Cisco SDM Express User's Guide

2.4

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: OL-7141-05

Cisco SDM Express User's Guide

CHAPTER 1

Cisco SDM Express

The Cisco SDM Express windows guide you through basic configuration of the router. After you complete the basic configuration, the router is available on the LAN, has a WAN connection, and has a firewall.

Welcome

This wizard guides you through a basic configuration that will help you do the following:

- Name the router.
- Specify a username and specify passwords.
- You can configure the router manually using the Cisco SDM Express wizard, or provision it with a configuration file loaded from a USB token or a USB flash device, Secure Device Provisioning (SDP), or Cisco Network Services, if supported by your Cisco IOS release.

  If you use Cisco Network Services to configure your router, you can provide Cisco Network Services parameters that will enable the router to contact a Cisco Network Services server and obtain a configuration.
- Change the factory default LAN IP address.

  This task is bypassed if SDP or Cisco Network Services is chosen for provisioning the router.
- Create a DHCP address pool for the LAN.

This task is bypassed if SDP or Cisco Network Services is chosen for provisioning the router.

- Identify DNS servers and your organization's domain name. Consult your network administrator or Internet service provider for this information.

  This task is bypassed if SDP or Cisco Network Services is chosen for provisioning the router.

- Create a WAN connection.
- Create a firewall for the LAN and WAN connections.
- Make settings that will enhance network security and performance.

To configure additional interfaces, and to make more advanced configuration settings, use Cisco Router and Security Device Manager (Cisco SDM). See Cisco Router and Security Device Manager for more information.

Basic Configuration

The Basic Configuration window lets you name the router that you are configuring, enter the domain name for your organization, and control access to Cisco SDM Express, Cisco Router and Security Device Manager, and the CLI.

Hostname Field

Enter the name you want to give the router.

Domain Name Field

Enter the domain name for your organization. An example of a domain name is *cisco.com*, but your domain name might end with a different suffix, such as *.org* or *.net*.

Username and Password Fields

You must set the username and password for Cisco SDM Express users and Telnet users.

Note You will use the username and password you set in this window the next time you use Cisco SDM Express, and thereafter, unless you change it. Make the password difficult to guess but easy for you to remember.

Username Field

Enter a username in this field.

Enter New Password Field

Enter the new password in this field. The password must be at least 6 characters.

Reenter New Password Field

Reenter the new password for confirmation.

Enable Secret Password Field

The enable secret password controls access to privileged EXEC mode by users who are accessing the router by means of Telnet or the console port. In privileged EXEC mode, users can make configuration changes and have access to other commands not available outside of this mode. You must enter the enable secret password in the **Enter Password** field, and reenter it in the **Reenter Password** field for confirmation. The password must be 6 characters or more.

Note Choose an enable secret password that you will remember but that will be difficult for others to guess. You will not be able to read it by viewing the configuration file because it is stored in encrypted form.

Router Provisioning

This window lists the options available for provisioning your router. Some of these options appear only if supported by your Cisco IOS release.

SDM Express

Choose this option to use Cisco SDM Express to manually provision your router.

USB Token or USB Flash

Choose this option if you have a USB token or USB flash device attached to your router and it contains the appropriate configuration file.

Note If both a USB token and a USB flash device are connected to your router, Cisco SDM Express will use the USB token. If you want to use the USB flash device connected to your router, all USB tokens must be removed from your router before running Cisco SDM Express.

Secure Device Provisioning

Choose Secure Device Provisioning (SDP) if your network administrator has given you information for provisioning your router with SDP.

Ensure the following before choosing the SDP option:

- There is IP connectivity between your router and the SDP server.
- Your web browser supports JavaScript.

If you choose SDP, a new browser window will automatically open after you complete the Cisco SDM Express wizard. The new browser window contains a wizard that guides you in provisioning your router with SDP.

For more information about SDP, go to

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

CNS Server

If your service provider has given you Cisco Network Services server information, choose this option. Click Cisco Network Services for more information.

Provision From USB Token

This window allows you to provision your router with a CCCD configuration file loaded from a USB token connected to your router. CCCD files are boot configuration files that can be loaded on USB tokens using TMS software.

Note This window appears only if a USB token is connected to your router. If both a USB token and a USB flash device are connected to your router, Cisco SDM Express will use the USB token. If you want to use the USB flash device connected to your router, all USB tokens must be removed from your router before running Cisco SDM Express.

When you provision your router with a CCCD configuration file, the file is merged with the running configuration, and it also becomes part of the startup configuration.

Caution Cisco SDM does not check the validity of configuration files you use to provision your router. Be sure that the contents of the configuration file you plan to use contain the appropriate settings.

To provision your router from a USB token, follow these steps:

Step 1 Choose the USB token name from the **Token Name** drop-down menu.

Step 2 Choose **Specify device and PIN** and enter a PIN in the Token PIN field if you do *not* want to use the default PIN to log in to the USB token.

If you choose **Specify device and default PIN**, the default PIN 1234567890 is used to log in to the USB token.

Step 3 Click **Login** to log in to the USB token.

If you are unable to log in to the USB token, your router cannot be provisioned from the USB token. Click the **Back** button and choose a different method to provision your router.

Step 4 Click **Preview CCCD** to display the contents of the file in the lower pane.

Provision From USB Flash

This window allows you to provision your router with a configuration file loaded from a USB flash device connected to your router. This window appears only if a USB flash device is connected to your router.

When you provision your router with a configuration file, the file is merged with the running configuration, and it also becomes part of the startup configuration.

Caution Cisco SDM does not check the validity of configuration files you use to provision your router. Be sure that the contents of the configuration file you plan to use contain the appropriate data.

To provision your router from a USB flash device, follow these steps:

Step 1 Enter the name of the configuration file, with full path, in the File Name field, or click **Browse** to open a file selection window.

The file must have the extension .cfg or the filename must be a CCCD file. CCCD files are boot configuration files.

Step 2 Click **Preview File** to display the contents of the file in the lower pane.

File Selection

This window allows you to load a file from your router. Only DOSFS file systems can be viewed in this window.

The left side of window displays an expandible tree representing the directory system on your Cisco router flash memory and on USB devices connected to that router.

The right side of the window displays a list of the names of the files and directories found in the directory that is specified in the left side of the window. It also shows the size of each file in bytes, and the date and time each file and directory was last modified.

You can choose a file to load in the list on the right side of the window. Below the list of files is a Filename field containing the full path of the specified file.

Note If you are choosing a configuration file to provision your router, the file must be a CCCD file or have a .cfg extension.

Name

Click **Name** to order the files and directories alphabetically based on name. Clicking **Name** again will reverse the order.

Size

Click **Size** to order the files and directories by size. Directories always have a size of zero bytes, even if they are not empty. Clicking **Size** again will reverse the order.

Time Modified

Click **Time Modified** to order the files and directories based on modification date and time. Clicking **Time Modified** again will reverse the order.

Wireless Interface Configuration

To configure the router wireless interface, click **Yes**. Cisco SDM Express will configure the router to bridge wireless traffic to the LAN interface. Click **No** if you do not want to configure the wireless interface. You can still configure LAN interface settings if you click **No**.

Cisco SDM Express enables you to configure one wireless interface. If there are additional wireless interfaces on your router, use the Wireless Application to configure them.

LAN Interface Configuration

This window lets you configure the LAN Ethernet interface IP address and subnet information.

If you need to change the LAN Ethernet interface's IP address and subnet information after completing the Cisco SDM Express wizard, you can do so by starting Cisco SDM Express again, clicking LAN and editing the address as necessary.

Interface/Bridge-to-Interface List

If the router has multiple LAN interfaces, the interfaces are displayed in this list. Select the LAN interface that you want to configure.

If the router has a wireless interface, and you clicked **Yes** in the Wireless Interface Configuration window, this list is labeled Bridge-to Interface. Select the interface to which you want to bridge wireless traffic.

IP Address Field

Enter the IP address for the LAN interface in dotted-decimal format. This can be a private IP address if you intend to use Network Address Translation (NAT) or Port Address Translation (PAT).

Note Make a note of this address. When you complete the Cisco SDM Express wizard and restart the router, use this address to run Cisco SDM Express. Do not use the address that was provided in the Quick Start Guide for the router.

Subnet Mask Field

Enter the subnet mask for the network. Obtain this value from your network administrator or service provider. 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. The value of the subnet mask also determines the number of hosts that can be on the LAN to which this router is connected.

Subnet Bits Field

Alternatively, enter the number of bits used to define the network and subnet portion of the IP address. Your network administrator or service provider may provide the subnet mask information in this form.

Wireless Parameters Fields

During initial configuration, these fields appear if the router has a wireless interface and you clicked **Yes** in the Wireless Interface Configuration window. If you are editing a configuration, these fields will appear if you made wireless settings during initial configuration. Wireless traffic will be bridged to this LAN interface.

Enter a Service Set Identifier (SSID) for this wireless traffic. The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity.

Note Changing a configured SSID value brings down the wireless connection.

If you are editing a LAN configuration after completing the Cisco SDM Express wizard and you want to configure advanced wireless parameters, click **Wireless** in the category bar.

Refresh, Apply Changes, Discard Changes Buttons

Visible if you are editing an initial configuration. Click Cisco SDM Express Buttons for more information**.**

DHCP Server Configuration

Dynamic Host Configuration Protocol (DHCP) is a simple form of addressing that is used when static addressing is not necessary and when you do not need to use port numbers for specific services. DHCP dynamically allocates an IP address to a host when it logs on to the network, and reclaims the address when it logs off. In this way, addresses can be reused when hosts no longer need them. Use DHCP for assigning addresses to resources (such as PCs) on your internal network.

Enable DHCP server on the LAN interface Check Box

Check to allow the router to assign private IP addresses to devices on the LAN. When enabled in this window, the DHCP server leases IP addresses to hosts for a period of one day. If you check this check box, you must enter values in the Starting IP Address and the Ending IP Address fields.

Starting IP Address Field

Cisco SDM Express enters the lowest address in the IP address range in this field, based on the IP address and subnet mask that you gave the LAN interface. You can change this value to a higher address value if you want to make the DHCP

address pool smaller, but you must enter an address in the same subnet as the address of the LAN interface, or Cisco SDM Express displays a message informing you that the address is invalid.

Ending IP Address Field

Cisco SDM Express enters the highest valid address in the IP address range in this field, based on the IP address and subnet mask that you gave the LAN interface. You can change this value to a lower address value if you want to make the DHCP address pool smaller, but you must enter an address in the same subnet as the address of the LAN interface, or Cisco SDM Express displays a message informing you that the address is invalid.

Domain Name Field

Visible after you have completed initial configuration. You can enter the domain name for your organization. An example of a domain name is *cisco.com*, but your domain name might end with a different suffix, such as *.org* or *.net*.

Import all DHCP option parameters to the DHCP server database Check Box

Visible after you have completed initial configuration. Check this option if you want to import DHCP option parameters to the DHCP server database and also send this information to DHCP clients on the LAN when they request IP addresses.

Primary Domain Name Server Field

Enter the IP address of the primary DNS server that the router will use. Your network administrator or service provider will provide you with the IP address.

The primary DNS server is the server that the router contacts first when attempting to resolve an IP address.

Secondary Domain Name Server Field

Enter the IP address of the secondary DNS server that the router will use, if one is available. Your network administrator or service provider will provide you with the IP address.

The secondary DNS server is the server that the router contacts if the primary server is not available.

Use these DNS values for DHCP clients Check Box

Available if a DHCP server is enabled on the LAN interface. Check if you want the router DHCP clients to be able to use the DNS servers whose IP addresses you enter in this window.

Refresh, Apply Changes, Discard Changes Buttons

Visible if you are editing an initial configuration. Click Cisco SDM Express Buttons for more information.

Internet (WAN): Ethernet Interface

Use this window to configure an Ethernet WAN interface.

Enable PPPoE Check Box

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

Address Type List

Select one of the following:

Static IP Address Option

If you choose static IP address, enter the IP address and subnet mask or the subnet bits in the fields provided.

Dynamic (DHCP Client) Option

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 Option

Select **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 the interface that you are configuring to use. If you did not choose Enable PPPoE, this option is not available.

Easy IP (IP Negotiated)

Select **Easy IP (IP Negotiated)** if the router will obtain an IP address by PPP/IPCP address negotiation. If you did not choose Enable PPPoE, this option is not available.

Authentication Type Check Box

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 Field

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

Password Field

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”.

Confirm Password Field

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

Refresh, Apply Changes, Discard Changes Buttons

Visible if you are editing an initial configuration. Click Cisco SDM Express Buttons for more information**.**

Internet (WAN): Autodetect Encapsulation

Cisco SDM Express supports autodetect on SB 106, SB 107, Cisco 836 and Cisco 837 routers. However, if you are configuring a Cisco 837 router running a Cisco IOS release 12.3(8)T or 12.3(8.3)T, the autodetect feature is not supported.

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

If Cisco SDM Express is unable to detect the type of encapsulation, you must specify the encapsulation and authentication types by clicking **User Specified**.

Status Icon and Enable or Disable Button

The Status icon is displayed when you are using Cisco SDM Express to edit an initial configuration. The Up arrow icon indicates the interface is up. The Down arrow icon indicates the interface is down.

The **Enable** or **Disable** button is available when you are using Cisco SDM Express to edit an initial configuration. If a selected interface is enabled, you can use the **Disable** button to shut down the interface. If a selected interface is shut down, you can use the **Enable** button to enable the interface.

Internet (WAN): User Specified Encapsulation

Use this window to configure a WAN interface when you are specifying the encapsulation.

Status Icon and Enable or Disable Button

The Status icon is displayed when you are using Cisco SDM Express to edit an initial configuration. The Up arrow icon indicates the interface is up. The Down arrow icon indicates the interface is down.

The **Enable** or **Disable** button is available when you are using Cisco SDM Express to edit an initial configuration. If a selected interface is enabled, you can use the **Disable** button to shut down the interface. If a selected interface is shut down, you can use the **Enable** button to enable the interface.

Encapsulation List

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. An ATM subinterface and a dialer interface are created when you configure PPPoE over an ATM interface. These logical interfaces will be visible in the Summary window. The PPPoE option is disabled if your router is running a release of Cisco IOS software that does not support PPPoE encapsulation.
PPPoA	Provides Point-to-Point Protocol over ATM encapsulation (AAL5 SNAP, and AAL5 MUX). The PPPoA option is disabled if your router is running a release of Cisco IOS software 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. This 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. This subinterface will be visible in the Summary window.

Virtual Path Identifier Field

Enter the Virtual Path Identifier (VPI) value obtained from your service provider or system administrator. The VPI is used in ATM switching and routing to identify the path used for a number of connections.

Virtual Circuit Identifier Field

Enter the Virtual Circuit Identifier (VCI) value obtained from your service provider or system administrator. The VCI is used in ATM switching and routing to identify a particular connection within a path that it may share with other connections.

Address Type List

Select one of the following:

- **Static IP Address**—If you choose static IP address, enter the IP address and subnet mask or the subnet 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**—Select **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 the interface that you are configuring to use.
- **Easy IP** (**IP Negotiated**)—Select **Easy IP (IP Negotiated)** if the router will obtain an IP address by PPP/IPCP address negotiation.

IP Address for Remote Connection in Central Office Field

If you are configuring a G.SHDSL connection, enter the IP address of the gateway 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 to the Internet or to your organization's WAN.

Authentication Type Check Box

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 Field

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

Password Field

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".

Confirm Password Field

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

Refresh, Apply Changes, Discard Changes Buttons

Visible if you are editing an initial configuration. Click Cisco SDM Express Buttons for more information**.**

WAN Interface Selection

Cisco SDM Express allows you to configure one WAN connection. If your router has multiple WAN interfaces, select the interface that you want to configure in this window. Select the interface you want to configure from the list, click **Add Connection**, and configure the connection in the dialog displayed.

Note If you do not configure a WAN connection, you will not be able to configure firewall, routing, Cisco Network Services, or SDP.

Add Connection, Edit, Delete Buttons

The **Add Connection** button is enabled if no WAN connection is configured yet. The **Edit** and **Delete** buttons are enabled if at least one WAN connection has been configured.

To configure an interface, select the interface and click **Add**.**Connection**. If this button is disabled, you can configure additional WAN connections using Cisco SDM, or delete a configured connection and configure a different one.

To edit an existing configuration, select the interface and click **Edit**.

To delete a configuration, select the interface and click **Delete**.

Enable or Disable Button

Available when you are using Cisco SDM Express to edit an initial configuration. If a selected interface is enabled, you can use the **Disable** button to shut down the interface. If a selected interface is shut down, you can use the **Enable** button to enable the interface.

Interface List

Displays the interface name, IP address, and interface type for all WAN interfaces. If no IP address is configured for an interface, the text "no IP address" is displayed.

Note If you did not configure the default LAN interface with a new IP address in the LAN Interface Configuration window, it is listed in this window, and can be configured as a WAN interface.

Refresh Button

Visible if you are editing an initial configuration. Click Cisco SDM Express Buttons for more information**.**

Serial Connection

Create or edit a serial connection in this window.

Encapsulation List

Select the encapsulation for this connection. If you are editing a connection, you cannot change the encapsulation type in this window. You must delete the connection, and then create a new connection with the encapsulation type you need.

- **Frame Relay**—A switched data link layer protocol that handles multiple virtual circuits using HDLC encapsulation between connected devices.
- **HDLC**—High-Level Data Link Control. A bit-oriented synchronous data link layer protocol developed by the International Standards Organization (ISO). HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.
- **PPP**—Point-to-Point Protocol.

Authentication Details

If you select PPP encapsulation, you can provide authentication information that your Internet service provider may require.

- **Username**—Enter exactly as given to you by your Internet service provider or network administrator and is used as the username for CHAP and/or PAP authentication.
- **Password**—Enter exactly as given to you by your service provider. Passwords are case sensitive. For example, the password "test" is not the same as "Test".
- **Confirm Password**—Reenter the same password that you entered in the previous box.

Address Type List

- **Static IP address**—Available with Frame Relay, PPP, and HDLC encapsulation types. If you choose static IP address, enter the IP address and subnet mask or the subnet bits in the fields provided.
- **IP Unnumbered**—Available with Frame Relay, PPP, and HDLC encapsulation types. Select **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 the interface that you are configuring to use.
- **IP Negotiated**—Available with PPP encapsulation type only. Select **Easy IP (IP Negotiated)** if the router will obtain an IP address by PPP/IPCP address negotiation.

IP Address and Subnet Mask Fields

If you select Static IP address, provide the IP address and subnet mask in these fields.

Frame Relay Configuration Settings Link

Click Frame Relay Configuration Settings for a description of the DLCI, LMI, and Use IETF Frame Relay Encapsulation fields.

Frame Relay Configuration Settings

DLCI Field

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 is disabled. If you need to change the DLCI, delete the connection and create it again.

LMI Type Field

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 Option

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

Cisco Option

LMI type defined jointly by Cisco and three other companies.

ITU-T Q.933 Option

ITU-T Q.933 Annex A.

Autosense Option

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 autosense fails, the router will use the Cisco LMI type.

Use IETF Frame Relay Encapsulation Check Box

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

Internet (WAN): Advanced Options

This window enables you to specify a default static route and to enable NAT on the router.

Create Default Route Check Box

A default static route specifies an IP address or interface that the router will send traffic to when the traffic is bound for a network that the router has not learned. If you select **Use This Interface as the Forwarding Interface**, the router will send all such traffic to the WAN interface you are configuring. If you select **Next Hop IP address**, specify an address that you want the router to forward such traffic to.

These fields do not appear if you selected a WAN interface with a dynamic IP address.

CNS Server Information

This window appears if you configured a WAN connection and chose to provision the router using the Cisco Network Services option. It lets you to enter the Cisco Network Services server information given to you by your service provider. Enter the IP address and login information of the Cisco Network Services server so that Cisco SDM Express can retrieve configuration information for your router.

Enter the CNS Server IP Address /Hostname Field

You must enter either the IP address or hostname of the Cisco Network Services server on your network. If you enter a hostname, you will have to provide the IP address of a DNS server able to resolve the hostname to an IP address.

Enter the CNS ID String Field

You must enter the device ID required to obtain the configuration file from the Cisco Network Services server.

Enter the CNS Password Field

Enter the password used to log in to the Cisco Network Services server with the user ID entered above.

Primary DNS Field

Enter the IP address of the primary Domain Name Server (DNS) that the router will use. Your network administrator or service provider will provide you with the IP address.

The primary DNS server is the server that the router contacts first when attempting to resolve an IP address.

Note If you enter a hostname to identify a Cisco Network Services server in the Enter the CNS Server IP Address /Hostname field, you must enter the IP address of a DNS server in the Primary DNS field.

Secondary DNS Field

Enter the IP address of the secondary domain name Server that the router will use, if one is available. Your network administrator or service provider will provide you with the IP address.

The secondary DNS server is the server that the router contacts if the primary server is not available.

Firewall Configuration

The Firewall Configuration window gives you the option of letting Cisco SDM Express configure a firewall on your WAN and LAN interfaces. You can apply a firewall during initial setup, or you can use Cisco SDM Express to apply it after giving the router its initial configuration.

If you let Cisco SDM Express configure the firewall, you can modify the firewall configuration later using the Cisco SDM Firewall Policy configuration feature.

Note

- This feature is available if the Cisco IOS release running on your router supports the Firewall feature set.
- The Firewall Configuration window does not appear if you did not configure a WAN interface.

The firewall protects your network in the following ways:

- Apply default access rules to inside and outside interfaces—Cisco SDM Express creates and applies a list of default access rules that, among other things, permit DNS and HTTP traffic and deny the private IP address space.
- Apply default inspection rules to outside interface—Cisco SDM Express creates and applies a list of default inspection rules.
- Enable IP Unicast Reverse-Path Forwarding (RPF) on the outside interface—IP Unicast RPF is a feature that causes the router to check the source address of any packet against the interface through which the packet entered the router. If the input interface is not a feasible path to the source address according to the routing table, the packet will be dropped. This source address verification is used to defeat IP spoofing.

If you choose to let the Cisco SDM Express configure the firewall, you can modify the firewall configuration later using Cisco SDM. If you choose not to have a firewall configured, you can configure one later using Cisco SDM Express or Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Security Settings

This window lets you disable features that are on by default in the Cisco IOS software and that can create security risks or make the router send messages at such a high volume that it would use up its available memory. You should leave the check boxes checked unless you know that your requirements are different. This help topic links to descriptions of each security setting that Cisco SDM Express makes.

You can use Cisco SDM Express to change security settings that you make in this window after you have completed initial configuration. If you want to change any of the individual settings listed under the setting groups described in this help page, you can do so by using Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable SNMP Services on Your Router Check Box

Check to disable the SNMP service on your router. For an explanation of why SNMP should be disabled, see the help topic Disable SNMP.

Disable Services that Involve Security Risks Check Box

Check to disable the following services on the router. For an explanation of why these services should be disabled, click the links below:

- Disable Finger Service
- Disable PAD Service
- Disable TCP Small Servers Service
- Disable UDP Small Servers Service
- Disable IP BOOTP Server Service
- Disable IP Identification Service
- Disable CDP
- Disable IP Source Route
- Disable IP Gratuitous ARPs
- Disable IP Redirects
- Disable IP Proxy ARP
- Disable IP Directed Broadcast
- Disable MOP Service
- Disable IP Unreachables
- Disable IP Mask Reply

Enable Services for Enhanced Security on the Router/Network Check Box

Check to enable the following security-enhancing features and services on your router. For an explanation of these services and features, click the links below:

- Enable Netflow Switching
- Enable TCP Keepalives for Inbound Telnet Sessions
- Enable TCP Keepalives for Outbound Telnet Sessions
- Enable Sequence Numbers and Time Stamps on Debugs
- Enable IP CEF
- Set Scheduler Interval
- Set Scheduler Allocate
- Set TCP Synwait Time
- Enable Logging
- Enable Unicast RPF on Outside Interfaces

Enhance Security on Router Access Check Box

Check to implement the following security-enhancing configurations on your router. For an explanation of these services and features, click the links below:

- Set Minimum Password Length to Less Than 6 Characters
- Set Authentication Failure Rate to Less Than 3 Retries
- Set Banner
- Enable Telnet Settings
- Enable SSH for Access to the Router

Encrypt Passwords Check Box

Check to enable password encryption. For more information, see the help topic Enable Password Encryption Service.

Synchronize the router date and time with my local PC settings Check Box

Checked by default. If you do not want to set the router date and time using the current settings for the PC on which you are running Cisco SDM Express, uncheck this check box.

Summary

The Summary window shows you the changes you have made to the router configuration. If you want to make changes to the configuration, click **Back** to return to the window you want to make changes in.

Click **Finish** to save the data you entered to the router configuration file.

Note When you click **Finish**, you will lose the connection to the router if you gave the LAN interface a new IP address as we recommend. To be able to reconnect to the router, you must ensure that the PC remains in the same subnet as the router and then enter the new IP address you gave the LAN interface. Click Reconnecting to the Router After Initial Configuration for more information.

Supplementary Help

The following help topics provide additional information.

Cisco Router and Security Device Manager

After you have used Cisco SDM Express to give your router a basic configuration, you can use Cisco Router and Security Device Manager (Cisco SDM) to configure additional connections, to fine-tune configurations you completed using Cisco SDM Express, and to configure advanced features such as Virtual Private Networks (VPNs) and Digital Certificates.

Cisco SDM may be installed on your router, or you may have received a CD that you can use to install Cisco SDM on your PC or on your router. If you downloaded Cisco SDM from Cisco.com, you can use the setup program to install Cisco SDM on your PC or on your router.

To start Cisco SDM, click **Cisco SDM** in the Tools menu.

Cisco Network Services

If your service provider has provided you Cisco Network Services server information, choose this option. When you choose this option, the Cisco SDM Express wizard collects information about your Cisco Network Services server and then displays the WAN configuration windows so that you can configure the WAN connection that will connect to the Cisco Network Services server and obtain the configuration. If your service provider has not provided Cisco Network Services server information, or you want to configure the router using Cisco SDM Express, do not select this option.

You will not be able to use Cisco Network Services if:

- Your router has no installed WAN interfaces, or the router has a WAN interface that Cisco SDM Express does not support. Cisco SDM Express must be able to configure a WAN interface in order for the router to obtain the Cisco Network Services configuration file. If Cisco SDM Express determines that it cannot configure a WAN interface, it will display an error message informing you that you cannot use Cisco Network Services. If there are no WAN interfaces installed on the router, and you still want to use Cisco Network Services, click Cancel to leave the Startup wizard, and close Cisco SDM Express. Then, install a WAN interface card supported by Cisco SDM Express, restart Cisco SDM Express, and select **CNS Server** (Cisco Network Services server) in the Startup wizard.

  For a list of supported interface cards, see the Cisco SDM Release Notes on:

  http://www.cisco.com/go/sdm

- You did not select this option, and configured a LAN and a WAN interface using Cisco SDM Express, and then returned to the Router Provisioning window and selected **CNS Server**. If you want to use Cisco Network Services, click **Cancel** to leave the Startup wizard and close Cisco SDM Express. Then restart Cisco SDM Express and select **CNS Server** in the Router Provisioning window.

Security Settings

The following topics describes security settings that Cisco SDM Express can make.

Disable SNMP

Cisco SDM Express disables the Simple Network Management Protocol (SNMP) whenever possible. SNMP is a network protocol that provides a facility for retrieving and posting data about network performance and processes. It is very widely used for router monitoring, and frequently for router configuration changes. Version 1 of SNMP, however, which is the most commonly used, is often a security risk for the following reasons:

- It uses authentication strings (passwords) called *community strings* which are stored and sent across the network in plain text.
- Most SNMP implementations send those strings repeatedly as part of periodic polling.
- It is an easily spoofable, datagram-based transaction protocol.

Because SNMP can be used to retrieve a copy of the network routing table and sensitive network information, we recommend disabling SNMP if your network does not require it. Cisco SDM Express will initially request to disable SNMP.

The configuration that will be delivered to the router to disable SNMP is as follows:

```
no snmp-server
```

Disable Finger Service

Cisco SDM Express disables the finger service whenever possible. Finger is used to learn which users are logged into a network device. Although this information is often not highly sensitive, it can sometimes be useful to an attacker.

In addition, the finger service can be used in a specific type of Denial-of-Service (DoS) attack called “Finger of death,” which involves sending a finger request to a specific computer every minute, but never disconnecting.

The configuration that will be delivered to the router to disable the Finger service is as follows:

```
no service finger

You can undo this fix using the SDM Security Audit feature. To learn
how, For more information, click Cisco Router and Security Device
Manager.
```

Disable PAD Service

Cisco SDM Express disables all packet assembler/disassembler (PAD) commands and connections between PAD devices and access servers whenever possible.

The configuration that will be delivered to the router to disable PAD is as follows:

```
no service pad
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable TCP Small Servers Service

Cisco SDM Express disables small services whenever possible. By default, Cisco devices running Cisco IOS release 11.3 or earlier offer the “small services”: echo, chargen, and discard. (Small services are disabled by default in Cisco IOS software release 12.0 and later.) These services, especially their User Datagram Protocol (UDP) versions, are infrequently used for legitimate purposes, but they can be used to launch Denial of Service (DoS) and other attacks that would otherwise be prevented by packet filtering.

For example, an attacker might send a Domain Name System (DNS) packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the router UDP echo port, the result would be the router sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet because it would be considered to be locally generated by the router itself.

Although most abuses of the small services can be avoided or made less dangerous by antispoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Because the services are rarely used, the best policy is usually to disable them on all routers of any description.

The configuration that will be delivered to the router to disable TCP small servers is as follows:

```
no service tcp-small-servers
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable UDP Small Servers Service

Cisco SDM Express disables small services whenever possible. By default, Cisco devices running Cisco IOS release 11.3 or earlier offer the "small services": echo, chargen, and discard. (Small services are disabled by default in Cisco IOS software release 12.0 and later.) These services, especially their UDP versions, are infrequently used for legitimate purposes, and they can be used to launch DoS and other attacks that would otherwise be prevented by packet filtering.

For example, an attacker might send a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the router UDP echo port, the result would be the router sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet because it would be considered to be locally generated by the router itself.

Although most abuses of the small services can be avoided or made less dangerous by antispoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Because the services are rarely used, the best policy is usually to disable them on all routers of any description.

The configuration that will be delivered to the router to disable UDP small servers is as follows:

```
no service udp-small-servers
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable IP BOOTP Server Service

Cisco SDM Express disables Bootstrap Protocol (BOOTP) service whenever possible. BOOTP allows both routers and computers to automatically configure necessary Internet information from a centrally maintained server upon startup, including downloading Cisco IOS software. As a result, BOOTP can potentially be used by an attacker to download a copy of a router's Cisco IOS software.

In addition, the BOOTP service is vulnerable to DoS attacks; therefore it should be disabled or filtered by a firewall.

The configuration that will be delivered to the router to disable BOOTP is as follows:

```
no ip bootp server
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable IP Identification Service

Cisco SDM Express disables identification support whenever possible. Identification support allows you to query a TCP port for identification. This feature enables an unsecure protocol to report the identity of a client initiating a TCP connection and a host responding to the connection. With identification support, you can connect a TCP port on a host, issue a simple text string to request information, and receive a simple text-string reply.

It is dangerous to allow any system on a directly connected segment to learn that the router is a Cisco device and to determine the model number and the Cisco IOS software release being run. This information may be used to design attacks against the router.

The configuration that will be delivered to the router to disable the IP identification service is as follows:

```
no ip identd
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable CDP

Cisco SDM Express disables Cisco Discovery Protocol whenever possible. Cisco Discovery Protocol is a proprietary protocol that Cisco routers use to identify each other on a LAN segment. This is dangerous in that it allows any system on a directly connected segment to learn that the router is a Cisco device and to determine the model number and the Cisco IOS software release being run. This information may be used to design attacks against the router.

The configuration that will be delivered to the router to disable Cisco Discovery Protocol is as follows:

```
no cdp run
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable IP Source Route

Cisco SDM Express disables IP source routing whenever possible. The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that the datagram will take toward its ultimate destination, and generally the route that any reply will take. These options are rarely used for legitimate purposes in networks. Some older IP implementations do not process source-routed packets properly, and it may be possible to crash machines running these implementations by sending them datagrams with source routing options.

Disabling IP source routing will cause a Cisco router to never forward an IP packet that carries a source routing option.

The configuration that will be delivered to the router to disable IP source routing is as follows:

```
no ip source-route
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Enable Password Encryption Service

Cisco SDM Express enables password encryption whenever possible. Password encryption directs the Cisco IOS software to encrypt the passwords, Challenge Handshake Authentication Protocol (CHAP) secrets, and similar data that are saved in its configuration file. This is useful for preventing casual observers from reading passwords, for example, when they happen to look over an administrator's shoulder.

The configuration that will be delivered to the router to enable password encryption is as follows:

```
service password-encryption
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Enable Netflow Switching

Cisco SDM Express enables Netflow switching whenever possible. Netflow switching is a Cisco IOS feature that enhances routing performance while using Access Control Lists (ACLs) and other features that create and enhance network security. Netflow identifies flows of network packets based on the source and destination IP addresses and TCP port numbers. Netflow then can use just the initial packet of a flow for comparison to ACLs and for other security checks, rather than having to use every packet in the network flow. This enhances performance, allowing you to make use of all of the router security features.

The configuration that will be delivered to the router to enable Netflow is as follows:

```
ip route-cache flow
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Enable TCP Keepalives for Inbound Telnet Sessions

Cisco SDM Express enables TCP keepalive messages for both inbound and outbound Telnet sessions whenever possible. Enabling TCP keepalives causes the router to generate periodic keepalive messages, letting it detect and drop broken Telnet connections.

The configuration that will be delivered to the router to enable TCP keepalives for inbound Telnet sessions is as follows:

```
service tcp-keepalives-in
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Enable TCP Keepalives for Outbound Telnet Sessions

Cisco SDM Express enables TCP keepalive messages for both inbound and outbound Telnet sessions whenever possible. Enabling TCP keepalives causes the router to generate periodic keepalive messages, letting it detect and drop broken Telnet connections.

The configuration that will be delivered to the router to enable TCP keepalives for outbound Telnet sessions is as follows:

```
service tcp-keepalives-out
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Enable Sequence Numbers and Time Stamps on Debugs

Cisco SDM Express enables sequence numbers and time stamps on all debug and log messages whenever possible. Time stamps on debug and log messages indicate the time and date that the message was generated. Sequence numbers indicate the sequence in which messages that have identical time stamps were generated. Knowing the timing and sequence that messages are generated is an important tool in diagnosing potential attacks.

The configuration that will be delivered to the router to enable time stamps and sequence numbers is as follows:

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timeout msec
service sequence-numbers
```

Enable IP CEF

Cisco SDM Express enables Cisco Express Forwarding or Distributed Cisco Express Forwarding whenever possible. Because there is no need to build cache entries when traffic starts arriving at new destinations, Cisco Express Forwarding behaves more predictably than other modes when presented with large volumes of traffic addressed to many destinations. Routes configured for Cisco Express Forwarding perform better under SYN attacks than routers using the traditional cache.

The configuration that will be delivered to the router to enable Cisco Express Forwarding is as follows:

```
ip cef
```

Set Scheduler Interval

Cisco SDM Express configures the scheduler interval on the router whenever possible. When a router is fast-switching a large number of packets, it is possible for the router to spend so much time responding to interrupts from the network interfaces that no other work gets done. Some very fast packet floods can cause this condition, which may stop administrative access to the router, a very dangerous condition when the device is under attack. Tuning the scheduler interval ensures that management access to the router is always available by causing the router to run system processes after the specified time interval even when CPU usage is at 100%.

The configuration that will be delivered to the router to tune the scheduler interval is as follows:

```
scheduler interval 500
```

Set Scheduler Allocate

On routers that do not support the command **scheduler interval**, Cisco SDM Express configures the **scheduler allocate** command whenever possible. When a router is fast-switching a large number of packets, it is possible for the router to spend so much time responding to interrupts from the network

interfaces that no other work gets done. Some very fast packet floods can cause this condition. It may stop administrative access to the router, which is very dangerous when the device is under attack. The **scheduler allocate** command guarantees a percentage of the router CPU processes for activities other than network switching, such as management processes.

The configuration that will be delivered to the router to set the scheduler allocate percentage is as follows:

```
scheduler allocate 4000 1000
```

Set TCP Synwait Time

Cisco SDM Express sets the TCP synwait time to 10 seconds whenever possible. The TCP synwait time is a value that is useful in defeating SYN flooding attacks, a form of Denial-of-Service (DoS) attack. A TCP connection requires a three-phase handshake to initially establish the connection. A connection request is sent by the originator, an acknowledgement is sent by the receiver, and then an acceptance of that acknowledgement is sent by the originator. After this three-phase handshake is complete, the connection is complete and data transfer can begin. A SYN flooding attack sends repeated connection requests to a host, and never sends the acceptance of acknowledgements that complete the connections, creating increasingly more incomplete connections at the host. Because the buffer for incomplete connections is usually smaller than the buffer for completed connections, this can overwhelm and disable the host. Setting the TCP synwait time to 10 seconds causes the router to shut down an incomplete connection after 10 seconds, preventing the buildup of incomplete connections at the host.

The configuration that will be delivered to the router to set the TCP synwait time to 10 seconds is as follows:

```
ip tcp synwait-time <10>
```

Enable Logging

Cisco SDM Express will enable logging with time stamps and sequence numbers whenever possible. Because it gives detailed information about network events, logging is critical in recognizing and responding to security events. Time stamps and sequence numbers provide information about the date, time, and sequence in which network events occur.

The configuration that will be delivered to the router to enable and configure logging is as follows, replacing <*log buffer size*> and <*logging server ip address*> with the appropriate values that you enter into Cisco SDM Express:

```
logging console critical
logging trap debugging
logging buffered <log buffer size>
logging <logging server ip address>
```

Enable Unicast RPF on Outside Interfaces

Cisco SDM Express enables unicast Reverse Path Forwarding (RPF) on all interfaces that connect to the Internet whenever possible. RPF is a feature that causes the router to check the source address of any packet against the interface through which the packet entered the router. If the input interface is not a feasible path to the source address according to the routing table, the packet will be dropped. This source address verification is used to defeat IP spoofing.

This works only when routing is symmetric. If the network is designed in such a way that traffic from host A to host B may normally take a different path than traffic from host B to host A, the check will always fail, and communication between the two hosts will be impossible. This sort of asymmetric routing is common in the Internet core. Ensure that your network does not use asymmetric routing before enabling this feature.

In addition, unicast RPF can be enabled only when IP Cisco Express Forwarding is enabled. Cisco SDM Express will check the router configuration to see if IP Cisco Express Forwarding is enabled. If IP Cisco Express Forwarding is not enabled, Cisco SDM Express will recommend that IP Cisco Express Forwarding be enabled and will enable it if the recommendation is approved. If IP Cisco Express Forwarding is not enabled, by Cisco SDM Express or otherwise, unicast RPF will not be enabled.

To enable unicast RPF, the following configuration will be delivered to the router for each interface that connects outside of the private network, replacing <*outside interface*> with the interface identifier:

```
interface <outside interface>
ip verify unicast reverse-path
```

Disable IP Gratuitous ARPs

Cisco SDM Express disables IP gratuitous Address Resolution Protocol (ARP) requests whenever possible. A gratuitous ARP is an ARP broadcast in which the source and destination MAC addresses are the same. It is used primarily by a host to inform the network about its IP address. A spoofed gratuitous ARP message can cause network mapping information to be stored incorrectly, causing network malfunction.

To disable gratuitous ARPs, the following configuration will be delivered to the router:

```
no ip gratuitous-arps
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable IP Redirects

Cisco SDM Express disables Internet Message Control Protocol (ICMP) redirect messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP redirect messages instruct an end node to use a specific router as its path to a particular destination. In a properly functioning IP network, a router will send redirects only to hosts on its own local subnets, no end node will ever send a redirect, and no redirect will ever be traversed more than one network hop. However, an attacker may violate these rules; some attacks are based on this. Disabling ICMP redirects will cause no operational impact to the network, and it eliminates this possible method of attack.

The configuration that will be delivered to the router to disable ICMP redirect messages is as follows:

```
no ip redirects
```

Disable IP Proxy ARP

Cisco SDM Express disables proxy Address Resolution Protocol (ARP) whenever possible. ARP is used by the network to convert IP addresses into MAC addresses. Normally ARP is confined to a single LAN, but a router can act as a

proxy for ARP requests, making ARP queries available across multiple LAN segments. Because proxy ARP breaks the LAN security barrier, use it only between two LANs with an equal security level, and only when necessary.

The configuration that will be delivered to the router to disable proxy ARP is as follows:

```
no ip proxy-arp
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable IP Directed Broadcast

Cisco SDM Express disables IP directed broadcasts whenever possible. An IP directed broadcast is a datagram 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 stream of replies, which can completely inundate the host whose address is being falsified.

Disabling IP directed broadcasts causes directed broadcasts that would otherwise be “exploded” into link-layer broadcasts at that interface to be dropped instead.

The configuration that will be delivered to the router to disable IP directed broadcasts is as follows:

```
no ip directed-broadcast
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable MOP Service

Cisco SDM Express will disable the Maintenance Operations Protocol (MOP) on all Ethernet interfaces whenever possible. MOP is used to provide configuration information to the router when communicating with DECNet networks. MOP is vulnerable to various attacks.

The configuration that will be delivered to the router to disable the MOP service on Ethernet interfaces is as follows:

```
no mop enabled
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable IP Unreachables

Cisco SDM Express disables Internet Message Control Protocol (ICMP) host unreachable messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP host unreachable messages are sent out 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.

The configuration that will be delivered to the router to disable ICMP host unreachable messages is as follows:

```
int <all-interfaces>
no ip unreachables
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Disable IP Mask Reply

Cisco SDM Express disables Internet Message Control Protocol (ICMP) mask reply messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. 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.

The configuration that will be delivered to the router to disable ICMP mask reply messages is as follows:

```
no ip mask-reply
```

You can undo this fix using the Cisco SDM Security Audit feature. To learn how, see the Security Audit online help in Cisco SDM. For more information, click Cisco Router and Security Device Manager.

Set Minimum Password Length to Less Than 6 Characters

Cisco SDM Express configures your router to require a minimum password length of 6 characters whenever possible. One method attackers use to crack passwords is to try all possible combinations of characters until the password is discovered. Longer passwords have exponentially more possible combinations of characters, making this method of attack much more difficult.

This configuration change will require every password on the router, including the user, enable, secret, console, AUX, tty, and vty passwords, to be at least 6 characters in length. This configuration change will be made only if the Cisco IOS version running on your router supports the minimum password length feature.

The configuration that will be delivered to the router is as follows:

```
security passwords min-length <6>
```

Set Authentication Failure Rate to Less Than 3 Retries

Cisco SDM Express configures your router to lock access after 3 unsuccessful login attempts whenever possible. One method of cracking passwords, called the “dictionary” attack, is to use software that attempts to log in using every word in a dictionary. This configuration causes access to the router to be locked for a period of 15 seconds after 3 unsuccessful login attempts, disabling the dictionary method of attack. In addition to locking access to the router, this configuration causes a log message to be generated after 3 unsuccessful login attempts, warning the administrator of the unsuccessful login attempts.

The configuration that will be delivered to the router to lock router access after 3 unsuccessful login attempts is as follows:

```
security authentication failure rate <3>
```

Set Banner

Cisco SDM Express configures a text banner whenever possible. In some jurisdictions, civil and/or criminal prosecution of users who break into your systems is made much easier if you provide a banner informing unauthorized users that their use is in fact unauthorized. In other jurisdictions, you may be forbidden to monitor the activities of even unauthorized users unless you have taken steps to notify them of your intent to do so. The text banner is one method of performing this notification.

The configuration that will be delivered to the router to create a text banner is as follows, replacing <*company name*>, <*administrator email address*>, and <*administrator phone number*> with the appropriate values that you enter into Cisco SDM Express:

```
banner ~
Authorized access only
This system is the property of <company name> Enterprise.
Disconnect IMMEDIATELY as you are not an authorized user!
Contact <administrator email address> <administrator phone number>.
~
```

Enable Telnet Settings

Cisco SDM Express secures the console, AUX, vty, and tty lines by implementing the following configurations whenever possible:

- Configures **transport input** and **transport output** commands to define which protocols can be used to connect to those lines.
- Sets the exec-timeout value to 10 minutes on the console and AUX lines, causing an administrative user to be logged out from these lines after 10 minutes of no activity.

The configuration that will be delivered to the router to secure the console, AUX, vty, and tty lines is as follows:

```
!
line console 0
transport output telnet
```

```
exec-timeout 10
login local
!
line AUX 0
transport output telnet
exec-timeout 10
login local
!
line vty ….
transport input telnet
login local
```

Enable SSH for Access to the Router

If the Cisco IOS release running on the router is a crypto image (an image that uses 56-bit Data Encryption Standard (DES) encryption and is subject to export restrictions), then Cisco SDM Express will implement the following configurations to secure Telnet access whenever possible:

- Enable Secure Shell (SSH) for Telnet access. SSH makes Telnet access much more secure.
- Set the SSH timeout value to 60 seconds, causing incomplete SSH connections to shut down after 60 seconds.
- Set the maximum number of unsuccessful SSH login attempts to two before locking access to the router.

The configuration that will be delivered to the router to secure access and file transfer functions is as follows:

```
ip ssh time-out 60
ip ssh authentication-retries 2
!
line vty 0 4
transport input ssh
!
```

Cisco SDM Express Buttons

Help Button

Click to open a new browser window and show information about the Cisco SDM Express window displayed.

About Button

Clicking **About** displays a window containing Cisco SDM Express version information. Click **Hardware and Software Details** in this window to display the following information.

Hardware Details:

- Router model type
- Total memory in the router
- Total flash capacity in the router
- Where the router boots from (for example: flash)

A diagram of the hardware configuration is also provided.

Software Details:

- The name of the Cisco IOS software the router is running
- The release of the Cisco IOS software
- The feature sets, such as Firewall and VPN, that the Cisco IOS software supports
- The version of Cisco SDM Express

Exit Button

After you complete an initial configuration, click **Exit** to close Cisco SDM Express.

Refresh Button

Visible if you are editing an initial configuration. Click **Refresh** to refresh the router data in Cisco SDM Express.

Apply Changes Button

Visible if you are editing an initial configuration. Click **Apply Changes** to deliver changes you have made to the router.

Discard Changes Button

Visible if you are editing an initial configuration. Click **Discard Changes** to clear the window of changes you have made.

Reconnecting to the Router After Initial Configuration

If you gave the router LAN interface a new IP address as recommended, you will lose your connection to the router after you deliver the configuration.

Follow this procedure to reconnect to the router after performing initial configuration with Cisco SDM Express.

Step 1 Place the PC on the same subnet as the router's LAN interface.

- If you configured the router as a DHCP server, you must configure the PC to obtain an IP address automatically, and then open a command window and enter the **ipconfig /release** command followed by the **ipconfig /renew** command.
- If the router is not configured as a DHCP server, you must give the PC a static IP address in the same subnet as the router. For example, if you changed the LAN IP address to 10.20.20.1 with a subnet mask of 255.255.255.224, you would give your PC an IP address between 10.20.20.2 and 10.20.20.30, and use the same subnet value

Step 2 If you configured a different LAN interface than the default interface, be sure to connect your PC to the LAN interface that you configured. For example, if you configured FE 0/1 and not FE 0/0 as the LAN interface, be sure to connect you PC to FE 0/1.

Step 3 After preparing the PC, reconnect your PC to the router by entering the new IP address that you gave the router's LAN interface in the browser (http://*new IP address)*. For example, if you changed the LAN IP address to 10.20.20.1, you would enter http://10.20.20.1 in the web browser to connect to your router again.

Step 4 After reconnecting, test your WAN connection to verify that you can connect to the Internet.

Click Testing Your WAN (Internet) Connection for more information.

Testing Your WAN (Internet) Connection

You can test your connection to the Internet by pointing your browser to a remote website, such as www.cisco.com. If you are able to connect to the remote website you entered, your WAN configuration works properly.

If you cannot connect to a remote website, you can use Cisco SDM to troubleshoot the connection by doing the following:

Step 1 Click **Cisco SDM** in the Tools menu to launch Cisco SDM.

Step 2 Log in to Cisco SDM and click **Interfaces and Connections**.

Step 3 Click the Edit tab and select the WAN connection you want to test.

Step 4 Click **Test Connection** and follow the instructions that appear. Cisco SDM reports on the possible problems and recommends actions.

SDP Troubleshooting Tips

Use this information before enrolling using Secure Device Provisioning (SDP) to prepare the connection between the router and the certificate server. If you experience problems enrolling, you can review these tasks to determine where the problem is.

When SDP is launched, you must minimize the browser window displaying this help topic so that you can view the SDP web application.

Troubleshooting Tips

These recommendations involve preparations on the local router and on the Certificate Authority (CA) server. You need to communicate these requirements to the administrator of the CA server. Ensure the following:

- The local router and the CA server have IP connectivity between each other. The local router must be able to ping the certificate server successfully, and the certificate server must be able to successfully ping the local router.
- The CA server administrator uses a web browser that supports JavaScript.
- The CA server administrator has enable privileges on the local router.
- The firewall on the local router will permit traffic to and from the certificate server.
- If a firewall is configured on the Petitioner and/or on the Registrar, you must ensure that the Firewall permits HTTP or HTTPS traffic from the PC from which the SDM /SDP application is invoked.

For more information about SDP, see the following web page:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

CHAPTER 2

Cisco SDM Express Edit Mode

Cisco SDM Express edit screens allow you to make changes to your LAN and WAN configurations, and change firewall, NAT, PAT, routing, and security settings.

Overview

The Overview window provides you with basic information about the router LAN, WAN, and Firewall configurations.

Icons

	Up. The interface is up.
	Active. The Firewall is active.
	Down. The interface is down.
	Inactive. The firewall is inactive

LAN Fields

The LAN fields display the interface, the IP address, and DHCP server information for the LAN connection.

- **Interface**—The name of the LAN interface. For example, Fast Ethernet 0. If Cisco SDM Express cannot identify the router's LAN interfaces, it displays the number of configured LAN interfaces in this field.
- **IP/Mask**—The IP address followed by the number of subnet bits, which represents the subnet mask. LAN IP addresses are often drawn from the private IP address range. For example an IP address of 10.10.10.1 using a subnet mask of 255.255.255.0 would be shown as 10.10.10.1/24.
- **DHCP Server**—Either **Configured** or **Not Configured**.
- **DHCP Pool**—If a DHCP server has been configured, this field contains the IP address range available to DHCP clients. For example, if the LAN interface is configured with an IP address in the 10.10.10.0 network, the DHCP pool may be configured with a range of addresses from 10.10.10.1 through 10.10.10.254.

If Cisco SDM Express cannot identify the LAN interfaces on the router, it displays the total number of supported LAN interfaces, and the total number of configured LAN interfaces.

Internet (WAN) Fields

The Internet fields display the WAN interface name, the type of WAN connection configured and the IP address subnet mask information.

- **Interface**—The name of the WAN interface, for example ATM 0/1. If Cisco SDM Express cannot identify the router's WAN interfaces, it displays the number of configured WAN interfaces in this field.
- **Connection Type**—The type of WAN connection, for example ADSL, or G.SHDSL
- **IP/Mask**—The IP address followed by the number of subnet bits, which represents the subnet mask. For example an IP address of 172.16.33.15 using a subnet mask of 255.255.255.0 would be shown as 172.16.33.15/24.

If Cisco SDM Express cannot identify the WAN interfaces on the router, it displays the total number of supported WAN interfaces, and the total number of configured WAN interfaces.

Firewall Fields

- **Firewall type**—Cisco SDM Express Default, Custom, or None.
- **Inside**—The IP address of the inside, or trusted, interface.

- **Outside**—The type of connection of the Internet interface.

Basic Configuration

This window displays the user accounts configured on the router, and enables you to change the enable secret password. The enable secret password must be used to enter IOS CLI Enable mode.

If you want to add or remove user accounts, you can do so using Cisco Router and Security Device Manager (SDM).

Edit/Delete Buttons

Use these buttons to manage the user accounts on the router. You can edit existing user accounts and delete existing accounts. If you need to create a new user account, you can use SDM to do so. For more information, click Cisco Router and Security Device Manager.

Note The Edit and Delete buttons are disabled when a user account created with the View option is selected.

Username/Login Password/Password is Encrypted Fields

This area lists the user accounts on the router.

Enable Secret Password Field

Enter the new password in these fields. Be sure to make a note of this password. It is stored in encrypted form on the router and cannot be read.

Hostname Field

You can edit the router's hostname if you want to do so.

Domain Name Field

You can edit the router's configured domain name.

Refresh/Apply Changes/Discard Changes Buttons

These buttons are visible if you editing an initial configuration. Click Cisco SDM Express Buttons for more information**.**

Edit a Username

Edit a user account in the fields provided in this window.

User Name Field

Edit the username in this field.

Password Field

Enter or edit the password in this field.

Reenter the password in the **Confirm Password** field. If the password and the confirm password do not match, an error message window will be displayed when you click **OK**.

When you click **OK**, the new or edited account information will appear in the Configure User Accounts for Telnet window.

Encrypt password using MD5 hash algorithm Checkbox

This is a read-only field that displays the current password MD5 encryption setting. A check mark indicates that the password is encrypted using the one-way Message Digest 5 (MD5) algorithm.

LAN

Bridge/Do not bridge LAN interface with wireless Checkbox

If your router has a wireless interface, you can bridge traffic from the wireless network to your Ethernet LAN. If you want to bridge traffic and share address space between the Ethernet LAN on your router, and the wireless network, click **Bridge LAN interface with wireless**.

LAN interface configuration Fields

You can edit the IP address and subnet mask of the LAN interface in these fields. See IP Address Field if you need more information about the IP address and subnet mask fields.

Wireless

The Wireless window appears when your router has a wireless interface. If you need to configure advanced wireless parameters, click **Launch Wireless Application**.

Refresh Button

This button is visible if you editing an initial configuration. Click Cisco SDM Express Buttons for more information**.**

WAN—Unable to Configure WAN Interface

This window appears when Cisco SDM Express is unable to configure the interface you have selected as a WAN interface. This might happen if the interface you selected is not supported by Cisco SDM Express, or if the interface has a partial configuration that was entered using the CLI.

You can select another interface to configure, or log on to the router and remove the configuration statements under the interface that you want to configure. Select **Telnet** from the Tools section, log onto the router and enter config mode. Use the CLI to remove the configuration statements. Then, return to Cisco SDM Express and configure the WAN interface.

No WAN Available

This window appears when Cisco SDM Express cannot detect a WAN interface on your router.

Delete Connection

When you delete a connection, there may be associated configuration commands that can either be retained in the configuration, or deleted along with the connection. Click **View Details** to display these associations. Click **Hide Details** to hide association details.

Click **Automatically delete all associations** if you want Cisco SDM Express to remove the associations along with the connection.

Click **I will delete the associations later** if you want to remove the associations yourself.

To delete the associations yourself, click **Telnet** in the tools menu, log in to the router, and enter the **enable** command to enter Enable mode. Then, remove the associated configuration commands by entering the **no** form of the command. For example, if the command **ip tcp adjust mss** is associated with the connection, enter:

```
no ip tcp adjust mss
```

Firewall

Use this window to enable a firewall if you did not enable it during initial setup, or to disable the firewall if you did enable it. If the Cisco IOS image the router is running does not support the Firewall feature set, you will not be able to enable a basic firewall on this router. You will not be able to use Cisco SDM Express to enable a basic firewall if your router is a modular router with multiple LAN or WAN interfaces.

See Firewall Configuration for a description of what a basic firewall will do.

Enable Firewall/Disable Firewall Buttons

Use these buttons to add or remove the basic firewall configuration.

Unable to configure Firewall Window

If Cisco SDM Express is unable to let you configure a firewall, the Unable to configure Firewall window is displayed. The following are reasons why you may not be able to configure a firewall:

- The router is a fixed-port router and there is not exactly one LAN and one WAN interface configured.
- The router is a modular router, or there are more than two interfaces configured.
- A firewall and/or access control lists have been applied to your router using other tools.

Refresh Button

This button is visible if you editing an initial configuration. Click Cisco SDM Express Buttons for more information**.**

NAT

If devices on the LAN have private addresses, you can allow them to share a single public IP address by using Network Address Translation (NAT). NAT uses port numbers to identify hosts, and the host services that you want to make available.

Click **Enable NAT** to use NAT on the router.

Unable to Configure NAT

If you are in SDM Express edit-mode, this window appears when Cisco SDM Express is not able to help you configure NAT. Cisco SDM Express may not be able to help you configure NAT for the following reasons.

- The router is a fixed-port router and there is not exactly one LAN and one WAN interface configured.
- The router is a modular router, or there are more than two interfaces configured.
- NAT is already configured on an interface.

Add Button

Click to add a new NAT rule.

Edit Button

Click to edit the chosen NAT rule.

Refresh Button

This button is visible if you editing an initial configuration. Click Cisco SDM Express Buttons for more information**.**

Add or Edit Address Translation Rule

In this window you can enter or edit the IP address translation information for a server.

Private IP Address

Enter the IP address that the server uses on your internal network. This is an IP address that cannot be used externally, on the Internet.

Public IP Address

Choose **IP address of WAN interface** to use the IP address of the router WAN interface. The configured IP address of the WAN interface appears to the right. Or choose **New IP address** and enter the server IP address.

Type of Server

Choose one of the following server types from the drop-down menu:

- Web server

  An HTTP host serving HTML and other WWW-oriented pages.
- Email server

  An SMTP server for sending Internet mail.
- Other

The server is not a web or email server, but requires port translation to provide service. This choise activates the Translated Port field and the Protocol drop-down menu.

If you do not choose a server type, all traffic intended for the public IP address you choose for the server will be routed to it, and no port translation will be done.

Original Port

Enter the port number used by the server to accept service requests from the internal network.

Translated Port

Enter the port number used by the server to accept service requests from the Internet.

Protocol

Choose TCP or UDP for the protocol used by the server with the original and translated ports.

Routing

The Routing window allows you to edit an existing default route when configuration changes indicate that editing the default route is advisable. For example, if you have changed a static IP address of a WAN interface, you may also need to change the IP address of the default gateway.

Enable Check Box

Check if you want to enable a default route. If a default route has already been defined, this box will be checked. Unchecking it disables the default route.

Forwarding (Next Hop) Field

You can specify an interface on the router as the next hop, or you can specify an IP address. If you click **Interface**, select the interface from the drop down list. If you click **IP address**, enter the IP address.

Refresh/Apply Changes/Discard Changes Buttons

These buttons are visible if you are editing an initial configuration. Click Cisco SDM Express Buttons for more information.

Security Settings

This window lets you disable features that are on by default in the Cisco IOS software, but that can create security risks, or make the router send messages at such a high volume that it would use up its available memory. You should leave the boxes checked unless you know that your requirements are different.

If you allow Cisco SDM Express to make these settings and you later want to change any of the individual setting described under these setting groups, you can do so by using SDM. For more information, click Cisco Router and Security Device Manager.

Select All (Recommended by Cisco) Checkbox

Clicking **Select All** lets you implement all security settings in this window. If you later decide you want to change the security settings, you can do so using Cisco SDM.

Disable Services that Involve Security Risks Checkbox

Check this box to disable the following services on the router. For an explanation of why these services should be disabled, click the links below:

- Disable Finger Service
- Disable PAD Service
- Disable TCP Small Servers Service
- Disable UDP Small Servers Service
- Disable IP BOOTP Server Service
- Disable IP Identification Service
- Disable CDP
- Disable IP Source Route
- Disable IP Gratuitous ARPs

- Disable IP Redirects
- Disable IP Proxy ARP
- Disable IP Directed Broadcast
- Disable MOP Service
- Disable IP Unreachables
- Disable IP Mask Reply

Enable Services for Enhanced Security on the Router/Network Checkbox

Check this box to enable the following security-enhancing features and services on your router. For an explanation of these services and features, click the links below:

- Enable Netflow Switching
- Enable TCP Keepalives for Inbound Telnet Sessions
- Enable TCP Keepalives for Outbound Telnet Sessions
- Enable Sequence Numbers and Time Stamps on Debugs
- Enable IP CEF
- Set Scheduler Interval
- Set Scheduler Allocate
- Set TCP Synwait Time
- Enable Logging

Encrypt Passwords Checkbox

Check this box to enable password encryption. For more information, see the help topic Enable Password Encryption Service.

Synchronize with my local PC clock Checkbox

Click this button to synchronize your router with the clock on your local PC.

Refresh/Apply Changes/Discard Changes Buttons

These buttons are visible if you are editing an initial configuration. Click Cisco SDM Express Buttons for more information.

Tools

Cisco SDM Express provides a number of tools that you can use

Ping Option

Click to open a window in which you can specify the source and destination of the ping. See Ping for more information.

Telnet Option

Displays the Windows Telnet dialog box, letting you connect to your router and access the Cisco IOS command-line interface (CLI) using the Telnet protocol.

Cisco SDM Option

Click to launch Cisco Router and Security Device Manager (SDM) . SDM allows you to perform advanced configurations.

Software Update Option

You can have Cisco SDM Express help you update the configuration software on your router. You can update from Cisco.com, or, if you have downloaded the SDM .zip file to your PC, you can update using that file. Click on any of the following for more information.

- Update SDM from Cisco.com
- Update SDM from Local PC
- Update SDM from CD

Ping

You can ping a peer device in this window. You can select both the source and destination of the ping operation. You may want to ping a remote peer after you reconfigure a WAN connection.

Source Field

Select or enter the IP address where you want the ping to originate. If the address you want to use is not in the list, you can enter a different one in the field. The ping can originate from any interface on the router. By default, the **ping** command originates from the outside interface with the connection to the remote device.

Destination Field

Select the IP address that you want to ping. If the address you want to use is not in the list, you can enter a different one in the field.

To ping a remote peer:

Specify the source and destination, and click **Ping**. You can read the output of the **ping** command to determine whether the ping was successful.

To clear the output of the ping command:

Click **Clear**.

Update SDM from Cisco.com

You can update Cisco SDM Express and SDM directly from Cisco.com. SDM checks Cisco.com for the versions available and informs you if there is a version newer than the one currently running on the router. You can then update SDM using the Update wizard.

To update SDM from Cisco.com:

Step 1 Select Update SDM from Cisco.com from the Tools menu. Selecting this option starts the update wizard.

Step 2 Use the update wizard to obtain the SDM files and copy them to your router.

CCO Login

You must provide a CCO login and password to access this web page. Provide a username and password, and then click OK.

If you do not have a CCO login and password, you can obtain one by opening a web browser and going to the Cisco website at the following link:

http://www.cisco.com

When the webpage opens, click Register and provide the necessary information to obtain a username and password. Then, try this operation again.

Update SDM from Local PC

You can update SDM using an SDM.zip file you have downloaded from Cisco.com. SDM provides an update wizard that will copy the necessary files to your router.

To update SDM from the PC you are using to run SDM follow these steps:

Step 1 Download the file sdm-v*nn*.zip from the following URL:

`http://www.cisco.com/cgi-bin/tablebuild.pl/sdm`

If there is more than one SDM .zip file, obtain the copy with the highest version number.

Step 2 Use the update wizard to copy the SDM files from your PC to the router.

Update SDM from CD

If you have the SDM CD, you can use it to update SDM on your router. To do so, follow these steps:

Step 1 Place the SDM CD in the CD drive on your PC.

Step 2 Select **Update SDM from CD**, and click **Update Software** in the General Instructions window after reading the text.

Step 3 SDM will enable you to locate the file SDM-Updates.xml on the CD. When you locate the file, click **Open**.

Step 4 Follow the instructions in the installation wizard.

Date and Time Properties

Use this window to make router date and time settings. You can have Cisco SDM Express synchronize settings with the PC, or you can make settings manually.

Synchronize with my local PC clock Checkbox

Check to set up Cisco SDM Express to synchronize router date and time settings with the date and time settings on the PC.

Synchronize Checkbox

Click to have Cisco SDM Express perform a synchronization. Cisco SDM Express adjusts date and time settings in this way only when you click **Synchronize; it does not automatically re synchronize with the PC during subsequent sessions. This button is disabled if you have not checked Synchronize with my local PC clock.**

Note You must make the Time Zone and Daylight Savings settings on the PC before starting Cisco SDM Express so that Cisco SDM Express will receive the correct settings when you click **Synchronize**.

Edit Date and Time Fields

Use this area to set the date and time manually. You can choose the month and the year from the drop-down lists, and choose the day of the month in the calendar. The fields in the Time area require values in 24-hour format. You can select your time zone based on Greenwich Mean Time (GMT), or you can browse the list for major cities in your time zone.

If you want the router to adjust time settings for daylight saving time and Standard time, check **Automatically adjust clock for daylight savings changes**.

Apply Button

Click to apply the date and time settings you have made in the Date, Time, and Time Zone fields.

Reset to Factory Defaults

You can reset the configuration of the router to factory defaults and save the current configuration to a file that can be used later. If you changed the router's LAN IP address from the factory value 10.10.10.1, you will lose the connection between the router and the PC because that IP address will change back to 10.10.10.1 when you reset.

Note The Reset to Factory Defaults feature is not supported on Cisco 3620, 3640, 3640A, and 7000 series routers.

Step 1: Save Running Config to PC

Save the router's running configuration to the PC in this step, so that you can restore it to your router if you need to. Use the **Browse** button to select the directory to store the configuration in.

Step 2: Write down these steps and then reset the router

Since you will lose contact with the router when you click **Reset**, you must understand how you are going to reconnect after you reset the router.

a) Configure the PC with an IP address on the 10.10.10.0 network

Configure the PC to be on the 10.10.10.0 subnet. Depending on the router, you must either configure the PC to obtain an IP address automatically, or configure it with a static IP address in the 10.10.10.0 subnet.

If you have a router listed in the following table, configure the PC to obtain an IP address automatically. Consult Reconfiguring Your PC with a Static or a Dynamic IP Address to learn how to do this.

If you have one of these routers, configure the PC to obtain an IP address automatically
SB10x, Cisco 83x, 85x, 87x, 1701, 1710, 1711, and 1712, 180x and 181x.

If you have a router listed in the following table, configure the PC with an IP address in the 10.10.10.0 subnet, between 10.10.10.2 and 10.10.10.6 using a subnet mask of 255.255.255.248. Consult Reconfiguring Your PC with a Static or a Dynamic IP Address to learn how to do this.

If you have one of these routers, configure the PC with a static IP address in the 10.10.10.0 subnet
Cisco 1721, 1751, 1760, 1841, 2600XM, 2691, 28xx, 36xx, 37xx, and 38xx.

b) Point your web browser to http(s)://10.10.10.1

After reset, the router has the original factory default IP address of 10.10.10.1, and you must use this address to reconnect.

c) Log into SDM Express again with username cisco and password cisco.

The username and password have also been returned to their default settings and these original values must be used to log on to Cisco SDM Express.

Refresh Button

This button is visible if you editing an initial configuration. Click Cisco SDM Express Buttons for more information.

Reconfiguring Your PC with a Static or a Dynamic IP Address

The process for giving the PC a static IP address or configuring it to obtain an IP address automatically varies slightly depending on the version of Microsoft Windows the PC is running.

Note Do not reconfigure the PC until after you reset the router.

Microsoft Windows NT

From the Control Panel, double-click the **Network** icon to display the Network window. Click **Protocols**, select the first TCP/IP Protocol entry, and click **Properties**. In the Properties window, select the Ethernet adapter used for this connection. Click **Obtain an IP Address Automatically** to obtain a dynamic IP address.

For a static IP address, click **Specify an IP address**. Enter the IP address 10.10.10.2 or any other address in the 10.10.10.0 subnet greater than 10.10.10.1. Enter the subnet 255.255.255.248. You can leave other fields blank. Click **OK**.

Microsoft Windows ME

From the Control Panel, double-click the **Network** icon to display the Network window. Double-click the TCP/IP Protocol entry with the Ethernet adapter being used for this connection to display TCP/IP **Properties**. In the IP address tab, click **Obtain an IP Address Automatically** to obtain a dynamic IP address.

For a static IP address, click **Specify an IP address**. Enter the IP address 10.10.10.2 or any other address in the 10.10.10.0 subnet greater than 10.10.10.1. Enter the subnet 255.255.255.248. You can leave other fields blank. Click **OK**.

Microsoft Windows 2000

From the Control Panel, select **Network and Dialup Connections/Local Area Connections**. Select the Ethernet adapter in the Connect Using field. Select Internet Protocol, and click Properties. Click **Obtain an IP Address Automatically** to obtain a dynamic IP address.

For a static IP address, click **Specify an IP address**. Enter the IP address 10.10.10.2 or any other address in the 10.10.10.0 subnet greater than 10.10.10.1. Enter the subnet 255.255.255.248. You can leave other fields blank. Click **OK**.

Microsoft Windows XP

Click **Start**, select **Settings**, **Network Connections**, and then select the LAN connection you will use. Click **Properties**, select **Internet Protocol TCP/IP**, and click the **Properties** button. Click **Obtain an IP Address Automatically** to obtain a dynamic IP address.

For a static IP address, click **Specify an IP address**. Enter the IP address 10.10.10.2 or any other address in the 10.10.10.0 subnet greater than 10.10.10.1. Enter the subnet 255.255.255.248. You can leave other fields blank. Click **OK**.

Feature Not Available

This window appears when the feature you are attempting to configure is not available. This may occur when the IOS image or the router hardware does not support the feature.

INDEX

L

M

N

P

R

S

T

U