CHAPTER 1

Cisco CP Express Wizard

These help topics introduce Cisco Configuration Professional Express (Cisco CP Express) wizard, describe the configurations you can perform with it, and explain the information required in each Cisco CP Express screen.

This chapter contains the following sections:

- Getting Started with Cisco CP Express
- Giving the Router a Basic Configuration
- Provisioning the Router
- Configuring the Wireless Interface
- Configuring the LAN Interface
- Configuring a Wireless Access Point
- Configuring a Wide Area Network Interface
- NAT, page 1-20
- Configuring a Firewall
- Configuring Security Settings
- Summary
- Wireless Network/Teleworker Support
- Supplementary Help

Getting Started with Cisco CP Express

The Cisco CP Express windows guide you through initial configuration of the router. With Cisco CP Express, you can provide the following configurations for the router:

- Local Area Network (LAN) configuration.
- DHCP Server Configuration
- Wide Area Network (WAN)
- Firewall
- Security Settings.
- Router Provisioning

After you complete the Cisco CP Express wizard and deliver the configuration to the router, you can continue to use Cisco CP Express to modify the configuration if that is necessary.

Cisco CP Express Interface

Cisco CP Express has three types of windows:

- The Overview screen—This window provides a snapshot of basic router information, enabling you to verify information at a glance without that you enter a configuration screen.
- Wizard screens—The first time that you run Cisco CP Express, you use the wizard screens. These screens guide you through the essential parts of the router configuration so that the router can start functioning on the network. Firewall, and security settings are included so that the router and the LAN that it serves are secure. The left pane of each screen shows you which part of the configuration you are completing. The right pane contains the configuration fields. If you need more information on a screen, just click the question mark (?) icon at the top of the screen.
- Edit screens—After you have completed initial configuration, you can return to Cisco CP Express to modify the router configuration if you need to do so.

Cisco CP Express and CCP

Cisco CP Express allows you to provide the router with the configuration essentials so that it can start working on the network.
Cisco Configuration Professional (Cisco CP) allows you to perform more advanced configurations on the router, such as Virtual Private Network (VPN) configurations, Intrusion Prevention System (IPS) configurations, and Network If Cisco CP is installed on the PC, you can start it on the PC and then provide the IP address of the router that you want to configure.

Screen Reference

The following topics describe the screens and dialog boxes that you use when viewing router information and getting started with Cisco CP Express:

- Welcome
- Overview

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 CP 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 CP. See Cisco Configuration Professional for more information.

Giving the Router a Basic Configuration

A basic configuration gives the router a name, creates a user account with a password, and creates the enable secret password. See the following section for more information.

- Basic Configuration Reference

Basic Configuration Reference

The following topic describes the Basic Configuration screen.

- Basic Configuration

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 CP Express, Cisco Configuration Professional (Cisco CP), and the CLI.

Hostname

Enter the name you want to give the router.

Domain Name

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

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

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

Username

Enter a username.

Enter New Password

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

Reenter New Password

Reenter the new password for confirmation.

Enable Secret Password

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.

Provisioning the Router

You can use Cisco CP Express to retrieve a configuration file from a network server, or from a USB flash device or token and load it in router memory.

The following topics describe the Cisco CP Express provisioning screens:

- Router Provisioning
- Provision From USB Token
- Provision From USB Flash
- File Selection
- CNS Server Information

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.

Cisco CP Express

Choose this option to use Cisco CP 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 CP 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 CP 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 CP 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/docs/ios/12_3t/12_3t14/feature/guide/gtadintr.html

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 CP 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 CP 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 CP 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 CP 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.

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 CP Express can retrieve configuration information for your router.

Enter the CNS Server IP Address /Hostname

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

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

Enter the CNS Password

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

Primary DNS

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

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.

Configuring the Wireless Interface

Cisco CP Express enables you to bridge the router wireless interface with a router LAN interface. Additionally, you can launch the Wireless Management application from Cisco CP Express.

The following topic describes the Wireless Interface Configuration screen:

- Wireless Interface Configuration

Wireless Interface Configuration

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

Configuring the LAN Interface

The Cisco CP Express wizard enables you to configure a LAN interface with an IP address, configure it as a DHCP server, and specify the IP address range that the DHCP server will use.

The following topics describe the LAN interface screens:

- LAN Interface Configuration
- DHCP Server Configuration

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 CP Express wizard, you can do so by starting Cisco CP 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

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 CP Express wizard and restart the router, use this address to run Cisco CP Express. Do not use the address that was provided in the Quick Start Guide for the router.

Subnet Mask

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

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

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 CP 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 CP 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

Cisco CP 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 CP Express displays a message informing you that the address is invalid.

Ending IP Address

Cisco CP 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 CP Express displays a message informing you that the address is invalid.

Domain Name

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

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

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 CP Express Buttons for more information.

Configuring a Wireless Access Point

If a wireless access point has been installed in the router, you can use the Cisco CP Express wizard to configure it. Cisco CP Express discovers the access point hardware and displays the appropriate configuration screens.

The wireless access point configuration screens are described in the following topics:

- Autonomous Wireless Configuration
- Wireless-LWAPP Host Router Configuration

Autonomous Wireless Configuration

If an image that supports autonomous wireless configuration is installed on the router access-point controller, Cisco CP Express displays the Autonomous Wireless Configuration screen.

Field Reference

Table 1-1 Autonomous Wireless Configuration

Element	Description
Autonomous Wireless Configuration	To configure the wireless access point controller to operate in autonomous mode, check **Autonomous Wireless Configuration**. **Note** This field appears when you are using the Cisco CP Express wizard.
Hostname	Enter a hostname for the access point controller. For example, 800-accesspoint.
Password and Confirm	Enter the password that you want to configure for the access point controller, and then reenter it to confirm it accuracy.
Static IP Address Fields	When you choose Static IP Address from the IP Address list, the IP Address and Subnet Mask fields are displayed.

Table 1-1 Autonomous Wireless Configuration (continued)

Element	Description
IP Address	Enter the IP address that you want to give the access point controller BVI interface. The IP address must be valid for the subnet mask used. For example, if the network address is 192.168.0.0 and the subnet mask is 255.255.255.248 the IP address must be in the range from 192.168.0.1 to 192.168.0.6.
Subnet Mask and Subnet Bits	To specify the subnet mask to use, either enter the mask in the Subnet Mask, or choose the number of subnet bits in the Subnet Bits field. If you choose subnet bits, Cisco CP Express enters the mask automatically. For example, if you choose 29 in the Subnet Bits field, Cisco CP Express enters 255.255.255.248 in the Subnet Mask field.
Dynamic IP Address Fields	When you choose Dynamic IP Address in the IP Address list, the Hostname field is displayed.
Hostname	If the Internet Service Provider (ISP) has provided a name for the DHCP server, enter it in the Hostname field.
No IP Address	When you choose No IP Address in the IP Address list, no IP address is configured on the router interface, and no fields are displayed in the IP Address box.
SSID and Encryption Fields	When no configured SSID is discovered in the controller configuration, the SSID and Encryption fields are displayed.
SSID	The service set identifier (SSID) - also called the radio SSID - is a unique identifier that clients use to associate with the access point radio. The SSID can be any alphanumeric, case-sensitive entry from 2 to 32 characters. Enter the SSID in this field.

Table 1-1 Autonomous Wireless Configuration (continued)

Element	Description
Encryption	Choose the type of encryption that you want to use for connections to the access point. The following encryption types are supported: • WEP—WEP (Wired Equivalent Privacy) is an 802.11 standard encryption algorithm originally designed to provide with a level of privacy experienced on a wired LAN. The standard defines WEP base keys of size 40 bits or 104 bits. • WPA—Wi-Fi Protected Access (WPA) permits wireless access to users authenticated against a database through the services of an authentication server, then encrypts their IP traffic with stronger algorithms than those used in WEP.
Key	Enter the key that the access point is to use for encryption.
Note	You can perform additional configuration of the access point by launching the access point application from this screen.
For advanced configuration of the internal access point, click on the link to launch the internal access point application.	To launch the internal access point application, click on the link showing the access point IP address. This application allows you to perform additional configuration tasks. If you need more information on the advanced configuration of the internal access point, refer to the *Cisco 860 and Cisco 880 Series Integrated Services Router Software Configuration Guide*. This guide is available at the following link: http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/860-880-890SCG.html

Wireless-LWAPP Host Router Configuration

If a Cisco IOS image that supports autonomous wireless Lightweight Access Point Protocol configuration is installed on the router access-point controller, Cisco CP Express displays the Wireless-LWAPP Configuration screen.

Note If you need to perform advanced configuration of the internal access point, you must use the Wireless LAN Controller management application associated with the controller.

Field Reference

Table 1-2 Wireless-LWAPP Host Router

Element	Description
Wireless-LWAPP Host Router Configuration	To configure the WLAN controller IP address to the router DHCP server, check **Wireless-LWAPP Host Router Configuration**.
Controller IP Address	Enter the IP address of the wireless LAN controller that is to receive the DHCP offer.
Note: For advanced configuration of the internal access point.....	Cisco CP Express allows you to perform the configuration tasks covered in this screen. To perform additional configuration of the access point, use the associated wireless management application, using the instructions provided.

Configuring a Wide Area Network Interface

Cisco CP Express allows you to configure one Wide Area Network (WAN) interface. If the router has more than one WAN interface, you can choose the interface to configure. Cisco CP Express supports the configuration of a variety of WAN interfaces.

For more information, see WAN Reference.

WAN Reference

- Configuring a Firewall
- WAN Interface Selection
- Internet (WAN): Ethernet Interface
- Internet (WAN): Autodetect Encapsulation
- Internet (WAN): User Specified Encapsulation
- Serial Connection
- Frame Relay Configuration Settings
- Internet (WAN): Advanced Options
- Internet (WAN): Cable Modem
- Add Cable Modem Connection
- Authentication

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 Cisco CP Express edit-mode, this window appears when Cisco CP Express is not able to help you configure NAT. Cisco CP 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 CP Express Buttons for more information**.**

WAN Interface Selection

Cisco CP 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 CP, 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 CP 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 CP 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

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 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

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 CP Express Buttons for more information**.**

Internet (WAN): Autodetect Encapsulation

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

If Cisco CP 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 CP 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 CP 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 CP 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 CP 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

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

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

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

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.

Enable Multilink PPP

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

Authentication 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

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

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

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 CP 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

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

Make these settings to configure a Frame Relay connection.

DLCI

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

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

LMI Type

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

ANSI 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 click **Use This Interface as the Forwarding Interface**, the router will send all such traffic to the WAN interface you are configuring. If you click **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.

Internet (WAN): Cable Modem

This screen allows you to configure a cable modem interface on the router. Cisco CP Express provides default cable modem configuration settings and configures the interface as a DHCP client that will receive an IP address from a DHCP Server.

Check **This wizard will configure a dynamic IP address (DHCP client) on the selected cable modem interface** to configure the cable modem interface as a DHCP client.

Add Cable Modem Connection

Cisco CP Express displays this message screen when you choose to configure a cable modem interface. It informs you that it will configure the interface as a DHCP client. A WAN interface configured as a DHCP client must obtain an IP address from a DHCP server provided by an ISP or by your organization.

Field Reference

Table 1-3 Cable Modem Configuration Message Buttons

Element	Description
OK	To allow Cisco CP Express to configure the cable modem interface with default settings, and to configure it as a DHCP client that will obtain a dynamic IP address from a DHCP server, click **OK**.
Cancel	If you do not want to configure the interface with the settings that Cisco CP Express uses, click **Cancel**

Authentication

This page is displayed if you enabled or are configuring:

- Point-to-Point Protocol (PPP) for a serial connection
- Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Protocol over ATM (PPPoA) encapsulation for an ATM connection
- PPPoE or PPPoA encapsulation for an Ethernet connection
- An ISDN BRI or analog modem connection

Your service provider or network administrator may use a Challenge Handshake Authentication Protocol (CHAP) password or a Password Authentication Protocol (PAP) password to secure the connection between the devices. This password secures both incoming and outgoing access.

Field Reference

Table 1-4 Authentication Screen

Element	Description
Authentication Type	Check the box for the type of authentication used by your service provider. If you do not know which type your service provider uses, you can check both boxes: the router will attempt both types of authentication, and one attempt will succeed. CHAP authentication is more secure than PAP authentication.
Username	The username is given to you by your Internet service provider or network administrator and is used as the username for CHAP or PAP authentication.
Password	Enter the password exactly as given to you by your service provider. Passwords are case sensitive. For example, the password cisco is not the same as Cisco.
Confirm Password	Reenter the same password that you entered in the previous box.

Configuring a Firewall

Cisco CP Express allows you to configure a firewall that uses default settings if you have configured a WAN interface on the router.

Note The Cisco IOS image on the router must support the Firewall feature set in order for you to be able to configure a firewall with Cisco CP Express.

The firewall protects your network in the following ways:

- Applies default access rules to inside and outside interfaces.
- Applies default inspection rules to outside interface—Cisco CP Express creates and applies a list of default inspection rules.
- Enables IP Unicast Reverse-Path Forwarding (RPF) on the outside interface.

If you choose to let the Cisco CP Express configure the firewall, you can modify the firewall configuration later using Cisco CP. If you choose not to have a firewall configured, you can configure one later using Cisco CP Express or Cisco CP.

The topic Firewall Configuration describes the screen.

Firewall Configuration

The Firewall Configuration window gives you the option of letting Cisco CP Express configure a firewall on your WAN and LAN interfaces. You can apply a firewall during initial setup.

If you let Cisco CP Express configure the firewall, you can modify the firewall configuration later using the Cisco CP 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 CP 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 CP 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 CP Express configure the firewall, you can modify the firewall configuration later using Cisco CP. If you choose not to have a firewall configured, you can configure one later using Cisco CP Express or Cisco CP. For more information, click Cisco Configuration Professional.

Configuring Security Settings

Some configuration settings that may compromise router and network security are enabled by default because they offer useful services. For example Cisco Discovery Protocol (CDP) enables an administrator to easily view information about neighboring routers on the network. However, CDP can be a security risk if the information that it provides gets into the wrong hands. Cisco CP Express lists common settings that pose security risks and allows you to disable them of you want to do so to secure the router and the network.

There are also settings, like TCP Syn Wait time, and logging that are disabled by default but that can protect the network against attacks and aid in troubleshooting when they are enabled. Cisco CP Express lists these settings and lets you choose whether to enable them or not.

The Security Setting screen is described in the following topic:

- Security Settings

The topics listed in the sections that follow describe the security settings that you can make in this screen.

Security Risks

These topics describe the settings that can be made to reduce general security risks:

- 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

Enhanced Security for the Router and the Network

These topics describe the settings that can be made to enhance security for the router and the network:

- 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

Enhanced Security for Router Access

These topics describe the settings that can be made to enhance security for router access:

- 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

Password Encryption

These topics describe the settings that can be made to enable encryption of passwords:

- Enable Password Encryption Service.

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 CP Express makes.

You can use Cisco CP 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 CP. For more information, click Cisco Configuration Professional.

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 CP 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.

Wireless Network/Teleworker Support

For information about how to use Cisco CP Express to configure the Teleworker Support feature, see the screencast at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional_express/scrcst/screencast/ccp_express_sc.html

Note You must have internet access to view the screencast.

Supplementary Help

The following help topics provide additional information.

- Cisco Configuration Professional
- Cisco Network Services
- Security Settings
- Cisco CP Express Buttons
- Reconnecting to the Router After Initial Configuration
- Testing Your WAN (Internet) Connection
- SDP Troubleshooting Tips

Cisco Configuration Professional

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

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

To start Cisco CP, click **CCP** 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 CP 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 CP 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 CP Express does not support. Cisco CP Express must be able to configure a WAN interface in order for the router to obtain the Cisco Network Services configuration file. If Cisco CP 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 CP Express. Then, install a WAN interface card supported by Cisco CP Express, restart Cisco CP Express, and select **CNS Server** (Cisco Network Services server) in the Startup wizard.

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

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

- You did not select this option, and configured a LAN and a WAN interface using Cisco CP 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 CP Express. Then restart Cisco CP Express and select **CNS Server** in the Router Provisioning window.

Security Settings

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

Disable SNMP

Cisco CP 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 CP 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 CP 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 Cisco CP Security Audit feature. To learn how, For more information, click Cisco Configuration Professional.

Disable PAD Service

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Disable TCP Small Servers Service

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Disable UDP Small Servers Service

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Disable IP BOOTP Server Service

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Disable IP Identification Service

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Disable CDP

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Disable IP Source Route

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Enable Password Encryption Service

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Enable Netflow Switching

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Enable TCP Keepalives for Inbound Telnet Sessions

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Enable TCP Keepalives for Outbound Telnet Sessions

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Enable Sequence Numbers and Time Stamps on Debugs

Cisco CP 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 CP 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 CP 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 CP 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 CP 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 CP 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 CP Express:

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

Enable Unicast RPF on Outside Interfaces

Cisco CP 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 CP Express will check the router configuration to see if IP Cisco Express Forwarding is enabled. If IP Cisco Express Forwarding is not enabled, Cisco CP 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 CP 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 CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Disable IP Redirects

Cisco CP 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 CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Disable IP Directed Broadcast

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Disable MOP Service

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Disable IP Unreachables

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Disable IP Mask Reply

Cisco CP 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 CP Security Audit feature. To learn how, see the Security Audit online help in Cisco CP. For more information, click Cisco Configuration Professional.

Set Minimum Password Length to Less Than 6 Characters

Cisco CP 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 CP 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 CP 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 CP 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 CP 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 CP 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 CP Express Buttons

Help Button

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

About Button

Clicking **About** displays a window containing Cisco CP 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 CP Express

Exit Button

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

Refresh Button

Visible if you are editing an initial configuration. Click **Refresh** to refresh the router data in Cisco CP 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 CP 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 CP to troubleshoot the connection by doing the following:

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

Step 2 Log in to Cisco CP 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 CP 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 SDP application is invoked.

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

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtadintr.html