first subscribe to the service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid, assigned SPID to the service provider when accessing the switch to initialize the connection.

Only the DMS-100 and NI switch types require SPIDs. The AT&T 5ESS switch type may support a SPID, and we recommend that you set up that ISDN service without SPIDs. In addition, SPIDs have significance at the local-access ISDN interface only. Remote routers never receive the SPID.

A SPID is usually a seven-digit telephone number with some optional numbers. However, service providers may use different numbering schemes. For the DMS-100 switch type, two SPIDs are assigned, one for each B channel.

SPID1

Enter the SPID to the first BRI B channel provided to you by your ISP.

SPID2

Enter the SPID to the second BRI B channel provided to you by your ISP.

Dialer Options

Both ISDN BRI and analog modem interfaces can be configured for dial-on-demand routing (DDR), which causes the connection to dial out and become active only under specified circumstances, thus saving connection time and cost. This window lets you configure options specifying when ISDN BRI or analog modem connections should be initiated and ended.

Dialer List Association

The dialer list lets you associate the ISDN BRI or analog modem connection with an ACL to identify *interesting traffic*. Identifying interesting traffic will cause the interface to dial out and establish a connection only when the router detects data traffic that matches the ACL.

Allow all IP traffic

Choose this option to cause the interface to dial out and establish a connection whenever there is any IP traffic being sent over the interface.

Filter traffic based on selected ACL

Choose this option to associate an ACL, which must be created using the rules interface, with the interface. Only traffic that matches the traffic identified in the ACL will cause the interface to dial out and establish a connection.

You can enter the ACL number you want to associate with the dialer interface to identify interesting traffic, or you can click the button next to the field to browse the list of ACLs or create a new ACL and choose it.

Timer Settings

Timer settings let you configure the maximum amount of time that a connection with no traffic stays active. By configuring timer settings, you can have connections that shut down automatically, saving you connection time and cost.

Idle timeout

Enter the number of seconds that are allowed to pass before an idle connection (one that has no traffic passing over it) is terminated.

Fast idle timeout

The fast idle timeout is used when one connection is active while a competing connection is waiting to be made. The fast idle timeout sets the maximum number of seconds with no interesting traffic before the active connection is terminated and the competing connection is made.

This occurs when the interface has an active connection to a next hop IP address and the interface receives interesting data with a different next hop IP destination. Because the dialer connection is point-to-point, the competing packet cannot be delivered until the current connection is ended. This timer sets the amount of time that must pass while the first connection is idle before that connection will be terminated and the competing connection made.

Enable Multilink PPP

Multilink PPP lets you load-balance data over multiple ISDN BRI B channels and asynchronous interfaces. With multilink PPP, when an ISDN connection is initially made, only one B channel is used for the connection. If the traffic load on the connection exceeds the specified threshold (entered as a percentage of total bandwidth), then a connection with a second B channel is made, and the data traffic is shared over both connections. This has the advantage of reducing connection time and cost when data traffic is low, and letting you use your full ISDN BRI bandwidth when it is needed.

Check this check box if you want to enable multilink PPP. Uncheck it if you do not.

Load Threshold

Use this field to configure the percentage of bandwidth that must be used on a single ISDN BRI channel before another ISDN BRI channel connection will be made to load-balance traffic. Enter a number between 1 and 255, where 255 equals 100 percent of bandwidth on the first connection being utilized.

Data Direction

Cisco SDM supports Multilink PPP only for outbound network traffic.

Backup Configuration

ISDN BRI and analog modem interfaces can be configured to work as backup interfaces to other, primary interfaces. In that case, an ISDN or analog modem connection will be made only if the primary interface goes down for some reason. If the primary interface and connection go down, the ISDN or analog modem interface will immediately dial out and try to establish a connection so that network services are not lost.

Enable Backup

Check if you want this ISDN BRI or analog modem interface to act as a backup connection. Uncheck this check box if you do not want the ISDN BRI or analog modem interface to be a backup interface.

Primary Interface

Choose the interface on the router that will maintain the primary connection. The ISDN BRI or analog modem connection will only be made should the connection on the chosen interface go down.

Tracking Details

Use this section to identify a specific host to which connectivity must be maintained. The router will track connectivity to that host, and if the router discovers that connectivity to the host specified was lost by the primary interface, this will initiate a backup connection over the ISDN BRI or analog modem interface.

Hostname or IP Address to be Tracked

Enter the hostname or IP address of the destination host to which connectivity will be tracked. Specify an infrequently contacted destination as the site to be tracked.

Track Object Number

This is a read-only field that displays an internal object number generated and used by Cisco SDM for tracking the connectivity to the remote host.

Next Hop Forwarding

These fields are optional. You can enter the IP address to which the primary and backup interfaces will connect when they are active. This is known as the next hop IP address. If you do not enter next hop IP addresses, Cisco SDM will configure static routes using the interface name. Note that when you back up a multipoint WAN connection, such as an Ethernet connection, you must enter next hop IP addresses in order for routing to occur properly, but when backing up a point-to-point connection, this information is not necessary.

Primary Next Hop IP Address

Enter the next hop IP address of the primary interface.

Backup Next Hop IP Address

Enter the next hop IP address of the ISDN BRI or analog modem backup interface.