



# CHAPTER 4

## Create Connection Wizards

---

The Create Connection wizards let you configure LAN and WAN connections for all Cisco SDM-supported interfaces.

### Create Connection

This window allows you to create new LAN and WAN connections.



**Note**

---

You cannot use Cisco SDM to create WAN connections for Cisco 7000 series routers.

---

#### Create a New Connection

Choose a connection type to configure on the physical interfaces available on your router. Only interfaces that have not been configured are available. When you click the radio button for a connection type, a use case scenario diagram appears illustrating that type of connection. If all interfaces have been configured, this area of the window is not displayed.

If the router has Asynchronous Transfer Mode (ATM) or serial interfaces, multiple connections can be configured from a single interface because Cisco Router and Security Device Manager II (Cisco SDM) configures subinterfaces for each interface of that type.

The Other (Unsupported by Cisco SDM) radio button appears if an unsupported logical or physical interface exists, or if a supported interface exists that has been given an unsupported configuration. When you click the Other (Unsupported by Cisco SDM) radio button, the Create New Connection button is disabled.

If the router has radio interfaces but you do not see a **Wireless** radio button, you are not logged on as an Cisco SDM Administrator. If you need to use the wireless application, go to the Cisco SDM Tools menu and choose **Wireless Application**.

### What Do You Want to Do?

If you want to:	Do this:
Learn how to perform configurations that this wizard does not help you with.	See one of the following procedures: <ul style="list-style-type: none"> <li>• <a href="#">How Do I View the IOS Commands I Am Sending to the Router?</a></li> <li>• <a href="#">How Do I Configure an Unsupported WAN Interface?</a></li> <li>• <a href="#">How Do I Enable or Disable an Interface?</a></li> <li>• <a href="#">How Do I View Activity on My WAN Interface?</a></li> <li>• <a href="#">How Do I Configure NAT on a WAN Interface?</a></li> <li>• <a href="#">How Do I Configure a Static Route?</a></li> <li>• <a href="#">How Do I Configure a Dynamic Routing Protocol?</a></li> <li>• <a href="#">How Do I Configure Dial-on-Demand Routing for My ISDN or Asynchronous Interface?</a></li> </ul>
Configure an interface that Cisco SDM does not support.	See the software configuration guide for the router to use the CLI to configure the interface.

## WAN Wizard Interface Welcome Window

This window lists the types of connections you can configure for this interface using Cisco SDM. If you need to configure another type of connection for this interface, you can do so using the CLI.

## ISDN Wizard Welcome Window

PPP is the only type of encoding supported over an ISDN BRI by Cisco SDM.

## Analog Modem Welcome Window

PPP is the only type of encoding supported over an analog modem connection by Cisco SDM.

## Aux Backup Welcome Window

The option to configure the AUX port as a dial-up connection only appears for the Cisco 831 and 837 routers.

The Aux dial-backup radio button is disabled if any of the following conditions exist:

- More than one default route exists.
- One default route exists and it is configured with an interface other than the primary WAN interface.

The Aux dial-backup option is not shown if any of the following conditions exist:

- The router is not using a Cisco IOS image that supports the Aux dial-backup feature.
- A primary WAN interface is not configured.
- The asynchronous interface is already configured.
- The asynchronous interface is not configurable by Cisco SDM because of the presence of unsupported Cisco IOS commands in the existing configuration.

## Select Interface

This window appears if there is more than one interface of the type you selected in the Create Connection window. Choose the interface that you want to use for this connection.

If you are configuring an Ethernet interface, Cisco SDM inserts the description text \$ETH-WAN\$ in the configuration file so that it will recognize the interface as a WAN interface in the future.

## Encapsulation: PPPoE

This window lets you enable Point-to-Point-Protocol over Ethernet (PPPoE) encapsulation. This is necessary if your service provider or network administrator requires remote routers to communicate using PPPoE.

PPPoE is a protocol used by many asymmetric digital subscriber line (ADSL) service providers. Ask your service provider if PPPoE is used over your connection.

If you choose PPPoE encapsulation, Cisco SDM automatically adds a dialer interface to the configuration, and this is shown in the Summary window.

### Enable PPPoE Encapsulation

If your service provider requires that the router use PPPoE, check this box to enable PPPoE encapsulation. Uncheck this box if your service provider does not use PPPoE. This check box will not be available if your router is running a version of Cisco IOS that does not support PPPoE encapsulation.

## IP Address: ATM or Ethernet with PPPoE/PPPoA

Choose the method that the WAN interface will use to obtain an IP address.

### Static IP Address

If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided.

### 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 that will assign addresses.

## IP Unnumbered

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 you want to use for the interface you are configuring.

## Easy IP (IP Negotiated)

Choose **Easy IP (IP Negotiated)** if the router will obtain an IP address through PPP/IPCP address negotiation.

## Dynamic DNS

Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

# IP Address: ATM with RFC 1483 Routing

Choose the method that the WAN interface will use to obtain an IP address.

## 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 that will assign addresses.

## IP Unnumbered

Click **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 you want to use for the interface you are configuring.

## Dynamic DNS

Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

# IP Address: Ethernet without PPPoE

Choose the method that the WAN interface will use to obtain an IP address.

## 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 that will assign addresses.

## Dynamic DNS

Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

# IP Address: Serial with Point-to-Point Protocol

Choose the method that the point-to-point interface will use to obtain an IP address.

## 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](#).

## IP Unnumbered

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 you want to use for the interface you are configuring.

## Easy IP (IP Negotiated)

Choose **Easy IP (IP Negotiated)** if the router will obtain an IP address through PPP/IPCP address negotiation.

## Dynamic DNS

Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

# IP Address: Serial with HDLC or Frame Relay

Choose the method that the WAN interface will use to obtain an IP address. If Frame Relay encapsulation is used, Cisco SDM creates a subinterface, and the IP address is assigned to the subinterface Cisco SDM creates.

## 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](#).

## IP Unnumbered

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 you want to use for the interface you are configuring.

## Dynamic DNS

Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

# IP Address: ISDN BRI or Analog Modem

Choose the method that the ISDN BRI or analog modem interface will use to obtain an IP address.

## 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](#).

## IP Unnumbered

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 that has the IP address that you want the interface that you are configuring to use.

## Easy IP (IP Negotiated)

Choose **IP Negotiated** if the interface will obtain an IP address from your ISP through PPP/IPCP address negotiation whenever a connection is made.

## Dynamic DNS

Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

# Authentication

This page is displayed if you enabled or are configuring:



- **PPP** for a serial connection
- **PPPoE** or PPPoA encapsulation for an ATM connection
- **PPPoE** or PPPoA encapsulation for an Ethernet connection
- 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.

## Authentication Type

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.

## Username

The username is given to you by your Internet service provider or network administrator and is used as the username for CHAP or PAP authentication.

## Password

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

## Confirm Password

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

# Switch Type and SPIDs

ISDN BRI connections require identification of the ISDN switch type, and in some cases, identification of the B channels using service profile ID (SPID) numbers. This information will be provided to you by your service provider.

## 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 NET3 switch 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 or PBX systems:
  - basic-qsig—PINX (PBX) switches with QSIG signaling per Q.931

## I Have SPIDs

Check this check box if your service provider requires SPIDs.

Some service providers use SPIDs to define the services that are subscribed to by an 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 the device accesses the switch to initialize the connection.

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

A SPID is usually a 7-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 for the first BRI B channel provided to you by your ISP.

### SPID2

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

## Dial String

Enter the phone number of the remote end of the ISDN BRI or analog modem connection. This is the phone number that the ISDN BRI or analog modem interface will dial whenever a connection is made. The dial string is provided to you by your service provider.

## 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.

Choose whether this ISDN BRI or analog modem connection should act as a backup connection.

Note the following prerequisites:

- The primary interface must be configured for site-to-site VPN.
- The Cisco IOS image on your router must support the SAA ICMP Echo Enhancement feature.

## Backup Configuration: Primary Interface and Next Hop IP Addresses

In order for the ISDN BRI or analog modem connection to act as a backup connection, it must be associated with another interface on the router that will act as the primary connection. The ISDN BRI or analog modem connection will be made only if the connection on the primary interface goes down.

### Primary Interface

Choose the router interface that will maintain the primary connection.

### Primary Next Hop IP Address

This field is optional. Enter the IP address to which the primary interface will connect when it is active, known as the *next hop IP address*.

### Backup Next Hop IP Address

This field is optional. Enter the IP address to which the backup interface will connect when it is active, known as the *next hop IP address*.

## Backup Configuration: Hostname or IP Address to Be Tracked

This screen lets you 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 has been lost by the primary interface, a backup connection will be initiated over the ISDN BRI or analog modem interface.

### IP Address to be Tracked

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

# Advanced Options

There are two advanced options available, based on the router's configuration: Default static route, and Port Address Translation (PAT). If the Static Route option is not visible in the window, a static route has already been configured on the router. If the PAT option is not visible, PAT has already been configured on an interface.

## Default Static Route

Check this box if you want to configure a static route to the outside interface to which outgoing traffic will be routed. If a static route has already been configured on this router, this box does not appear.

### Next Hop Address

If your service provider has given you a next-hop IP address to use, enter the IP address in this field. If you leave this field blank, Cisco SDM will use the WAN interface that you are configuring as the next-hop interface.

## Port Address Translation

If devices on the LAN have private addresses, you can allow them to share a single public IP address. You can ensure that traffic goes to its proper destination by using PAT, which represents hosts on a LAN with a single IP address and uses different port numbers to distinguish the hosts. If PAT has already been configured on an interface, the PAT option will not be visible.

### Inside Interface to be Translated

Choose the inside interface connected to the network whose host IP addresses you want to be translated.

# Encapsulation

In this window, choose the type of encapsulation that the WAN link will use. Ask your service provider or network administrator which type of encapsulation is used for this link. The interface type determines the types of encapsulation available.

## Autodetect

Click **Autodetect** to have Cisco SDM discover the encapsulation type. If Cisco SDM succeeds, it will automatically supply the encapsulation type and other configuration parameters it discovers.



### Note

Cisco SDM supports autodetect on SB106, SB107, Cisco 836, and Cisco 837 routers. However if you are configuring a Cisco 837 router and the router is running Cisco IOS Release 12.3(8)T or 12.3(8.3)T, the autodetect feature is not supported.

## Available Encapsulations

The encapsulations available if you have an ADSL, G.SHDSL, or ADSL over ISDN interface are shown in the following table.

Encapsulation	Description
PPPoE	Provides Point-to-Point Protocol over Ethernet encapsulation. This is available when you have selected an Ethernet interface or an ATM interface. An ATM subinterface and a dialer interface will be created when you configure PPPoE over an ATM interface.  The PPPoE radio button will be disabled if your router is running a Cisco IOS that does not support PPPoE encapsulation.
PPPoA	Point-to-Point protocol over ATM. This option is available when you have selected an ATM interface. An ATM subinterface and a dialer interface will be created when you configure PPPoA over an ATM interface.  The PPPoA radio button will be disabled if your router is running a Cisco IOS that does not support PPPoA encapsulation.
RFC 1483 routing with AAL5-SNAP	This option is available when you have selected an ATM interface. An ATM subinterface will be created when you configure an RFC 1483 connection. The subinterface will be visible in the Summary window.
RFC 1483 routing with AAL5-MUX	This option is available when you have selected an ATM interface. An ATM subinterface will be created when you configure an RFC 1483 connection. The subinterface will be visible in the Summary window.

The encapsulations available if you have a serial interface are shown in the following table.

Encapsulation	Description
<b>Frame Relay</b>	Provides Frame Relay encapsulation. This option is available if you have selected a serial interface. A serial subinterface is created when you create a Frame Relay connection. This subinterface will be visible in the Summary window.  <b>Note</b> If a Frame Relay serial connection has been added to the interface, only Frame Relay encapsulation will be available in this window when subsequent serial connections are configured on the same interface.
<b>Point-to-Point Protocol</b>	Provides <b>PPP</b> encapsulation. This option is available when you have selected a serial interface.
<b>High Level Data Link Control</b>	Provides <b>HDLC</b> encapsulation. This option is available when you have selected a serial interface.

## PVC

ATM routing uses a two-layer hierarchical scheme, virtual paths and virtual channels, denoted by the virtual path identifier (**VPI**) and virtual channel identifier (**VCI**), respectively. A particular virtual path may carry a number of different virtual channels corresponding to individual connections. When switching is performed based on the VPI, all cells on that particular virtual path are switched regardless of the VCI. An ATM switch may route according to VCI, VPI, or both VCI and VPI.

### VPI

Enter the VPI value obtained from your service provider or system administrator. 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.

## VCI

Enter the VCI value obtained from your service provider or system administrator. 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. Enter the VCI value given to you by your service provider.

## Cisco IOS Default Values

The values shown in the following table are Cisco IOS defaults. Cisco SDM will not overwrite these values if they have been changed during a prior configuration, but if your router has not been previously configured, these are the values that will be used:

Connection Type	Parameter	Value
ADSL	<ul style="list-style-type: none"> <li>Operating mode</li> </ul>	<ul style="list-style-type: none"> <li>Auto</li> </ul>
G.SHDSL	<ul style="list-style-type: none"> <li>Operating mode</li> <li>Line rate</li> <li>Equipment type</li> </ul>	<ul style="list-style-type: none"> <li>Annex A (United States)</li> <li>Auto</li> <li>CPE</li> </ul>
ADSL over ISDN	<ul style="list-style-type: none"> <li>Operating mode</li> </ul>	<ul style="list-style-type: none"> <li>Auto</li> </ul>

# Configure LMI and DLCI

If you are configuring a connection with Frame Relay encapsulation, you must specify the protocol used to monitor the connection, called the Local Management Identifier (LMI), and provide a unique identifier for this particular connection, called a data link connection identifier (DLCI).

## LMI Type

Ask your service provider which of the following LMI types you should use.



LMI Type	Description
ANSI	Annex D defined by American National Standards Institute (ANSI) standard T1.617.
Cisco	LMI type defined jointly by Cisco Systems and three other companies.
ITU-T Q.933	ITU-T Q.933 Annex A.
Autosense	The default. This setting allows the router to detect which LMI type is being used by communicating with the switch and to then use that type. If <b>autosense</b> fails, the router will use the Cisco LMI type.

## DLCI

Enter the DLCI in this field. This number must be unique among all DLCIs used on this interface.

## Use IETF Frame Relay Encapsulation

Internet Engineering Task Force (IETF) encapsulation. This option is used with connecting to non-Cisco routers. Check this box if you are connecting to a non-Cisco router on this interface.

# Configure Clock Settings

The Clock Settings window is available when you are configuring a T1 or E1 link. The default Frame Relay clock settings are shown in this page. You should not change them unless you know you have different requirements.

## Clock Source

Internal specifies that the clock be generated internally. Line specifies that the clock source be taken from the network. The clock synchronizes data transmission. The default is **line**.

## T1 Framing

This field configures the **T1** or E1 link for operation with D4 Super Frame (sf) or Extended Superframe (esf). The default is **esf**.

## Line Code

This field configures the router for operation on binary 8-zeros substitution (B8ZS) or alternate mark inversion (AMI) **T1** lines. The **b8zs** setting ensures density on a T1 or E1 line by substituting intentional bipolar violations in bit positions 4 and 7 for a sequence of eight zero bits. When the router is configured with the AMI setting, you must use the data-coding inverted setting to ensure density on the T1 line. The default is **b8zs**.

## Data Coding

Click **inverted** if you know that user data is inverted on this link, or if the Line Code field is set to AMI. Otherwise leave this set to the default value **normal**. Data inversion is used with bit-oriented protocols such as **HDLC**, **PPP**, and Link Access Procedure, Balanced (**LAPB**) to ensure density on a **T1** line with **AMI** encoding. These bit-oriented protocols perform “zero insertions” after every five “one” bits in the data stream. This has the effect of ensuring at least one zero in every eight bits. If the data stream is then inverted, it ensures that at least one out of every eight bits is a one.

Cisco SDM will set data coding to inverted if the line code is AMI and there are no time slots configured for 56 kbps. If you do not want to use inverted data coding with the AMI line code, you must use the CLI to configure all time slots to 56 kbps.

## Facilities Data Link (FDL)

This field configures the router behavior on the Facilities Data Link (FDL) of the Extended Superframe. When configured with **att**, the router implements AT&T TR 54016. When configured with **ansi**, it implements ANSI T1.403. When you choose both, the router implements both **att** and **ansi** choices. When you choose none, the router ignores the FDL. The default is **none**. **If T1 or E1 framing is set to sf**, Cisco SDM will set FDL to **none** and make this field read-only.

## Line Build Out (LBO)

This field is used to configure the line build out (LBO) of the T1 link. The LBO decreases the transmit strength of the signal by  $-7.5$  or  $-15$  decibels. It is not likely to be needed on actual T1 or E1 lines. The default is **none**.

## Remote Loopback Requests

This field specifies whether the router will go into loopback mode when a loopback code is received on the line. Choosing **full** causes the router to accept full loopbacks, while choosing **payload-v54** will cause the router to choose payload loopbacks.

## Enable Generation/Detection of Remote Alarms

Check this box if you want the router T1 link to generate remote alarms (yellow alarms) and to detect remote alarms being sent from the peer on the other end of the link.

The remote alarm is transmitted by a router when it detects an alarm condition: either a red alarm (loss of signal) or a blue alarm (unframed 1s). The receiving channel service unit/data service unit (CSU/DSU) then knows that there is an error condition on the line.

This setting should only be used when T1 framing is set to **esf**.

# Delete Connection

You can delete a WAN connection that appears in the Edit Interface/Connections window. This window appears when you are deleting an interface configuration, and when the connection you want to delete contains associations such as access rules that have been applied to this interface. This window gives you the opportunity to save the associations for use with another connection.

When you delete a connection, the Create New Connection list is refreshed if the deletion makes a connection type available that was not available before the deletion.

You can automatically delete all associations that the connection has, or delete the associations later.

**To view the associations that the connection has:**

Click **View Details**.

**To delete the connection and all associations:**

Click **Automatically delete all associations**, and then click **OK** to cause Cisco SDM to delete the connection and all of the associations.

**To manually delete the associations:**

To manually delete the associations, click **View Details** to see a list of the associations that this connection has. Make note of the associations, choose **I will delete the associations later**, and then click **OK**. You can manually delete the associations using the instructions in the following list.

The possible associations and the instructions for deleting them are:

- **Default Static Route**—The interface is configured as the forwarding interface for a default static route. To delete the static route with which this interface is associated, click **Configure**, then click **Routing**. Click the static route in the Static Routing table, and click **Delete**.
- **Port Address Translation**—PAT is configured, using the interface on which this connection was created. To delete the PAT association, click **Configure**, then click **NAT**. Click the rule associated with this connection, and click **Delete**.
- **NAT**—The interface is designated as either a NAT inside or NAT outside interface. To delete the NAT association, click **Configure**, then click **Interfaces and Connections**. Click the connection in the interface list, and then click **Edit**. Click the **NAT** tab, then choose **None** from the NAT drop-down menu.
- **ACL**—An ACL is applied to the interface on which the connection was created. To delete the ACL, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, then click **Edit**. Click the **Association tab**, then in the Access Rule group, click the ... button next to both the Inbound and Outbound fields, and click **None**.

- **Inspect**—An inspection rule is applied to the interface on which the connection was created. To delete the inspection rule, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, then click **Edit**. Click the **Association tab**, then in the Inspection Rule group, for both the Inbound and Outbound fields, choose **None**.
- **Crypto**—A crypto map is applied to the interface on which the connection was created. To delete the crypto map, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, and then click **Edit**. Click the **Association tab**, then in the VPN group, in the IPsec Policy field, click **None**.
- **EZVPN**—An Easy VPN is applied to the interface on which the connection was created. To delete the Easy VPN, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, and then click **Edit**. Click the **Association tab**, then in the VPN group, in the Easy VPN field, click **None**.
- **VPDN**—VPDN commands that are required for a PPPoE configuration are present in the router configuration. If there are any other PPPoE connections configured on the router, do not delete the VPDN commands.
- **ip tcp adjust mss**—This command is applied to a LAN interface to adjust the TCP maximum size. If there are any other PPPoE connections configured on the router, do not delete this command.
- **Backup connection**—When a backup connection is configured for the primary interface. To delete the backup association, click **Configure**, then click **Interfaces and Connections**. Click the Backup interface in the Interface List, then click **Edit**. Click the **Backup tab** and uncheck the **Enable Backup** check box.
- **PAT on Backup connection**—PAT is configured on the backup interface. To delete the PAT association, click **Configure**, then click **NAT**. Click the rule associated with this connection, and then click **Delete**.
- **Floating Default Route on Backup connection**—The Backup interface is configured with a floating default static route. To delete the floating static route, click **Configure**, then click **Routing**. Click the floating static route in the Static Routing table, and click **Delete**.

## Summary

This screen displays a summary of the WAN link that you configured. You can review this information, and if you need to change anything, you can click the Back button to return to the screen on which you need to make changes.

### Test the connectivity after configuring

Check this box if you want Cisco SDM to test the connection you have configured after it delivers the commands to the router. Cisco SDM will test the connection and report results in another window.

### To save this configuration to the router's running configuration and leave this wizard:

Click **Finish**. Cisco SDM saves the configuration changes to the router's running configuration. The changes will take effect immediately, but will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the Cisco SDM Preferences window, the Deliver window appears. In this window, you can view the CLI commands that you are delivering to the router.

## Connectivity testing and troubleshooting

This window allows you to test a configured connection by pinging a remote host. If the ping fails, Cisco SDM reports the probable cause and suggests actions you can take to correct the problem.

### Which connection types can be tested?

Cisco SDM can troubleshoot ADSL, G.SHDSL V1 and G.SHDSL V2 connections, using PPPoE, AAL5SNAP or AAL5MUX encapsulation.

Cisco SDM can troubleshoot Ethernet connections with PPPoE encapsulation.

Cisco SDM cannot troubleshoot unencapsulated Ethernet connections, Serial and T1 or E1 connections, Analog connections, and ISDN connections. Cisco SDM provides basic ping testing for these connection types.

## What is Basic Ping Testing?

When Cisco SDM performs basic ping testing, it does the following:

1. Checks the interface status to see if it is up or down.
2. Checks DNS Settings, whether they be Cisco SDM default options or user-specified hostnames.
3. Checks for DHCP and IPCP configurations on the interface.
4. Exits interface test.
5. Pings the destination.

Cisco SDM reports the results of each of these checks in the Activity/Status columns. If the ping succeeds, then the connection will be reported as successful. Otherwise the connection is reported down, and the test that failed is noted.

## How does Cisco SDM Troubleshoot?

When Cisco SDM troubleshoots a connection, it performs a more extensive check than the basic ping test. If the router fails a test, Cisco SDM performs additional checks so it can provide you with the possible reasons for failure. For example, if Layer 2 status is down, Cisco SDM attempts to determine the reason(s), reports them, and recommends actions you can take to rectify the problem. Cisco SDM performs the following tasks:

1. Checks interface status. If the Layer 2 protocol is up, Cisco SDM goes to step 2.

If Layer 2 protocol status is down, Cisco SDM checks ATM PVC status for XDSL connections, or PPPoE status for encapsulated Ethernet connections.

- If the ATM PVC test fails, Cisco SDM displays possible reasons for the failure and actions you can take to correct the problem.
- If the PPPoE connection is down, there is a cabling problem, and Cisco SDM displays appropriate reasons and actions.

After performing these checks, the test is terminated and Cisco SDM reports the results and suggests actions.

2. Checks DNS Settings, whether they be Cisco SDM default options or user-specified hostnames.
3. Checks DHCP or IPCP configuration and status. If the router has an IP address through either DHCP or IPCP Cisco SDM goes to step 4.

If the router is configured for DHCP or IPCP but has not received an IP address through either of these methods, Cisco SDM performs the checks in step 1. The test terminates and Cisco SDM reports the results and suggests actions.

4. Pings the destination. If the ping succeeds, Cisco SDM reports success.

If the ping fails on an xDSL connection with PPPoE encapsulation, Cisco SDM checks:

- the ATM PVC status
- the PPPoE tunnel status
- the PPP authentication status

After performing these checks, Cisco SDM reports the reason that the ping failed.

If the ping fails on an Ethernet with PPPoE encapsulation connection, Cisco SDM checks:

- the PPPoE tunnel status
- the PPP authentication status

After performing these checks, Cisco SDM reports the reason that the ping failed.

If the ping fails on an xDSL connection with AAL5SNAP or AAL5MUX encapsulation, Cisco SDM checks the ATM PVC status and reports the reason the ping failed.

## IP Address/Hostname

Specify the server name to ping to test WAN interface.

### Automatically determined by SDM

Cisco SDM pings its default host to test WAN interface. Cisco SDM detects the router's statically configured DNS servers, and dynamically imported DNS servers. Cisco SDM pings these servers, and if successful pings exit through the interface under test, Cisco SDM reports success. If no pings succeeded, or successful pings were not found to exit the interface under test, Cisco SDM reports failure.

### User Specified

Specify the IP address of hostname of your choice for testing WAN interface.



## Summary

Click this button if you want to view the summarized troubleshooting information.

## Details





Click this button if you want to view the detailed troubleshooting information.

## Activity

This column displays the troubleshooting activities.

## Status

Displays the status of each troubleshooting activity by the following icons and text alerts:

-  The connection is up.
-  The connection is down.
-  Test is successful.
-  Test failed.

## Reason

This box provides the possible reason(s) for the WAN interface connection failure.

## Recommended action(s)

This box provides a possible action/solution to rectify the problem.

## What Do You Want to Do?

If you want to:	Do this:
Troubleshoot the WAN interface connection.	Click <b>Start</b> button.  When test is running, <b>Start</b> button label will change to <b>Stop</b> . You have option to abort the troubleshooting while test is in progress.
Save the test report.	Click <b>Save Report</b> button to save the test report in HTML format.  This button will be active only when test is in progress or when the testing is complete.

## How Do I...

This section contains procedures for tasks that the wizard does not help you complete.

## How Do I View the IOS Commands I Am Sending to the Router?

See [How Do I View the IOS Commands I Am Sending to the Router?](#)

## How Do I Configure an Unsupported WAN Interface?

Cisco SDM does not support configuration of every [WAN](#) interface that your router might support. If Cisco SDM discovers an interface in your router that it does not support, or a supported interface with an unsupported configuration, Cisco SDM displays a radio button labeled Other (Unsupported by Cisco SDM). The unsupported interface is displayed in the Interfaces and Connections window, but it cannot be configured using Cisco SDM.

To configure an unsupported interface, you must use the router command-line interface ([CLI](#)).

## How Do I Enable or Disable an Interface?

You can disable an interface without removing its configuration, and you can reenable an interface that you have disabled.

- 
- Step 1** Click **Configure** on the Cisco SDM toolbar.
  - Step 2** Click **Interfaces and Connections** in the left frame.
  - Step 3** Click the interface that you want to disable or enable.
  - Step 4** If the interface is enabled, the Disable button appears below the Interface List. Click it to disable the interface. If the interface is currently disabled, the Enable button appears in that location. Click that button to disable the interface.
- 

## How Do I View Activity on My WAN Interface?

You can view activity on a [WAN](#) interface by using the Monitor feature in Cisco SDM. Monitor screens can display statistics about the WAN interface, including the number of packets and bytes that have been sent or received by the interface, and the number of send or receive errors that have occurred. To display statistics about a WAN interface:

- 
- Step 1** From the toolbar, click **Monitor**.
  - Step 2** From the left frame, click **Interface Status**.
  - Step 3** In the Select an Interface field, choose the WAN interface for which you want to view statistics.
  - Step 4** Choose the data item(s) you want to view by checking the associated check box(es). You can view up to four statistics at a time.
  - Step 5** Click **Show Details** to see statistics for all selected data items.

The Interface Details screen appears, displaying the statistics you selected. The screen defaults to showing real-time data, for which it polls the router every 10 seconds. If the interface is up and there is data transmitting across it, you should see an increase in the number of packets and bytes transferred across the interface.

---

## How Do I Configure NAT on a WAN Interface?

---

- Step 1** Click **Configure** on the Cisco SDM toolbar.
- Step 2** Click **NAT** in the left frame.
- Step 3** In the NAT window, click **Designate NAT interfaces**.
- Step 4** Find the interface for which you want to configure NAT.
- Step 5** Check **inside(trusted)** next to the interface to designate the interface as an inside, or trusted interface. An inside designation is typically used to designate an interface serving a LAN whose resources must be protected. Check **outside(untrusted)** to designate it as an outside interface. Outside interfaces typically connect to an untrusted network. Click **OK**.

The interface is added to the pool of interfaces using NAT.

- Step 6** Review the Network Address Translation Rules in the NAT window. If you need to add, delete, or modify a rule, click the appropriate button on the NAT window to perform the configuration you need.
- 

For more information, click the following links:

- [Add or Edit Static Address Translation Rule: Inside to Outside](#)
- [Add or Edit Static Address Translation Rule: Outside to Inside](#)
- [Add or Edit Dynamic Address Translation Rule: Inside to Outside](#)
- [Add or Edit Dynamic Address Translation Rule: Outside to Inside](#)

## How Do I Configure NAT on an Unsupported Interface?

Cisco SDM can configure Network Address Translation (NAT) on an interface type unsupported by Cisco SDM. Before you can configure the firewall, you must first use the router CLI to configure the interface. The interface must have, at a minimum, an IP address configured, and it must be working. To verify that the connection is working, verify that the interface status is “Up.”

After you have configured the unsupported interface using the CLI, you can configure NAT using Cisco SDM. The unsupported interface will appear as “Other” on the router interface list.

## How Do I Configure a Dynamic Routing Protocol?

To configure a [dynamic routing](#) protocol:

- 
- Step 1** From the toolbar, click **Configure**.
  - Step 2** From the left frame, click **Routing**.
  - Step 3** In the Dynamic Routing group, click the dynamic routing protocol that you want to configure.
  - Step 4** Click **Edit**.  
The Dynamic Routing dialog box appears, displaying the tab for the dynamic routing protocol you selected.
  - Step 5** Using the fields in the Dynamic Routing dialog box, configure the dynamic routing protocol. If you need an explanation for any of the fields in the dialog box, click **Help**.
  - Step 6** When you have finished configuring the dynamic routing protocol, click **OK**.
-

## How Do I Configure Dial-on-Demand Routing for My ISDN or Asynchronous Interface?

ISDN BRI and asynchronous connections are dial-up connections, meaning that in order to establish a connection, the router must dial a preconfigured phone number. Because the cost of these types of connections is usually determined by the amount of time that a connection was established, and in the case of an asynchronous connection, that a phone line will be tied up, it is often desirable to configure Dial-on-Demand Routing (DDR) for these connection types.

Cisco SDM can help you configure DDR by:

- Letting you associate a rule (or ACL) with the connection, which causes the router to establish the connection only when it recognizes network traffic that you have identified as interesting with the associated rule.
- Setting idle timeouts, which cause the router to end a connection after a specified amount of time when there is no activity on the connection.
- Enabling multilink PPP, which causes an ISDN BRI connection to use only one of the two B channels unless a specified percentage of bandwidth is exceeded on the first B channel. This has the advantage of saving costs when network traffic is low and the second B channel is not needed, but letting you utilize the full bandwidth of your ISDN BRI connection when needed.

To configure DDR on an existing ISDN BRI or asynchronous connection:

- 
- Step 1** Click **Configure** on the Cisco SDM toolbar.
  - Step 2** Click **Interfaces and Connections** in the left frame.
  - Step 3** Click the ISDN or asynchronous interface on which you want to configure DDR.
  - Step 4** Click **Edit**.  
The Connection tab appears.
  - Step 5** Click **Options**.  
The Edit Dialer Option dialog box appears.
  - Step 6** If you want the router to establish the connection only when it recognizes specific IP traffic, click the **Filter traffic based on selected ACL** radio button, and either enter a rule (ACL) number that will identify which IP traffic should cause the router to dial out, or click the **...** button to browse the list of rules and choose the rule that you want to use to identify IP traffic from that list.

- Step 7** If you want to configure the router to end the connection when the connection is idle, i.e., no traffic passes across it, for a specified amount of time, in the **Idle timeout** field, enter the number of seconds the connection can remain idle before the router ends the connection.
- Step 8** If you are editing an ISDN connection, and you would like to use your second B channel only when the traffic on the first B channel exceeds a certain threshold, check the **Enable MultiLink PPP** check box, then in the **Load Threshold** field, enter a number between 1 and 255, where 255 equals 100% of bandwidth, that will determine the threshold on the first B channel. When traffic on that channel exceeds that threshold, it will cause the router to connect the second B channel. In addition, in the **Data direction** field, you can choose whether this threshold should apply to outbound or inbound traffic.
- Step 9** Click **OK**.
- 

## How Do I Edit a Radio Interface Configuration?

You must use the Wireless Application to edit an existing radio interface configuration.

---

- Step 1** Click **Configure** on the Cisco SDM toolbar.
- Step 2** Click **Interfaces and Connections** in the left frame, and then click the Edit Interface/Connection tab.
- Step 3** Choose the radio interface and click **Edit**. In the Connections tab, you can change the IP address or bridging information. If you want to change other wireless parameters, click **Launch Wireless** Application.
-

