Installing Cisco Business Communications Solution Verfied Designs

Cisco IPC Express Software Release 1.5.7
September 2005

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-8181-01

Installing Cisco Business Communications Solution Verified Designs

CONTENTS

Introduction

This guide describes installing Cisco Business Communications Solution Verified Designs (BCS Verified Designs) using Cisco IP Communications (IPC) Express Quick Configuration Tool (QCT).

QCT is a GUI application provided for Cisco partners and resellers. You can use QCT to configure all Cisco CallManager Express (CME) supported platforms to enable the simple configuration of a basic telephony system that is typically less than 50 IP phones. In addition, QCT recognizes any Advanced Integrated Module (AIM) or network modules with Cisco Unity Express (CUE), thus providing voice-mail and Auto Attendant (AA) capability to the Cisco CME system.

QCT generates a complete telephony configuration file, which can be automatically downloaded to the Cisco router that support Cisco CME and Cisco CUE.

This guide also includes procedures for continuing the installation of Cisco BCS Verified Designs using the Cisco command-line interface (CLI).

Finally, this guide includes a procedure for adding security to the voice network using Cisco Security Device Manager.

Contents

This chapter contains the following sections:

Documentation Organization

This document includes the following sections:

Table 1 Document Organization

Title	Description
Introduction	High-level description of Cisco BCS Verified Designs procedures and concepts. Includes hardware and software prerequisites as well as download prerequisites.
Installing Required Software	Basic steps to download and install the software required to install Cisco BCS Verified Designs.
Configuring Cisco Business Communications Solution Verified Designs	Step-by-step procedures for using Cisco IPC Express QCT to configure Cisco BCS Verified Designs.
Continuing the Cisco BCS Verified Designs Configuration Using CLI	Step-by-step procedures for using the Command Line Interface (CLI) to create subinterfaces for voice and data, configure DHCP IP addressing pool for the data network, and configure separate VLANs for data and voice.
Configuring Security on the Voice Network	Step-by-step procedures for using Cisco Security Device Manager to configure security on the voice network.
Appendix A: Cisco CallManager Express Bundles	Special configurations for Cisco BCS Verified Designs.
Appendix B: QCT Utilities	Features that allow the uploading of previously saved configuration files; an installation and debug log; and serial port communications selec-tion.
Appendix C: Cisco BCS Verified Designs Configuration Example	A sample Cisco BCS Verified Designs configura-tion.

Required Steps to Install Cisco BCS Verified Designs

Follow these required steps to install Cisco BCS Verified Designs.

Step 1 Use Cisco IPC Express QCT to enter the system and phone parameter information listed on the Cisco BCS Planning Worksheet. (Refer to Configuring Cisco Business Communications Solution Verified Designs, page 17.)

Step 2 Continue the Cisco BCS Verified Designs installation by creating subinterfaces for VLANs, a DHCP IP addressing pool for the data network, and separate data and voice VLANs using CLI. (Refer to Continuing the Cisco BCS Verified Designs Configuration Using CLI, page 57.)

Step 3 Add security to the voice network using Cisco Security Device Manager. (Refer to Configuring Security on the Voice Network, page 71.)

Prerequisites

This section describes prerequisites for using QCT with Cisco BCS Verified Designs.

Required PC Setup

On some PCs, it might be necessary to change Internet options that prevent the appearance of pop-ups and change a security setting to allow active content to run files on the PC.

If necessary, choose **Internet Options** under the Tools menu on your browser. Under *Privacy*, remove any check in the *Block Pop-ups* check box. Under *Advanced/Security*, choose **Allow Active Content to Run Files on My Computer**.

Cisco Business Communications Solution Verified Designs Planning Worksheet

Use the *Cisco Business Communications Solution Verified Designs Planning Worksheet* to collect the necessary information from network administrators before installing Cisco BCS Verified Designs.

Hardware Requirements

Cisco BCS Verified Designs deploy based on Cisco ISR platforms, which include both the Cisco 2800 and the Cisco 3800 product families.

Cisco routers are normally shipped with Cisco voice services hardware and other optional equipment that you ordered already installed. To install any Cisco router or optional voice services hardware, see “Related Documents” section on page 6.

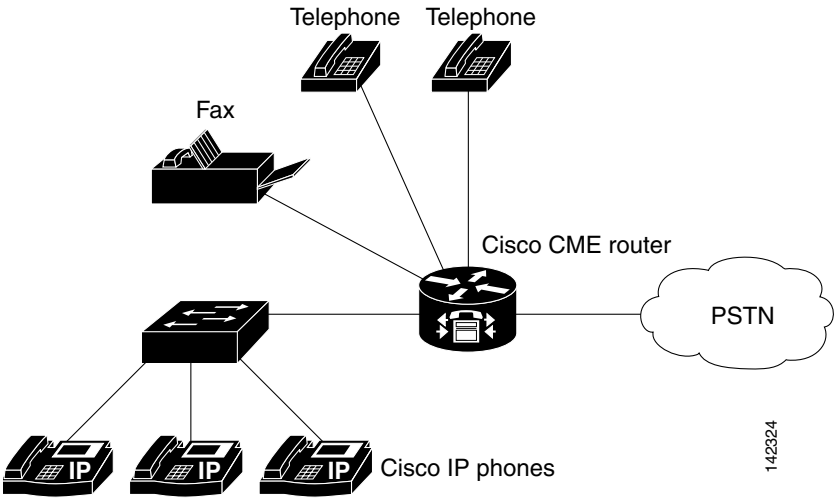
Console Port Connection

Cisco IPC Express QCT requires the use of a console cable to connect the serial port on your PC to the router's console port. If you need assistance in connecting your PC to your router's console port, see your router's installation and upgrade guide.

Hardware Configuration

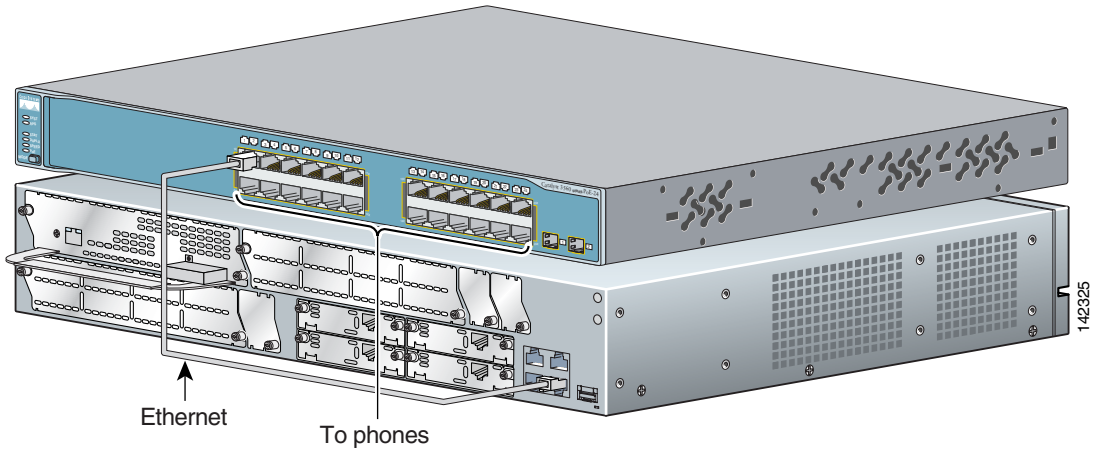
Figure 1 shows a typical deployment of a Cisco BCS Verified Designs system with several Cisco IP phones connected to it. The Cisco CME router is connected to the PSTN.

Figure 1 Cisco BCS Verified Designs System



This guide assumes the Cisco BCS Verified Designs IP network is installed and operational. Figure 2 shows a typical Cisco BCS Verified Designs hardware connection for the router and switch.

Figure 2 Cisco BCS Verified Designs Hardware Configuration (Typical)



Software Requirements

The Cisco router should be preloaded with the latest Cisco IOS, Cisco CME basic, and Cisco CME GUI software versions. In the event that the appropriate software versions are not installed, you will be required to download and extract the required software images and files.

Software Version

Cisco BCS Verified Designs was tested and installed using Cisco IOS Version 12.3(11)T6.

Cisco IPC Express Quick Configuration Tool

Download Cisco IPC Express QCT to your PC before installing Cisco BCS Verified Designs (refer to Installing Cisco IPC Express QCT, page 7).

Cisco Security Device Manager

Download Cisco Security Device Manager (Cisco SDM) to your PC before installing Cisco BCS Verified Designs (see Installing Cisco Security Device Manager, page 12). You must also download the Advanced IP Services software for firewall configuration. Table 2 lists the required Advanced IP Services software package for Cisco ISR router types.

Table 2 Cisco Advanced IP Services Software

Cisco ISR Router Type	Advanced IP Services Software
Cisco 2801	S280UAISK9-12311T
Cisco 2811 through Cisco 2851	S28NUAISK9-12311T
Cisco 3825	S382UAISK9-12311T
Cisco 3845	S384UAISK9-12311T

Related Documents

Table 3 provides useful links to help ensure that your routers, switches, network module and AIM cards, IP phones, and cables are properly installed.

Table 3 Related Documents

Related Topic	Document Title
Planning worksheet	*Cisco Business Communications Solution Verified Designs Planning Worksheet*
Installing AIM Voice or CUE modules	*Installing Advanced Integration Modules in Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers*
Installing AIM	*AIM Installation Quick Start Guide*
Installing internal modules	*Installing and Upgrading Internal Modules in Cisco 2800 Series Routers*
Cisco CME and Cisco CUE	*Cisco CallManager Express 3.2 System Administrator's Guide*
Cisco IOS Release 12.3(11)T software	*Cisco IOS Software Releases 12.3T*

What to Do Next

You are now ready to download the required software to install Cisco BCS Verified Designs (see the "Installing Required Software" chapter).

Installing Required Software

This chapter describes procedures to download and install the required software for installing Cisco BCS Verified Designs. Download all software to your PC *before* configuring Cisco BCS Verified Designs.

Contents

This chapter contains the following sections:

Installing Cisco IPC Express QCT

Perform the following steps to install Cisco IPC Express QCT on your PC.

Note Before installing Cisco IPC Express QCT, make sure that you are a member of the Administrators group under Control Panel > User Account settings.

Note This installation procedure assumes the use of Windows XP. If you are using another Windows operating system, your display may differ slightly.

Step 1 Download the Cisco IPC Express QCT 1.5.7*x*.zip file from the following location:

http://www.cisco.com/cgi-bin/tablebuild.pl/cme-qct

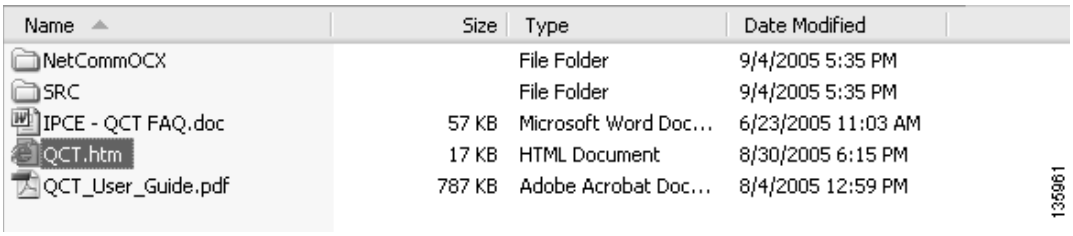
Note You must have a valid Cisco CCO account to download Cisco IPC Express QCT.

Note Cisco IPC Express QCT is supported only under Windows Internet Explorer version 5.5 or later.

Step 2 Unzip and extract the files into an existing folder on your PC.

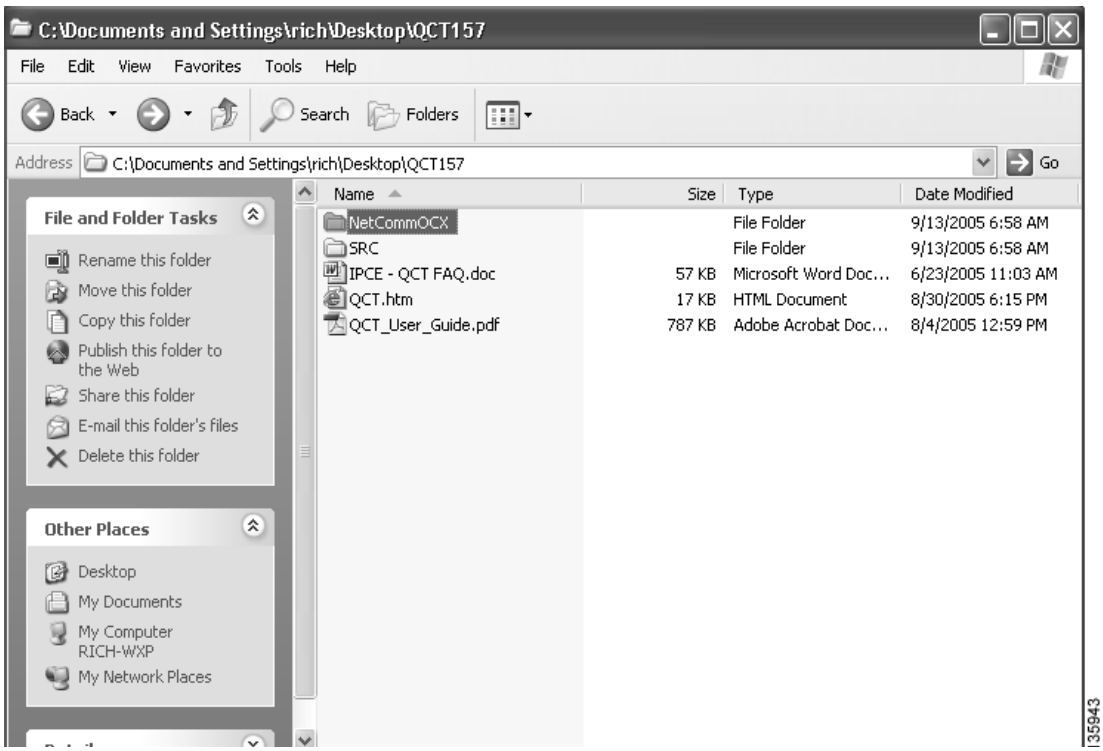
Files will automatically install into your specified folder location, creating a number of subfolders (see Figure 3):

Figure 3 Cisco IPC Express QCT Extracted Files



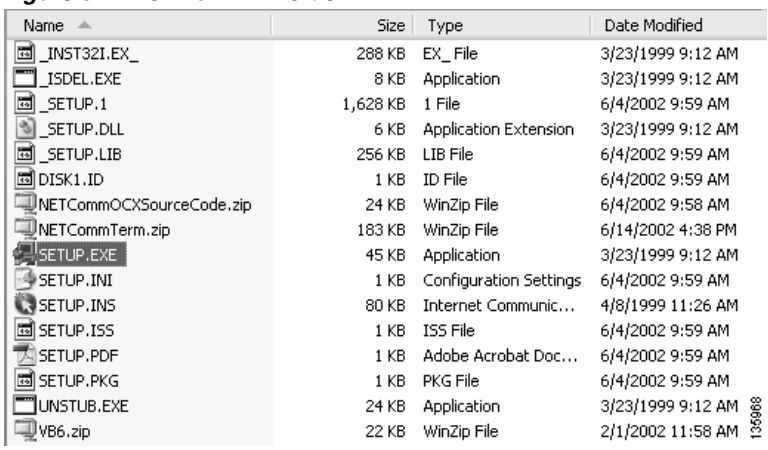
Step 3 Open the Cisco IPC Express QCT subfolder NetCommOCX (see Figure 4).

Figure 4 QCT NetCommOCX Folder



Step 4 Click **SETUP.EXE** to install the necessary serial communications drivers (see Figure 5).

Figure 5 SETUP.EXE folder

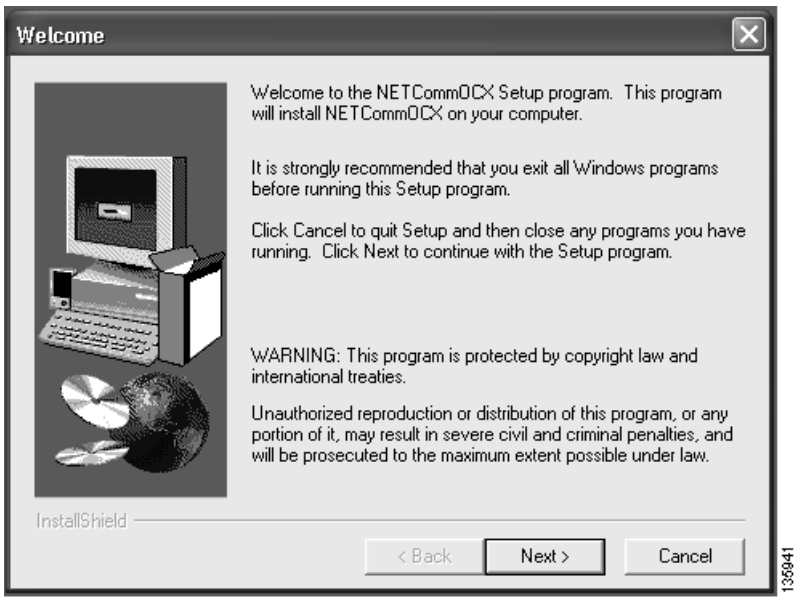


Name	Size	Type	Date Modified
INST32I.EX	288 KB	EX_ File	3/23/1999 9:12 AM
_ISDEL.EXE	8 KB	Application	3/23/1999 9:12 AM
_SETUP.1	1,628 KB	1 File	6/4/2002 9:59 AM
_SETUP.DLL	6 KB	Application Extension	3/23/1999 9:12 AM
_SETUP.LIB	256 KB	LIB File	6/4/2002 9:59 AM
DISK1.ID	1 KB	ID File	6/4/2002 9:59 AM
NETCommOCXSourceCode.zip	24 KB	WinZip File	6/4/2002 9:58 AM
NETCommTerm.zip	183 KB	WinZip File	6/14/2002 4:38 PM
SETUP.EXE	45 KB	Application	3/23/1999 9:12 AM
SETUP.INI	1 KB	Configuration Settings	6/4/2002 9:59 AM
SETUP.INS	80 KB	Internet Communic...	4/8/1999 11:26 AM
SETUP.ISS	1 KB	ISS File	6/4/2002 9:59 AM
SETUP.PDF	1 KB	Adobe Acrobat Doc...	6/4/2002 9:59 AM
SETUP.PKG	1 KB	PKG File	6/4/2002 9:59 AM
UNSTUB.EXE	24 KB	Application	3/23/1999 9:12 AM
VB6.zip	22 KB	WinZip File	2/1/2002 11:58 AM

135968

The NetCommOCX Welcome banner appears (see Figure 6).

Figure 6 NetCommOCX SETUP.EXE Welcome Banner

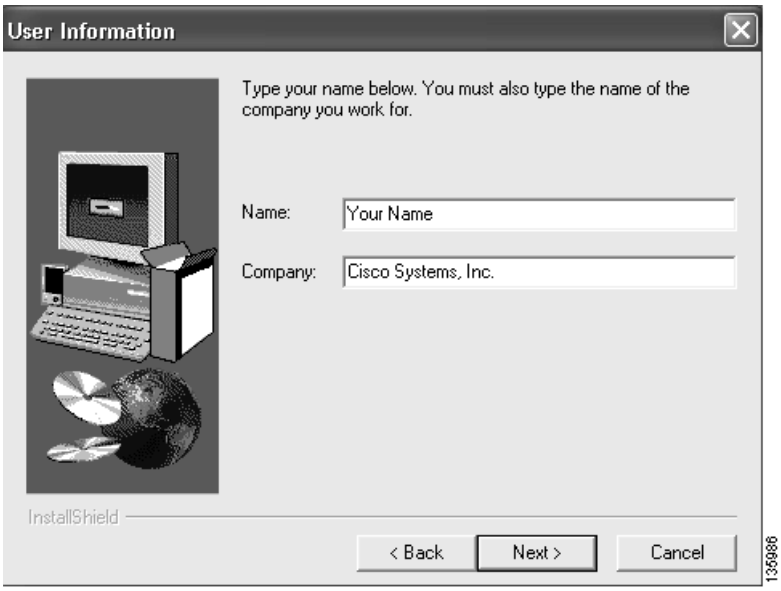


135941

Step 5 Click **Next**.

Step 6 Enter your name and company name in the User Information dialog (see Figure 7).

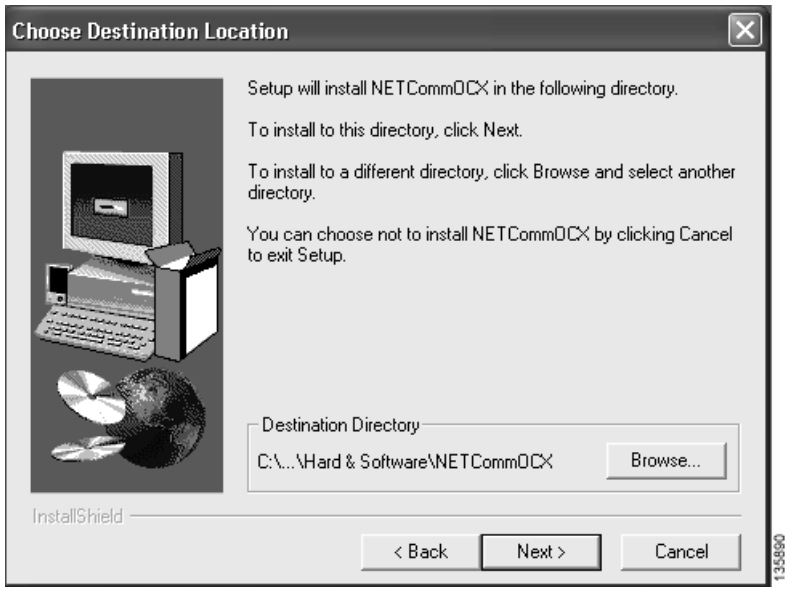
Figure 7 Install User Information Dialog



Step 7 Click **Next**.

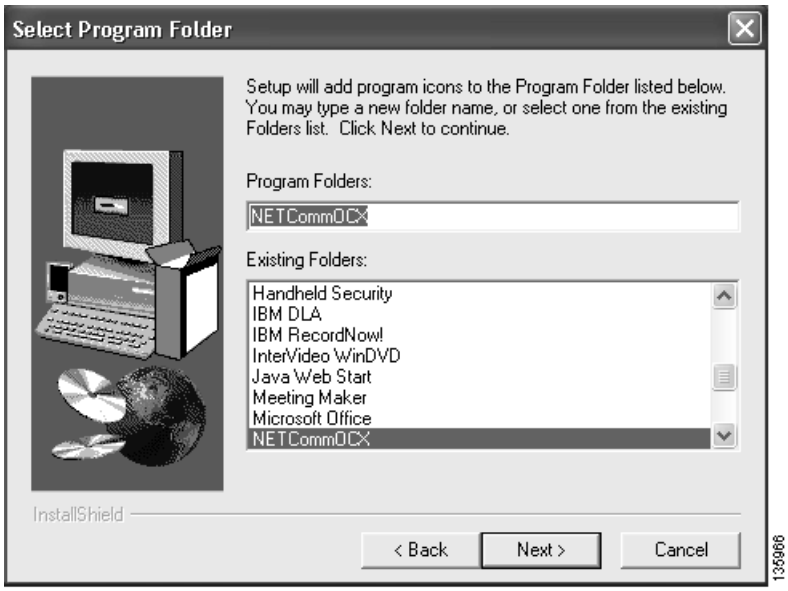
Step 8 Accept the default directory location by clicking **Next**. Or click **Browse** to specify a new destination directory on your PC (see Figure 8).

Figure 8 Install Choose Destination Location Dialog



Step 9 Specify your program folder location by entering a new name in the Program Folders field or highlight an existing folder in the Existing Folders scroll area (see Figure 9).

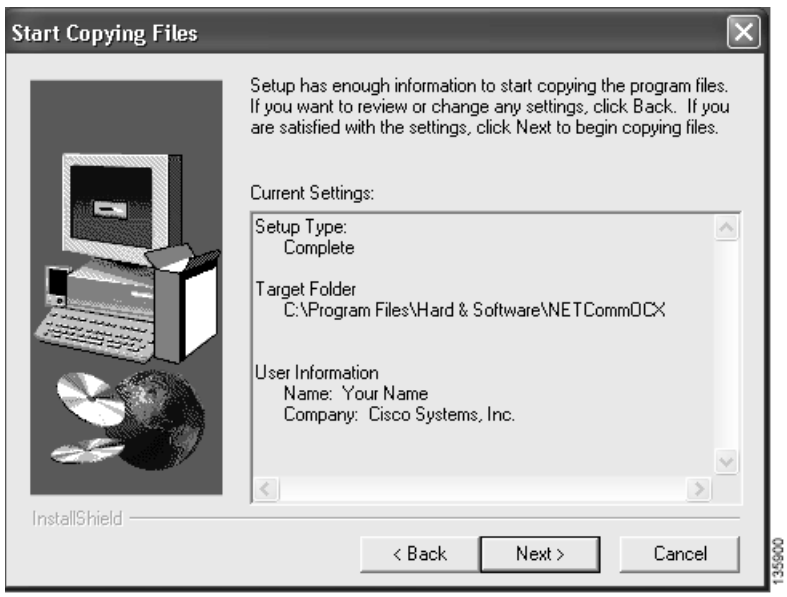
Figure 9 Install Select Program Folder Dialog



Step 10 Click **Next**.

Setup is now ready to begin copying files (see Figure 10).

Figure 10 Start Copying Files Dialog



Step 11 Click **Next**.

Step 12 When setup has completed, click **Finish** (see Figure 11).

Figure 11 Install Setup Complete Dialog

Note Do not use the Yes, Launch the program file checkbox with this release. To launch Cisco IPC Express QCT refer to Launching Cisco IPC Express QCT, page 18.

Installing Cisco Security Device Manager

This section describes the steps necessary for installing Cisco Security Device Manager (Cisco SDM). For complete information on downloading and installing Cisco SDM, see the SDM Downloading and Installing User Guide at:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_installation_guide09186a00803e4727.html

For complete information on using Cisco SDM, see the Cisco Security Device Manager User's Guide at:

http://www.cisco.com/application/pdf/en/us/guest/products/ps5318/c1626/ccmigration_09186a0080458d7f.pdf

Step 1 Download the sdm-v*nn*.zip file at http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm.

Log in using your Cisco.com login user ID and password, and follow the instructions on the Cisco SDM Software page to download the *sdm.vnn.zip* file and the SDM release notes.

Step 2 Double-click the **sdm-v*nn*.zip** file, and extract the files to a directory on your PC.

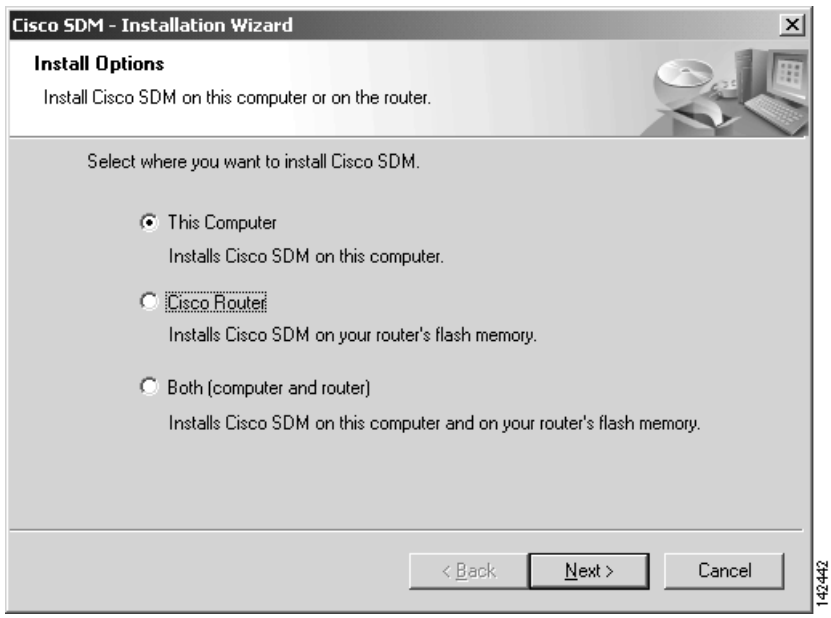
Step 3 In the directory to which you extracted the contents of the sdm-v*nn*.zip file, double-click the **setup.exe** file. The Cisco SDM Welcome dialog appears (see Figure 12):

Figure 12 Cisco SDM Welcome Dialog

Step 4 Click **Next** to display the License screen, accept the license agreement terms, and click **Next** to continue.

Step 5 When the Install Options dialog appears (see Figure 13), specify to install Cisco SDM on your PC (This Computer).

Figure 13 Cisco SDM Install Options Dialog



Step 6 Click **Next**.

After the components are installed, the Cisco SDM Installation Wizard Complete screen appears (see Figure 14):

Figure 14 Cisco SDM Installation Wizard Complete Dialog

Step 7 If you want to start Cisco SDM when you dismiss the wizard, click **Launch Cisco SDM**. Click **Finish** to dismiss the wizard.

What to Do Next

After installing the required Cisco IPC Express QCT and SDM files, you are ready to enter configuration parameters about your system. See “Configuring Cisco Business Communications Solution Verified Designs” chapter.

Configuring Cisco Business Communications Solution Verified Designs

This chapter describes how to enter configuration information for your Cisco BCS Verified Designs system using QCT. Once all the necessary information is entered, QCT generates a configuration file containing all the required CLI commands that you can upload to your router.

Contents

This chapter provides the following sections:

Launching Cisco IPC Express QCT

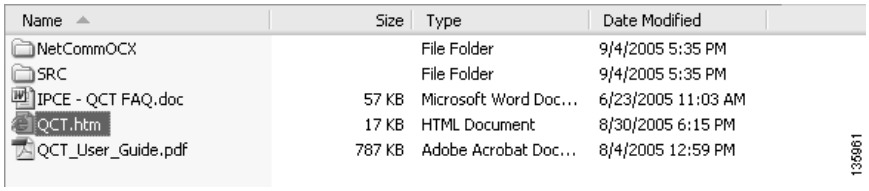
Perform the following steps to launch Cisco IPC Express QCT.

Step 1 Ensure that your PC is connected to the router's console port.

Step 2 Open the directory on your PC in which you installed Cisco IPC Express QCT.

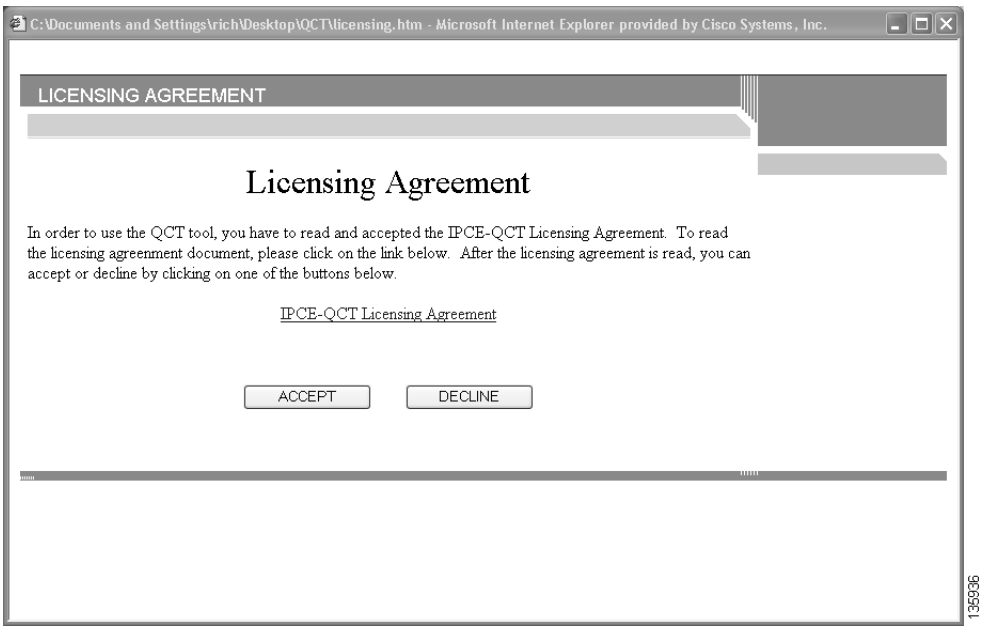
Step 3 Click **QCT.htm** to launch Cisco IPC Express QCT (see Figure 15).

Figure 15 QCT.htm File Location



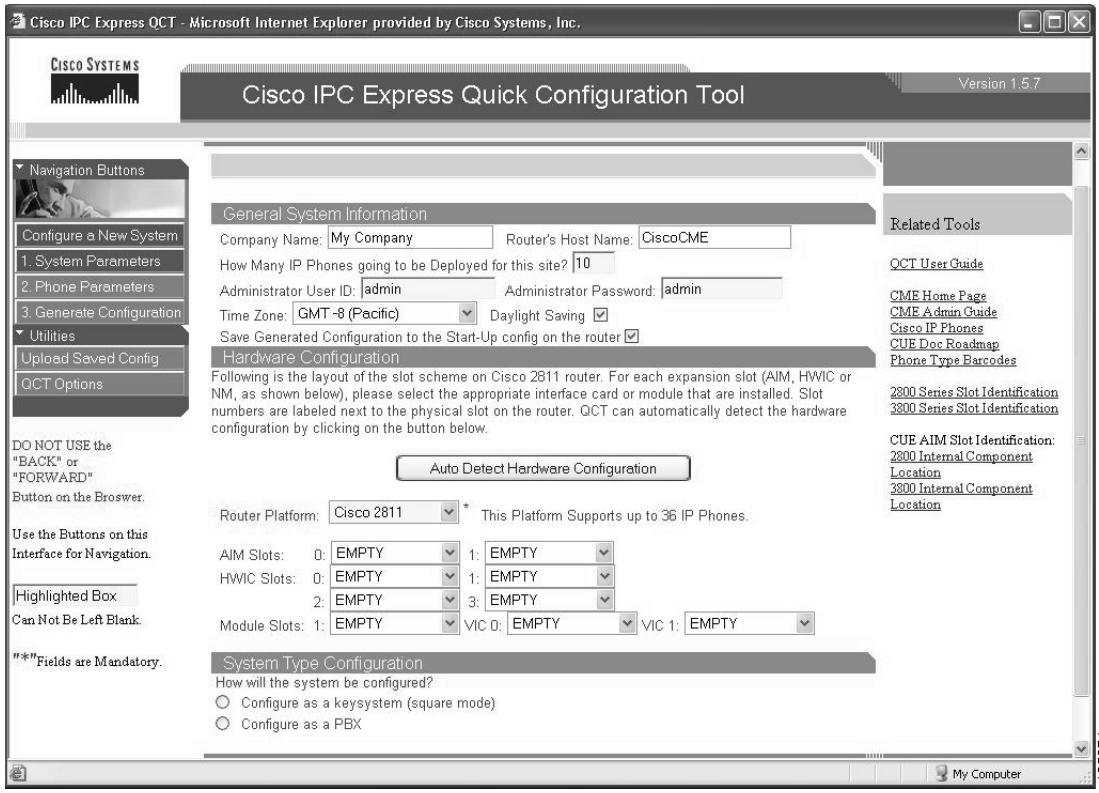
Step 4 Click **Accept** to acknowledge the licensing agreement (see Figure 16).

Figure 16 QCT Licensing Agreement



Cisco IPC Express QCT is now ready to use (see Figure 17).

Figure 17 Cisco IPC Express Quick Configuration Tool Window



Default Values

Cisco IPC Express QCT windows provide recommended, default telephony-service parameters that you can accept to quickly configure your telephony system. Accept these parameters or change any value. These default values may not be appropriate for every system.

Note The installation of Cisco BCS Verified Designs did not use most default values.

Navigating in Cisco IPC Express QCT

Cisco IPC Express QCT provides navigation buttons to move from one configuration window to the next (see Figure 18).

Figure 18 Quick Configuration Tool Navigation Buttons

Configuring System Parameters

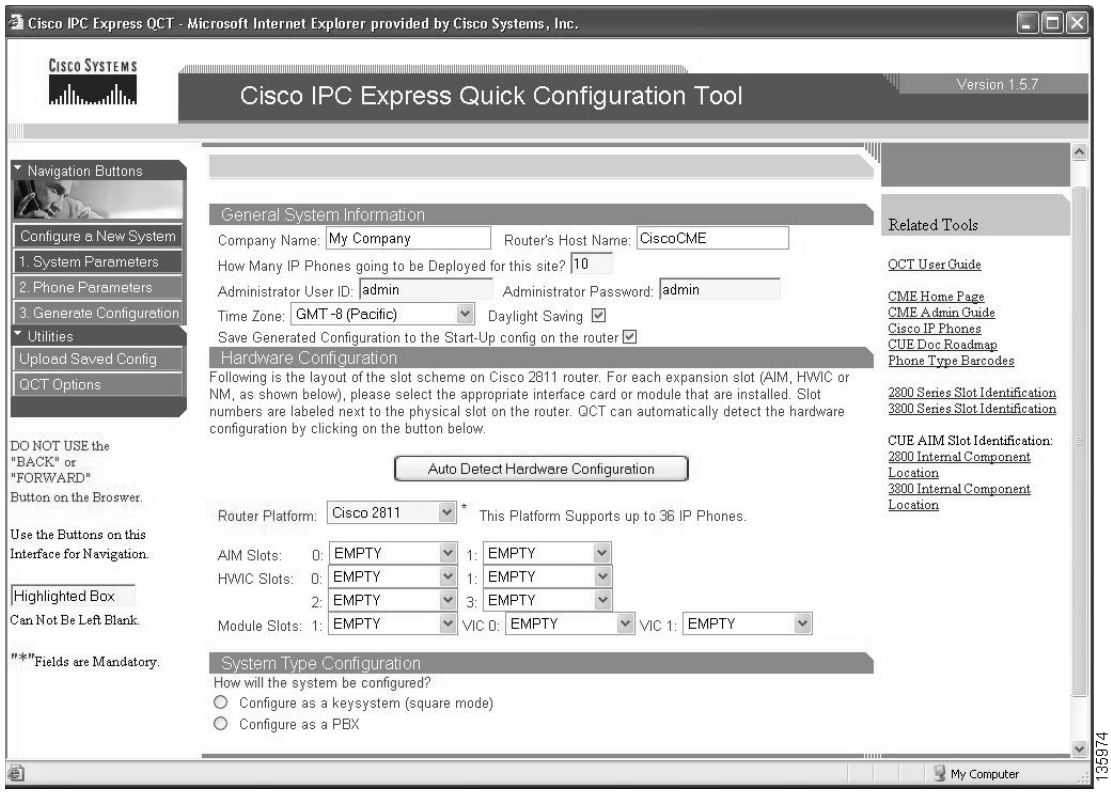
Use the information from your *Cisco Business Communications Solution Verified Designs Planning Worksheet* and perform these steps to enter your information into the System Parameters window.

Step 1 Click **System Parameters** to activate the System Parameters window (see Figure 19):

Figure 19 Systems Parameters Button

The System Parameters window appears (see Figure 20):

Figure 20 System Parameters Window



Configuring General System Information

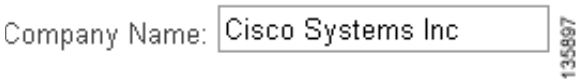
Perform the following steps to enter your general Cisco CME information in the General System Information area of the System Parameters window.

Step 2 Enter the name of your company (see Figure 21):

Figure 21 Company Name Field

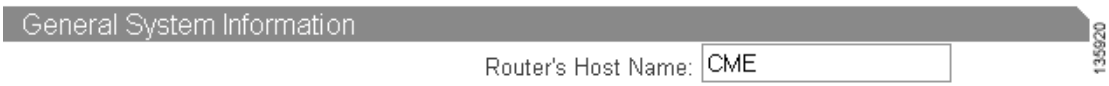
See Figure 22 for an example:

Figure 22 Specifying Company Name (Example)



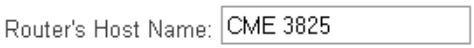
Step 3 Enter your router's host name (see Figure 23):

Figure 23 Router's Host Name Field



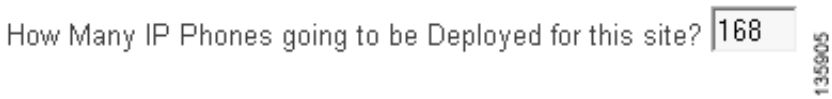
See Figure 24 for an example:

Figure 24 Specifying Router Host Name (Example)



Step 4 Specify the number of IP phones deployed at your site (see Figure 25). This number is dependent on the type of router that you are using. For example, the Cisco 3825 supports up to a maximum of 168 IP phones. The number of IP phones deployed could be less than the maximum supported. To determine the number of IP phones supported by voice-bundled routers, see "Appendix A: Cisco CallManager Express Bundles" section on page 95.

Figure 25 Specifying Number of IP Phones Deployed

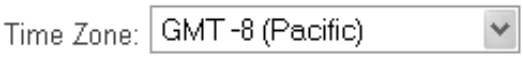


Step 5 Enter your administrator's user ID and password (see Figure 26). Accept the default user ID and password, or enter new values.

Figure 26 Specifying Administrator User ID and Password

Step 6 Specify your time zone from the drop-down menu (see Figure 27):

Figure 27 Specifying Time Zone

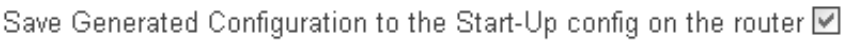


Step 7 If appropriate, check the check box to enable daylight saving (see Figure 28):

Figure 28 Specifying Daylight Saving

Step 8 To save the generated configuration to the start-up configuration on the router, check the following check box (see Figure 29):

Figure 29 Specifying Whether to Save Generated Configuration to Start-Up



This completes the General System Information area of the System Parameters window. Proceed to "Hardware Configuration" section on page 24.

Hardware Configuration

The Hardware Configuration area of the System Parameters window provides a visual layout of your router configuration.

Perform the following steps to detect your Cisco CME hardware configuration in the Hardware Configuration area of the System Parameters window.

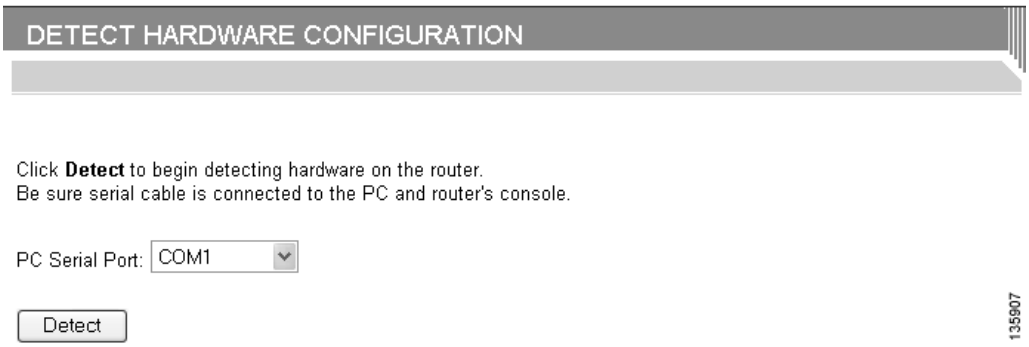
Step 9 Ensure tht your router is powered on and has been running at least five minutes.

Step 10 Click **Auto Detect Hardware Configuration** (see Figure 30):

Figure 30 Auto Detect Hardware Configuration Button

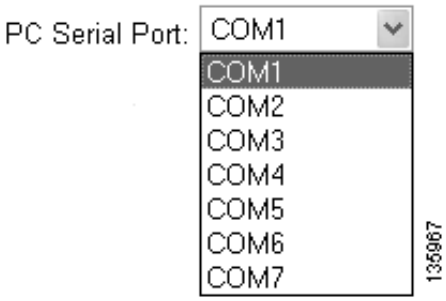
The Detect Hardware Configuration window appears (see Figure 31):

Figure 31 Detect Hardware Configuration Windown



Step 11 Connect a console cable from the PC's serial port to the router's console port and specify from the drop-down menu which PC serial port is being used (see Figure 32):

Figure 32 Specifying PC COM Port

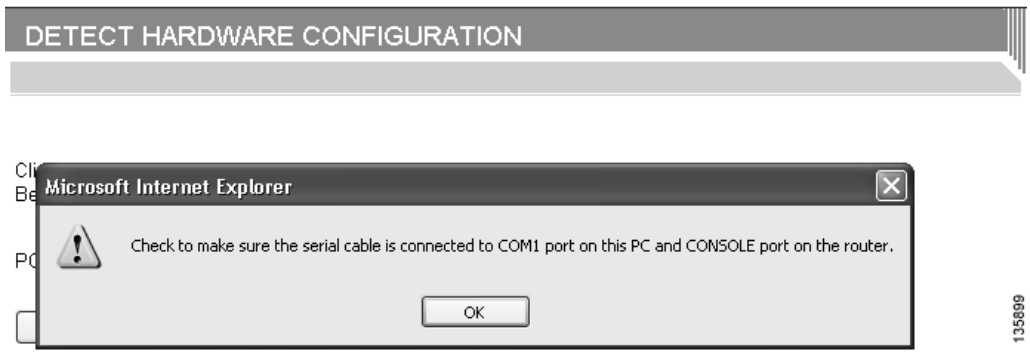


Step 12 Press **Detect** (see Figure 33):

Figure 33 Detect Button

Step 13 Confirm that your serial cable is properly connected by clicking **OK** in the confirmation dialog box (see Figure 34):

Figure 34 COM Port Confirmation

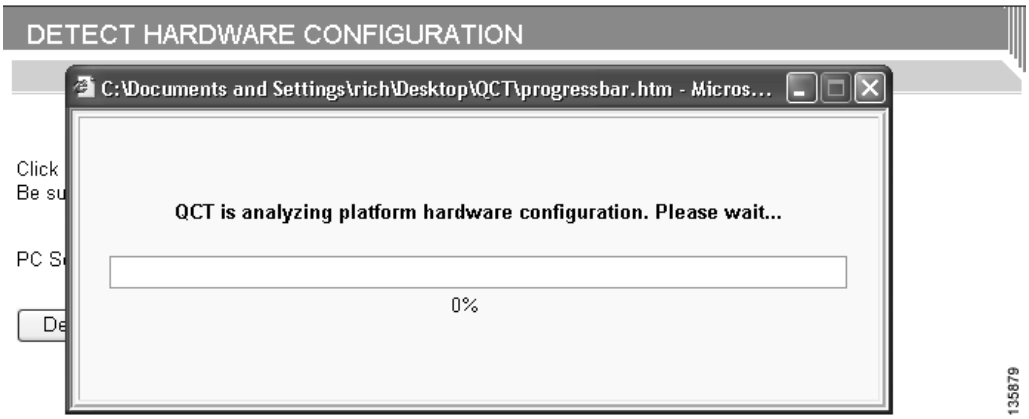


Step 14 Click **Yes** to accept any ActiveX control from an Internet Explorer dialog box (see Figure 35):

Figure 35 Detect Hardware Active X Dialog

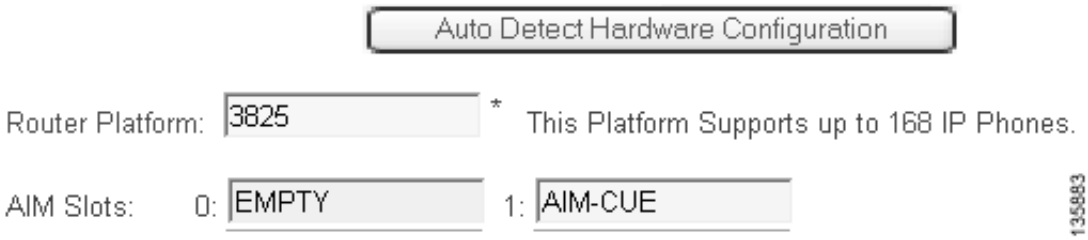
Cisco IPC Express QCT begins to analyze your installed hardware (see Figure 36):

Figure 36 Hardware Detection Analyzing Pop-Up



Following hardware detection, the Hardware Configuration area shows installed hardware in your router. Figure 37 shows an installed AIM-CUE card as an example.

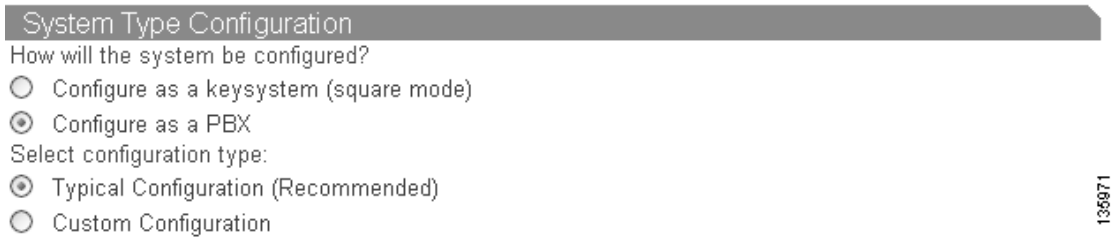
Figure 37 Analyzed Detected Hardware (Example)



Your Options for System Type and Configuration

You must instruct QCT how your system will be configured. The System Type Configuration area of the System Parameters window provides radio buttons to allow you to specify *how your system will be configured* and the *configuration type* (see Figure 38).

Figure 38 System Type and Configuration Type Selection



Keysystems and PBXs

When setting up a Cisco IPC Express system, you need to decide if call handling should be similar to that of a PBX or similar to that of a keyswitch.

Note Cisco BCS Verified Designs was configured using the PBX:Custom selection.

Keysystem

In a keysystem, you can set up most of your phones to have a nearly identical configuration, in which each phone is able to answer any incoming PSTN call on any line. For example, you have four incoming PSTN lines that each appear as shared lines on four different phones. Each phone has the same shared lines. Keysystems can be used when no internal call switching is necessary.

In the keysystem model, when an incoming call arrives, it rings all available IP phones. When multiple calls are present within the system at the same time, each individual call (ringing or waiting on hold) is visible and can be directly selected by pressing the corresponding line button on an IP phone. In this model, calls can be moved between phones simply by putting the call on hold at one phone and selecting the call using the line button on another phone.

PBX

The PBX model allows the IP phones in your system to have a single unique extension number. PBX configurations are usually required for larger companies who need both internal (extension numbers) and external (PSTN) phone capabilities.

The PBX model also enables your configuration to support features such as intercom, call park, hunt groups, and caller ID blocking.

Typical or Custom Configuration

Choose typical if you are setting up a voice-only system. Choose custom if you want to customize the IP addressing for the system.

Perform the following steps to select *how your system will be configured* and the *configuration type*.

Step 15 Click the **Configure as a keysystem** or **Configure as a PBX** radio button to select how your system will be configured.

Step 16 Click the **Typical Configuration** or **Custom Configuration** radio button to select how your system will be configured.

Selecting System Type and Configuration Type

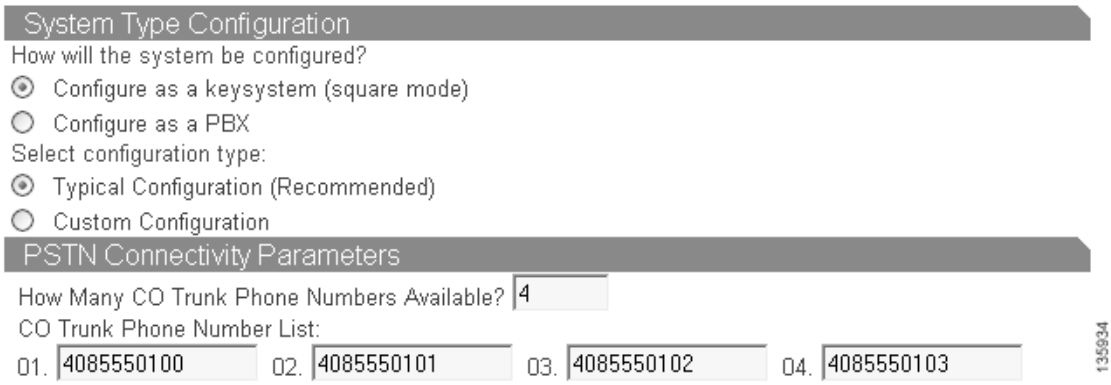
Once you select *how your system will be configured* and the *configuration type*, see the following sections to help you finish your system-type configuration. If you select:

- Configure as a Keysystem and Typical Configuration, see the "Configuring Keysystem:Typical Configurations" section on page 29.
- Configure as a Keysystem and Custom Configuration, see the "Configuring Keysystem:Custom Configurations" section on page 30.
- Configure as a PBX and Typical Configuration, see the "Configuring PBX:Typical Configurations" section on page 34.
- Configure as a PBX and Custom Configuration, see the "Configuring PBX:Custom Configurations" section on page 36.

Configuring Keysystem:Typical Configurations

If you selected Keysystem and Typical Configuration from the System Type Configuration area of the QCT Systems Parameters window, enter PSTN connectivity information (see Figure 39).

Figure 39 Keysystem:Typical Configuration Fields

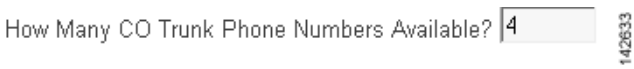


Configuring PSTN Connectivity Parameters

Perform the following steps to configure optional PSTN connectivity parameters.

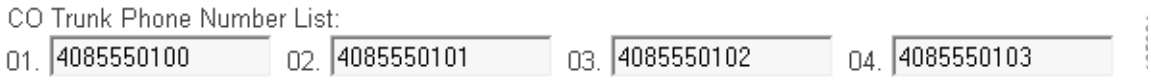
Step 1 Specify the number of available trunk phone numbers (see Figure 40):

Figure 40 Specifying Available Trunk Phone Numbers



Step 2 Enter the trunk phone numbers (see Figure 41):

Figure 41 Specifying Trunk Phone Numbers



After entering your PSTN connectivity parameters, you are ready to perform any necessary configuration for your IP phones.

Step 3 Add voice-mail parameters (see the “Configuring IP Phone Parameters” section on page 46).

Configuring Keysystem:Custom Configurations

If you selected Keysystem and Custom Configuration from the System Type Configuration area of the QCT Systems Parameters window, new information fields appears as shown in Figure 42.

Figure 42 Keysystem:Custom Configuration Fields

General Phone Parameters
First Extension Number: 2001 dual-line ☑
Network Parameters
DHCP Network IP Address: 10.1.10.0 Subnet Mask: 255.255.255.0
DHCP Excluded Address: 10.1.10.1 to 10.1.10.10
CME IP Address: 10.1.10.1 Subnet Mask: 255.255.255.0
NTP Server 1 IP Address: NTP Server 2 IP Address:
PSTN Connectivity Parameters
Secondary Dialtone Digit (for outgoing call): 9 Emergency Number: 911
How Many CO Trunk Phone Numbers Available? 4
CO Trunk Phone Number List:
01. 4085550100 02. 4085550101 03. 4085550102 04. 4085550103
Voice Mail Parameters
Configure a General Delivery Mailbox using CUE? ☐
Advanced CME Features Parameters
Paging ☑
Paging Parameters
Number of Paging Groups: 1

Configuring General Phone Parameters

Perform the following steps to configure general phone information.

Step 1 Enter the first extension number (see Figure 43):

Note *Do not* use the digit 9 as the first digit of any extension number. The digit 9 is reserved for secondary dial tone.

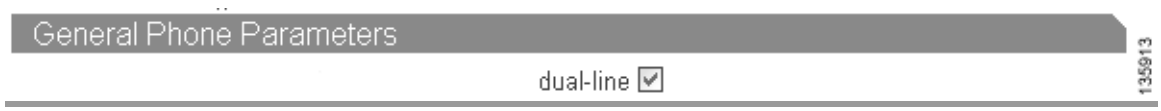
Figure 43 Specifying General Phone Parameters

General Phone Parameters
First Extension Number: 2001

135915

Step 2 Specify if this extension is a dual-line phone (two phone extensions, same number for each IP phone) by checking the dual-line check box (see Figure 44):

Figure 44 Specifying Dual-Line



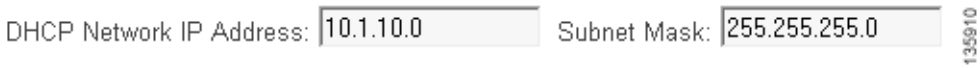
Configuring Network Parameters

Perform the following steps to configure network parameters for your IP phones.

Step 1 Enter the IP address and subnet mask of your Dynamic Host Configuration Server (DHCP) server (see Figure 45):

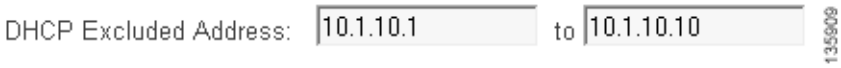
Note The IP addresses shown in Figure 45 are examples only. Enter your DHCP server IP address information from your *Cisco Business Communications Solution Verified Designs Planning Worksheet*.

Figure 45 Specifying DHCP Network IP Address and Subnet Mask



Step 2 Specify your DHCP excluded address range (see Figure 46):

Figure 46 Specifying DHCP Excluded Addresses



Step 3 Specify your Cisco CME router's IP address and subnet mask (see Figure 47):

Figure 47 Specifying Cisco CME Router IP Address and Subnet Mask

Step 4 If required, enter the IP addresses for your Network Time Protocol (NTP) servers (see Figure 48). NTP allows you to synchronize your Cisco CME router to a single clock on a network, which is known as the clock master. NTP is disabled on all interfaces by default.

Note NTP is not required for Cisco Business Communications Solution Verified Designs.

Figure 48 Specifying NTP Server IP Address (Optional)

NTP Server 1 IP Address: NTP Server 2 IP Address:

Configuring PSTN Connectivity Parameters

Perform the following steps to configure optional PSTN connectivity parameters.

Step 1 Enter a digit that you would press to select secondary dial tone (see Figure 49):

Figure 49 Specifying Secondary Dial Tone Digit

Secondary Dialtone Digit (for outgoing call): 9

Step 2 Specify the emergency number (see Figure 50):

Figure 50 Specifying Emergency Number

Emergency Number: 911

Step 3 Specify the number of available trunk phone numbers (see Figure 51):

Figure 51 Specifying Available Trunk Phone Number

How Many CO Trunk Phone Numbers Available? 4

142633

Step 4 Enter the trunk phone numbers (see Figure 52):

Figure 52 Specifying Trunk Phone Numbers

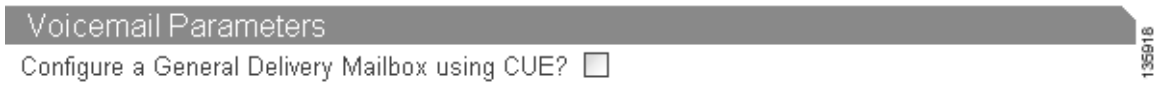
CO Trunk Phone Number List:
01. 4085550100 02. 4085550101 03. 4085550102 04. 4085550103

Configuring Voice-Mail Parameters

If you have an installed AIM card, enter voice-mail configuration information.

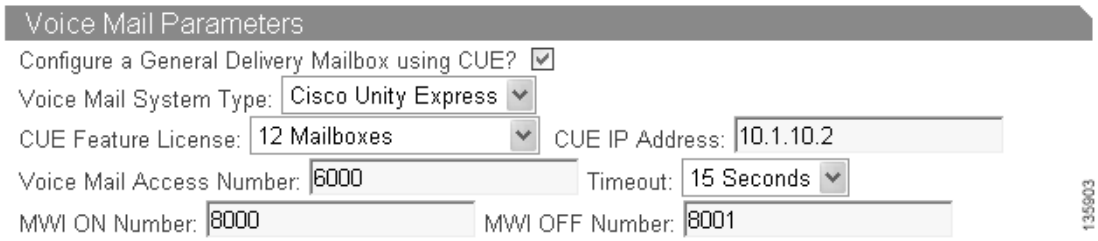
Step 1 Specify whether to configure a general delivery mailbox for Cisco CUE by checking the check box (see Figure 53):

Figure 53 Specifying General Delivery Mailbox



If you are configuring a general delivery mailbox, enter additional voice-mail parameters as illustrated in Figure 54:

Figure 54 Voicemail Parameters Fields

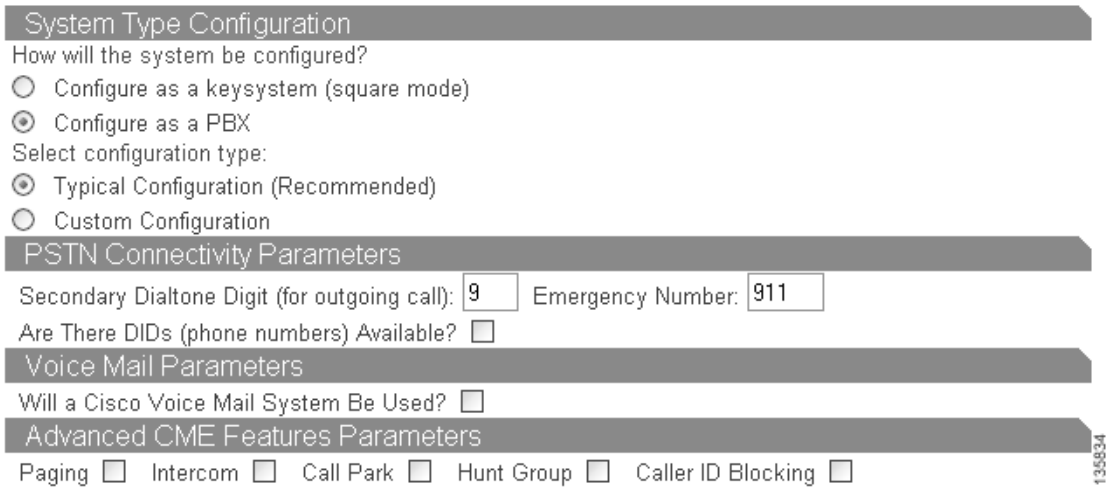


Step 2 For detailed information on adding voice-mail parameters, see the "Configuring Voice-Mail Parameters" section on page 39.

Configuring PBX:Typical Configurations

If you selected PBX and Typical Configuration from the System Type Configuration area of the QCT Systems Parameters window, enter additional configuration parameters as shown in Figure 55.

Figure 55 PBX:Typical Configuration Fields

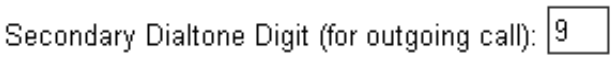


Configuring PSTN Connectivity Parameters

If your hardware configuration contains a 4-port FXO card, perform the following steps to enter optional PSTN connectivity parameters.

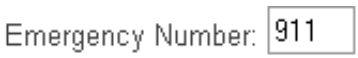
Step 1 Enter a digit that you would press to select secondary dial tone (see Figure 56):

Figure 56 Specifying Secondary Dial Tone Digit



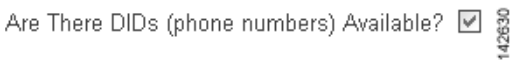
Step 2 Specify the emergency number (see Figure 57):

Figure 57 Specifying Emergency Number



Step 3 Specify if there are Direct Inward Dial (DID) phone numbers available (see Figure 58):

Figure 58 Specifying Available DIDs

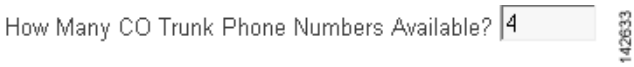


Step 4 If DIDs are available, enter the first phone numbers (see Figure 59):

Figure 59 Specifying First Phone Numbers

Step 5 Specify the number of available phone numbers (see Figure 60):

Figure 60 Specifying Available Phone Number



Configuring Voice-Mail Parameters

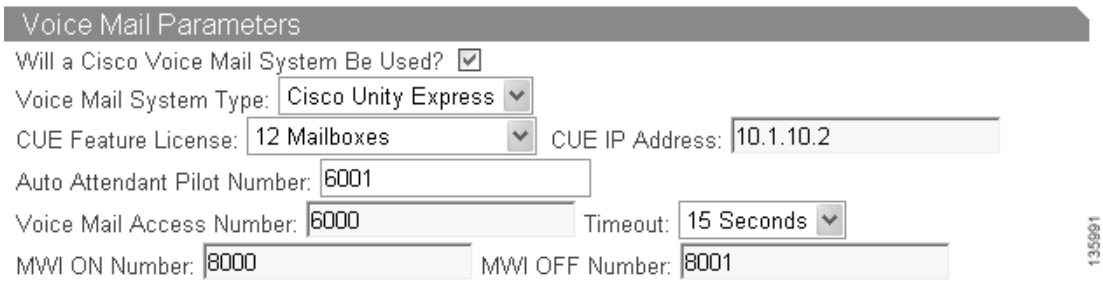
If you have an installed AIM card, enter voice-mail configuration information.

Step 1 Specify if you are using Cisco Unity Express voice mail by checking the check box (see Figure 61):

Figure 61 Specifying Cisco Voice Mail

If you are using Cisco Unity Express voice mail, additional information fields appear (see Figure 62):

Figure 62 Cisco Voice-Mail Parameters Fields

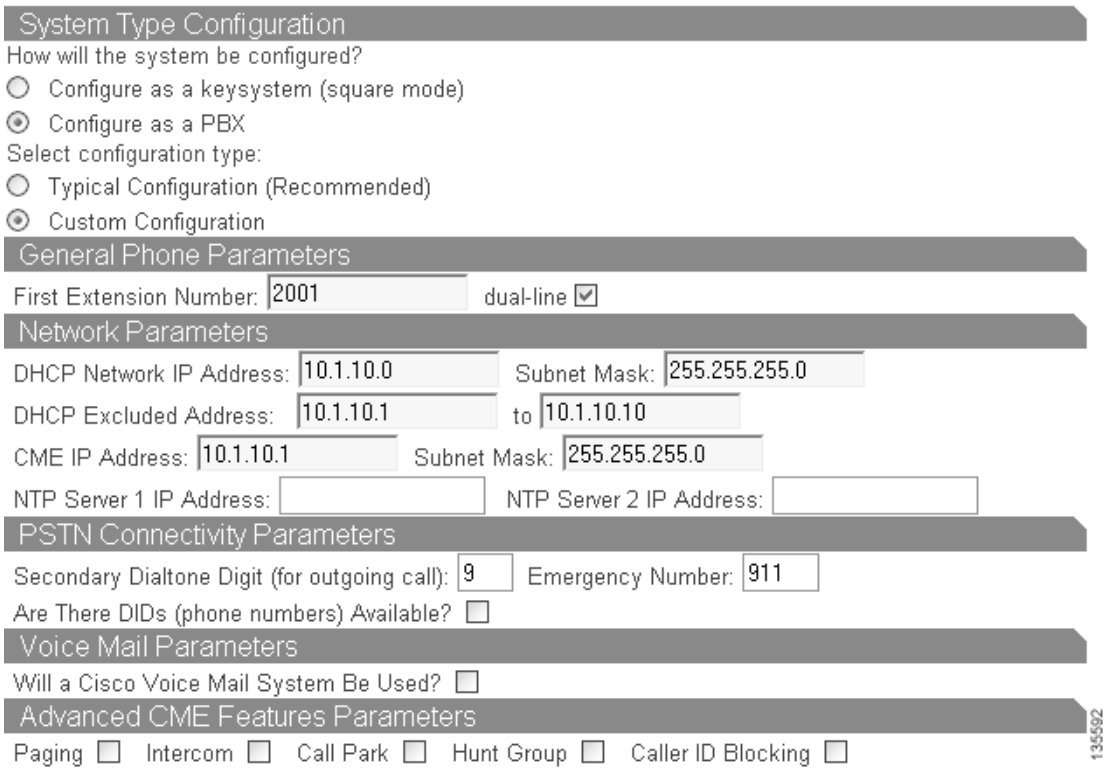


Step 2 For detailed information on adding voice-mail parameters, see the "Configuring Voice-Mail Parameters" section on page 39).

Configuring PBX:Custom Configurations

If you selected PBX and Custom Configuration from the System Type Configuration area of the Systems Parameters window, enter additional configuration parameters as illustrated in Figure 63.

Figure 63 PBX:Custom Parameters



Configuring General Phone Parameters

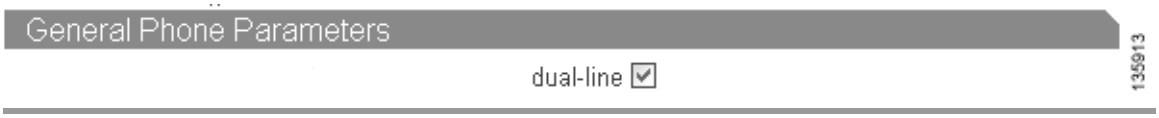
Perform the following steps to configure general phone information.

Step 1 Enter the first extension number of your IP phones (see Figure 64):

Figure 64 Specifying First Extension Number

Step 2 Specify if this extension is a dual-line phone by checking the dual-line check box (see Figure 65):

Figure 65 Specifying Dual-Line Phone



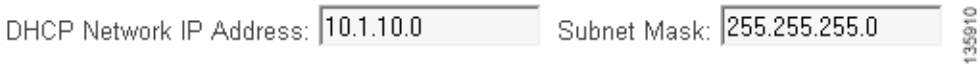
Configuring Network Parameters

Perform the following steps to configure network parameters.

Step 1 Enter the IP address and subnet mask of your DHCP server (see Figure 66):

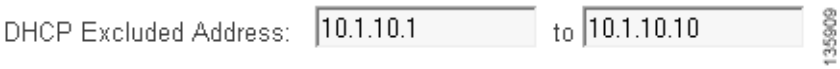
Note The following IP addresses are examples only. Enter your DHCP server IP address information from your *Cisco Business Communications Solution Verified Designs Planning Worksheet*.

Figure 66 Specifying DHCP IP Address and Subnet Mask



Step 2 Specify your DHCP Excluded Address range (see Figure 67):

Figure 67 Specifying DHCP Excluded Addresses



Step 3 Specify your Cisco CME router's IP address and subnet mask (see Figure 68):

Figure 68 Specifying Cisco CME Router IP Address and Subnet Mask

Step 4 Enter the IP addresses and subnet masks for your NTP servers (see Figure 69):

Figure 69 Specifying NTP Server IP Addresses

Configuring PSTN Connectivity Parameters

Perform the following steps to configure optional PSTN connectivity parameters.

Step 1 Enter a digit you would press to select secondary dial tone (see Figure 70):

Figure 70 Specifying Secondary Dialtone Digit

Secondary Dialtone Digit (for outgoing call): 9

Step 2 Specify the emergency number (see Figure 71):

Figure 71 Specifying Emergency Number

Emergency Number: 911

Step 3 Specify if there are Direct Inward Dial (DID) phone numbers available by checking the check box (see Figure 72):

Figure 72 Specifying Available DIDs

Are There DIDs (phone numbers) Available? ☑ 142630

Step 4 If DIDs are available, enter the first phone numbers (see Figure 73):

Figure 73 Specifying First Phone Numbers

First Phone Number: 4085550100 142631

Step 5 Specify the number of available phone numbers (see Figure 74):

Figure 74 Specifying Available Phone Numbers

How Many CO Trunk Phone Numbers Available? 4 142633

Step 6 Add voice-mail parameters (see the "Configuring Voice-Mail Parameters" section on page 39).

Configuring Voice-Mail Parameters

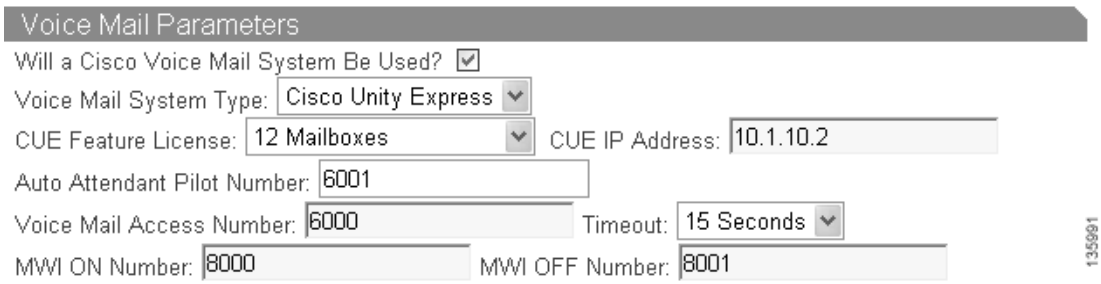
Perform the following steps to configure voice-mail parameters.

Step 1 Specify if you are using Cisco Unity Express voice mail by checking the check box (see Figure 75):

Figure 75 Specifying Cisco Voicemail Parameters

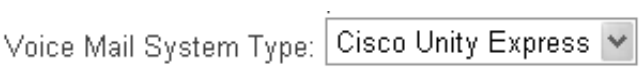
If you are using Cisco Unity Express voice mail, additional information fields appear (see Figure 76):

Figure 76 Cisco Voice-Mail Parameter Fields



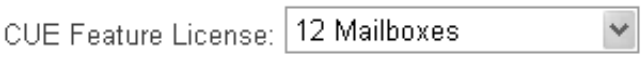
Step 2 In the Voice Mail System Type drop-down menu, select Cisco Unity Express (see Figure 77):

Figure 77 Specifying Voice Mail System Type



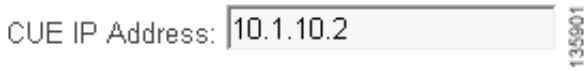
Step 3 Specify the Cisco CUE Feature License by selecting the number of mailboxes from the drop-down menu (see Figure 78):

Figure 78 Specifying Cisco CUE Licensing



Step 4 Specify the IP address of the Cisco CUE router (see Figure 79):

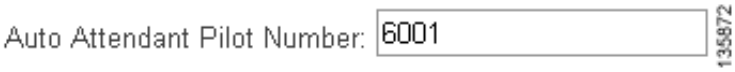
Figure 79 Specifying Cisco CUE IP Address



Step 5 Specify the Auto Attendant pilot number (see Figure 80):

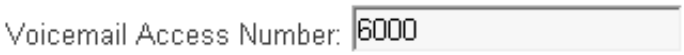
Note Remember not to use digit 9 for any extension.

Figure 80 Specifying Auto Attendant Pilot Number



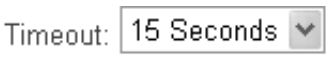
Step 6 Specify your voice-mail access number (see Figure 81):

Figure 81 Specifying Voice-Mail Access Number



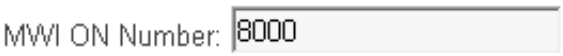
Step 7 Specify the voice-mail timeout from the drop-down menu (see Figure 82):

Figure 82 Specifying Voice-Mail Timeout



Step 8 Specify your message-waiting indicator (MWI) On number (see Figure 83):

Figure 83 Specifying MWI On



Step 9 Specify your message-waiting indicator (MWI) Off number (see Figure 84):

Figure 84 Specifying MWI Off

This completes the voice-mail parameters section.

Step 10 Enter advanced Cisco CME features (see the "Configuring Advanced Cisco CME Features Parameters" section on page 41).

Configuring Advanced Cisco CME Features Parameters

Follow the procedure in this section if you wish to configure additional features for your telephony network (see Figure 85).

Figure 85 Advanced Cisco CME Feature Parameter Fields

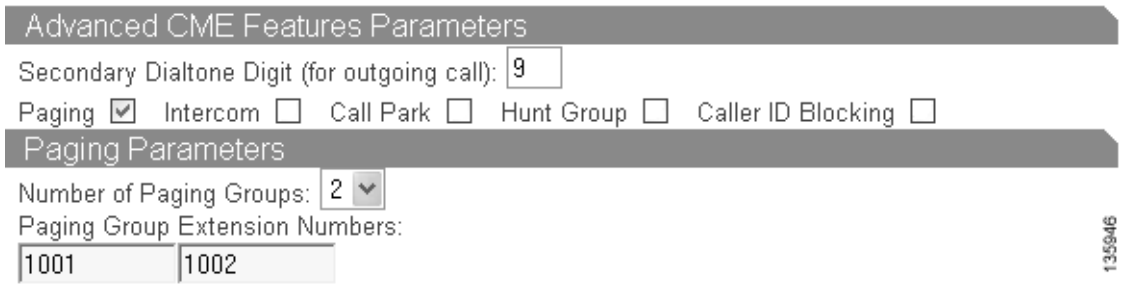
Additional Cisco CME features include the following:

- Paging (see the "Configuring Paging" section on page 41)
- Intercom (see the "Configuring Intercom" section on page 42)
- Call Park (see the "Configuring Call Park" section on page 42)
- Hunt Group (see the "Configuring Hunt Groups" section on page 43)
- Caller ID Blocking (see the "Configuring Caller ID Blocking Parameters" section on page 45)

Configuring Paging

Step 1 To enable paging, check in the Paging check box (see Figure 86):

Figure 86 Specifying Paging Parameters



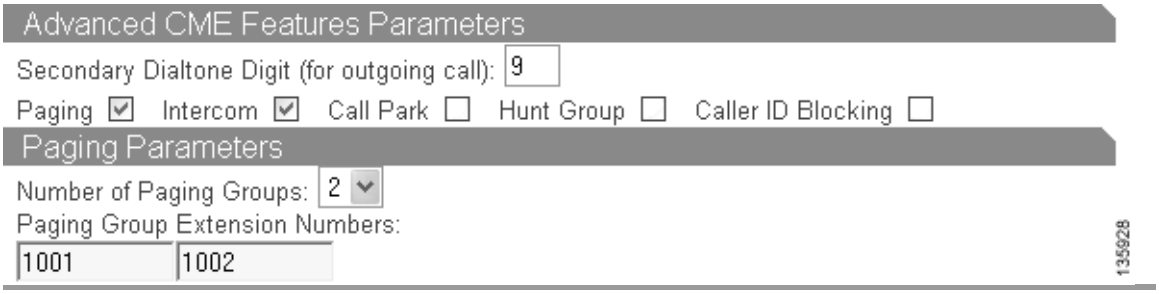
a. Specify the number of paging groups from the drop-down menu.

b. Enter the paging group extension numbers.

Configuring Intercom

Step 1 To enable intercom between IP phones, check Intercom check box (see Figure 87):

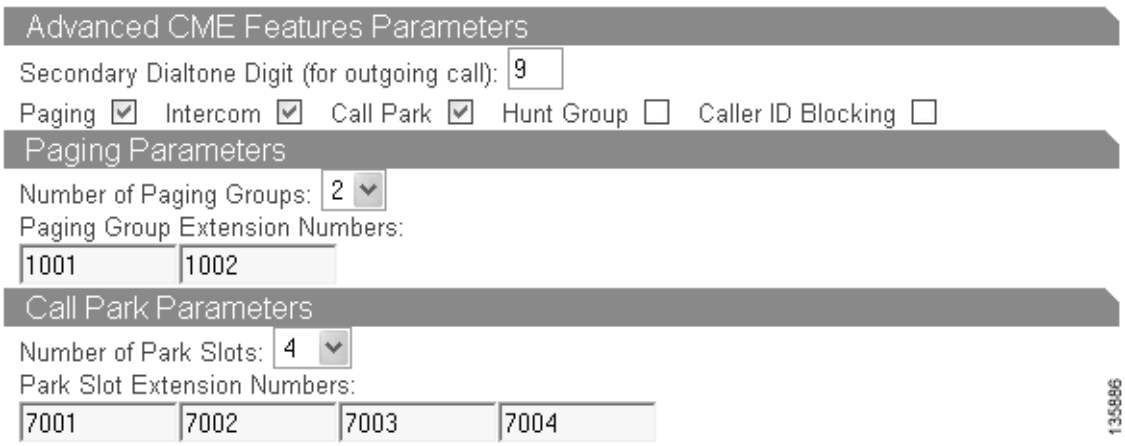
Figure 87 Specifying Intercom



Configuring Call Park

Step 1 To enable call park, check the Call Park check box (see Figure 88):

Figure 88 Specifying Call Park

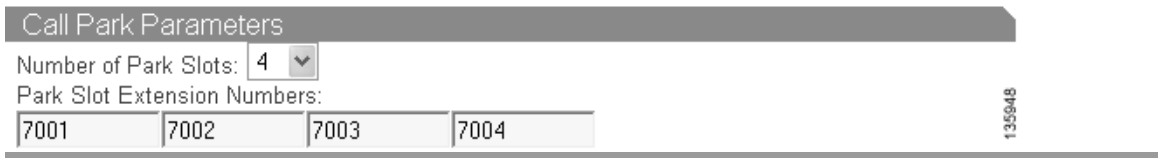


a. Specify the number of park slots from the drop-down menu (see Figure 89):

Figure 89 Specifying Number of Park Slots

b. Enter your park slot extension numbers (see Figure 90):

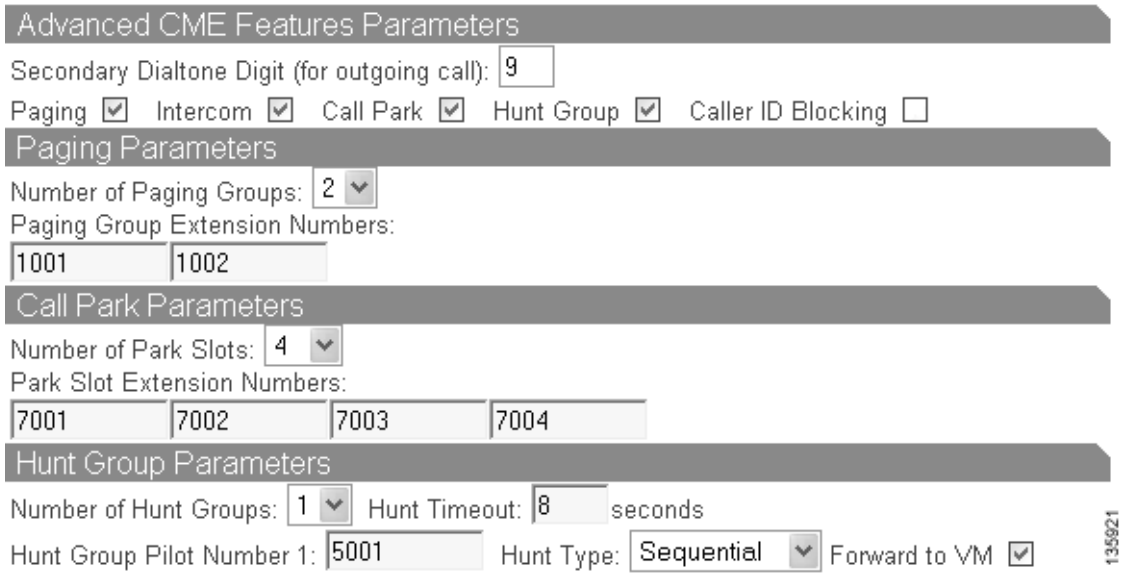
Figure 90 Specifying Park Slot Extension Numbers



Configuring Hunt Groups

Step 1 Enable hunt groups by checking the Hunt Group check box (see Figure 91):

Figure 91 Specifying Hunt Groups

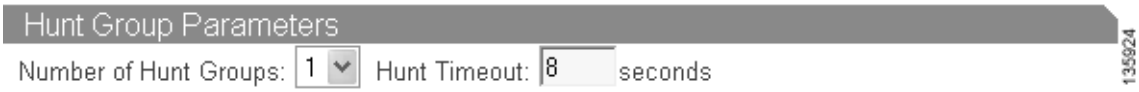


Step 2 Specify the number of hunt groups from the drop-down menu (see Figure 92):

Figure 92 Specifying Number of Hunt Groups

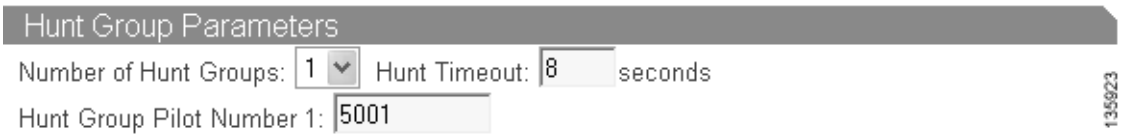
Step 3 Enter the hunt timeout value in seconds (see Figure 93):

Figure 93 Specifying Hunt Group TImeout



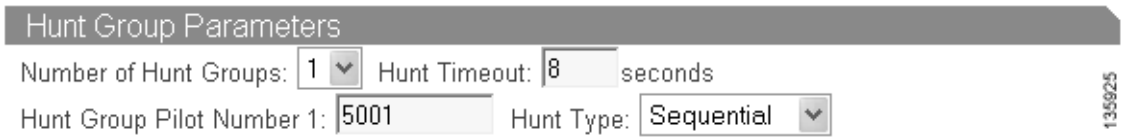
Step 4 Enter your hunt group pilot numbers (see Figure 94):

Figure 94 Specifying Hunt Group Pilot Number



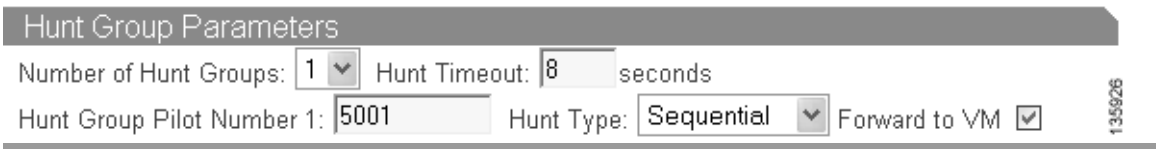
Step 5 Specify your hunt type from the drop-down menu (see Figure 95):

Figure 95 Specifying Hunt Type



Step 6 Enable whether to send the hunt groups to voice mail by checking the Forware to VM check box (see Figure 96):

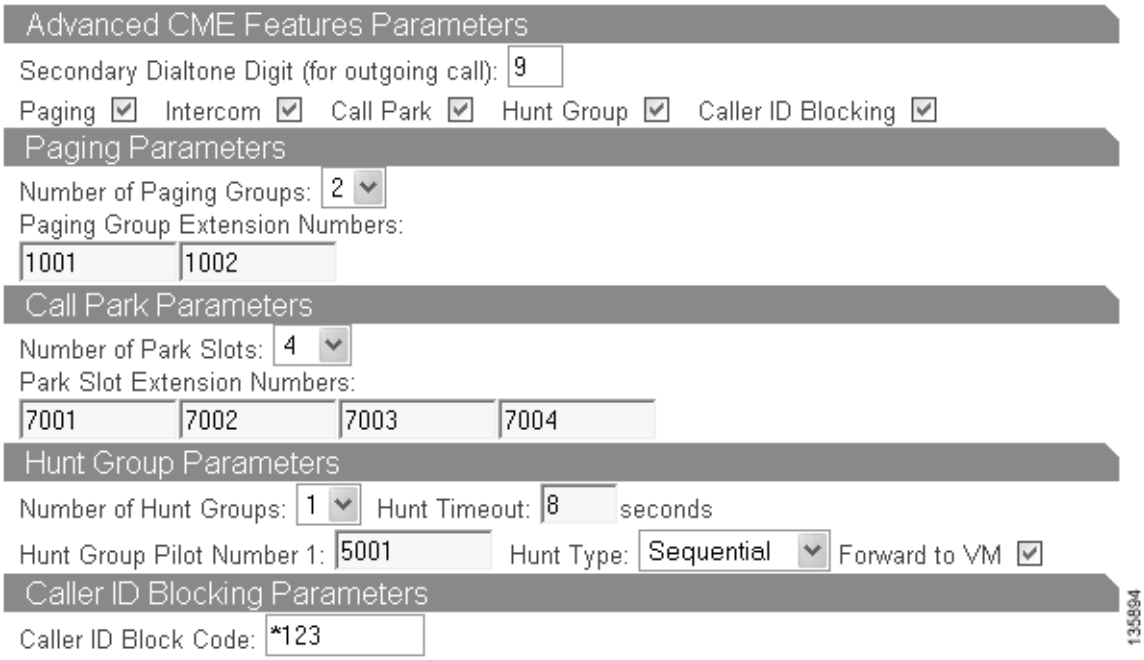
Figure 96 Specifying Hunt Group to Voice-Mail



Configuring Caller ID Blocking Parameters

Step 1 To enable caller ID blocking parameters, check the Caller ID Blocking check box (see Figure 97):

Figure 97 Specifying Call ID Blocking



Step 2 Enter your caller ID block code (see Figure 98):

Figure 98 Specifying Caller ID Block Code

Note Enter an asterisk (*) before the caller ID block code.

This completes the configuration of Advanced CME features parameters.

Step 3 Configure your IP phones (see the "Configuring IP Phone Parameters" section on page 46).

Configuring IP Phone Parameters

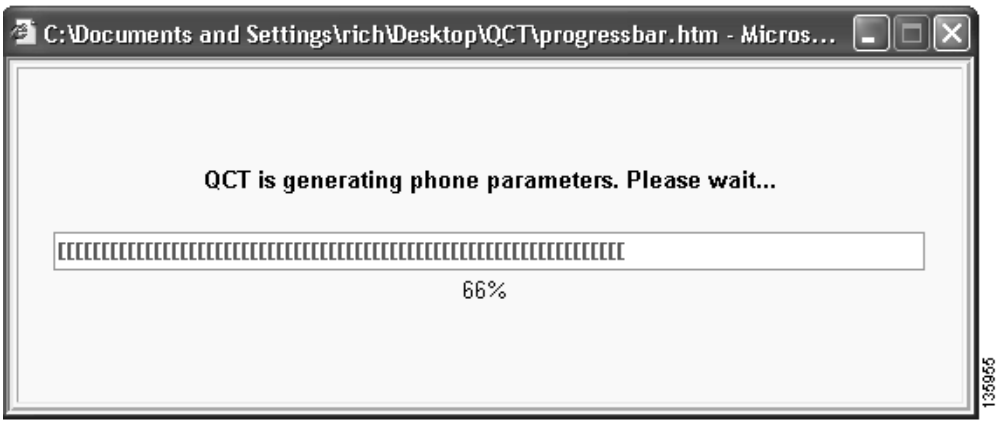
After configuring all your system parameters, proceed to the Phone Parameters window of Cisco IPC Express QCT.

Step 1 Click **Go To Phone Parameters** button (see Figure 99):

Figure 99 Go To Phone Parameters Button

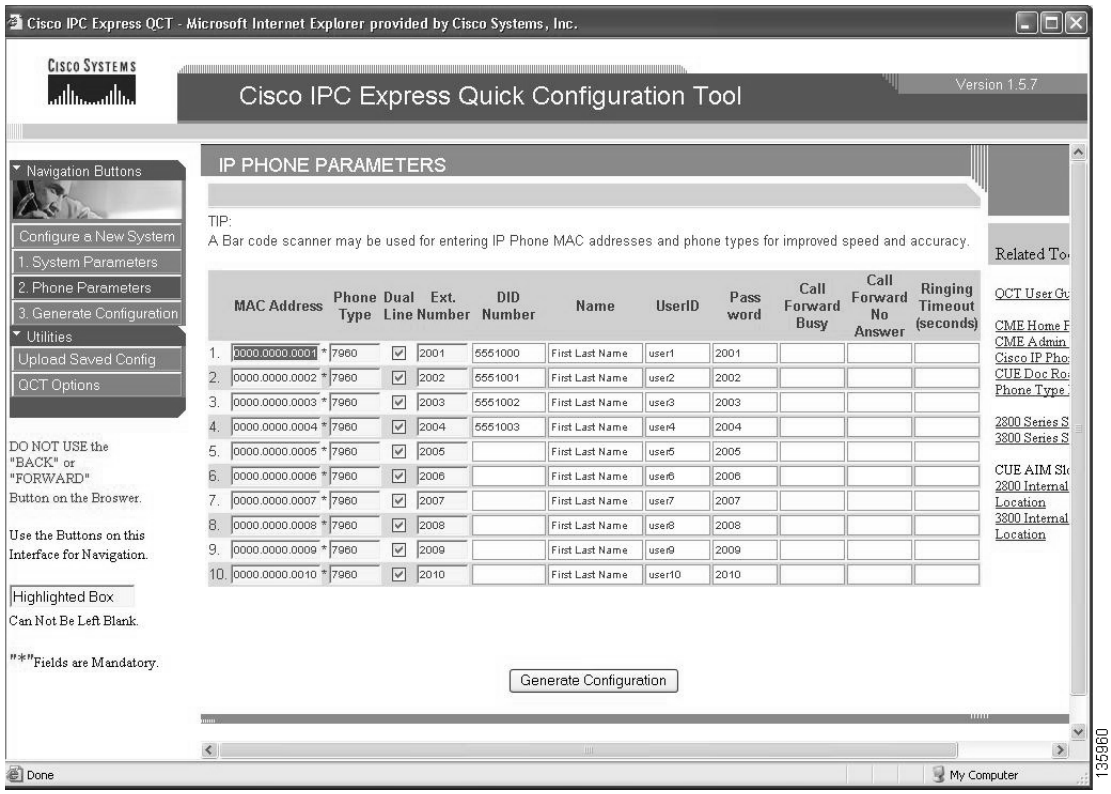
QCT begins to automatically generate your phone parameters information (see Figure 100):

Figure 100 Analyzing IP Phone Parameters



The IP Phone Parameters window appears (see Figure 101):

Figure 101 IP Phone Parameters Window



The IP Phone Parameters window allows you to enter specific telephony information for each IP phone in your system. The IP Phone Parameters window contains slightly different information depending on the system configuration type you chose.

Step 2 If you chose:

- Keysystem, see the “Configuring Keysystem IP Phone Parameters” section on page 48.
- PBX, see the “Configuring PBX IP Phone Parameters” section on page 50.

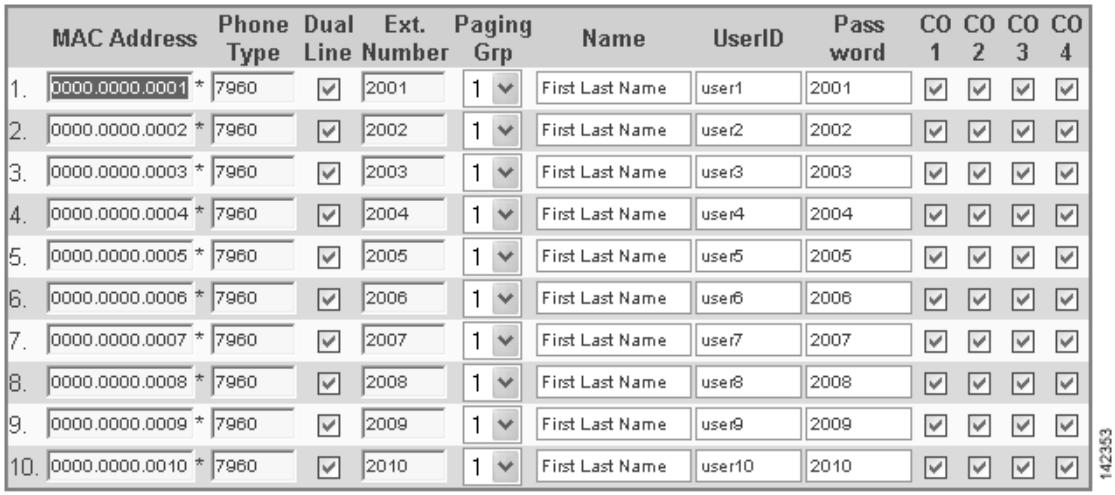
Configuring Keysystem IP Phone Parameters

Perform the following steps to enter keysystem IP phone parameters.

Step 1 Click the **Phone Parameters** button to activate the IP Phone Parameters window.

The Keysystem IP Phone Parameters window appears (see Figure 102):

Figure 102 Keysystem IP Phone Parameters Window



Each input field is tab indexed to allow you to flow from one field to the next to enter information.

Tip You may use a bar-code scanner to enter IP phone MAC address and phone types. Cisco has tested a bar-code scanner from Flic™.

Step 2 Edit any default phone parameter to suit your network.

Table 4 Keysystem IP Phone Parameters Screen Fields

Field	To Set
MAC Address	Enter, or scan, the MAC address of each IP phone. MAC addresses are located on the bottom of the IP phone.
Phone Type	Specify the IP phone type.
Dual-Line	Enter a check next to the IP phone you want to have two lines for each extension.
Extension Number	Enter the extension number for each IP phone.
Paging Group	Specify from the drop-down menu the paging group you want to associate with each IP phone.
Name	Enter the name to associate with each IP phone. The name will appear in the IP phone display.
User ID	Enter a user ID for each IP phone.

Table 4 Keysystem IP Phone Parameters Screen Fields

Field	To Set
Password	Enter a password for each IP phone.
CO	Specify with a check the CO trunk phone numbers associated with each IP phone.

What to Do Next

Once you finish entering your keysystem configuration parameters, generate the configuration (see the "Generating Configurations" section on page 52).

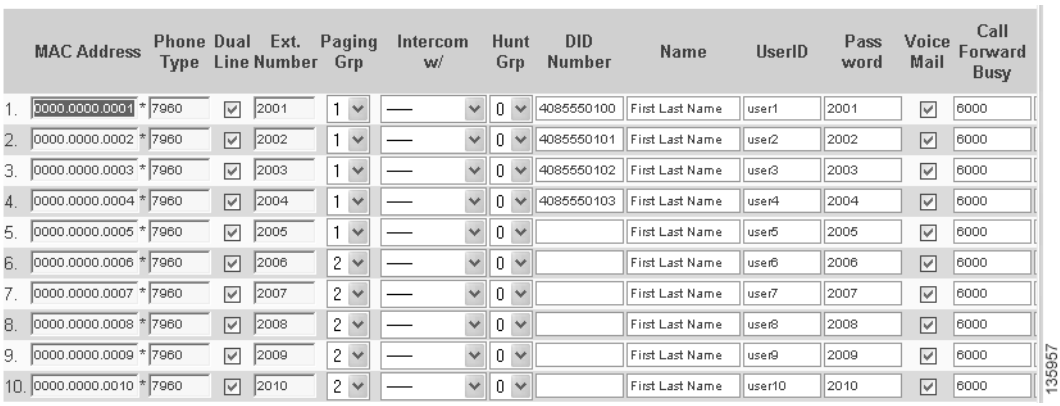
Configuring PBX IP Phone Parameters

Perform the following steps to enter PBX IP phone parameters.

Step 1 Click the **Phone Parameters** button to activate the IP Phone Parameters screen.

The PBX IP Phone Parameters window appears (see Figure 103):

Figure 103 PBX IP Phone Parameters Window



	MAC Address	Phone Type	Dual Line	Ext. Number	Paging Grp	Intercom w/	Hunt Grp	DID Number	Name	UserID	Pass word	Voice Mail	Call Forward Busy
1.	0000.0000.0001 *	7960	☑	2001	1	—	0	4085550100	First Last Name	user1	2001	☑	6000
2.	0000.0000.0002 *	7960	☑	2002	1	—	0	4085550101	First Last Name	user2	2002	☑	6000
3.	0000.0000.0003 *	7960	☑	2003	1	—	0	4085550102	First Last Name	user3	2003	☑	6000
4.	0000.0000.0004 *	7960	☑	2004	1	—	0	4085550103	First Last Name	user4	2004	☑	6000
5.	0000.0000.0005 *	7960	☑	2005	1	—	0		First Last Name	user5	2005	☑	6000
6.	0000.0000.0006 *	7960	☑	2006	2	—	0		First Last Name	user6	2006	☑	6000
7.	0000.0000.0007 *	7960	☑	2007	2	—	0		First Last Name	user7	2007	☑	6000
8.	0000.0000.0008 *	7960	☑	2008	2	—	0		First Last Name	user8	2008	☑	6000
9.	0000.0000.0009 *	7960	☑	2009	2	—	0		First Last Name	user9	2009	☑	6000
10.	0000.0000.0010 *	7960	☑	2010	2	—	0		First Last Name	user10	2010	☑	6000

135957

The fields on the IP Phone Parameters window are tab indexed to flow from one field to the next.

Tip QCT supports the use of a bar-code scanner to enter IP phone MAC addresses and phone types. Cisco BCS Verified Designs has tested a bar-code scanner from Flic™.

Step 2 Edit any default phone parameter to suit your network (see Table 5).

Table 5 PBX IP Phone Parameters Screen Fields

Field	To Set
MAC Address	Enter, or scan, the MAC address of each IP phone. MAC addresses are located on the bottom of the IP phone.
Phone Type	Specify the IP phone type.
Dual-Line	Enter a check next to the IP phone you want to have two lines for each extension.
Extension Number	Enter the extension number for each IP phone.
Paging Group	Specify from the drop-down menu the paging group you want to associate with each IP phone.
Intercom	Specify from the drop-down menu the IP phone you want to intercom with this IP phone.

Table 5 PBX IP Phone Parameters Screen Fields

Field	To Set
Hunt Group	Specify from the drop-down menu the hunt group associated with each IP phone.
DID Number	Enter the Direct Inward Dial number for each IP phone. DID numbers accept both 7- and 10-digit numbers.
Name	Enter the name to associate with each IP phone. The name will appear in the IP phone display.
User ID	Enter a user ID for each IP phone.
Password	Enter a password for each IP phone.
Voicemail	Enter a check to specify voicemail for each IP phone.
Call Forward Busy	Enter the extension number where you want to transfer calls to if an incoming call to an extension is busy.
Call Forward No Answer	Enter the extension number where you want to transfer calls to if an incoming call to an extension is not answered.
Ringing Timeout	Specify a value in seconds before transferring an unanswered call to another extension.

What to Do Next

Once you finish entering your PBX configuration parameters, generate the configuration (see the "Generating Configurations" section on page 52).

Generating Configurations

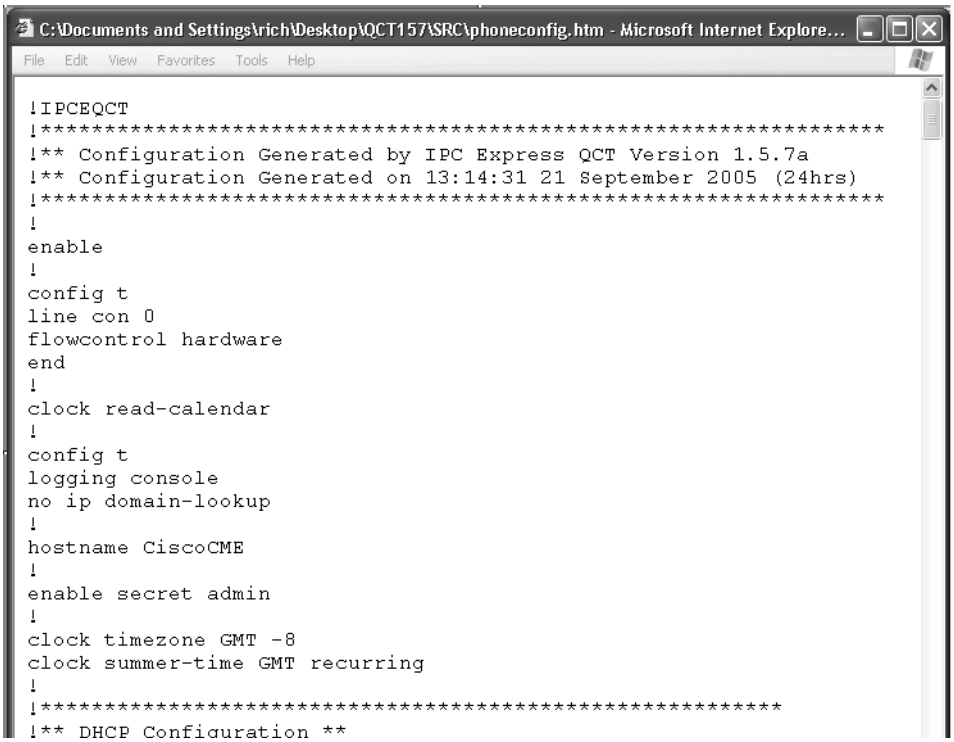
Once you enter all your system and phone parameters, generate your router configuration:

Step 1 Click the **Generate Configuration** button (see Figure 104):

Figure 104 Generate Configuration Button

Once your configuration generates, it will automatically display (see Figure 105):

Figure 105 Display of Generated Configuration

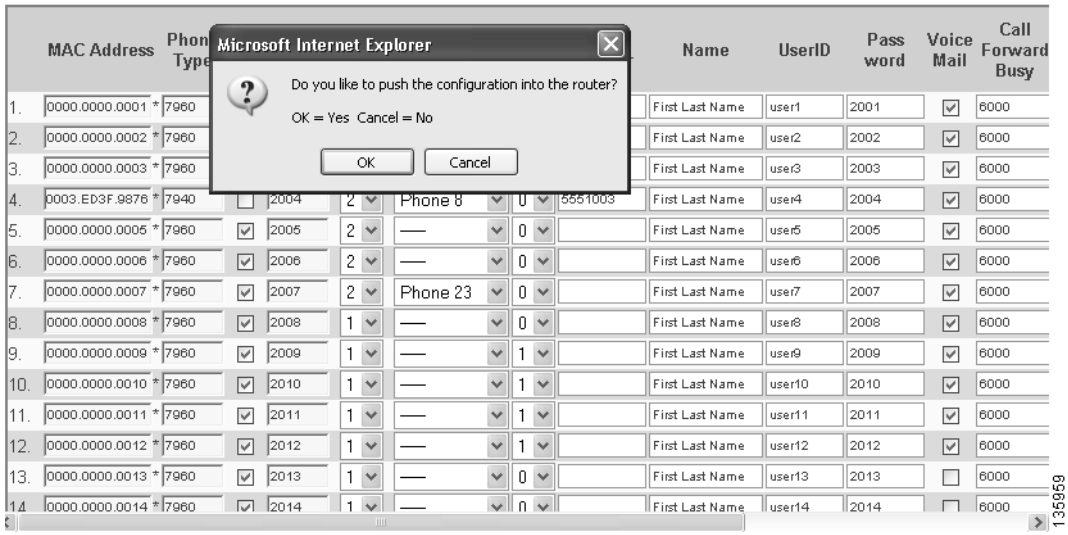


Note The generated configuration displays if the Display Configuration check box is selected on the QCT Options window (see the "Display Configuration" section on page 100).

Step 2 Save the router configuration.

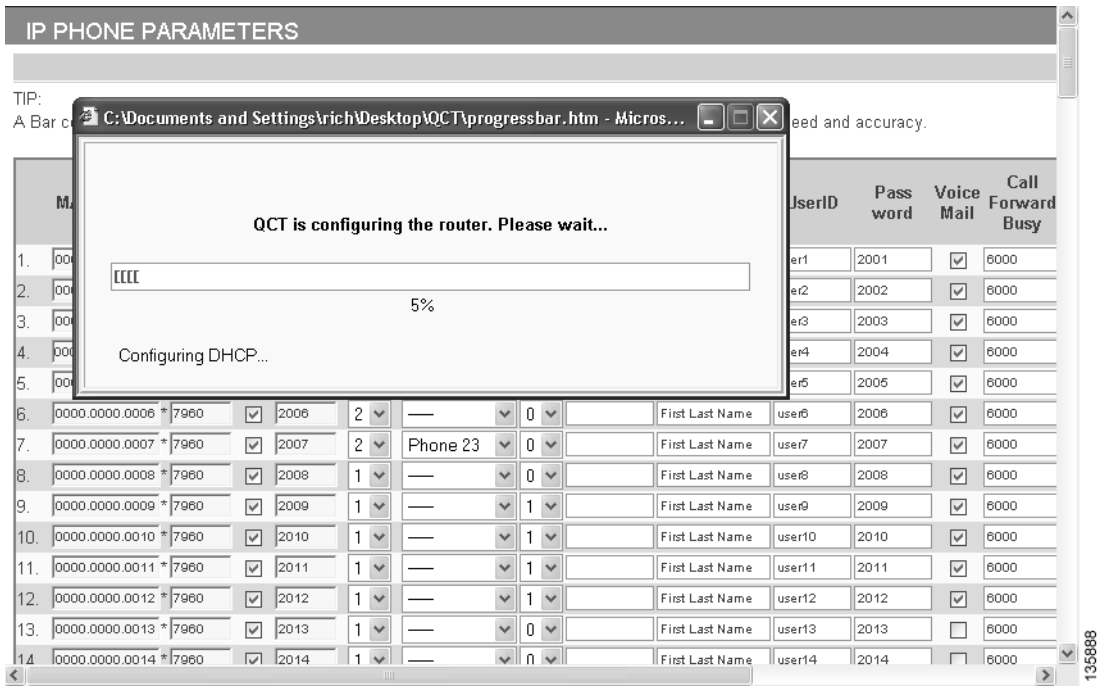
Step 3 When prompted, click **Yes** to push the configuration to the router (see Figure 106):

Figure 106 Confirming Pushing Configuration to Router



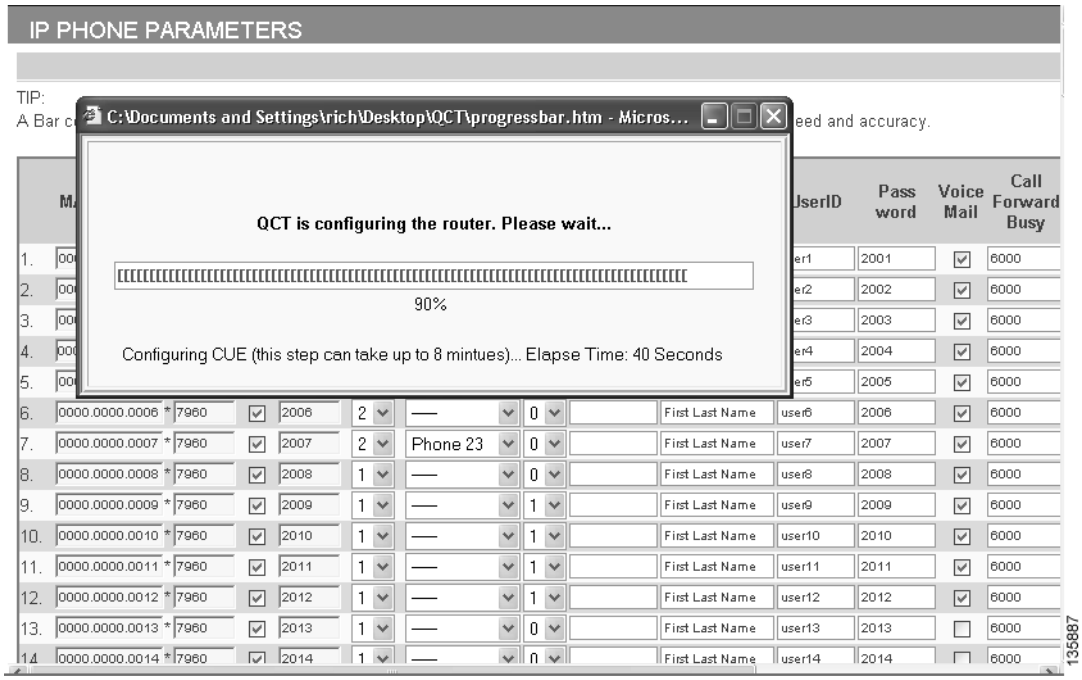
QCT begins to generate your configuration (see Figure 107).

Figure 107 Generating Configuration



QCT continues to generate your Cisco CUE voice-mail configuration (see Figure 108).

Figure 108 Generating Cisco CUE Voice Mail



QCT informs you when it is finished (see Figure 109):

Figure 109 Confirming Generated Configuration

Step 4 Click **OK**.

Your router is now configured. See Appendix C: Cisco BCS Verified Designs Configuration Example, page 101 for an example of a typical Cisco Business Communications Solution configuration file.

You can upload any saved configuration to your router (see the "Uploading Saved Configurations" section on page 97).

Testing the Installation

Perform the following steps to test the initial Cisco BCS Verified Designs configuration.

Step 1 Reboot the router.

Step 2 Connect the router to a nonconfigured switch (default switch configuration only).

Step 3 Connect preconfigured (MAC address previously entered in the IP Phone Parameters window) IP phones to the switch.

Step 4 Press the **settings** button on the IP phone and look under Network Configuration to make sure that the IP phones are receiving the appropriate IP addressing from the DHCP server.

Once the IP addressing is received (this could take several minutes), two connected IP phones should be able to call each other.

What to Do Next

After entering configuration parameters for Cisco SOCC, you are ready to use the command line interface (CLI) to continue your installation. See the "Continuing the Cisco BCS Verified Designs Configuration Using CLI" section on page 57.

Continuing the Cisco BCS Verified Designs Configuration Using CLI

This chapter describes the procedures using the command line interface (CLI) to continue Cisco Business Communications Solution Verified Designs configuration. Perform the procedures in this chapter using a terminal emulation utility such as Hyperterminal through the console port of your router.

Each procedure provides a list of summary and detailed steps that you can follow. Follow the detailed steps if you need examples and explanations of each CLI entry.

Contents

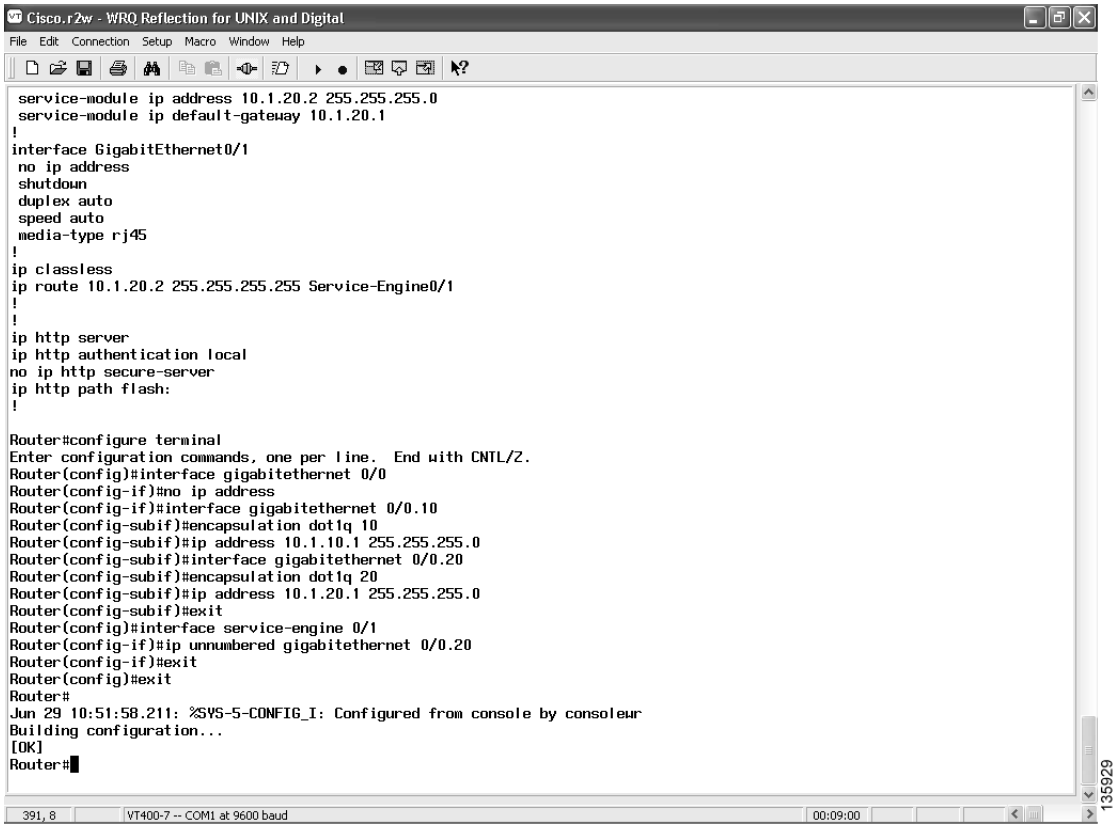
This chapter provides the following sections:

Configuring Subinterfaces for VLANs

This task creates subinterfaces for a Cisco LAN switch that will be carry voice and data on the network.

Summary steps (see Figure 110) list the steps necessary to configure the subinterfaces. For detailed steps including examples, see Table 6.

Figure 110 CLI for Configuring Subinterfaces for VLANs



Summary Steps

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot/port*
4. **no ip address**
5. **interface gigabitethernet** *slot/port.subinterface*
6. **encapsulation dot1q** *vlan-id*
7. **ip address subnet mask**
8. **interface gigabitethernet** *slot/port.subinterface*
9. **encapsulation dot1q** *vlan-id*
10. **ip address subnet mask**
11. **exit**

12. **interface service-engine** *slot/port*
13. **ip unnumbered gigabitethernet** *slot/port.subinterface*
14. **exit**
15. **exit**
16. **wr**

Note It is recommended to save a copy of the router configuration for backup purposes.

Detailed Steps

Table 6 Detailed Steps for Configuring Subinterfaces for VLANs

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router>`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/0`	Configures the interface and enters interface configuration mode.
Step 4	**no ip address** **Example:** `Router(config-if)# no ip address`	Disables IP processing for the specified interface.
Step 5	**interface gigabitethernet** *slot/port.subinterface* **Example:** `Router(config)# interface gigabitethernet 0/0.10`	Configures the subinterface and enters subinterface configuration mode. It is recommended to set the subinterface to the same value as the *vlan-id*.
Step 6	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-subif)# encapsulation dot1q 10`	Sets 802.1q encapsulation for the subinterface.
Step 7	**ip address** *ip-address subnet mask* **Example:** `Router(config-subif)# ip address 10.1.10.1 255.255.255.0`	Sets the IP address for the subinterface.

	Command or Action	Purpose
Step 8	**interface gigabitethernet** *slot/port.subinterface* **Example:** `Router(config-subif)# interface gigabitethernet 0/0.20`	Configures the subinterface. It is recommended to set the subinterface to the same value as the *vlan-id*.
Step 9	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-subif)# encapsulation dot1q 20`	Sets 802.1q encapsulation for the subinterface.
Step 10	**ip address** *ip-address subnet mask* **Example:** `Router(config-subif)# ip address 10.1.20.1 255.255.255.0`	Sets the IP address for the subinterface.
Step 11	**exit** **Example:** `Router(config)# exit`	Exits subinterface configuration mode.
Step 12	**interface service-engine** *slot/port* **Example:** `Router(config)# interface service-engine 0/1`	Enters interface configuration mode for a network module (NM) or an advanced integration module (AIM) in slot 0, port 1.
Step 13	**ip unnumbered gigabitethernet** *slot/port.subinterface* **Example:** `Router(config-if)# ip unnumbered gigabitethernet 0/0.20`	Enables IP processing on the gigabitethernet subinterface without assigning an explicit IP address to the subinterface. This subinterface represents the IP address of the Cisco CME router.
Step 14	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 15	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 16	**wr** **Example:** `Router# wr`	Writes the changes to the configuration file.

Testing the Installation

At this point, IP phones should no longer be connected to Cisco CME. No dial tone should be present if the speaker button is pressed.

Note If the IP phones seem as if they still have a configuration, the phones have not timed out yet.

What to Do Next

Once you configure subinterfaces for a Cisco LAN switch using Summary or Detailed Steps, proceed to configure your DHCP IP address pool for the data network (see the "Configuring a DHCP IP Address Pool for the Data Network" section on page 62).

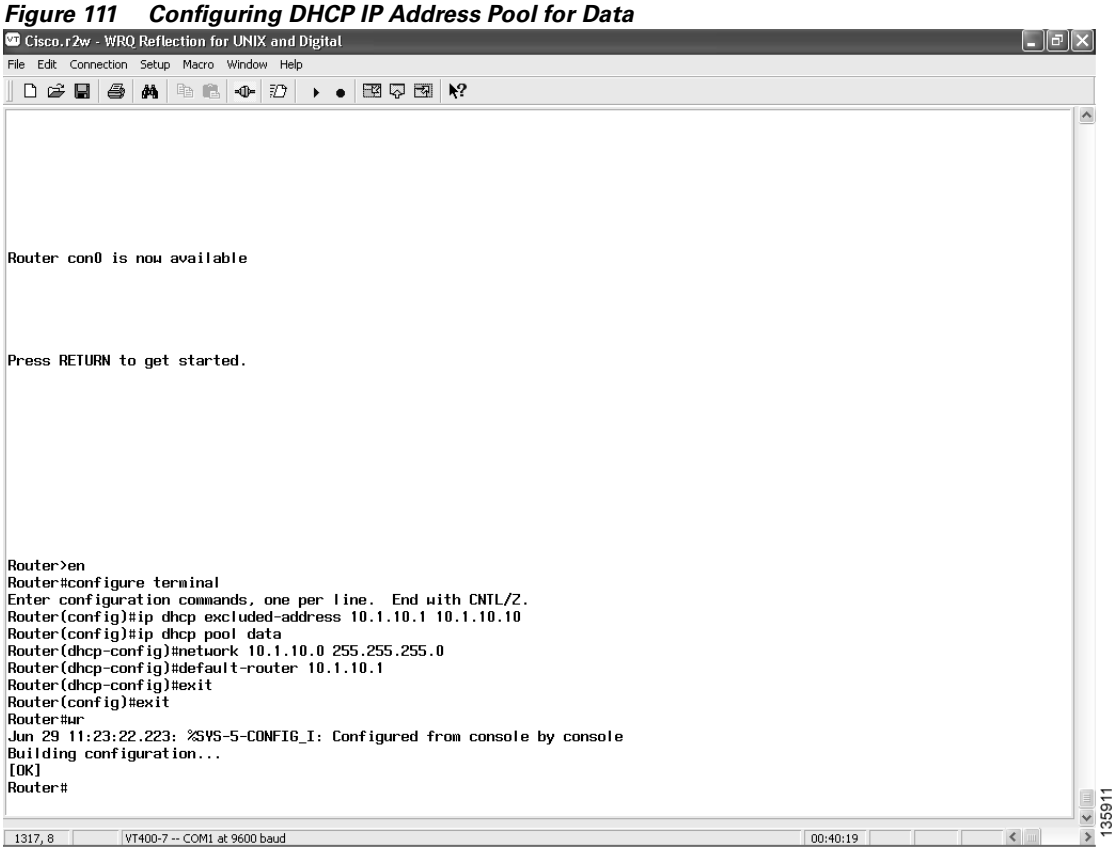
Configuring a DHCP IP Address Pool for the Data Network

This section describes the configuration of a DHCP IP address pool for your data network. If you do not already have a DHCP pool setup for your data, use this section to set up the data IP subnet.

This procedure creates a large shared pool of IP addresses, in which all DHCP clients receive the same information.

Summary steps (see Figure 111) list the steps necessary to set up a DHCP IP address pool for the data network. For detailed steps with examples, see Table 7.

Figure 111 Configuring DHCP IP Address Pool for Data



Summary Steps

1. **enable**
2. **configure terminal**
3. **ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]
4. **ip dhcp pool** *pool-name*
5. **network** *ip-address* [*mask* | */prefix-length*]
6. **default-router** *ip-address*
7. **exit**
8. **exit**

9. **wr**

Note It is recommended to save a copy of the router configuration for backup purposes.

Detailed Steps

Table 7 Detailed Steps for Configuring a DHCP IP Address Pool

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router>enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp excluded-address** *low-ip-address* [*high-ip address*] **Example:** `Router(config)# dhcp excluded-address 10.1.10.1 10.1.10.10`	Specifies IP addresses that should not be assigned to clients.
Step 4	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool data`	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.
Step 5	**network** *ip-address* [*mask* | **/***prefix-length*] **Example:** `Router(dhcp-config)# network 10.1.10.1 255.255.255.0`	Specifies the IP address of the DHCP address pool and the optional mask or number of bits in the address prefix, preceded by a forward slash.
Step 6	**default-router** *ip-address* **Example:** `Router(dhcp-config)# default-router 10.1.10.1`	Specifies the router to which the IP phones are connected. This router is either a Cisco CME router or any Cisco router attached to the Cisco CME router. **Note** As long as the Cisco IP phones have connection to the Cisco CME router, the Cisco IP phones can get the required network details.
Step 7	**exit** **Example:** `Router(dhcp-config)# exit`	Exits DHCP pool configuration mode.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 9	**wr** **Example:** `Router# wr`	Writes the changes to the configuration file.

Testing the Installation

The DHCP server is now set up for the data side of the network. Perform the following steps to ensure that DHCP is properly set up.

Step 1 Enter the **show ip dhcp server stat** command to ensure that the DHCP server is running and to display any queries made to it.

Step 2 Enter the **show ip dhcp pool** command to display configured DHCP pools.

What to Do Next

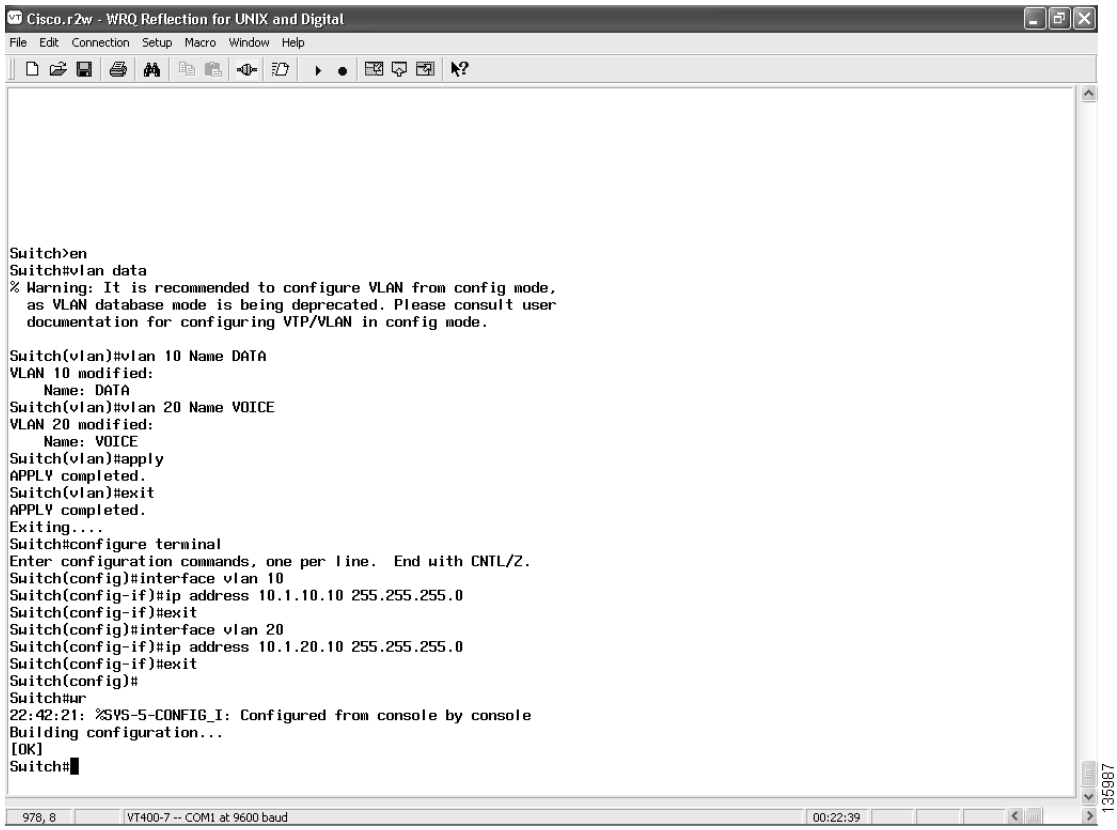
Once you configure a DHCP IP pool for the data network using the Summary or Detailed Steps, proceed to configure separate voice and data VLANs for the data network (see the "Configuring Separate Data and Voice VLANs" section on page 65).

Configuring Separate Data and Voice VLANs

It is recommended that you create separate VLANs for voice and data on your switch.

Summary steps (see Figure 112) list the steps necessary to set up separate VLANs for your voice and data networks. For detailed steps with examples, see Table 8.

Figure 112 Configuring Separate Data and Voice VLANs



Summary Steps

1. **enable**
2. **vlan data**
3. **vlan** *vlan-number* **name** *vlan-name* (for data)
4. **vlan** *vlan-number* **name** *vlan-name* (for voice)
5. **apply**
6. **exit**
7. **configure terminal**
8. **interface vlan** *vlan-number*
9. **ip address** *ip-address subnet mask*
10. **exit**
11. **interface vlan** *vlan-number*
12. **ip address** *ip-address subnet mask*
13. **exit**
14. **exit**
15. **wr**

Note It is recommended to save a copy of the switch configuration for backup purposes.

Detailed Steps

Table 8 Detailed Steps for Configuring Separate Data and Voice VLANs

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch>enable`	Enters privileged EXEC mode.
Step 2	**vlan data** **Example:** `Switch# vlan data`	Enters VLAN configuration mode and defines a string used to name the VLAN.

Step 3	**vlan** *vlan-number* **name** *vlan-name*
	
	Example:
	`Switch(vlan)# vlan 10 name DATA`
	`VLAN 10 modified`
	`Name: DATA`
		Configures the specified VLAN and defines a text string used as the name of the VLAN.

	Command or Action	Purpose

Step 4	**vlan** *vlan-number* **name** *vlan-name*
	
	Example:
	`Switch(vlan)# vlan 20 name VOICE`
	`VLAN 20 modified`
	`Name: VOICE`
		Configures the specified VLAN and defines a text string used as the name of the VLAN.

Step 5	**apply**
	
	Example:
	`Switch(vlan)# apply`
	`APPLY completed.`
		Saves changed configuration parameters.

Step 6	**exit**
	
	Example:
	`Switch(vlan)# exit`
	`APPLY completed`
	`Exiting....`
		Exits VLAN configuration mode.

Step 7	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 8	**interface** *vlan-number* **Example:** `Switch(config)# interface vlan 10`	Configures the specified interface type and enters interface configuration mode.

Step 9	**ip address** *ip-address subnet mask*
	
	Example:
	`Switch(config-if)# ip address 10.1.10.10`
	`255.255.255.0`
		Assigns an IP address to the VLAN.

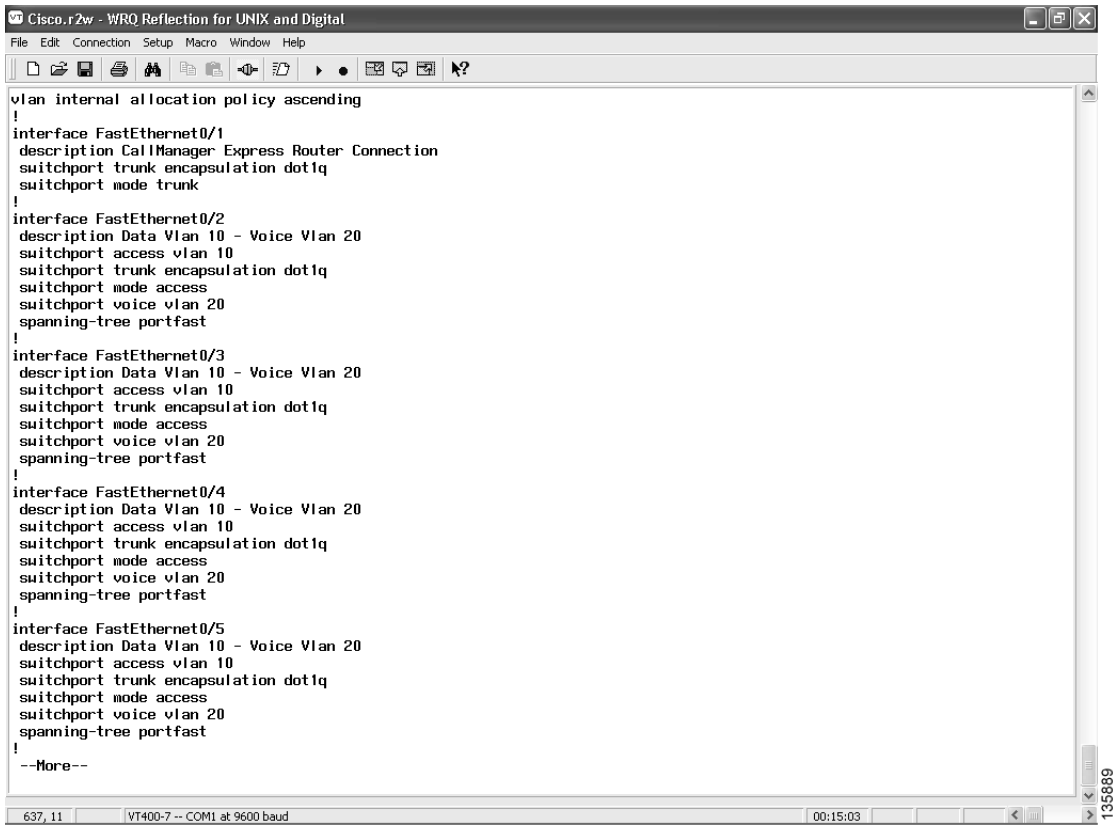
Step 10	**exit** **Example:** `Switch(config-if)# exit`	Exits interface configuration mode.
Step 11	**interface** *vlan-number* **Example:** `Switch(config)# interface vlan 20`	Configures the specified interface type and enters interface configuration mode.

Step 12	**ip address** *ip-address subnet mask*
	
	Example:
	`Switch(config-if)# ip address 10.1.20.10`
	`255.255.255.0`
		Assigns an IP address to the VLAN.

	Command or Action	Purpose
Step 13	**exit** **Example:** `Switch(config-if)# exit`	Exits interface configuration mode.
Step 14	**exit** **Example:** `Switch(config)# exit`	Exits global configuration mode.
Step 15	**wr** **Example:** `Switch# wr`	Writes the changes to the configuration file.

Figure 113 summarizes the LAN switch interface configuration.

Figure 113 LAN Switch Interface Configuration



This completes the voice network configuration.

Testing the Installation

VLANs are now configured on the switch. Use the **show interface** command to verify that the VLANs are configured. IP addresssing will not appear in any routing table until the interfaces are running.

Once the switch is configured, IP phones and stations should connect using different IP addressing.

Step 1 Enter the **ipconfig** command to see the IP configuration.

Step 2 Press **settings** on the IP phone and look for IP addressing under Network Configuration.

Step 3 Plug in multiple IP phones and initiate a call.

What to Do Next

To configure security on the voice network, see the "Configuring Security on the Voice Network" section on page 71.

Configuring Security on the Voice Network

This chapter describes the procedure for configuring security on your Cisco BCS Verified Designs network using Cisco Security Device Manager (SDM). Cisco SDM is a web-based device management tool supported on Cisco ISR routers. Cisco SDM provides smart wizards to help you add security to your voice network.

When configuring security on Cisco Business Communications Solution Verified Designs, accept all default values presented by the Cisco SDM windows. This enables a generic security level that provides basic security for the voice network.

Contents

This chapter contains the following sections:

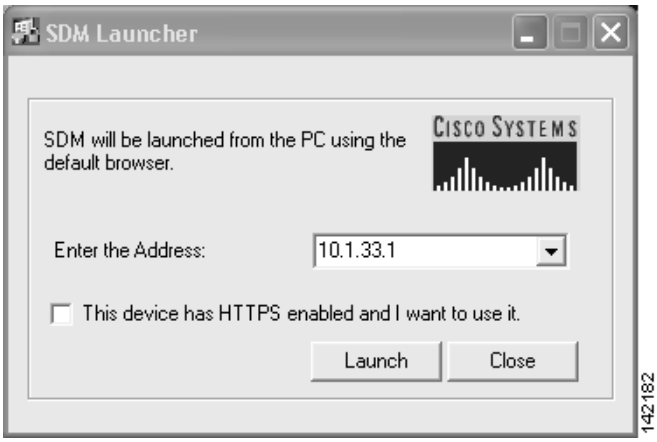
Launching Cisco SDM

Step 1 Launch Cisco SDM from the Start menu on your PC (see Figure 114):

Figure 114 Launching Cisco SDM

Step 2 When prompted, enter the IP address of your Cisco CME router (see Figure 115):

Figure 115 SDM Launcher



Step 3 Enter your SDM level-15 username and password (see Figure 116):

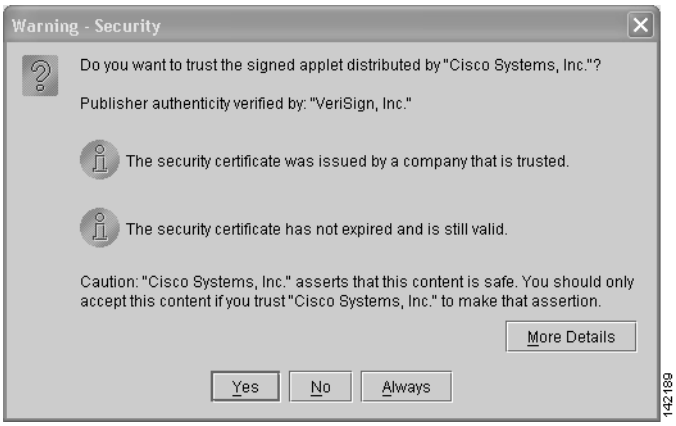
Figure 116 Level_15 Access Prompt

Note If you need to create a user account defined with privilege level 15 (enable privileges), enter the following command in global configuration mode, replacing *username* and *password* with the strings that you want to use:

Router(config)# **username** *username* **privilege 15 secret 0** *password*

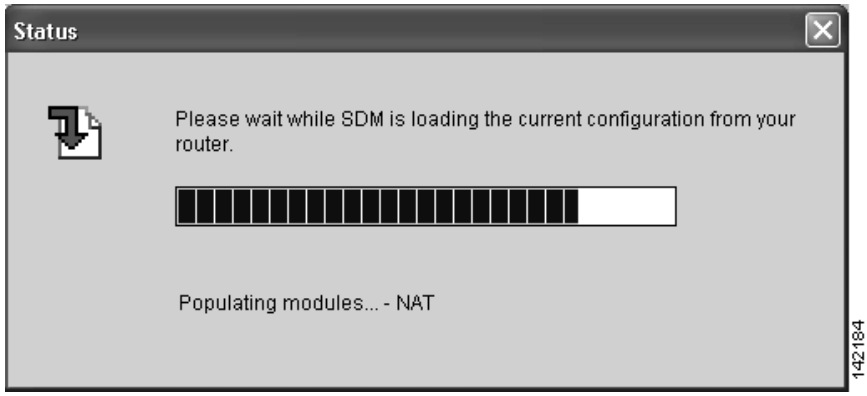
Step 4 Click **Yes** on any security warning that you receive (see Figure 117):

Figure 117 Security Warning



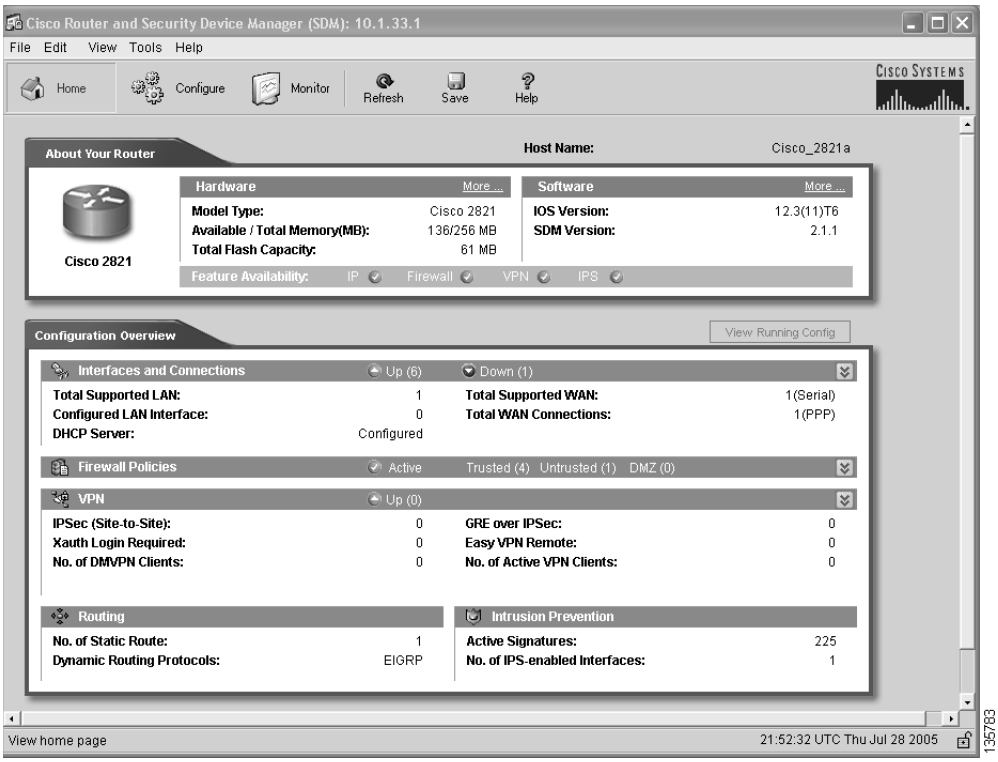
Cisco SDM downloads the current configuration (see Figure 118):

Figure 118 SDM Status Dialog



Once Cisco SDM installs, the Cisco SDM home page appears (see Figure 119):

Figure 119 SDM Home Page



Step 5 Click **Configure** on the Cisco SDM Home page menu.

The Cisco SDM task bar appears on the left (see Figure 120):

Figure 120 Cisco SDM Task Bar

Configuring Intrusion Prevention

The Intrusion Prevention System (IPS) is a Cisco SDM feature that allows you to configure signatures on the router to detect and prevent intrusive traffic on your network. The file ips.tar must be present in router flash or disk memory for IPS to run, and the Cisco IOS image on the router must support IPS.

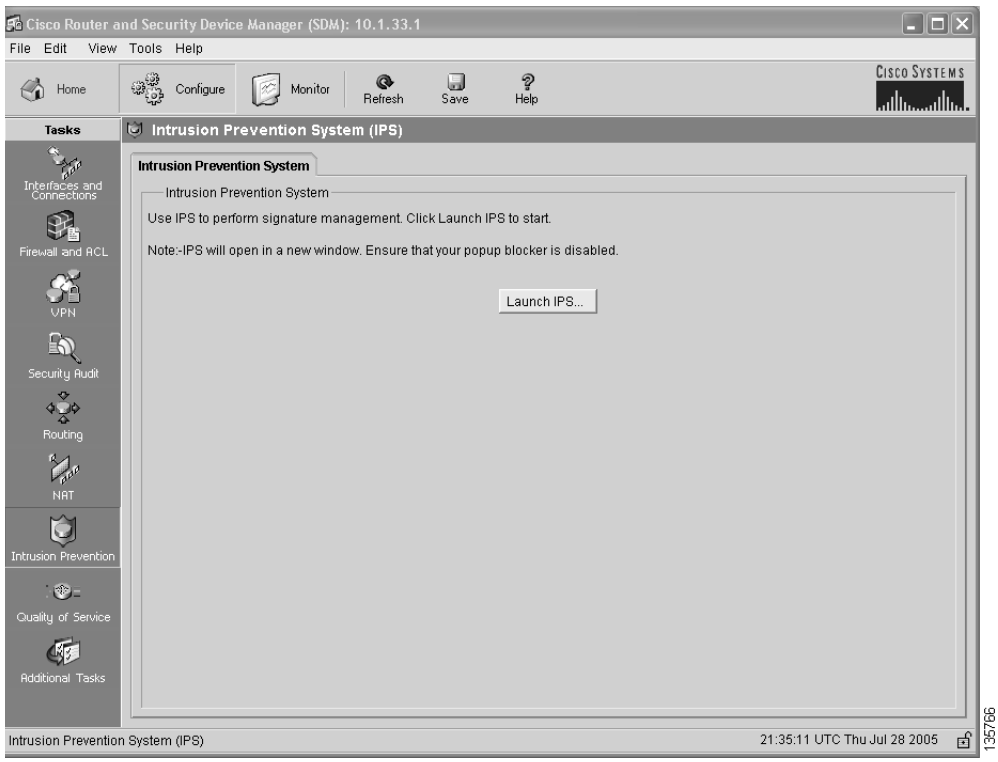
IPS allows you to selectively enable, disable, edit, and delete signatures the router uses. You can select the interfaces and traffic directions on which to apply IPS, create rules that determine which traffic is examined, import Signature Definition Files (SDFs), and specify SDF locations for the router.

Perform the following steps to configure intrusion protection for your voice network.

Step 1 Click **Intrusion Prevention** from Tasks.

The Cisco IPS window appears (see Figure 121).

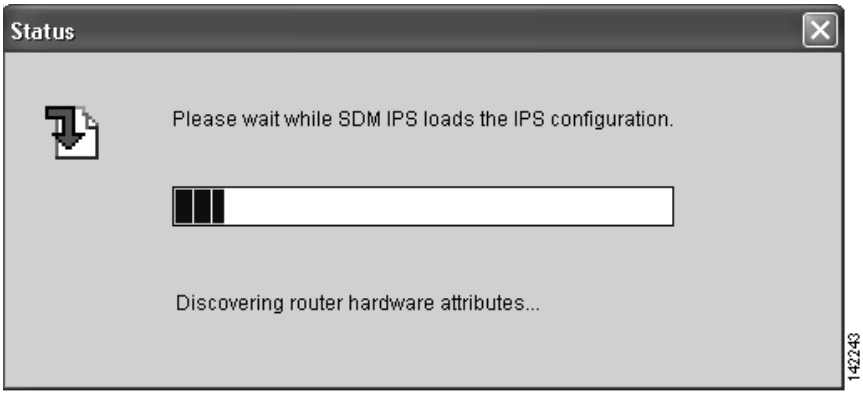
Figure 121 Cisco SDM Intrusion Prevention System



Step 2 Click **Launch IPS.**

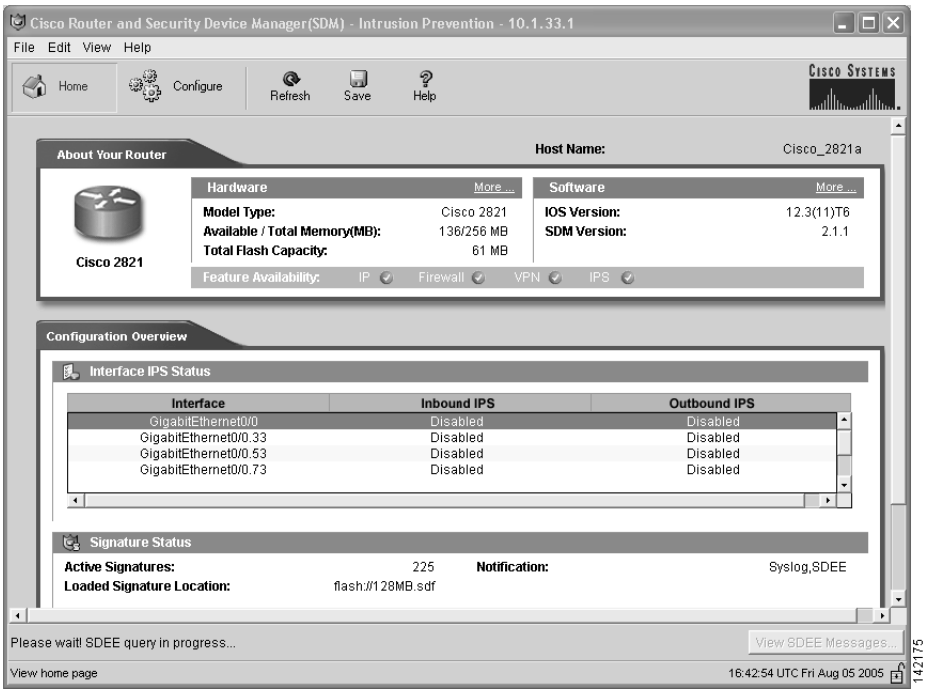
Once Cisco SDM loads the IPS configuration (see Figure 122),

Figure 122 IPS Configuration Status Message



the Cisco SDM Intrusion Prevention window appears (see Figure 123):

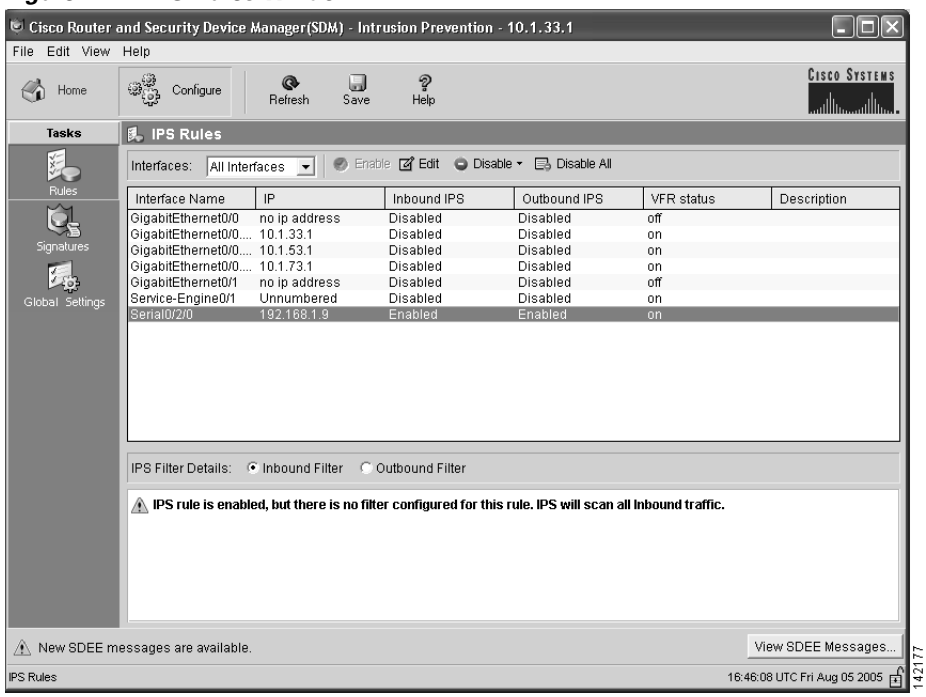
Figure 123 Cisco SDM Intrusion Prevention System



Step 3 Click **Configure**.

The IPS Rules window appears (seeFigure 124):

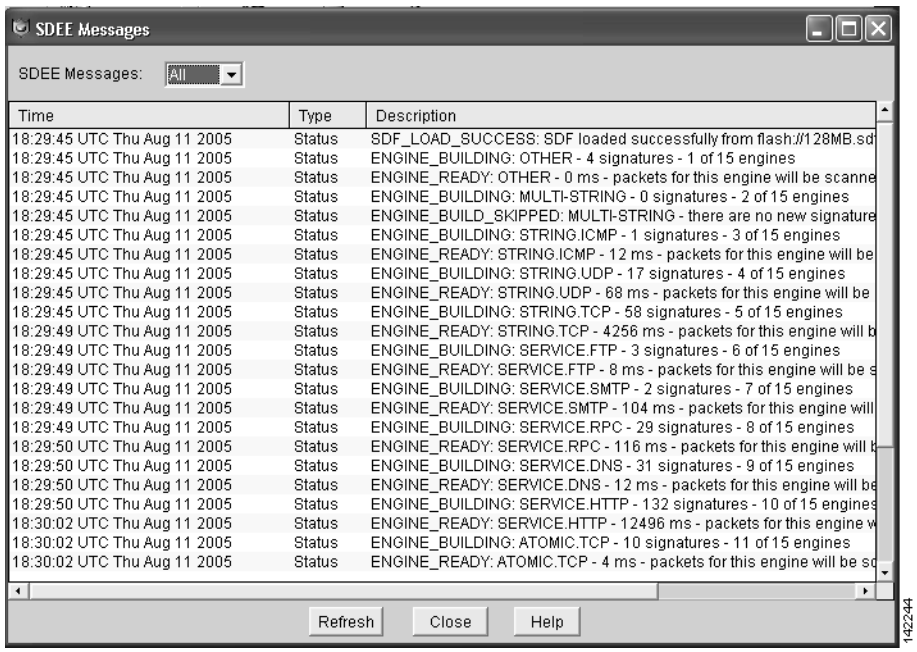
Figure 124 IPS Rules Window



The IPS Rules window automatically configures its rules set for Cisco Business Communications Solution Verified Designs.

If desired, click **View SDEE Messages** to view message (see Figure 125):

Figure 125 SDEE Messages

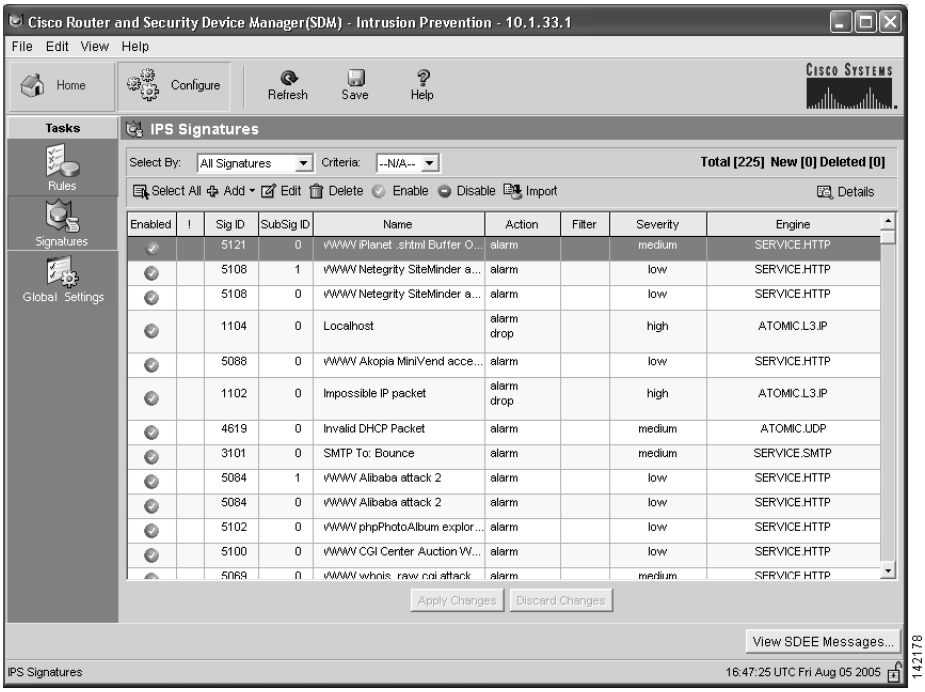


Step 4 When you finish viewing SDEE messages, click **Close**.

Step 5 Click **Signatures**.

The IPS Signatures window appears (see Figure 126):

Figure 126 IPS Signatures

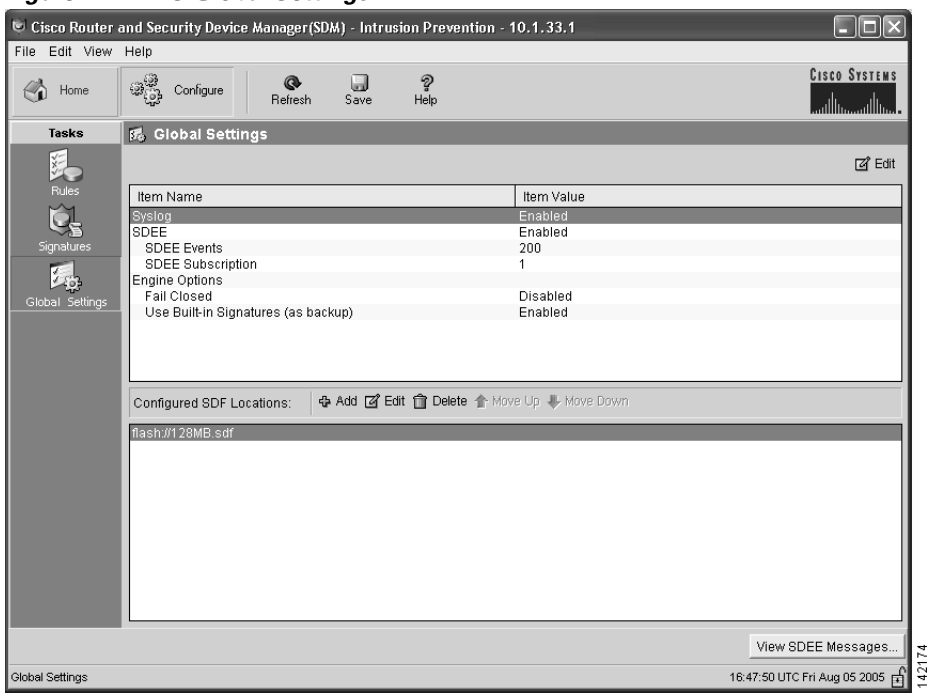


IPS Ssignatures are automatically assigned to Cisco Business Communications Solution Verified Designs.

Step 6 Click **Global Settings**.

The IPS Global Settings window appears (see Figure 127):

Figure 127 IPS Global Settings

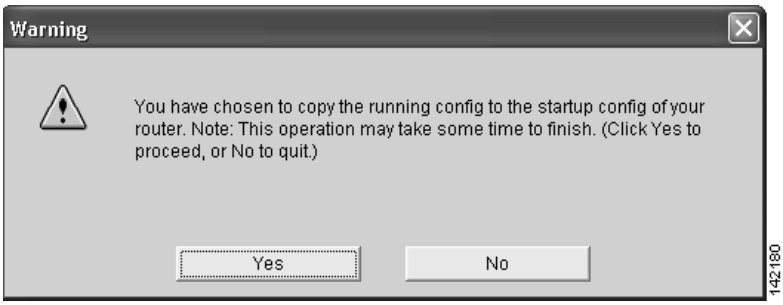


IPS global settings appear for the network.

Step 7 Click **Save**.

Step 8 Click **Yes** to copy the configuration to the router (see Figure 128):

Figure 128 Acknowledging Configuration Copying



Step 9 When you are finished with IPS, select exit from the File menu and click **Yes** to confirm your exit (see Figure 129):

Figure 129 Exiting IPS

Configuring a Basic Firewall

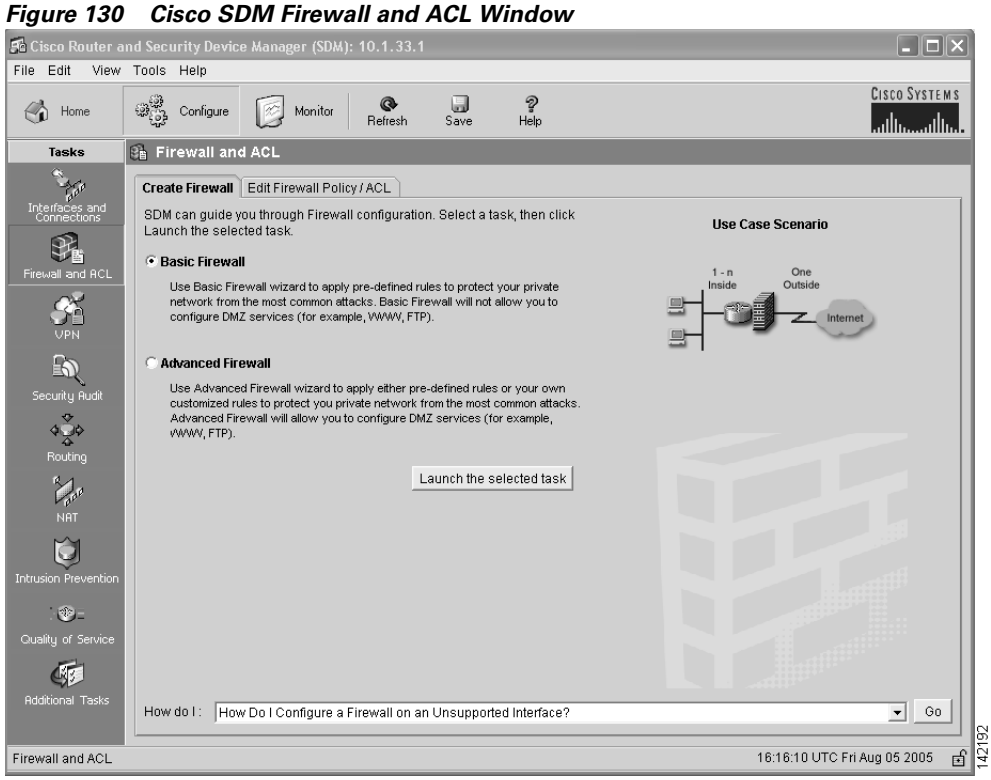
A firewall is a set of rules used to protect the resources of your LAN. These rules filter the packets arriving at the router. If a packet does not meet the criteria specified in the rule, it is dropped. If it does meet the criteria, it is allowed to pass through the interface that the rule is applied to. Cisco SDM Firewall Wizard secures your firewall by using predefined rules to protect your voice network from the most common outside attacks.

Perform the following steps to configure a basic firewall for the voice network.

Step 1 Click **Firewall and ACL** from Tasks.

The Cisco SDM Firewall and ACL window appears (see Figure 130):

Figure 130 Cisco SDM Firewall and ACL Window

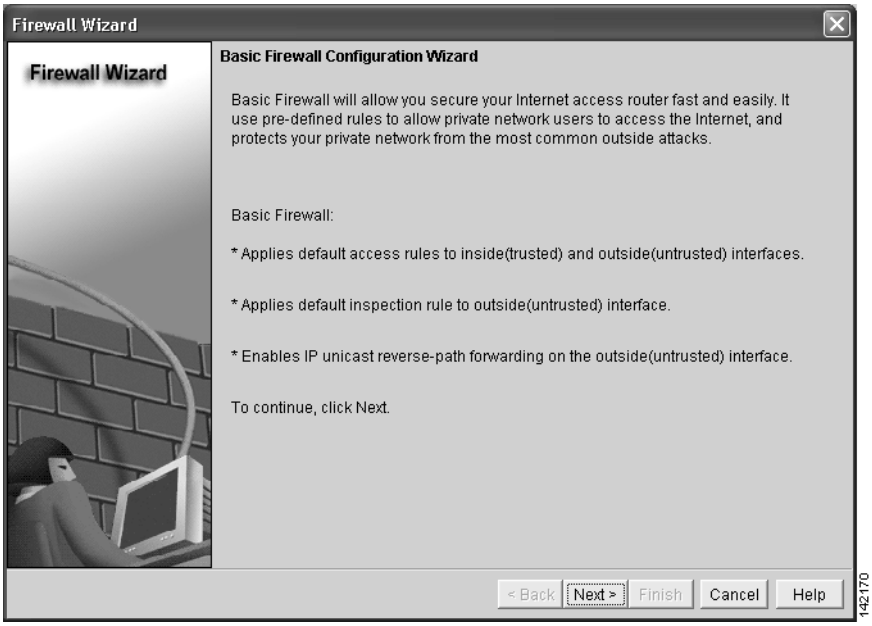


Step 2 Select **Basic Firewall**.

Step 3 Click **Launch the selected task**.

The Cisco SDM Basic Firewall Configuration Wizard window appears (see Figure 131):

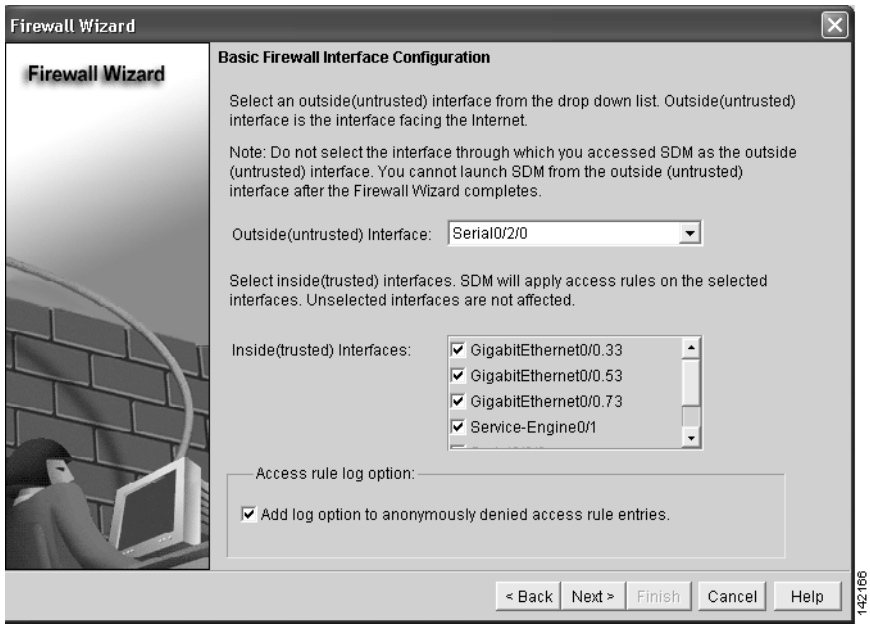
Figure 131 Cisco SDM Firewall Wizard



Step 4 Click **Next**.

The Basic Firewall Interface Configuration window appears (see Figure 132):

Figure 132 Basic Firewall Interface Configuration Window

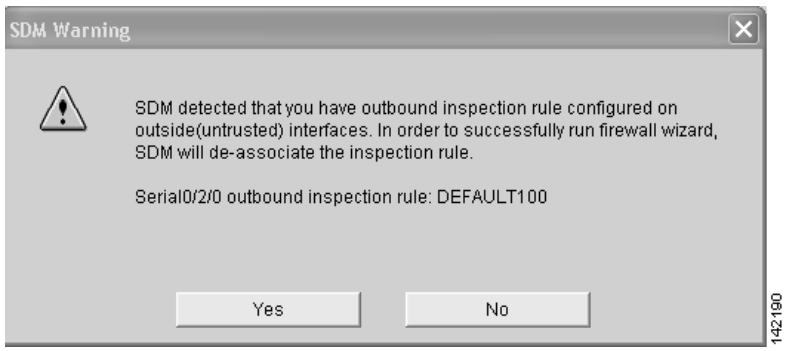


Step 5 By default, the outside untrusted interface appears in the drop-down menu.

Step 6 Click **Next**.

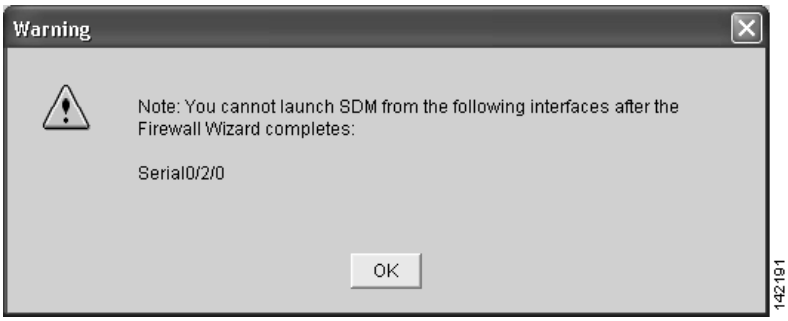
Step 7 Click **Yes** to acknowledge any warning that appears (see Figure 133):

Figure 133 Cisco SDM Detection Warning



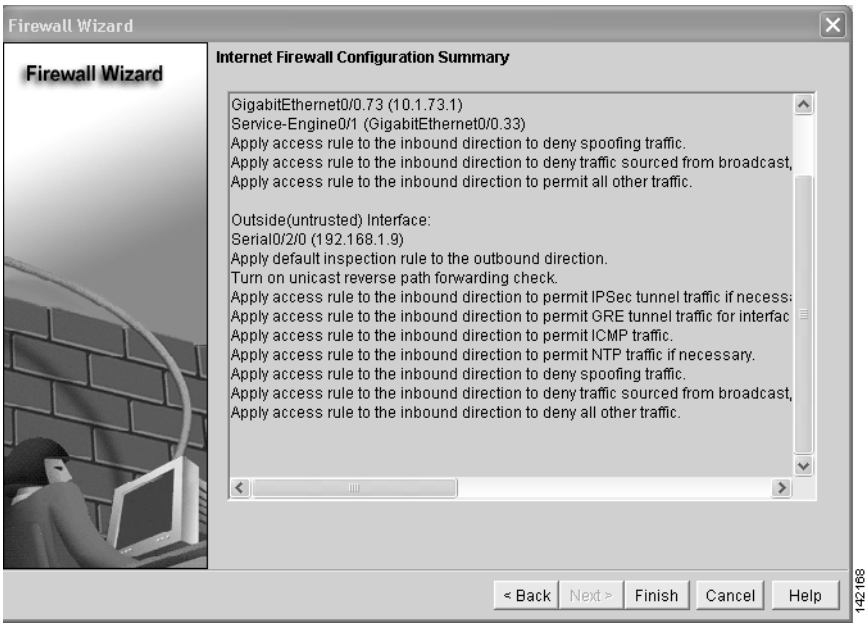
Step 8 Click **OK** to acknowledge any warning that appears (see Figure 134):

Figure 134 Cisco SDM Launch Warning



The Firewall Summary window appears (see Figure 135):

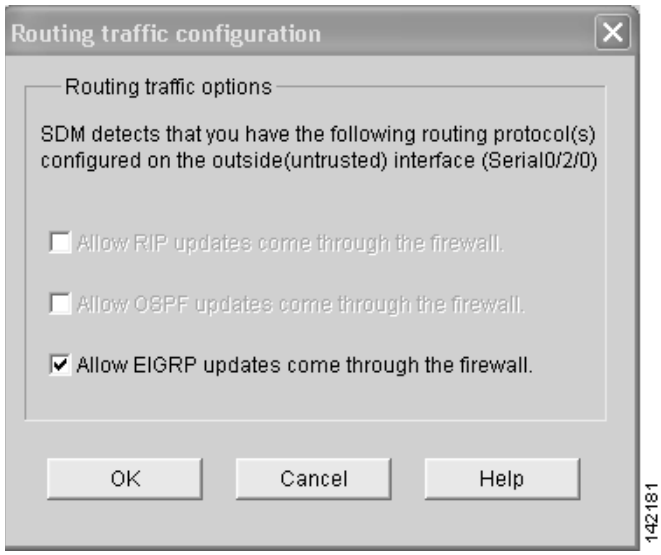
Figure 135 Cisco SDM Firewall Summary Window



Step 9 Click **Finish**.

The Routing Traffic Configuration dialog appears (see Figure 136):

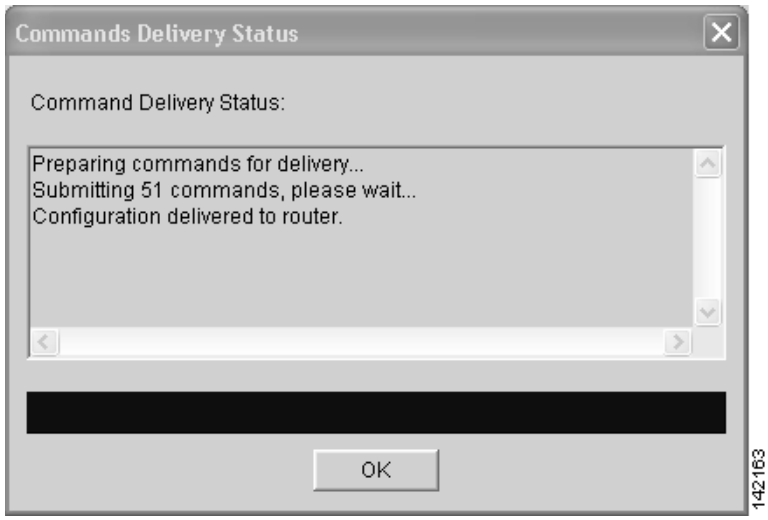
Figure 136 Routing Traffic Configuration Dialog



Step 10 Click **OK**.

The Command Delivery Status dialog appears (see Figure 137):

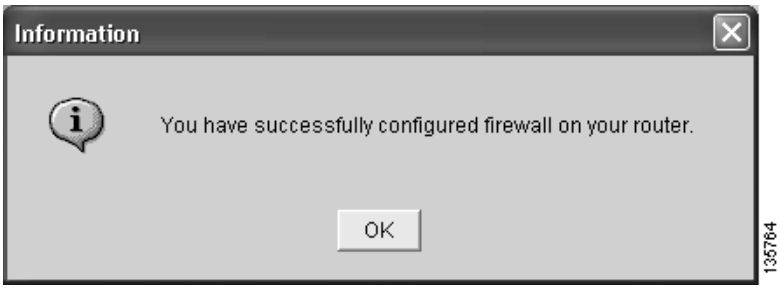
Figure 137 Command Delivery Status Dialog



Step 11 Click **OK**.

The successfully configured firewall dialog appears (see Figure 138):

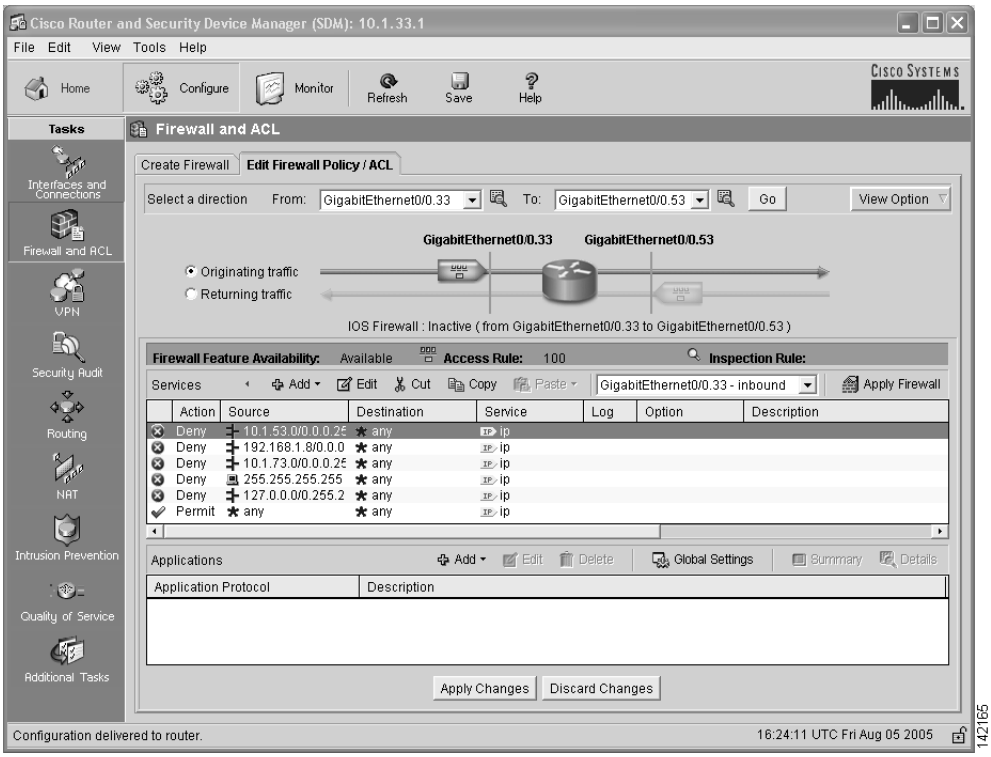
Figure 138 Successfully Configured Firewall Dialog



Step 12 Click **OK**.

The Edit Firewall Policy window appears (see Figure 139):

Figure 139 Edit Firewall Policy/ACL Window



Step 13 Click **Save** to save the firewall configuration.

Click **Yes** to acknowledge the write to startup warning (see Figure 140):

Figure 140 Cisco SDM Write to Startup Config Warning

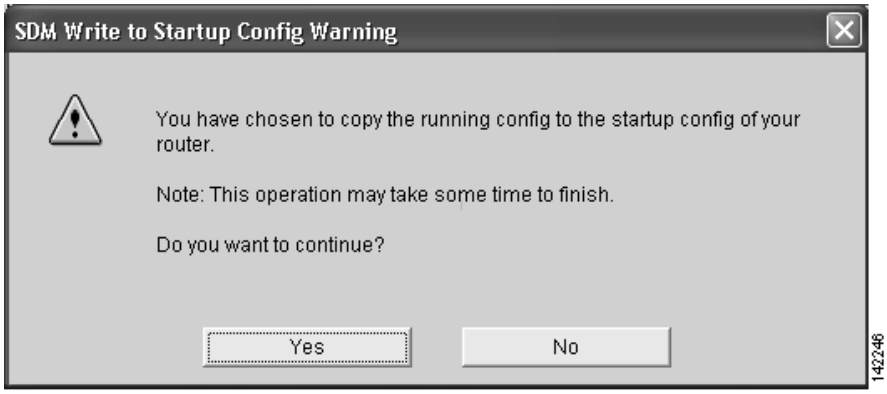
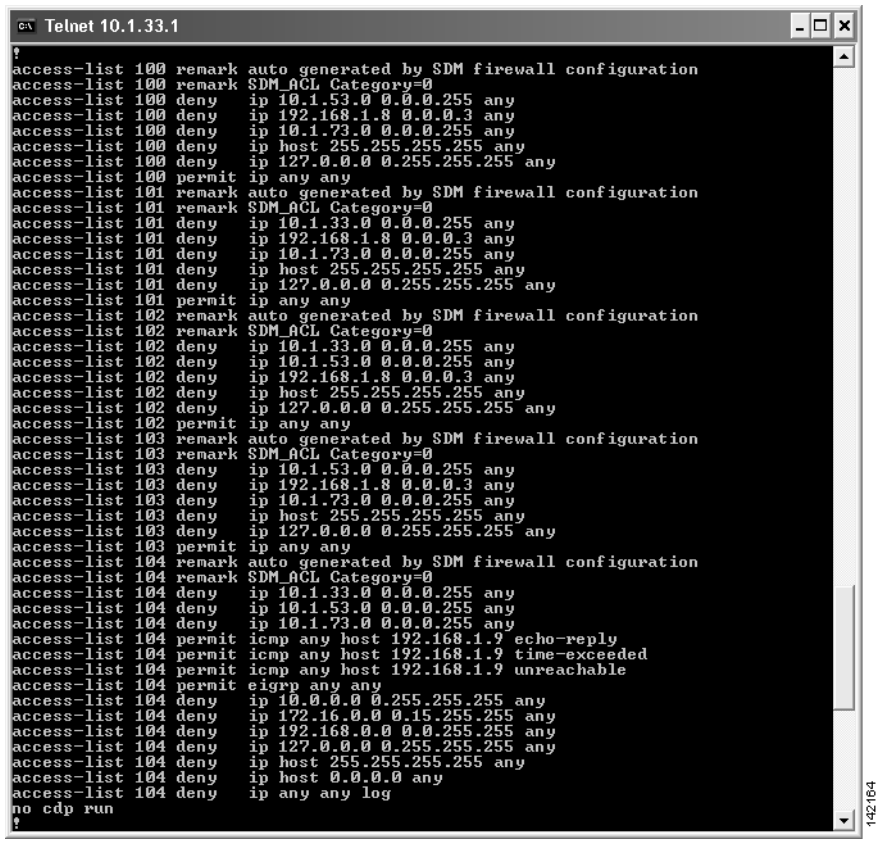


Figure 141 shows an example of the firewall configuration.

Figure 141 Firewall Configuration



Performing a Security Audit

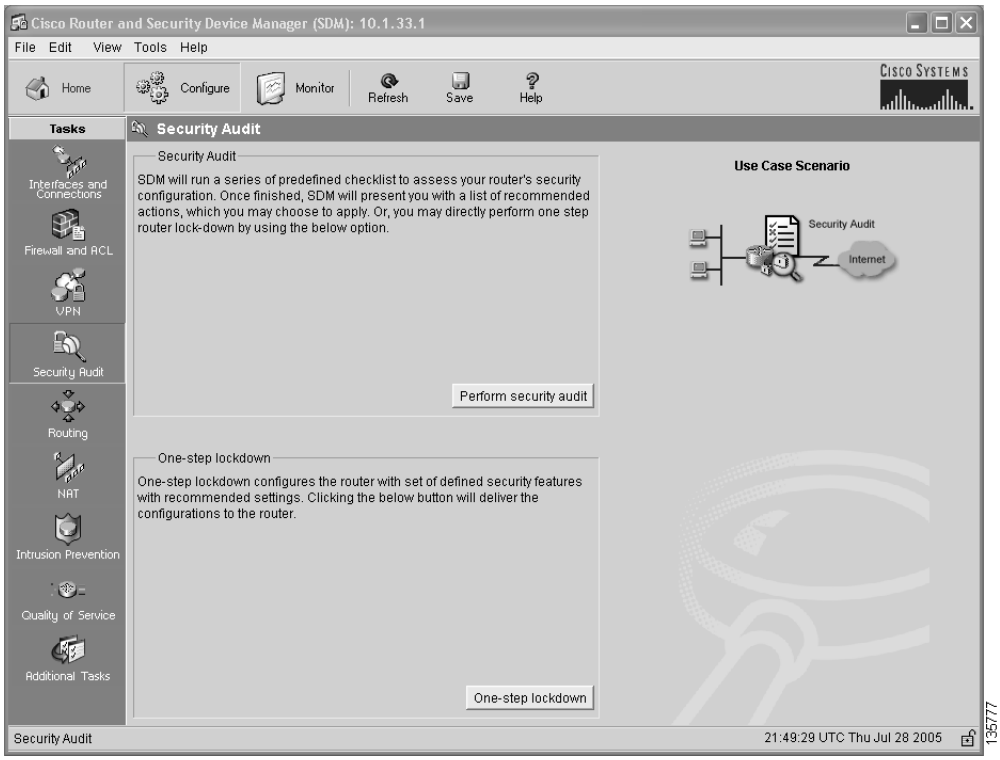
The Security Audit wizard tests your router configuration to determine if any potential security problems exist in the configuration, and then presents you with a window that lets you identify which of those security problems you want to fix. Once the problems are identified, the Security Audit wizard makes the necessary changes to the router configuration to fix those problems.

Perform the following steps to have Cisco SDM perform a security audit and then fix the problems that it finds.

Step 1 Click **Security Audit** from Tasks.

The Cisco SDM Security Audit window appears (see Figure 142):

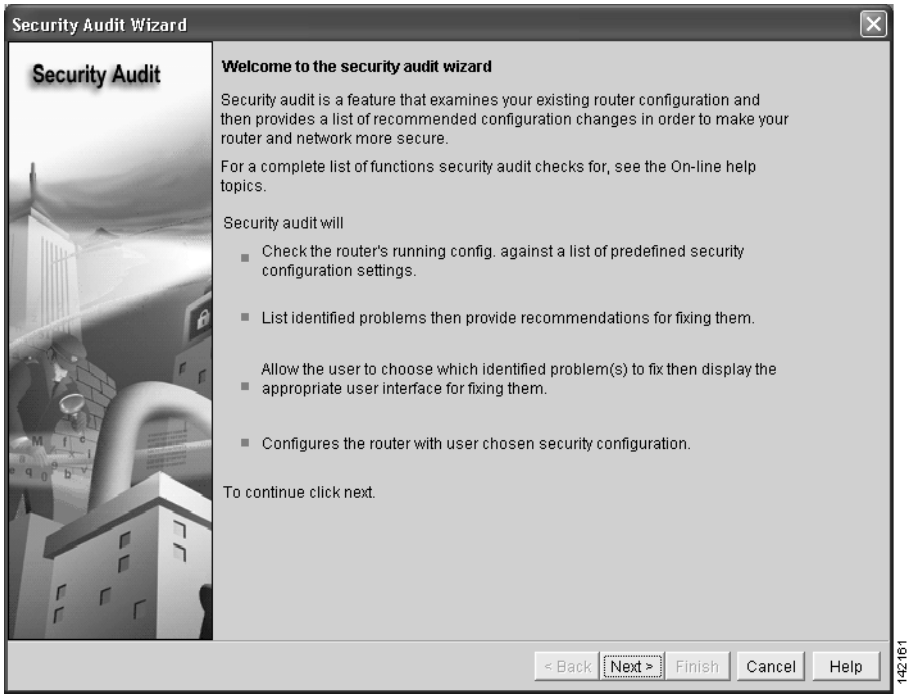
Figure 142 Cisco SDM Security Audit Window



Step 2 Click **Perform security audit**.

The Security Audit Wizard Welcome window appears (see Figure 143):

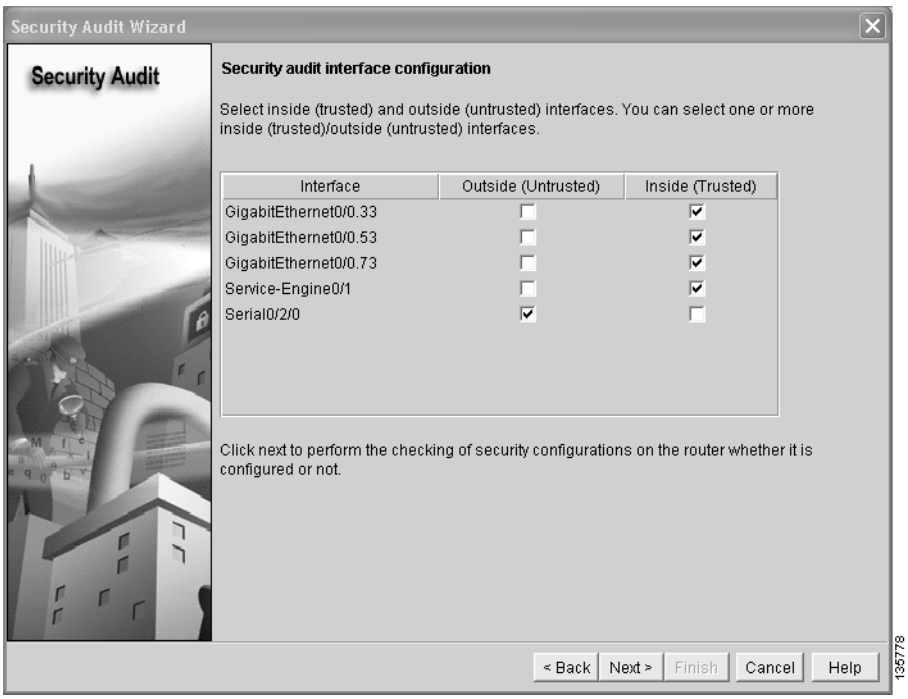
Figure 143 Cisco SDM Security Audit Wizard Welcome Window



Step 3 Click **Next**.

The Security Audit Interface Configuration window appears (see Figure 144):

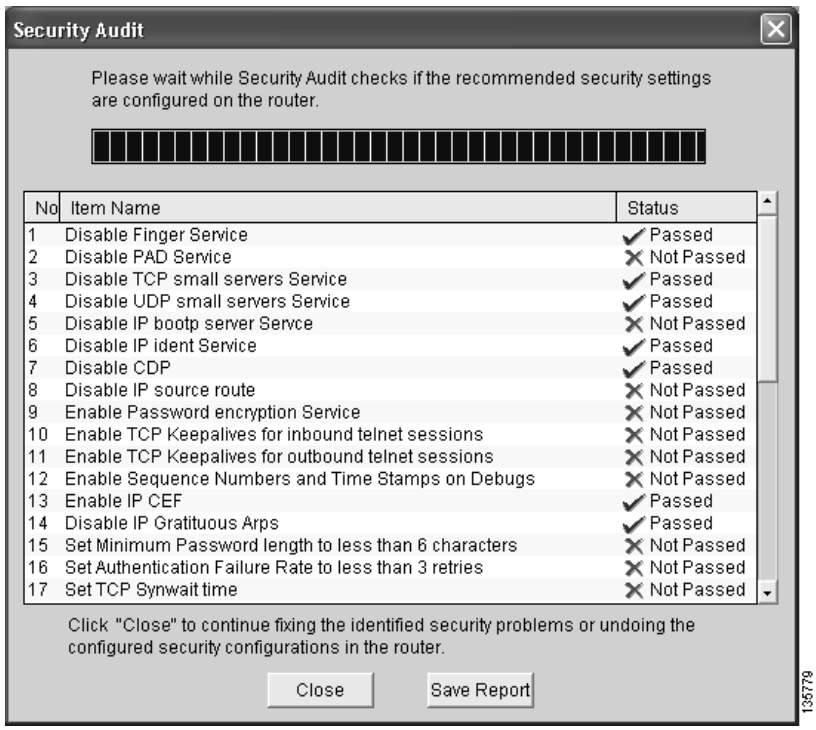
Figure 144 Cisco Security Audit Interface Configuration Window



Step 4 Click **Next**.

The Security Audit wizard tests your router configuration to determine which possible security problems may exist. A window showing the progress of this action appears (see Figure 145), listing all of the configuration options being tested, and whether the current router configuration passes those tests.

Figure 145 Security Audit Actions

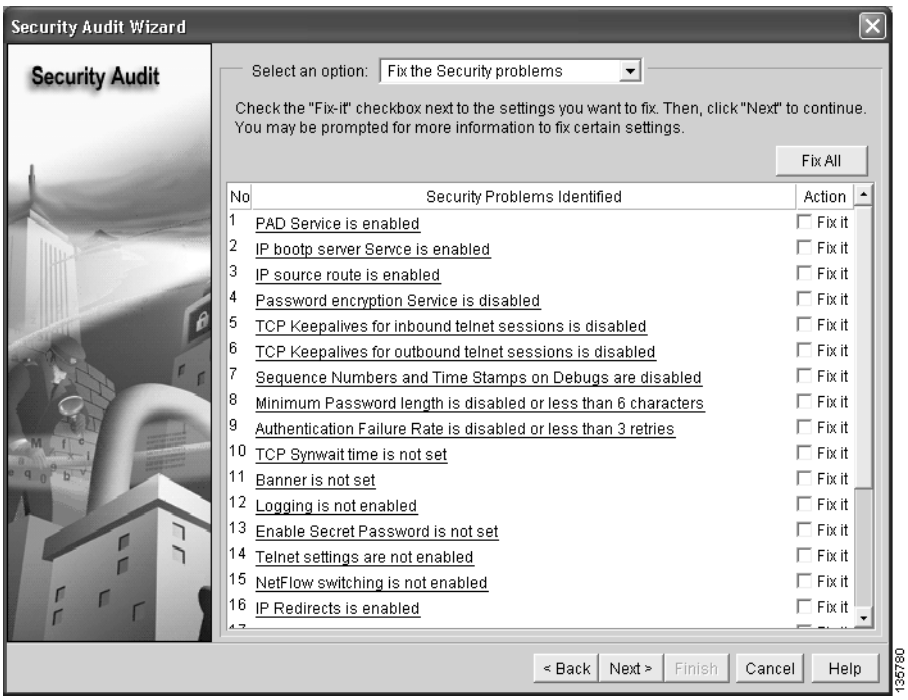


If you want to save this report to a file, click **Save Report**.

Step 5 Click **Close**.

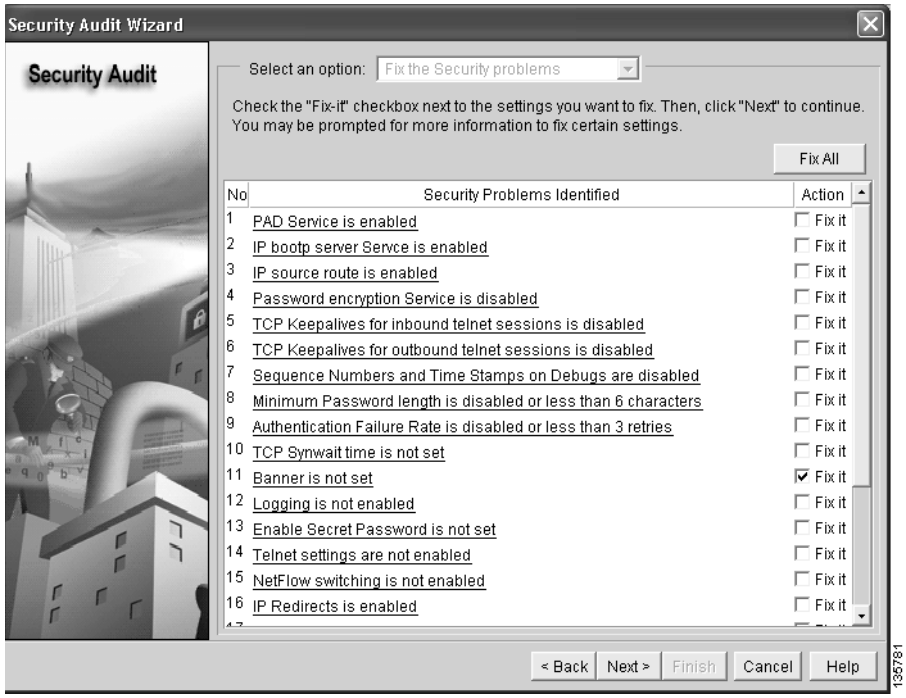
The Security Audit Report Card window appears, showing a list of possible security problems (see Figure 146):

Figure 146 Cisco Security Audit Report Card



Step 6 Check the Fix it check boxes next to any problems that you want Cisco SDM to fix (see Figure 147). For a description of the problem and a list of the Cisco IOS commands that will be added to your configuration, click the problem description to display a help page about that problem.

Figure 147 Cisco SDM Fix It Boxes



Step 7 Click **Next**.

Step 8 The Security Audit wizard may display one or more windows requiring you to enter information to fix certain problems. Enter the information as required and click **Next** for each of those windows. For more information on security audit fix it procedures, see the Security Audit chapter of the Cisco SDM User's Guide.

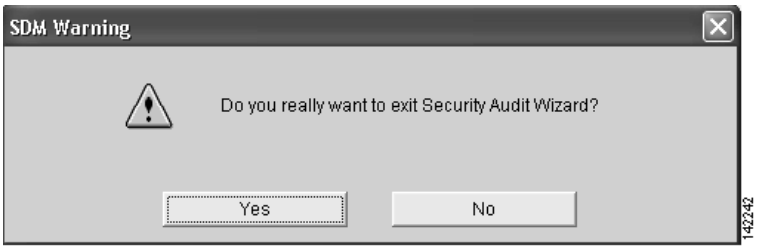
The Summary page shows a list of all the configuration changes that Security Audit will make.

Step 9 Click **Finish** to deliver those changes to your router.

Security is now configured on the voice network.

Step 10 Click **Yes** to exit Security Audit Wizard (see Figure 148):

Figure 148 Exiting Security Audit Wizard



The installation of Cisco BCS Verified Designs is now finished.

Appendix A: Cisco CallManager Express Bundles

Use this appendix to determine the number of IP phones supported by Cisco voice bundles.

See Cisco CallManager Express Bundles at:

http://www.cisco.com/en/US/netsol/ns339/ns395/ns359/ns331/netbr09186a0080201ec8.html.

Appendix B: QCT Utilities

This appendix describes QCT utilities.

QCT utilities allow you to perform the following operations:

- Uploading Saved Configurations, page 97
- Configuring QCT Options, page 99

Uploading Saved Configurations

QCT allows you to upload previously-saved router configurations. Using QCT, you can browse to a locally-stored router configuration file on your PC and download it to any router.

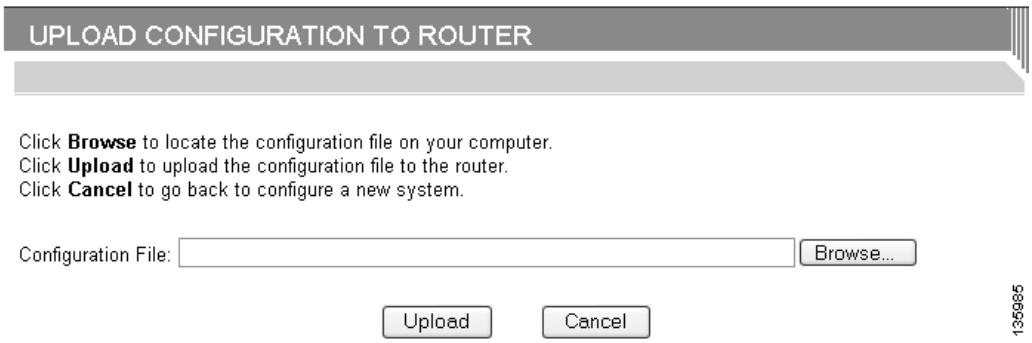
To upload a saved configuration to your router, perform the following steps.

Step 1 Click **Upload Saved Config** (see Figure 149):

Figure 149 Upload Saved Config Button

The Upload Configuration to Router window appears (see Figure 150):

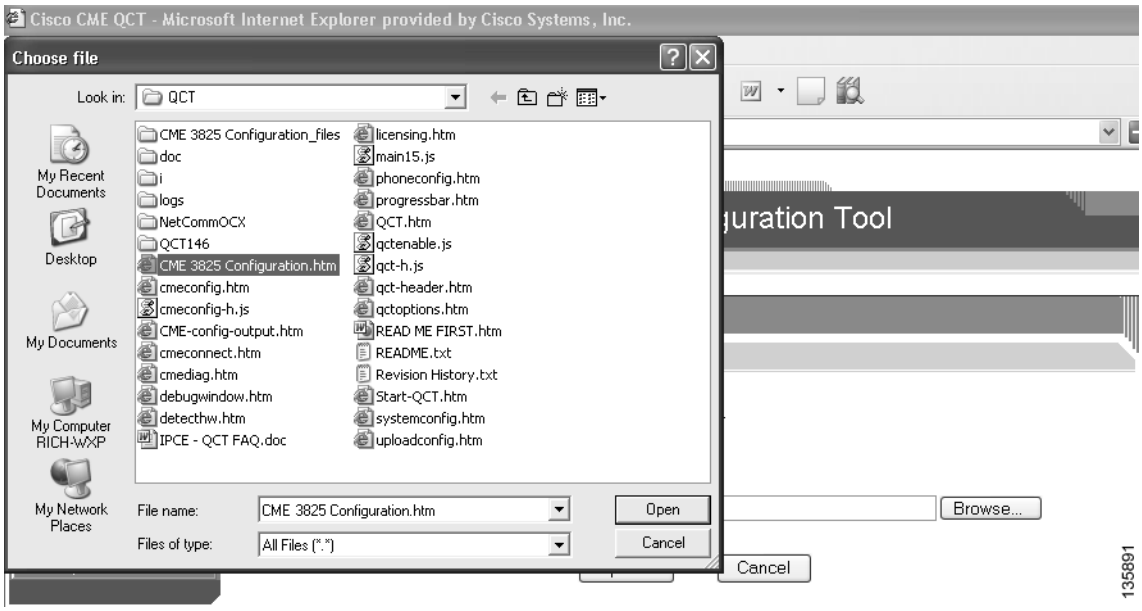
Figure 150 Upload Configuration Window



Step 2 Click **Browse** to locate the configuration file on your PC.

Step 3 In the Choose File dialog that appears, browse to the file's location on your PC and select the configuration file (see Figure 151):

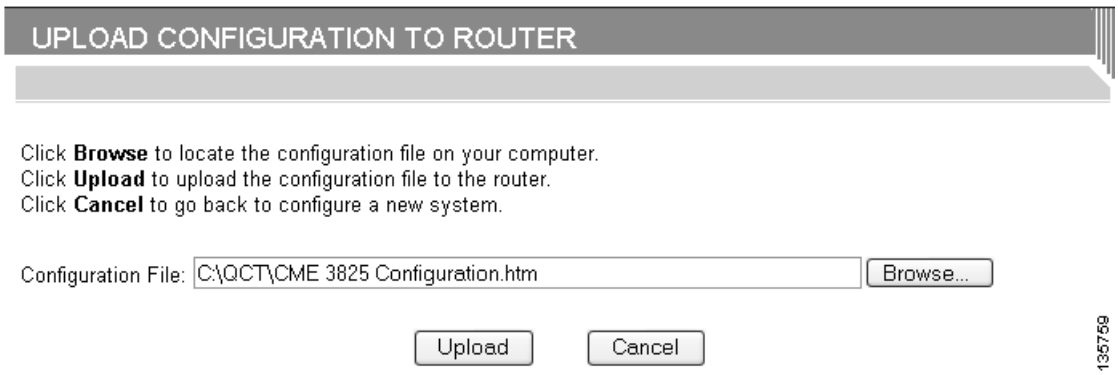
Figure 151 Upload Choose File Dialog



Step 4 Click **Open**.

The Configuration File field in the Upload Configuration to Router window's shows the file path that you chose (see Figure 152):

Figure 152 Upload Configuration File Path



Step 5 Ensure that your router is powered on.

Step 6 Click **Upload**.

Your router loads with the new configuration.

Configuring QCT Options

The QCT Options window allows you to enable specific diagnostics for your system.

Note Any enabled QCT option will be valid only until you create a new system.

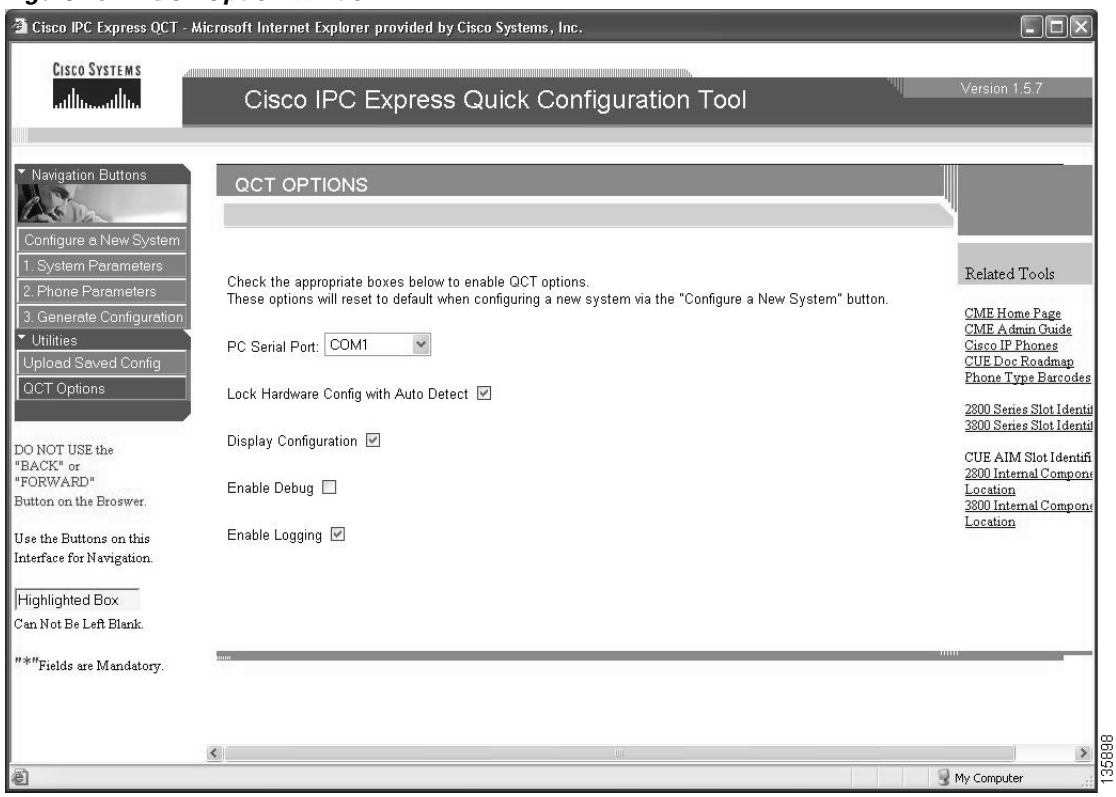
Perform the following steps to configure QCT options.

Step 1 Click the **QCT Options** button (see Figure 153):

Figure 153 QCT Options Button

The QCT Options window appears (see Figure 154):

Figure 154 QCT Option Window

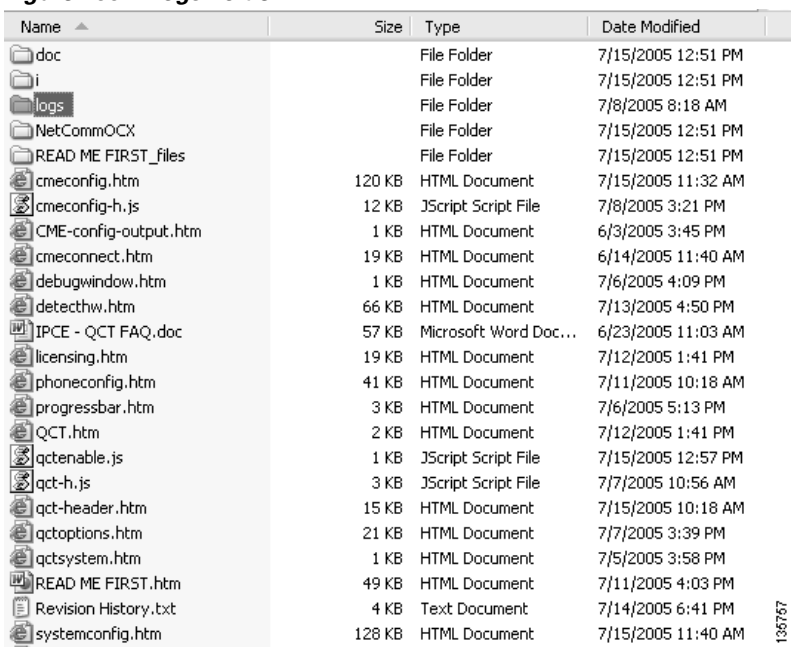


Step 2 Enter the information listed in Table 9.

Table 9 Cisco QCT Options Field Descriptions

Field Name	Enter or Specify	Purpose
PC Serial Port	The PC serial COM port from the drop-down menu.	Allows communications to Cisco IPC Communications Express system.
Lock Hardware Configuration with Auto Detect	• To enable any QCT option, enter a check in the appropriate check box. • To leave any QCT option disabled, leave the appropriate check box blank.	After auto-detecting hardware using the Auto Detect Hardware Configuration button, deselecting this checkbox allows changes to the Hardware Configuration section on the System Parameters window.
Display Configuration		Enables the display of the configuration on your PC when the Generate Configuration button is pressed.
Enable Debug		Enables debugging after pushing configuration to router.
Enable Logging		Enables logging after pushing configuration to router. Log information is stored in a folder named logs inside your locally installed QCT folder (see Figure 155).

Figure 155 Logs Folder



Name	Size	Type	Date Modified
doc		File Folder	7/15/2005 12:51 PM
i		File Folder	7/15/2005 12:51 PM
logs		File Folder	7/8/2005 8:18 AM
NetCommOCX		File Folder	7/15/2005 12:51 PM
READ ME FIRST_files		File Folder	7/15/2005 12:51 PM
cmeconfig.htm	120 KB	HTML Document	7/15/2005 11:32 AM
cmeconfig-h.js	12 KB	JScript Script File	7/8/2005 3:21 PM
CME-config-output.htm	1 KB	HTML Document	6/3/2005 3:45 PM
cmeconnect.htm	19 KB	HTML Document	6/14/2005 11:40 AM
debugwindow.htm	1 KB	HTML Document	7/6/2005 4:09 PM
detecthw.htm	66 KB	HTML Document	7/13/2005 4:50 PM
IPCE - QCT FAQ.doc	57 KB	Microsoft Word Doc...	6/23/2005 11:03 AM
licensing.htm	19 KB	HTML Document	7/12/2005 1:41 PM
phoneconfig.htm	41 KB	HTML Document	7/11/2005 10:18 AM
progressbar.htm	3 KB	HTML Document	7/6/2005 5:13 PM
QCT.htm	2 KB	HTML Document	7/12/2005 1:41 PM
qctenable.js	1 KB	JScript Script File	7/15/2005 12:57 PM
qct-h.js	3 KB	JScript Script File	7/7/2005 10:56 AM
qct-header.htm	15 KB	HTML Document	7/15/2005 10:18 AM
qctoptions.htm	21 KB	HTML Document	7/7/2005 3:39 PM
qctsystem.htm	1 KB	HTML Document	7/5/2005 3:58 PM
READ ME FIRST.htm	49 KB	HTML Document	7/11/2005 4:03 PM
Revision History.txt	4 KB	Text Document	7/14/2005 6:41 PM
systemconfig.htm	128 KB	HTML Document	7/15/2005 11:40 AM

135757

Appendix C: Cisco BCS Verified Designs Configuration Example

This appendix shows an example of a Cisco BCS Verified Designs configuration file. Descriptive statements are included for each subsection in the configuration file.

```
Building configuration...

Current configuration : 11927 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Cisco_2801a
!
boot-start-marker
boot system flash:c2801-ipvoice-mz.123_11_T6.bin
boot system flash:
boot system flash:c2801-spservicek9-mz.2005-05-16.ESE_20050516_123_11_T6.bin
boot system flash:
boot-end-marker
!
enable password cisco
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmisnmp-timeout 180
no aaa new-model
ip subnet-zero
ip cef
!
!
ip dhcp excluded-address 10.1.31.1 10.1.31.20
ip dhcp excluded-address 10.1.51.1 10.1.51.20
ip dhcp excluded-address 10.1.71.1 10.1.71.20
!
! The commands below define DHCP for data, voice, and wireless LAN. Option 150 should point to voice mail.
!
ip dhcp pool Data
   network 10.1.31.0 255.255.255.0
   default-router 10.1.31.1
!
ip dhcp pool Voice
   network 10.1.51.0 255.255.255.0
   default-router 10.1.51.1
   option 150 ip 10.1.51.1
!
ip dhcp pool WLAN
   network 10.1.71.0 255.255.255.0
   default-router 10.1.71.1
!
!
no ip domain lookup
no ftp-server write-enable
!
```

```
!
!
! The statements below enable H.323 to H.323, H.323 to SIP, in Cisco IOS software so that
H.323 calls to IP phones at this site can roll over to voice mail.

voice service voip
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 supplementary-service h450.12
 h323
! Translation rules manipulate digits of calling- or called-numbers (depending on how they
are referred to in the subsequent "voice translation-profile" command).

! Translation rules use regular expressions to state what numbers, or patterns, should be
substituted for what other numbers and can be much more sophisticated than the basic ones
used below.

voice translation-rule 101
 rule 1 /^101/ /1/
 rule 2 /^202/ /2/
 rule 3 /^252/ /2/
 rule 4 /^303/ /3/
 rule 5 /^353/ /3/
 rule 6 /^404/ /4/
 rule 7 /^454/ /4/
 rule 8 /^505/ /5/
 rule 9 /^555/ /5/
!
!
voice translation-profile 101
 translate called 101
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.1.10.2 255.255.255.255
 h323-gateway voip interface
h323-gateway voip bind srcaddr 10.1.10.1
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.31
 encapsulation dot1Q 31
 ip address 10.1.31.1 255.255.255.0
!
interface FastEthernet0/0.51
 encapsulation dot1Q 51
 ip address 10.1.51.1 255.255.255.0
!
interface FastEthernet0/0.71
 encapsulation dot1Q 71
 ip address 10.1.71.1 255.255.255.0
!
```

```
interface Service-Engine0/0
 ip unnumbered FastEthernet0/0.31
 service-module ip address 10.1.31.2 255.255.255.0
 service-module ip default-gateway 10.1.31.1
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
speed auto
!
interface Serial0/3/0
bandwidth 512
 ip address 192.168.1.2 255.255.255.252
 encapsulation frame-relay
!
router eigrp 100
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
ip classless
!
!
ip http server
no ip http secure-server
ip http path flash:
!
! The statements below define the TFTP server for the IP phone loads.
!
tftp-server flash:ATA030100SCCP040211A.zup
tftp-server flash:CP7902040000SCCP040701A.sbin
tftp-server flash:CP7905040000SCCP040701A.sbin
tftp-server flash:P00403020214.bin
tftp-server flash:CP7912040000SCCP040701A.sbin
tftp-server flash:S00103020002.bin
tftp-server flash:P00503010100.bin
tftp-server flash:cmterm_7936.3-3-5-0.bin
tftp-server flash:P00303020214.bin
tftp-server flash:P00305000301.sbn
tftp-server flash:cmterm_7920.3.3-01-08.bin
!
control-plane
!
!
!
voice-port 0/3/0
!
voice-port 0/3/1
!
sccp local FastEthernet0/0.31
sccp ccm 10.1.31.1 identifier 1
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register mtp001121fb0366
!
```

```
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec gsmfr
 maximum sessions 5
 associate application SCCP
!
! 1 is the Cisco Unity Express pilot number and 1980 is the voice-mail pilot number. Calls
to these numbers are directed via SIP to Cisco Unity Express at its IP address. The
translation rule defined earlier is used here to translate DID numbers to the extensions
before the call is routed to Cisco Unity Express. DTMF relay to Cisco Unity Express must
be via SIP-Notify, and G.711 "no vad" must be configured on this dial-peer.
!
dial-peer voice 1 voip
 description ** cue voicemail pilot number **
 destination-pattern 1480
 session protocol sipv2
 session target ipv4:10.1.31.2
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!

dial-peer voice 2 voip
 description ** cue auto attendant number **
 destination-pattern 1490
 session protocol sipv2
 session target ipv4:10.1.31.2
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!

dial-peer voice 102 voip
 description Call to Cisco_2811a
 translation-profile outgoing 101
 destination-pattern 15....
 session target ipv4:10.1.32.1
 dtmf-relay h245-alphanumeric
!

dial-peer voice 103 voip
 description Call to Cisco_2821a
 translation-profile outgoing 101
 destination-pattern 20....
 session target ipv4:10.1.33.1
 dtmf-relay h245-alphanumeric
!

dial-peer voice 106 voip
 description Call to Cisco_2851a
 translation-profile outgoing 101
 destination-pattern 35....
 session target ipv4:10.1.36.1
 dtmf-relay h245-alphanumeric
!
```

```
dial-peer voice 108 voip
 description Call to Cisco_3825a
translation-profile outgoing 101
 destination-pattern 45....
 session target ipv4:10.1.38.1
 dtmf-relay h245-alphanumeric
codec g771ulaw
!

dial-peer voice 104 voip
 description Call to Callmanager
 translation-profile outgoing 101
 destination-pattern 25....
 session target ipv4:10.1.33.97
 dtmf-relay h245-alphanumeric
no vad
!

dial-peer voice 4980 voip
 description Unity Voice Mail
 destination-pattern 4980
 session target ipv4:10.1.38.1
 dtmf-relay h245-alphanumeric
!
! The commands below following the "telephony-service" keyword is the main Cisco CME
configuration for this  router. Key considerations include the following:
! - The "load" command associates a type of Cisco IP phone with a phone firmware file.
! - The "max-ephones" and "max-dn" commands specify the maximum number of phones and
extensions supported on this system.
! - The "source-address" provides the IP address and port through which IP phones
communicate with the Cisco CME router.
! - The "system message" ??.
! - The "sdspfarm" commands ??.
! - The "create cnf-files" command generates the XML configuration  files required for IP
phones.
! - The "voicemail" command defines the voice mail pilot number as 1480.
! - The "max-conferences" command specifies that the maximum  number of three-party
conferences simultaneously supported by this Cisco CME system is eight.
! - The "web admin" commands define the Cisco CME system administrator and customer
administrator accounts.
! - The "dn-webedit" and "time-webedit" commands enable the ability to add extensions
(ephone-dns) and allow
! - The "transfer-system" command defines the types of  transfer (blind and consult)
supported by the Cisco CME system.
! - The "secondary dialtone" command defines the ?? by the Cisco CME system.

telephony-service
 load 7960-7940 P00303020214
 load 7920 cmterm_7920.3.3-01-08.bin
load 7912 CP7912040000SCCP040701A.sbin
 max-ephones 24
 max-dn 72
 ip source-address 10.1.31.1 port 2000
 system message CME on 2801
 sdspfarm units 5
 sdspfarm transcode sessions 10
 sdspfarm tag 1 mtp001121fb0366
 create cnf-files version-stamp Jan 01 2002 00:00:00
 voicemail 1480
 max-conferences 8
 web admin system name cmeadmin password cmeadmin
 dn-webedit
 time-webedit
```

```
 transfer-system full-consult
 secondary-dialtone 9
!
!
! The definitions of the Cisco CME IP phone extensions (ephone-dn) start below. Key
considerations include the following:
! - The "dual-line" designation ensures that transfers and conferences can be done on the
phone.
! - The "number" keyword provides the extension digits, and the "secondary" field ensures
that DID numbers for this extension are also matched to this ephone-dn.
! - The "name" keyword provides the name that will be used on the phone display.
! - The "call-forward busy and noan" keywords provide the voice-mail pilot number (1480)
where calls must be forwarded when the user is busy on the phone or when the call is not
answered (after a timeout of the given number of seconds).

ephone-dn  1  dual-line
 number 1000
 label 1000
 description First Last Name
 name First Last Name
call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  2  dual-line
 number 1001
 label 1001
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  3  dual-line
 number 1002
 label 1002
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  4  dual-line
number 1003
 label 1003
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  5  dual-line
 number 1004
 label 1004
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
```

```
ephone-dn  6  dual-line
 number 1005
 label 1005
 description First Last Name
 name First Last Name
 call-forward busy 1480
call-forward noan 1480 timeout 10
!
!
ephone-dn  7  dual-line
 number 1006
 label 1006
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  8  dual-line
 number 1007
 label 1007
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  9  dual-line
 number 1008
label 1008
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  10 dual-line
 number 1009
 label 1009
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  11  dual-line
 number 1010
 label 1010
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  12  dual-line
 number 1011
 label 1011
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
```

```
ephone-dn  13  dual-line
 number 1012
 label 1012
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  14  dual-line
 number 1013
 label 1013
description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  15  dual-line
 number 1014
 label 1014
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  16  dual-line
 number 1015
 label 1015
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  17  dual-line
 number 1016
 label 1016
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  18  dual-line
 number 1017
 label 1017
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  19  dual-line
 number 1018
 label 1018
 description First Last Name
name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
```

```
ephone-dn  20  dual-line
 number 1019
 label 1019
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  21  dual-line
 number 1020
 label 1020
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  22  dual-line
 number 1021
 label 1021
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  23  dual-line
 number 1022
 label 1022
 description First Last Name
 name First Last Name
 call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  24  dual-line
 number 1023
 label 1023
 description First Last Name
 name First Last Name
call-forward busy 1480
 call-forward noan 1480 timeout 10
!
!
ephone-dn  25
 number 1488....
 mwi on
!
!
ephone-dn  26
 number 1489....
 mwi off
!
!
```

```
! The following block of commands provides all the "ephone" definitions on the system.
These represent the physical phone parameters such as their MAC addresses, the user ID
(called username) associated with the phone, the button layouts, and the phone type. Key
considerations include the following:

! - The "username" is used by the end users to log in to Cisco CME to get a web display of
their phone settings.
! - The "type" command specifies the IP phone type (in this case a Cisco 7960 IP Phone).
! - The "button" command provides the button layout on the phone. Button 1 has ??, etc.

ephone  1
 username "user1" password null
 mac-address 0030.94C2.5DF0
 type 7960
 button  1:1
!
!
!
ephone  2
 username "user2" password null
 mac-address 0012.D984.B03E
 type 7912
 button  1:2
!
!
!
ephone  3
 username "user3" password null
 mac-address 0000.0000.0001
 type 7960
 button  1:3
!
!
!
ephone  4
 username "user4" password null
 mac-address 0000.0000.0002
 type 7960
 button  1:4
!
!
!
ephone  5
 username "user5" password null
 mac-address 0000.0000.0003
 type 7960
 button  1:5
!
!
!
ephone  6
 username "user6" password null
 mac-address 0000.0000.0004
 type 7960
 button  1:6
!
!
!
```

```
ephone  7
 username "user7" password null
 mac-address 0000.0000.0005
 type 7960
 button  1:7
!
!
!
ephone  8
 username "user8" password null
 mac-address 0000.0000.0006
 type 7960
 button  1:8
!
!
!
ephone  9
 username "user9" password null
 mac-address 0000.0000.0007
 type 7960
 button  1:9
!
!
!
ephone  10
 username "user10" password null
 mac-address 0000.0000.0008
 type 7960
 button  1:10
!
!
!
ephone  11
 username "user11" password null
 mac-address 0000.0000.0009
 type 7960
 button  1:11
!
!
!
ephone  12
 username "user12" password null
 mac-address 0000.0000.000A
 type 7960
 button  1:12
!
!
!
ephone  13
 username "user13" password null
 mac-address 0000.0000.000B
 type 7960
 button  1:13
!
!
!
ephone  14
 username "user14" password null
 mac-address 0000.0000.000C
 type 7960
button  1:14
!
!
!
```

```
ephone  15
 username "user15" password null
 mac-address 0000.0000.000D
 type 7960
 button  1:15
!
!
!
ephone  16
 username "user16" password null
 mac-address 0000.0000.000E
 type 7960
 button  1:16
!
!
!
ephone  17
 username "user17" password null
 mac-address 0000.0000.000F
type 7960
 button  1:17
!
!
!
ephone  18
 username "user18" password null
 mac-address 0000.0000.0010
 type 7960
 button  1:18
!
!
!
ephone  19
 username "user19" password null
 mac-address 0000.0000.0011
 type 7960
 button  1:19
!
!
!
ephone  20
 username "user20" password null
mac-address 0000.0000.0012
 type 7960
 button  1:20
!
!
!
ephone  21
 username "user21" password null
 mac-address 0000.0000.0013
 type 7960
 button  1:21
!
!
!
ephone  22
 username "user22" password null
 mac-address 0000.0000.0014
 type 7960
 button  1:22
!
!
!
```

```
ephone  23
username "user23" password null
 mac-address 0000.0000.0015
 type 7960
 button  1:23
!
!
!
ephone  24
 username "user24" password null
 mac-address 0000.0000.0016
 type 7960
 button  1:24
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line 2
no activation-character
no exec
transport preferred none
transort input all
transport output all
line vty 0 4 password cisco
 login
!
end
```

A

C

D

E

G

H

I

K

L

N

P

Q

R

S

U

V