

Cisco Unified PhoneProxy Installation and Quick Start Guide

Release 1.0(3)

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-11698-01

THIS PRODUCT CONTAINS CRYPTOGRAPHIC FEATURES AND IS SUBJECT TO UNITED STATES AND LOCAL COUNTRY LAWS GOVERNING IMPORT, EXPORT, TRANSFER AND USE. DELIVERY OF CISCO CRYPTOGRAPHIC PRODUCTS DOES NOT IMPLY THIRD-PARTY AUTHORITY TO IMPORT, EXPORT, DISTRIBUTE OR USE ENCRYPTION. IMPORTERS, EXPORTERS, DISTRIBUTORS AND USERS ARE RESPONSIBLE FOR COMPLIANCE WITH U.S. AND LOCAL COUNTRY LAWS.

By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>.

If you require further assistance please contact us by sending email to export@cisco.com.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UDP's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark

of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

© 2006 Cisco Systems, Inc. All rights reserved.

Cisco Unified PhoneProxy Administration Guide

CONTENTS

Preface	1
Overview	1
Audience.....	1
Obtaining Documentation, Obtaining Support, and Security Guidelines.....	1
Notational Conventions.....	2
Regulatory Compliance	2
Safety Instructions	3
Safety Warnings	3
Preparation and Unpacking.....	4
Site Requirements for the Cisco Unified PhoneProxy	4
Unpacking the Cisco Unified PhoneProxy	4
Physical Description of the Cisco Unified PhoneProxy	5
Installation	6
Rack Ventilation Requirements.....	6
Installation Procedure for Standard Two and Four-Post Racks	6
Cisco Unified PhoneProxy Control Buttons, Indicators, and Ports	8
Startup and Configuration.....	11
Simple Remote IP Phone Deployment.....	11
Cisco Unified PhoneProxy Configuration.....	12
User Account Creation	14
IP Phone Configuration.....	21
Connecting IP Phone to Cisco Unified CallManager	21
Connecting IP Phone to Cisco Unified PhoneProxy.....	23
User Activation and Inactivation.....	25
Activating Users	25
Inactivating Users	27
Appendix A	29
Third Party Cable/DSL Router Configuration	29
Explicit UDP forwarding.....	29

Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain additional information.

Overview

This document describes the procedures for installing the 1-rack unit (RU) Cisco Unified PhoneProxy appliance and performing the initial start-up and configuration procedure. After completing the steps outlined in this manual, you should have a functioning Cisco Unified PhoneProxy appliance setup with a basic configuration.

Audience

The *Cisco Unified PhoneProxy Installation and Quick Start Guide* assumes the reader has a basic understanding of Cisco CallManager architecture and system administration and is intended for the following audience:

- Trained, qualified network installation and support technicians

- System and network administrators familiar with IP telephony

For additional information about managing a Cisco Unified PhoneProxy deployment and the usage of the PhoneProxy command shell, please read the *Cisco Unified PhoneProxy Administration Guide* and the *Cisco Unified PhoneProxy CLI Reference Guide*.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Notational Conventions

The following section summarizes the general notational conventions used in this document. The conventions are

Convention	Description
	NOTE: A note provides important information, helpful suggestions, or reference material.
	CAUTION: A caution indicates a potential risk for damage to hardware or loss of data, and describes how to avoid the problem.
	WARNING: A warning indicates potential hazardous risk that could result in serious damage or physical harm.

Regulatory Compliance

The Cisco Unified PhoneProxy complies with the following safety and electromagnetic compatibility (EMC) regulations.

The product described in this manual complies with all applicable European Union (CE) directives if it has a CE marking. For computer systems to remain CE compliant, only CE-compliant parts may be used. Maintaining CE compliance also requires proper cable and cabling techniques.

This equipment has been tested and verified to comply with the limits for a Class A digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area (domestic environment) is likely to cause harmful interference, in which case the user will be required to correct the interference (take adequate measures) at their own expense.

Safety Instructions

Follow all safety cautions to protect the system from potential damage or loss of data, and follow all safety warnings to ensure your own personal safety.

The chassis cover should only be removed by Cisco personnel. There are no customer-serviceable components in the Cisco Unified PhoneProxy. Repairs to the system must be performed by a Cisco service technician.



NOTE: *Opening the system chassis will void the warranty of your Cisco Unified PhoneProxy.*

Make sure the voltage and frequency of your power outlet match the Cisco Unified PhoneProxy electrical ratings. The building and/or power source must provide overload protection.

Plug the system into properly grounded electrical outlets to help prevent electric shock.

Use a surge suppressor, line conditioner, or uninterruptible power supply to protect the system from sudden increases or decreases in electrical power.

Locate the system away from heat sources and do not block system vents. The chassis intake ambient air temperature should not exceed 40 °C (104 °F).

Avoid uneven mechanical loading when installing this system in a rack. If the rack has a stabilizer, make sure it is firmly attached before installing or removing the system.

Do not place a monitor or other objects on top of the Cisco Unified PhoneProxy. The chassis cover is not designed to support weight.

Safety Warnings



The power supply in this product contains no user-serviceable parts. Refer servicing only to qualified Cisco personnel.

The system is designed to operate in a typical office environment. Choose a site that is:

- Clean and free of airborne particles (other than normal room dust).

- Well-ventilated and away from heat sources, including direct sunlight.

- Away from sources of vibration or physical shock.

- Isolated from strong electromagnetic fields.

- Provided with a properly grounded wall outlet.

- Provided with sufficient space to access the power supply cord, because it serves as the product's main power disconnect.

Preparation and Unpacking

This chapter describes site requirements, unpacking instructions, and a physical description of the Cisco Unified PhoneProxy.

Site Requirements for the Cisco Unified PhoneProxy

The Cisco Unified PhoneProxy can be installed on a tabletop as a freestanding device or it can be rack-mounted in a four-post or two-post rack. If the Cisco Unified PhoneProxy is installed on a tabletop, locate the system away from heat sources in an area that provides unobstructed airflow to the chassis cooling vents. If the system is installed in a rack, the chassis intake ambient air temperature should not drop below 0 °C (32 °F) or exceed 40 °C (104 °F).



CAUTION: Make sure the voltage and frequency of the power source matches the system's electrical ratings, and that the building and/or power source provides overload protection.

Specification	Description
Operating temperatures	0 °C to 40 °C (32 °F to 104 °F)
Storage temperatures	-20 °C to 80 °C (-4 °F to 176 °F)
Relative humidity	10% to 90% (Non-condensing)

Unpacking the Cisco Unified PhoneProxy

Do not unpack the system until you are ready to install it. Storing the chassis in its shipping container helps protect the system from accidental damage.

Verify Contents of the Shipping Container

When you unpack the shipping container, confirm that you received the following items:

- 1 Cisco Unified PhoneProxy
- 1 Power cord
- 1 RJ45-to-DB9 serial port adapter cable
- 2 Rack mount ears, labeled A in Figure 1 below
- 8 Screws for rack mount ear installation, labeled B in Figure 1 below
- 4 Rubber appliance feet for table installation, labeled C in Figure 1 below

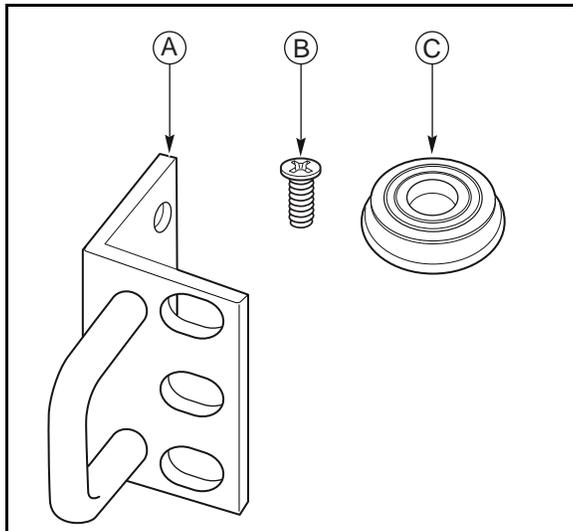


Figure 1 - Accessories included in the shipping container.

If any items are missing from your shipment, please contact Cisco support at <http://www.cisco.com>.

Physical Description of the Cisco Unified PhoneProxy

The Cisco Unified PhoneProxy is housed in a 1-RU (rack unit) chassis. The chassis is 16.8" (42.6 cm) wide, 14.4" (36.5 cm) deep, and 1.71" (4.4 cm) tall. It weighs 17 lbs (8 kg) at sea level. The Cisco Unified PhoneProxy is designed to fit standard 19" server racks. Additionally, all the connectors and indicators, except for power, are located on the front panel.

Installation

This chapter provides instructions for mounting the Cisco Unified PhoneProxy in standard 19" two- or four-post system racks. It also describes features of the Cisco Unified PhoneProxy, including I/O ports, control button functions, and LED indications.

Carefully read all **cautions** and **warnings** before you begin the rack installation procedure.



CAUTION: Do not place keyboards, monitors or other objects on top of the Cisco Unified PhoneProxy appliance. The chassis cover is not designed to support additional weight.

CAUTION: The rack installation procedures should be performed by trained service technicians.



WARNING: Always install the appliance in the lowest available position in the rack. Installing a system in a high position in the rack first could cause the rack to become unbalanced and tip over.

Rack Ventilation Requirements

Proper airflow is required for the Cisco Unified PhoneProxy to operate correctly. Please follow these guidelines when choosing where to rack the system:

Ensure that the rack is ventilated. Enclosed racks require louvered fronts and backs with a fan to dissipate heat generated by the Cisco Unified PhoneProxy.

Ensure that there is adequate ventilation for enclosed racks with top-mounted ventilation fans. Heat generated by equipment mounted in the bottom of the rack can be drawn up into equipment mounted in the top of the rack.

When table-mounting the Cisco Unified PhoneProxy, ensure that there is no obstruction of the vents on the side and rear of the system.

Installation Procedure for Standard Two and Four-Post Racks

The Cisco Unified PhoneProxy can be installed into standard 19" two or four-post server racks. The appliance can be racked without the assistance of rails or a tray.

To install the Cisco Unified PhoneProxy, perform the following steps:

1. Attach the supplied rack mount ears to the front of the Cisco Unified PhoneProxy. The rack mount ears are each attached using four screws as illustrated in Figure 2 below.

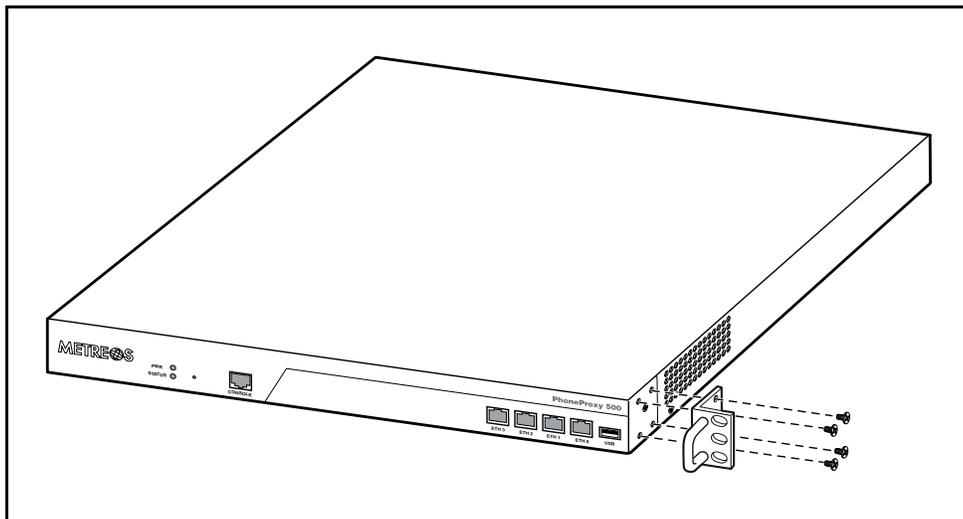


Figure 2 - Attaching the rack mount ears.

2. Install the appliance in the rack as illustrated below in Figure 3. Attach the rack mount ears using rack mount screws that are appropriate for your rack type. When installing the appliance in a four-post rack the system will not be secured to the two rear posts.

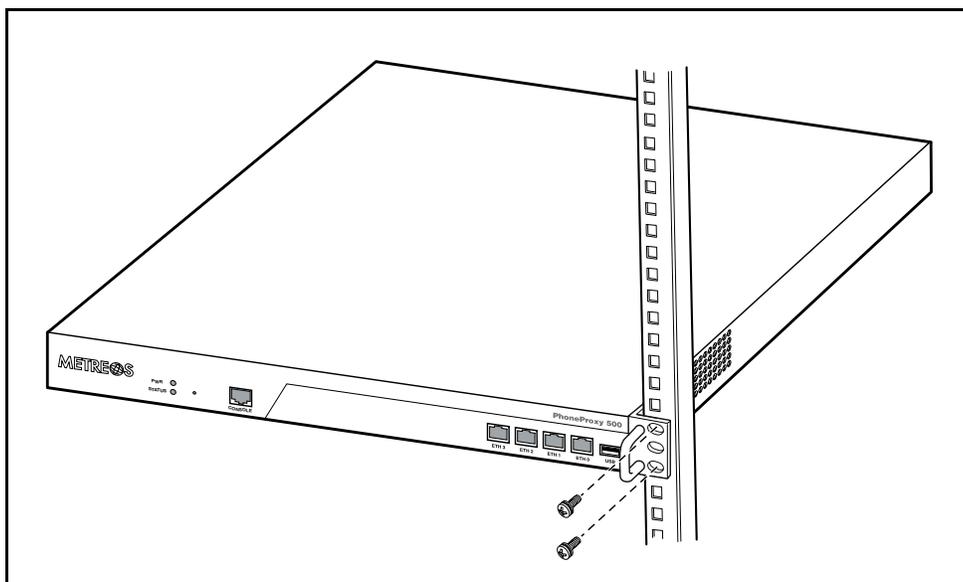


Figure 3 - Attaching the Cisco Unified PhoneProxy to the rack posts.

Cisco Unified PhoneProxy Control Buttons, Indicators, and Ports

The figures below provide the locations and descriptions of the status lights and network interfaces that can be found on the front panel of the Cisco Unified PhoneProxy.

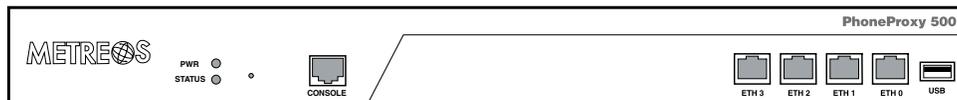


Figure 4 - Front panel view

Component	Description
Pwr LED	Indicates the system is powered on
Status LED	Indicates the hard drive activity
Console Interface	Allows access to the console via included RJ45-to-DB9 adapter cable
Cluster	Provides a cluster interface for connecting multiple Cisco Unified PhoneProxy devices together. (only used when clustering)
South	Connects to the internal network, also known as the Voice VLAN or the Cisco Unified CallManager network
North	Connects to the external network, also known as the public network or the data VLAN
Management	Connects the Cisco Unified PhoneProxy to a dedicated network for administration and management (if Management interface is not enabled, South performs this function)
USB	USB port (reserved for future use)

The figures below provide the locations and descriptions of the exhaust fan and power components found on the back panel of the Cisco Unified PhoneProxy.



Figure 5. Back panel view

Component	Description
Exhaust Fan	Ensure proper ventilation
Power Switch	Switch to 0 for off and 1 for on
Power Plug Socket	Plug power cable in here

RJ45-to-DB9 Serial Port Adapter Cable

The console port on the front of the Cisco Unified PhoneProxy chassis uses an RJ45 connector. The system ships with an RJ45-to-DB9 adapter cable that can be used to connect the system to a serial terminal.

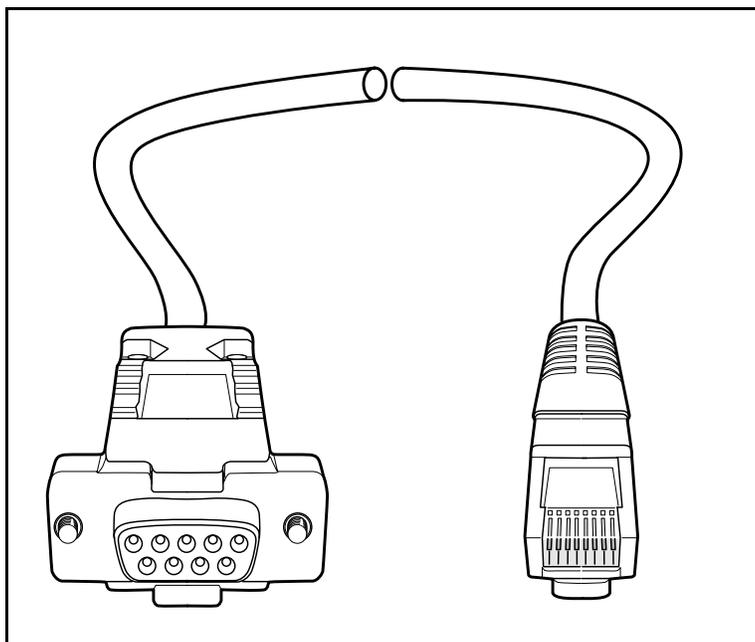


Figure 6 - RJ45 to DB9 Serial Adapter Cable.

RJ45-to-DB9 Serial Port Adapter Pin Assignments

To connect the Cisco Unified PhoneProxy to a system that requires a RJ45 connector, use the following table of pin assignments to create a compatible cable.

RJ-45	Signal	Abbreviation	DB-9
1	Request to Send	RTS	7
2	Data Terminal Ready	DTR	4
3	Transmit Data	TD	3
4	Signal Ground	SGND	5
5	Ring Indicate	RI	9
6	Receive Data	RD	2
7	Data Carrier Detect or Data Set Ready	DCD or DSR	1 or 6
8	Clear to Send	Clear to Send	8

Startup and Configuration

Simple Remote IP Phone Deployment

This section describes the steps to setup a Remote IP Phone deployment. This is an example designed to get you familiar with the setup and configuration of Cisco Unified PhoneProxy. It does not represent the only possible production deployment. For information on the various production deployment possibilities, please refer to the *Cisco Unified PhoneProxy Administration Guide*.

Remote IP Phone Configuration

In this example, the Cisco Unified PhoneProxy is configured to bridge IP Phones on the public network to a CallManager network inside the corporate firewall (see Figure below).

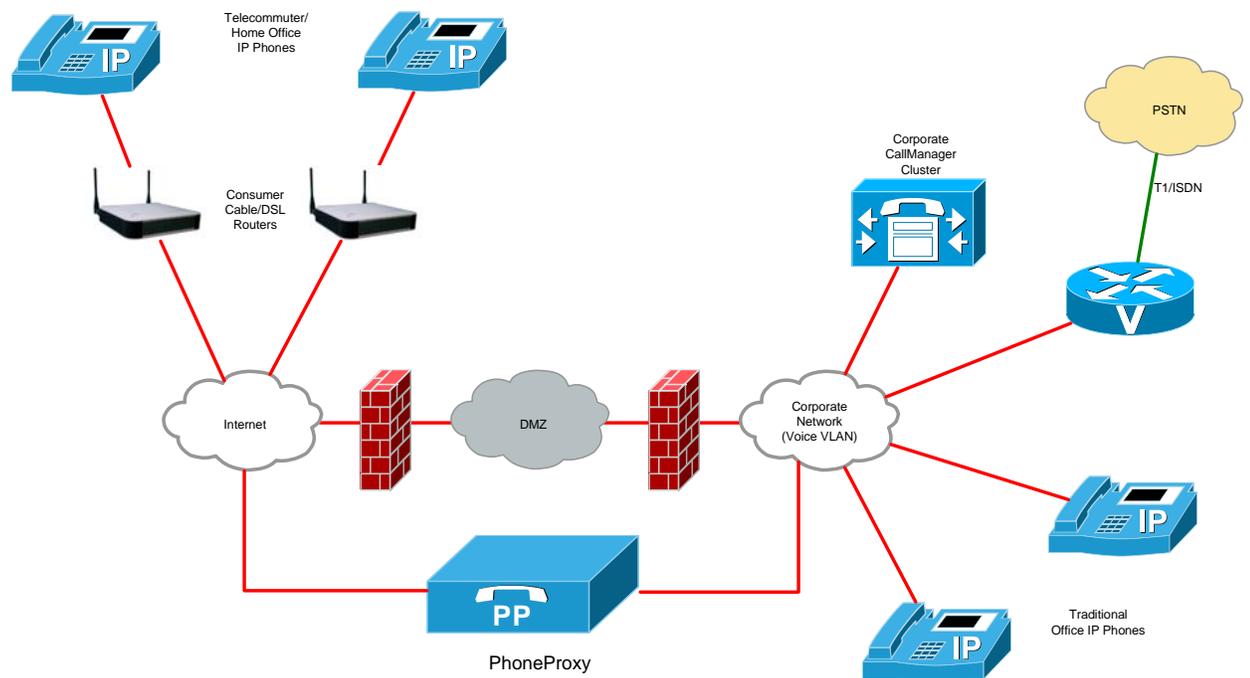


Figure 7 - Remote IP Phones

The Cisco Unified PhoneProxy is directly connected to the public network on its North interface and directly connected to the voice network on its South interface. If your deployment requires that the Cisco Unified PhoneProxy cluster be bracketed by firewalls, refer to the *Cisco Unified PhoneProxy Administration Guide* for information on the required firewall configuration.

Collect the Hardware

You will need the following hardware for this example:

- 1 Cisco Unified PhoneProxy appliance
- 2 IP Phones
- 1 CallManager
- 1 Consumer-grade Cable/DSL Router
- Computer with Management Console installed. (See Appendix A)

Two network cables should be plugged into the Cisco Unified PhoneProxy. One cable should connect the South interface (eth1) on the PhoneProxy box to the network with the CallManager. The other cable should connect the North interface (eth2) on the PhoneProxy box with the DHCP router. The IP phones are also plugged into the DHCP router.



NOTE: All of these cables being connected to the router should be plugged into normal ports rather than WAN ports.

Cisco Unified PhoneProxy Configuration

Before you begin configuration you will want to collect the following information for your Cisco Unified PhoneProxy deployment.

Input	Description
<password>	The desired admin account's password for the Cisco Unified PhoneProxy cluster (this password should be a strong password—see page 16 for strong password requirements)
<nodename>	The hostname for the Cisco Unified PhoneProxy, e.g., phoneproxy (this is not the fully qualified name)
<dnsdomain>	The DNS domain suffix of the Cisco Unified PhoneProxy (<nodename>.<dnsdomain> should be the fully-qualified name of the PhoneProxy)
<north-ip>, <north-netmask>	The address and netmask of the Cisco Unified PhoneProxy's North interface (the subnet of this interface must be on the public network and the actual IP address of this interface must be directly accessible from the public network, i.e. not obscured by a NAT)

<south-ip>, <south-netmask>	The address and netmask of the Cisco Unified PhoneProxy's South interface (the subnet of this interface must be on the private network shared by Cisco Unified CallManager and the other IP telephony endpoints. This IP address should appear to the CallManger cluster just as any other IP Telephony endpoint would, i.e. directly accessible and not obscured by a NAT)
<defaultgateway>	The default North-side (external) router (if multiple subnets exist on the south-side of Cisco Unified PhoneProxy, those routes must be explicitly configured)
<timezone>	The timezone the PhoneProxy server is in. (for example, US/Central)
<ntp>	(optional) The NTP server to use for keeping time (ideally, South-side)
<dns1>, <dns2>	IP address of the network's South-side (internal) DNS server(s)
<sid>	The station identifier for each of the IP phone(s) that will be remotely deployed. (for example, SEP001647051B3A)

After you have determined all the necessary information, you can begin the initial startup and configuration of your Cisco Unified PhoneProxy.



NOTE: The CLI is case-sensitive, and all commands are all lower case. Refer to the Cisco Unified PhoneProxy CLI Reference Guide for a detailed explanation of command purpose and syntax.

Procedure

1. Connect the RJ45 side of the included RJ45-to-DB9 serial adapter cable to the console port on the Cisco Unified PhoneProxy. Connect the DB9 side to a standard serial port of a computer or terminal server.
2. Power on the Cisco Unified PhoneProxy.
3. Connect to the device using HyperTerminal or a similar terminal interface, using the following serial connection settings.

Setting	Value
Baud	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	Hardware

4. Login using admin as the username and cisco as the password. You will immediately be required to change to a more secure password.

5. At the command prompt type the following commands:

```
> set interface north address <north-ip> netmask <north-netmask> enable
> set interface south address <south-ip> netmask <south-netmask> enable
> set defaultgateway <gateway>
> set nodename <nodename>
> set dns domain <dnsdomain>
> set time timezone <timezone>
> set dns primary <dns1> secondary <dns2>
> set ntp server <ntp> enable
> set phoneproxy activation idletimeout 1200
> save config
```



NOTE: After the configuration items have been saved, the Cisco Unified PhoneProxy can be remotely accessed via SSH. For example, if the South address is 10.1.14.99 then at a command prompt, type:

ssh admin@10.1.14.99 then, when prompted, enter the password.

After the configuration has been saved, the Cisco Unified PhoneProxy may be accessed by the Cisco Unified PhoneProxy Management Console.

User Account Creation

Licensing

Each Cisco Unified PhoneProxy comes with 25 right-to-use licenses; each license entitles you configure one (1) PhoneProxy user using the Cisco Unified PhoneProxy User Management Console. To purchase additional right-to-use licenses, you must contact your Cisco reseller.

Cisco Unified PhoneProxy licensing is based upon the number of configured users, regardless of how many are actively registered or engaged in calls at any given time.

For Example, if you would like to configure 100 users with the ability to activate IP Phones through your Cisco Unified PhoneProxy, you will need 100 right-to-use licenses, regardless of whether 10, 20, or all 100 are actively registered and engaged in calls. See the *Cisco Unified PhoneProxy Administration Guide* for more information on differences between activation and registration.

Creating Users

For IP phones to make and receive calls through a Cisco Unified PhoneProxy cluster, the phones must have a user account created. User account management is handled by the Cisco Unified PhoneProxy Management Console.



NOTE: The Cisco Unified PhoneProxyManagement Console version 1.0(x) only supports the US-EN locale on Microsoft Windows XPsp2 and Windows 2003 Server. To verify your PC is configured this way, go to the Windows Control Panel and look for Regional and Language options. In there, change “Standards and Formats” under “Regional Options” to English(United States).

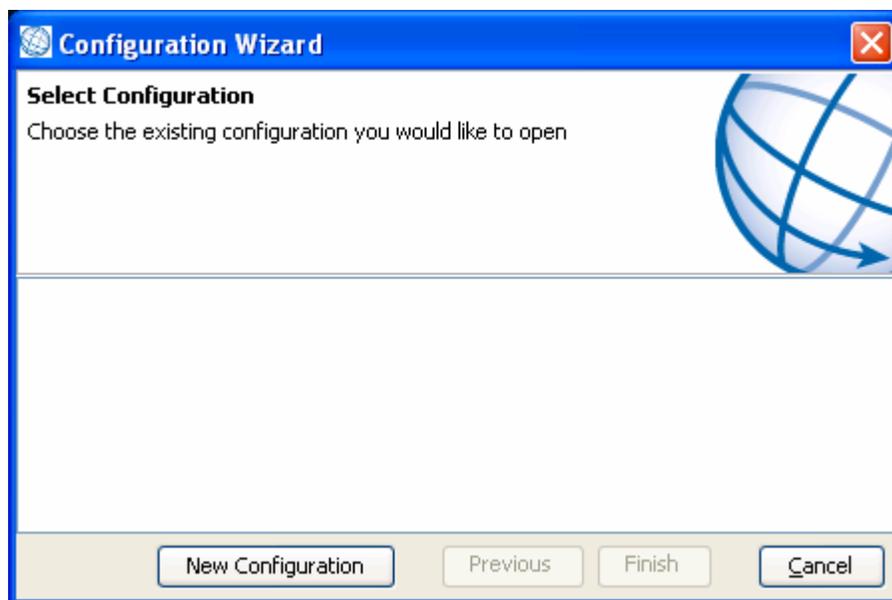
The Cisco Unified PhoneProxy Management Console is a Windows application that must be installed on the administrator’s computer. The software is not included in the box, you can download it from the Cisco CCO website at <http://www.cisco.com/cgi-bin/tablebuild.pl/CUPP>.

Double-clicking the executable file will start the installation process. The Cisco Unified PhoneProxy Management Console requires that J2SE v1.5 is installed. If the Java software is not installed on the computer already, the installer will download and install it.

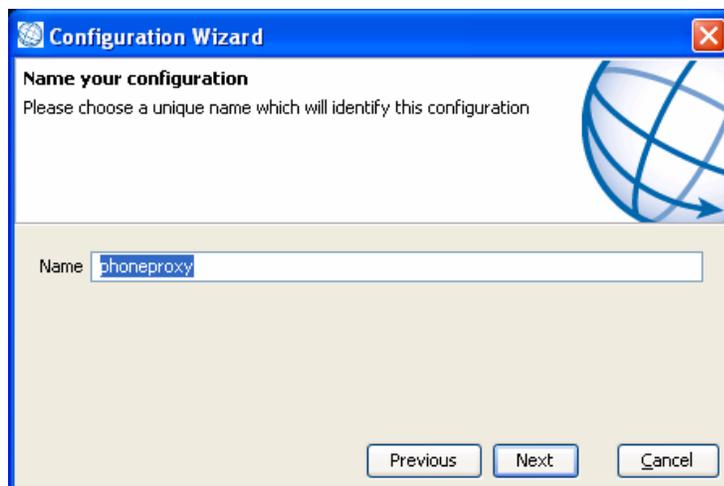
Once the console software is installed, users can be created as follows:

Procedure

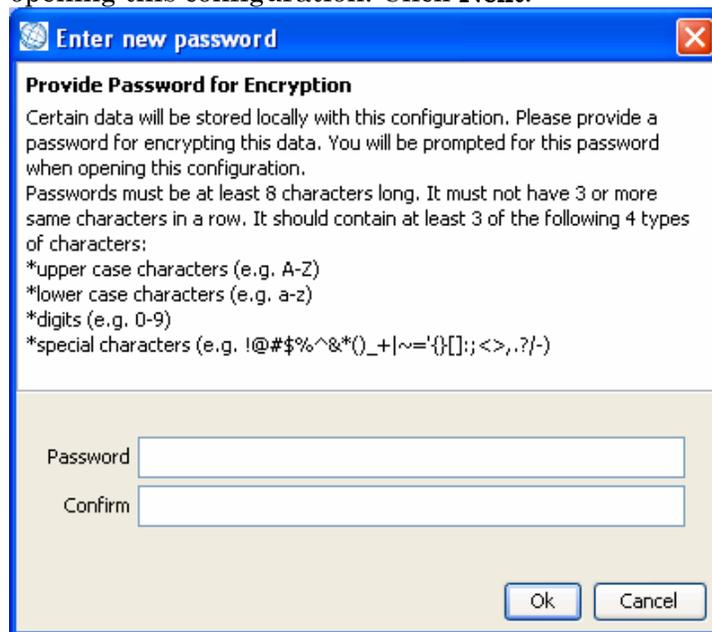
1. When the management console is first opened, you will be presented the option to create a new configuration. Click **New Configuration**.



- Choose a unique name for this configuration. This name will identify the configuration profile that contains all the users and settings you are about to configure. Click **Next**.



- Provide a strong password for encryption of certain data that will be stored locally with this configuration. You will be prompted for this password when opening this configuration. Click **Next**.



NOTE: Strong passwords must be at least 8 characters long and contain at least 3 of the following 4 types of characters:

- *upper case characters (e.g. A-Z)
- *lower case characters (e.g. a-z)
- *digits (e.g. 0-9)
- *special characters (e.g. !@#\$%^&*()_+|~='{}[];:<>.,?/-)



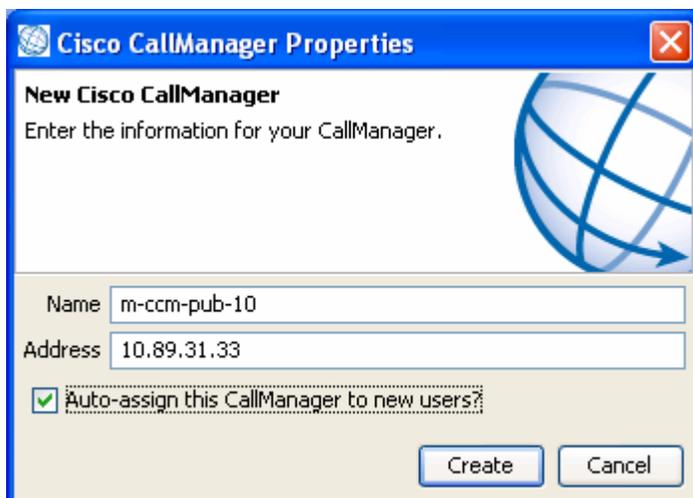


NOTE: This password cannot be retrieved. If it is forgotten, you will be unable to open the configuration and a new configuration file must be created.

- Click Add on the next screen to define a Cisco CallManager.



- In the window that pops up, enter the **Name** and **IP Address** of the CallManager TFTP server. This is the publisher server of the CallManager cluster. Click **Create**.



NOTE: The checkbox labeled “Auto-assign this CallManager to new users” sets this CallManager as the default CallManager for new users.

- You will be returned to a window with your newly configured CallManager listed. Click **Next**.



- You will now be presented with the screen to specify how you would like to provide information about your cluster of PhoneProxys. Choose the option to **Connect to the Master Proxy and Download**. Click **Next**.



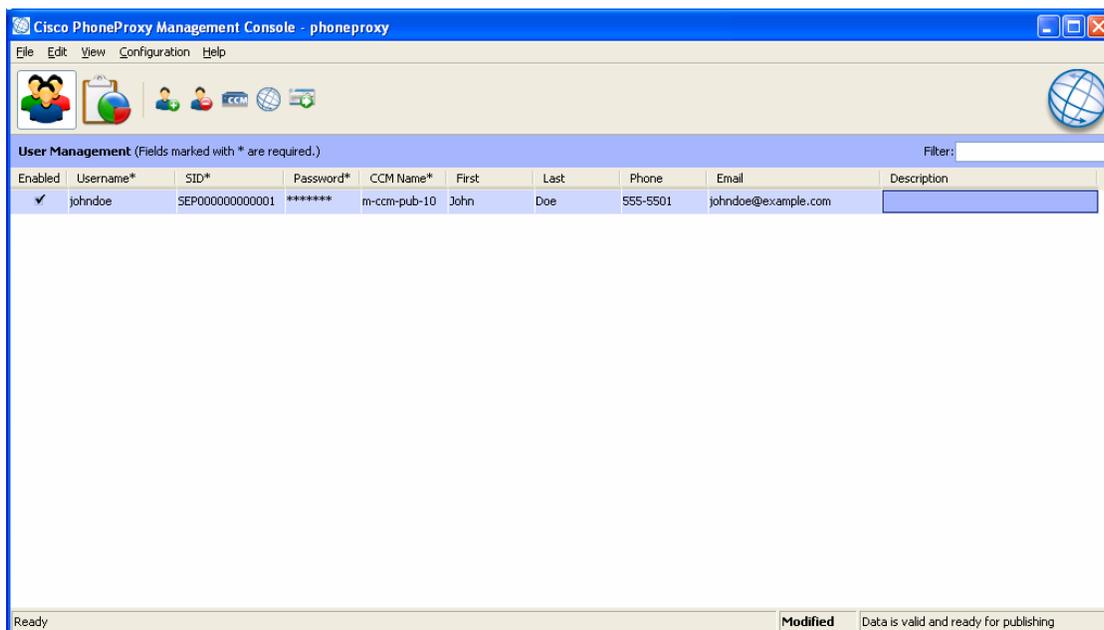
8. Enter the **IP Address** of the south interface of the Cisco Unified PhoneProxy and also supply the **Username** (admin) and the **Password**. Click **Next**.

The screenshot shows a window titled "Configuration Wizard" with a globe icon and a close button. The main heading is "Provide proxy data" with the instruction "Provide master proxy data". Below this are three input fields: "Address" containing "192.168.28.130", "Username" containing "admin", and "Password" containing "*****". At the bottom right are three buttons: "Previous", "Next", and "Cancel".

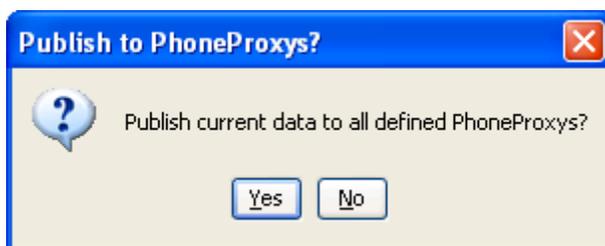
9. After it connects to the Cisco Unified PhoneProxy, you should be shown a confirmation screen to verify the proxies that will be imported. Click **Next**.

The screenshot shows a window titled "Configuration Wizard" with a globe icon and a close button. The main heading is "Import cluster.xml contents" with the instruction "Review the contents of your cluster.xml file and specify how the contents are to be imported." Below this is a text area containing "The following proxies will be imported." followed by "phoneproxy" on a new line. At the bottom right are three buttons: "Previous", "Next", and "Cancel".

10. The next screen will present you with several methods to populate your configuration with users. Since you are setting up a new configuration for the first time, choose **Skip** and then click **Finish**, because there will be no configurations available to import.
11. Click the **Add User** button to display a line where user settings are entered.



12. Enter the Username, the IP Phone's SID, the user's password, and choose the CallManager from the drop down list.
13. Click **File** then **Save** to save the configuration settings. You should notice that the status bar will change to reflect that the status is "Saved".
14. The status bar says the "Data is valid and ready for publishing." Click on the **Publish** button to send the current data to the Cisco Unified PhoneProxy cluster.



15. After the files have been transferred, you can use the Cisco Unified PhoneProxy command line interface to verify the users were provisioned successfully.

At the command shell prompt, type:

```
> show user
name      sid          addr          duration connected
----      ---          ---          -
johndoe   SEP000000000001 [inactive]
```

IP Phone Configuration

To connect and register an IP Phone through Cisco Unified PhoneProxy, some settings need to be configured on the IP Phone. This configuration is often easiest if the IP phone has already been provisioned in the Cisco Unified CallManager and registered at least once. This is so that the IP phone will already have the firmware load Cisco Unified CallManager is expecting. Steps 1 through 18 briefly outline how this should be done. If you encounter difficulty registering the IP phone to the CallManager, please contact your CallManager administrator.



***NOTE:** In this example, the IP phone is a Cisco 7960 IP Phone. The concepts will be the same for other models of the phone, but the location of certain menu options may be different.*

Connecting IP Phone to Cisco Unified CallManager (before connecting to Cisco Unified PhoneProxy)

Procedure

1. Connect the IP Phone to the South network.
2. Plug the power cord into the IP phone.
3. When you can, display the Settings menu by pressing the **Settings** button on the IP Phone.
4. Select the **Network Configuration** option by pressing the appropriate key on the phone dial pad (option 3 on a 7960 IP Phone), or scroll down to the option and press **Select**.
5. Next, highlight **Erase Configuration** (option 33).
6. Press ****#** on the IP phone to unlock the setting for modification. You should notice a SoftKey labeled “Yes” appears.
7. Press the **Yes** SoftKey and then press the **Save** SoftKey. The IP phone will reset.
8. During the reset the phone will display several messages. The first message is “Configuring VLAN” then “Configuring IP.” After the Configuring IP message, press the **Settings** button.
9. Choose the option for **Network Configuration** (option 3).
10. Verify that the IP phone has been given an **IP address** (option 6).
11. Next, scroll down to option 32, **Alternate TFTP**.
12. Press ****#** on the IP phone to unlock the setting for modification. You should notice a SoftKey labeled “Yes” appears.

13. Press the **Yes** SoftKey and then press the **Save** SoftKey. The IP phone will reset.



***NOTE:** Depending on your network configuration, the phone may connect to some CallManager at this point. That is okay.*

14. When you are able to, bring up the Settings menu by pressing the **Settings** button on the IP Phone.
15. Choose **Network Configuration** (option 3).
16. Go to option 8, **TFTP Server**, and unlock the setting by pressing ****#**. A SoftKey labeled **Edit** should appear.
17. Press the **Edit** SoftKey.
18. Enter the IP address for the CallManager (e.g. 10.1.14.25) Then press the SoftKey labeled **Validate**, and then press **Save**. The phone will reset and may change IP addresses. This may happen multiple times.

At this point, your phone should be provisioned and connected to the CallManager. If you have difficulty connecting, do not continue and contact your CallManager administrator for assistance.

To be sure that everything is functioning thus far, do a quick test by calling another phone that is known to be setup properly. Be sure that there is two-way audio.

Connecting IP Phone to Cisco Unified PhoneProxy

Now that the IP phone has registered successfully to the Cisco Unified CallManager, we will modify the settings to have it register through the Cisco Unified PhoneProxy instead of directly to the CallManager. If you have not yet successfully registered directly to the CallManager, revisit the previous section titled *Connecting IP Phone to Cisco Unified CallManager (before connecting to Cisco Unified PhoneProxy)*.

The key change to the IP phone involves TFTP Server settings. The TFTP Server setting on the IP Phone will be changed to be the IP address of Cisco Unified PhoneProxy's North interface.

After this change is made, the IP phone is ready to be deployed to the remote location.

When testing an IP phone, it is often best to connect the IP phone to a LAN port on a consumer-grade Cable/DSL router. The WAN port of the Cable/DSL router should be configured to have a valid north-side subnet and be accessible to the Cisco Unified PhoneProxy. This configuration will simulate a remote home user.

The following procedure assumes the IP phone is connected to a consumer-grade Cable/DSL router and that router's WAN port is on the same subnet as the Cisco Unified PhoneProxy's North interface.

Procedure

1. Disconnect the IP phone from the South network and connect it to the North network. The phone will reset when it notices that the network connectivity has changed.
2. When you are able to, bring up the Settings menu by pressing the **Settings** button on the IP Phone.
3. Choose Network Configuration (option 3).
4. Go to option 8, **TFTP Server**, and unlock the setting by pressing * * #. A SoftKey labeled **Edit** should appear.
5. Press the **Edit** SoftKey.
6. Enter the IP address for the Cisco Unified PhoneProxy's North interface. (e.g. 192.168.1.2) Then press the SoftKey labeled **Validate**, and then press **Save**. The phone will reset and will change IP addresses.
7. During the reset, the phone will display several messages. The first message is "Configuring VLAN" then "Configuring IP." After the Configuring IP message, press the **Settings** button.
8. Choose Network Configuration (option 3).

9. Highlight IP address (option 6), and write down the IP address. You will need this when activating the user account in the next section.

Sometimes it takes several cycles for the IP phone to connect. If the phone has not received an IP address after a few minutes, try power cycling the IP phone. Finally, if it still is not obtaining an IP address, there may be a problem with the router or the network cable.



***NOTE:** Your phone will still not be able to connect at this point because the phone has not been activated. When you see the IP phone display “configuring CM list,” proceed to the next section and activate the phone.*

User Activation and Inactivation

After the IP Phone has been configured with the correct TFTP address and has proper network connectivity, it is ready to be activated. Account activation is the process of authenticating the remote IP Phone's IP address with the Cisco Unified PhoneProxy. This authentication step is a key component to PhoneProxy's security model, in that authentication of the IP address is how PhoneProxy is able to make the correct judgments on what IP traffic to bridge between the public and private networks. Once, the remote IP Phone's address is activated, the remote IP Phone is able to complete its registration and then be able to place and receive calls.

Activating Users

The activation of the IP Phone can be done by the administrator through the Cisco Unified PhoneProxy command shell, or the by the remote end user through a webpage.

Self-activation by End-User via the PhoneProxy User Activation Page

In this process—the standard for Cisco Unified PhoneProxy—the end-user self-activates by logging into the user activation web page.

This page is accessible by navigating to `http://<northip>/activation/activate_user` where `<northip>` is the north-side IP address of the Cisco Unified PhoneProxy.

NOTE: *The activation webpage can also be accessed by navigating directly to the North-side IP address, `http://<northip>/`*



The IP Address is pre-filled by the form to match the IP address of the machine of the web browser that made the request. In the use case where the user and

the remote IP Phone are behind the same Cable/DSL router, i.e. same NAT gateway, this should automatically be the correct IP.

The user should enter their Cisco Unified PhoneProxy userid and password to activate their remote IP Phone.

Activating a User via Web Services

In addition to user's activating themselves via the User Activation web page, a user can be activated via a Web Service hosted on the Cisco Unified PhoneProxy. Refer to the *Cisco Unified PhoneProxy Administration Guide* for more information.

Administrator Activating a User via PhoneProxy Command Shell

A provisioned account can also be activated manually by the Cisco Unified PhoneProxy administrator using the PhoneProxy command shell. The administrator will need to know the account username and the remote IP address of the phone to be activated.

At the command shell prompt, type:

```
> set user active name <username> address <IP address>
```

If the activation was successful, the shell will return no message; otherwise, the system will return a `UserAuthFailure` error.

Post Activation

After the remote IP Phone is authorized to connect, it may take the phone more than one cycle to register completely. Once the phone does register, it is ready to make and receive calls. The administrator can use the `show user` command to verify the activation status as well as the duration of time the account has been registered.

At the command shell prompt, type:

```
> show user
name          sid          addr          duration connected
----          -
marge         SEP0003E348E321 [inactive]
homer         SEP001647051B3A 192.168.1.100 2m 40s *
```

Setting the “activation idletimeout”

For security reasons, a user's account will automatically inactivate if the connection goes idle for a determined number of seconds. When a phone registers with a Cisco Unified PhoneProxy, the phone will establish and maintain a SCCP

connection indefinitely. This active SCCP connection is monitored by the PhoneProxy and as long as this SCCP connection remains up, PhoneProxy will treat the remote IP phone as active.

The remote IP Phone will be treated as idle when it is physically disconnected, or if a network event occurs that causes the active SCCP connection between the remote IP Phone and Cisco Unified PhoneProxy to be dropped. After the remote IP Phone is idle, it has a pre-determined amount of time to re-establish a SCCP connection before the remote IP address is inactivated. The administrator can configure the number of seconds before an idle account times out by configuring PhoneProxy's `idletimeout` parameter.

At the command shell prompt, type:

```
> set phoneproxy activation idletimeout <seconds>
```

The default value is 300 seconds. This means the user must connect their phone within five minutes of activation or they will have to reactivate.

Inactivating Users

An IP phone that has successfully connected can be inactivated either explicitly by marking the IP phone as inactive via any one of the user inactivation web-page, through the user-activation web-service or via the CLI, or by implicitly inactivating the user through a global activation authorization timeout.

Administrator Inactivating a User via PhoneProxy Command Shell

The administrator can utilize the command shell to immediately inactivate an account. While this will not interrupt the audio stream of an active call, the phone will display "CM down features disabled" and the phone will not be able to perform any more functions. For example, the phone will not be able to make a new call or put the current call on hold.

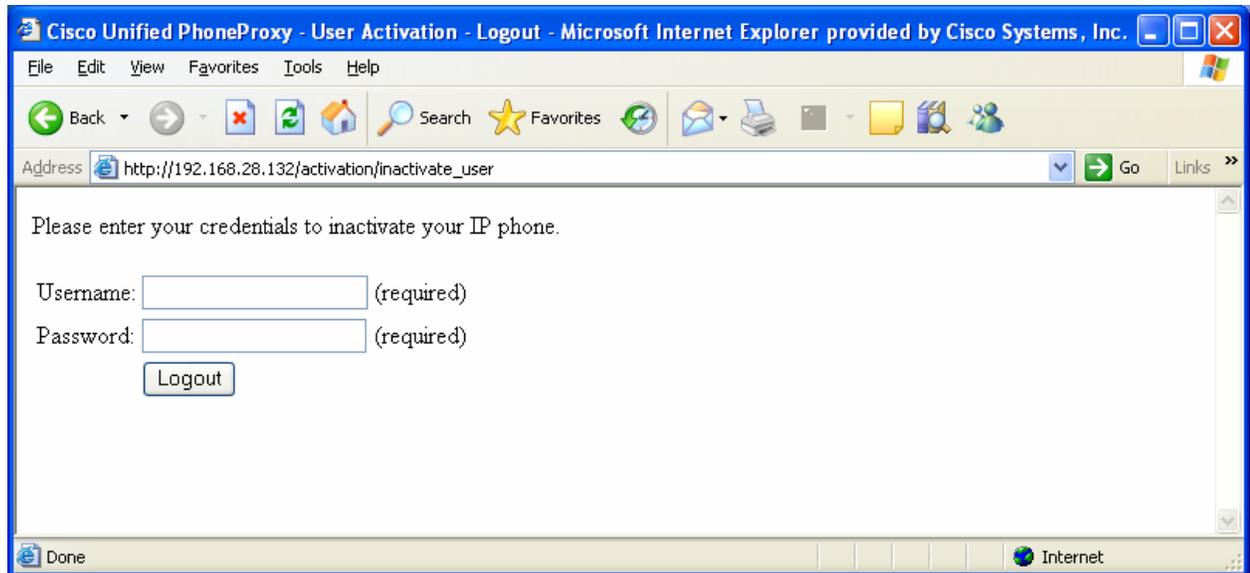
At the command shell prompt, enter:

```
> set user inactive name <username>
```

Self Inactivation via the Web interface

An end user may also self-inactivate by entering his username and password into Cisco Unified PhoneProxy's user inactivation web page on the PhoneProxy North interface. The address for this page is:

http://<northipaddress>/activation/inactivate_user where <northipaddress> is the north-side IP address of the Cisco Unified PhoneProxy.



Setting the “activation authtimeout”

For security reasons, a user can be required to re-authenticate after a specified amount of time by configuring the activation authtimeout. This setting controls the number of seconds before an activated connection's authorization times out.

At the command shell prompt, type:

```
> set phoneproxy activation authtimeout <seconds>
```

The default value is 0, indicating that activated, connected phones will not timeout.

Appendix A

Third Party Cable/DSL Router Configuration

Remote IP Phone's are often situated behind a 3rd party Cable/DSL router. These routers are usually configured to perform Network Address Translation (NAT). This allows the router to have a single public IP address on one side and a private IP network on the other. For media to reach an IP phone situated behind a NAT-capable router, the router must forward the UDP packets containing the RTP stream to the IP phone.

Cable/DSL routers vary widely on both how UDP packet forwarding occurs and some older Cable/DSL routers do not forward UDP at all. Most new routers support Stateful Packet Inspection. For most of these routers UDP port forwarding will occur automatically. Other routers require explicit UDP packet forwarding to work at all.

Regardless of the Cable/DSL router used, explicit UDP packet forwarding will always provide the best audio experience for the end-user. See the *Cisco Unified PhoneProxy Administration Guide* for a detailed explanation of UDP packet forwarding and various trade-offs between automatic and explicit forwarding.

Explicit UDP forwarding

The NAT-capable router should be configured to forward the UDP ports 1024-65535 to the IP address of the IP phone.

As an alternative of explicit UDP forwarding, some Cable/DSL routers will require you to designate the IP Phone as a *DMZ Host*. For Cable/DSL routers this is a special host that receives all incoming connections from the public network.

There is no functional difference in a Cisco Unified PhoneProxy deployment between a IP Phone that has UDP ports explicitly forwarded or an IP Phone designated as a DMZ Host. The choice is entirely dependent upon the capabilities and preference of the end-user.

Configure your router

Your firewall/router needs to be configured to forward a range of UDP ports to the IP phone. This will allow the IP phone to receive audio when you make/receive calls.



NOTE: *Different Cable/DSL routers have different procedures for this configuration. Furthermore most NAT-capable routers will only allow a given port range to be forwarded to a single IP address*

The configuration of each brand/model of firewall/router is different, but the task is the same. For specific instructions for your brand and model of router, please contact the manufacturer's website.

Linksys Routers

Procedure

1. From your web browser, connect to your router's administrative webpage. For Linksys this is typically something like *http://192.168.1.1*
2. Click on **Applications & Gaming** or the **Port Forwarding** tab (whichever is present on your router)
3. You will see a table to which you will need to add an entry, enter the following values:

Application	Start	End	Protocol	IP Address	Enabled
<i>IP Phone</i>	1024	65535	UDP	<i>Phone IP address</i>	Checked
<i>TFTP</i>	69	69	UDP	<i>Phone IP address</i>	Checked

4. Click on "Save Settings" and the port forwarding is done.

After the port forwarding has been configured, you can make and receive calls. To test make a call to your home phone or cell phone and confirm that you can hear what each end of the call is saying from each phone.

For more information on 3rd Party Cable/DSL routers and troubleshooting see the *Cisco Unified PhoneProxy Administration Guide*.