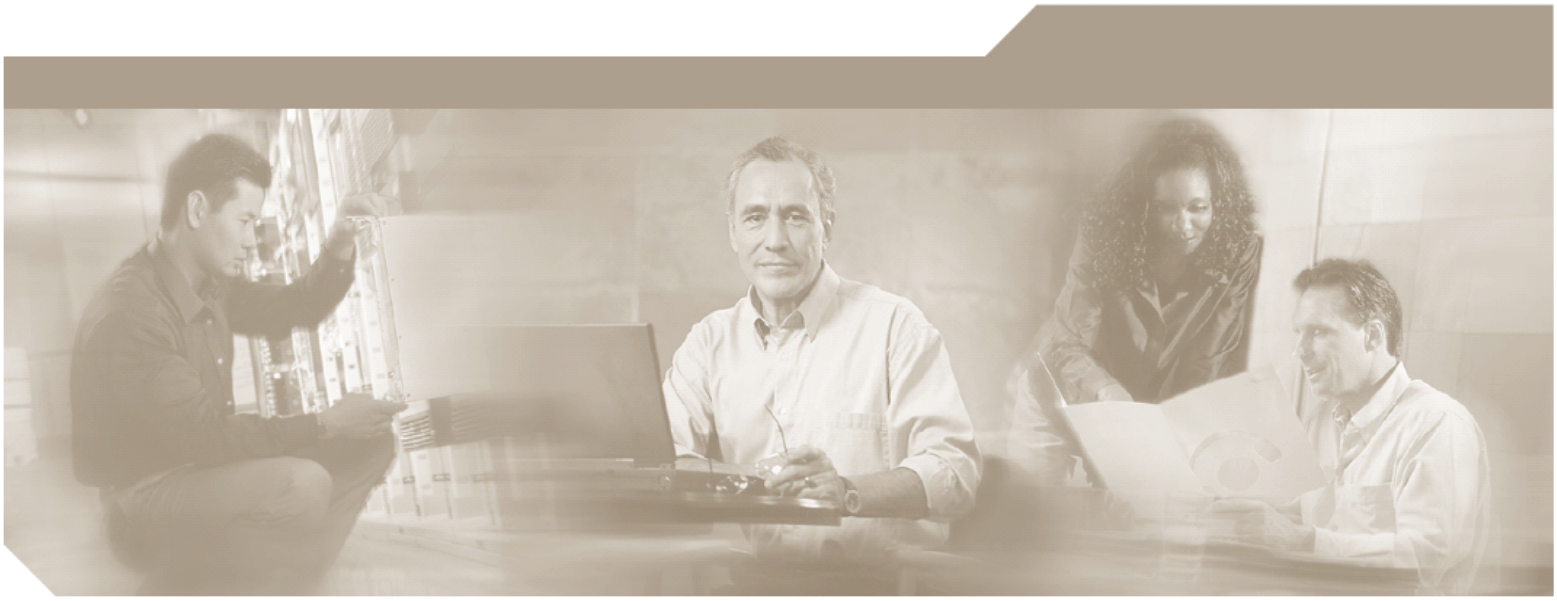

Cisco Unified PhoneProxy Administration Guide

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-11699-01

Cisco Unified PhoneProxy Administration Guide

CONTENTS

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 how to maintain a Cisco Unified PhoneProxy deployment, including managing users and appliances, applying system updates, and monitoring system logs and performance.

Audience

The *Cisco Unified PhoneProxy Administration Guide* assumes the reader has a basic understanding of Cisco Unified 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 installation and initial configuration, or the usage of the Cisco Unified PhoneProxy command shell, read the *Cisco Unified PhoneProxy Installation and Quick Start Guide* and the *Cisco Unified PhoneProxy CLI Reference Guide.*

Related Documentation

Documentation on Cisco Unified Communications products is located at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites are located at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at *tech-doc-store-mkpl@external.cisco.com* or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents

on Cisco.com. You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:
For Emergencies only—*security-alert@cisco.com*

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

For Nonemergencies—*psirt@cisco.com*

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the Tools & Resources link under Documentation & Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)— You require information or assistance with Cisco product capabilities, installation, or configuration

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

• The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

http://www.cisco.com/offer/subscribe

• The Cisco Product Quick Reference Guide is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

• Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

• Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

http://www.ciscopress.com

• Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private Internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/ipj

• Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

http://www.cisco.com/en/US/products/index.html

• Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

http://www.cisco.com/discuss/networking

• "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

• World-class networking training is available from Cisco. You can view current offerings at this URL:

http://www.cisco.com/en/US/learning/index.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.

Cisco Unified PhoneProxy Concepts and Terminology

IP Telephony Service Gateway

Cisco Unified PhoneProxy bridges IP telephony between the corporate IP telephony network and the corporate data network or the Internet in a secure manner.

In many situations, such as those listed, it is desirable to provide IP telephony service to a user who does not otherwise have direct access to the corporate IP telephony network. Some of these situations are:

A telecommuter who works primarily from the home or a small leased space, off the corporate network.

A user who wants to use Cisco IP Communicator as a primary IP endpoint on the corporate data network, but cannot because the corporate data network is separated from the corporate voice network by a firewall.

One solution is to provide a VPN tunnel for the off-network user and allow IP telephony over the tunnel. Unfortunately, VPN tunnels would suppress QoS information about the media stream and can result in less than optimal audio quality.

Another solution is to open a firewall to allow the necessary communication protocols to enter the corporate voice network from the appropriate remote IP addresses. This would allow the voice traffic to be tagged appropriately by the connecting network (and preserve QoS); however, maintaining the firewall can consume IT resources.

The ideal solution is Cisco Unified PhoneProxy, a special purpose firewall that is IP telephony-aware. PhoneProxy dynamically opens the only the ports necessary for a given endpoint and a given call and closes them immediately when they are no longer needed. PhoneProxy also maintains a list of authorized remote endpoints and endpoint users and supports encryption of the connections to the remote endpoints.

Cisco Unified PhoneProxy Concepts

Cisco Unified PhoneProxy is based on the following concepts:

North Network – Cisco Unified PhoneProxy refers to the network where all the remote IP telephony endpoints reside as the North Network. This network could be a distinct data network in a corporate network or it could be a public network like the Internet.

South Network – Cisco Unified PhoneProxy refers to the corporate voice network as the South network. Cisco Unified PhoneProxy lives on the South Network much like a Cisco Unified CallManager, or another voice gateway might live on this network.

Provisioning – Provisioning refers to the process of defining users and devices in Cisco Unified PhoneProxy through the User Management Console. Only devices and users provisioned in PhoneProxy will be allowed to bridge from the North to the South networks.

Activation – Activation and its opposite, inactivation, refer to the authorization process that Cisco Unified PhoneProxy requires remote IP telephony endpoints to execute before they are allowed to register with their Cisco Unified CallManagers through PhoneProxy. After an IP telephony endpoint is registered, it will remain activated until it either loses its registration or is explicitly inactivated.

Registration – Registration is the process an IP telephony endpoint executes to request configuration information from its designated Cisco Unified CallManager and place itself into service. A device that is successfully registered may make and receive calls just as if it were on the corporate voice network.

Cisco Unified PhoneProxy in a Nutshell

Cisco Unified PhoneProxy is an IP telephony Services gateway based on firewall technology. It bridges IP telephony communication between two separate networks.

Cisco Unified PhoneProxy maintains a list of authorized IP telephony endpoints and users. This list is used to authenticate users and to balance load in a cluster.

Cisco Unified PhoneProxy dynamically authorizes and deauthorizes remote endpoints for access without requiring the remote endpoint to tunnel through a VPN.

Cisco Unified PhoneProxy supports *security transcoding*, encrypting the North traffic for security, again without requiring a VPN and also without requiring that Cisco Unified CallManager security be enabled.

Before an IP phone on the North side can make or receive calls, it must be explicitly activated by the user.

An IP phone remains activated for as long as is can maintain a SCCP connection with the Cisco Unified PhoneProxy, or until it is explicitly in-activated by the user, the administrator or a configurable management policy.

After activated, the Cisco Unified PhoneProxy proxies all protocols: Skinny Client Control Protocol (SCCP), Real Time Protocol (RTP), Trivial File Transfer Protocol (TFTP) and HTTP from the IP phone to the South network.

Only one device per user may be provisioned in a given Cisco Unified PhoneProxy cluster.

Only provisioned and activated IP phone devices are allowed to send SCCP, TFTP, and HTTP requests through the Cisco Unified PhoneProxy.

To the phone, Cisco Unified PhoneProxy appears as a Cisco Unified CallManager, an IP telephony endpoint and an HTTP-Proxy server.

To the Cisco Unified CallManager, the Cisco Unified PhoneProxy appears as an IP telephony endpoint.

Cisco Unified PhoneProxy is a NAT firewall that manages the forwarding of RTP streams based upon the state of SCCP messages. This base firewall function is augmented by smart protocol proxies (TFTP, SCCP, RTP, etc.) that are together designed to present the illusion to the North IP telephony endpoint that it is actually participating on the corporate voice VLAN.

HTTP requests to IP phones are not proxied and cannot be proxied due to the architecture of Cisco Unified CallManager. There is no method to register with CallManager an alternate URL for an IP phone to receive HTTP requests. To CallManager, all proxied IP Phones appear to have the same IP address and therefore the same HTTP POST URL.

Deployment Use Cases

The purpose of Cisco Unified PhoneProxy is to allow IP telephony endpoints to be deployed onto networks that are firewalled or physically separated from the organization's Voice VLAN.

Cisco Unified PhoneProxy has been designed to address two specific use cases:

Data VLAN to Voice VLAN bridging for Cisco IP Communicator users on the corporate data network

IP phone @ Home for telecommuters

Data/Voice VLAN Bridging

In this use case, the customer wants to maintain a separation between the voice VLAN and the data VLAN but still support Cisco IP Communicator deployments (of potentially mobile workers).

Cisco Unified PhoneProxy allows the customer to maintain the separation without having to open the voice VLAN to traffic from each of the Cisco IP Communicator hosts.

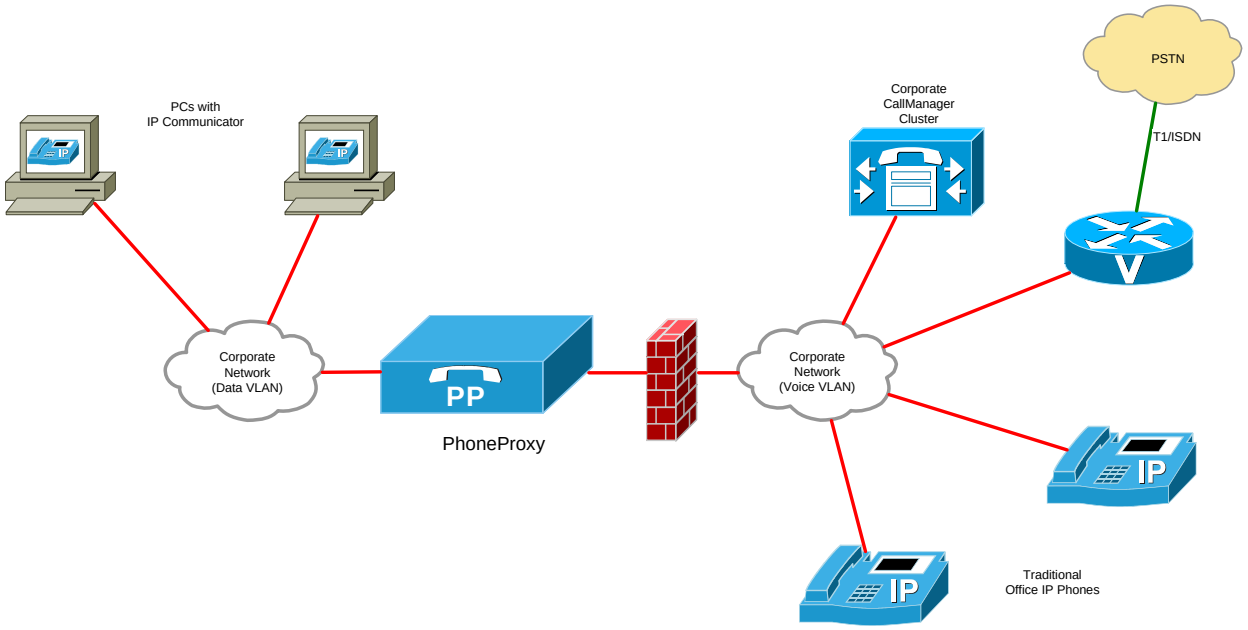

Figure 1 - Data VLAN to Voice VLAN Bridging

IP phone @ Home

In this use case, the customer wants to provide IP telephony service to remote workers without needing to provide a dedicated hardware VPN at the remote location.

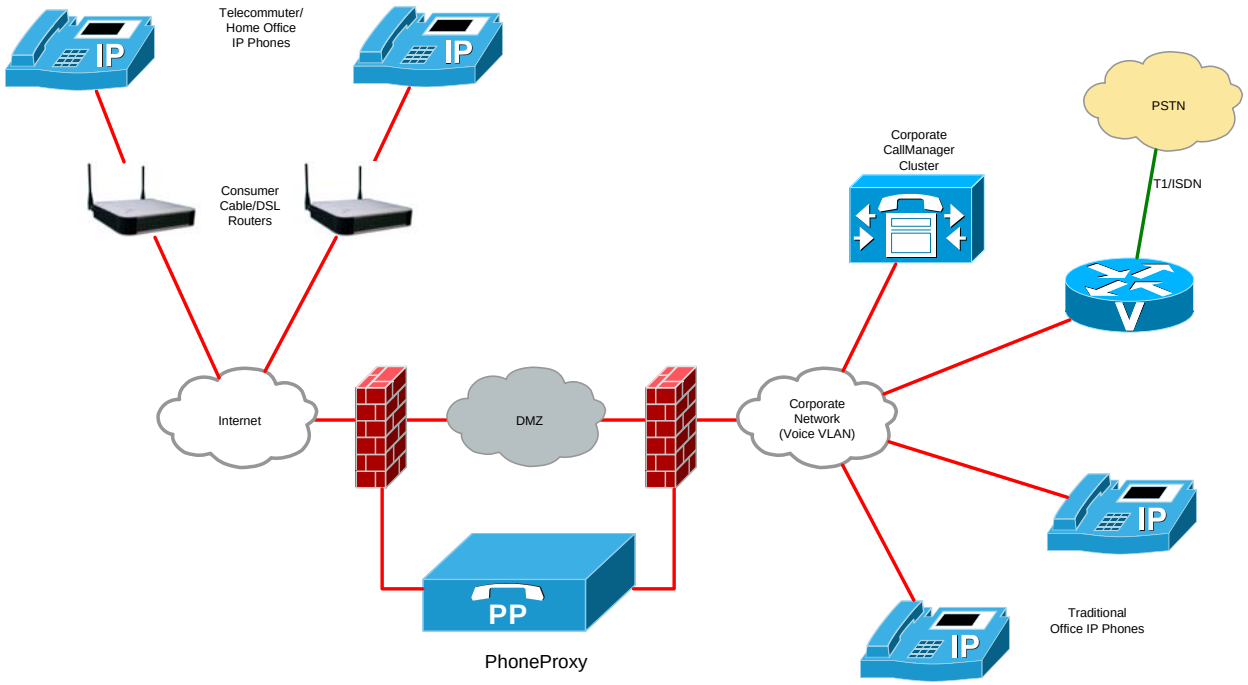

Figure 2 - Remote IP Phones

Encrypted Communications

Cisco Unified PhoneProxy supports encrypted communications with remote IP telephony endpoints. PhoneProxy will establish Secure SCCP connections with encryption capable endpoints and require all media to and from remote endpoints be transported over Secure RTP (SRTP).

Cisco Unified PhoneProxy Clustering

Each Cisco Unified PhoneProxy will support 1,000 IP telephony endpoints and 100 concurrent call legs. Like Cisco Unified CallManager, PhoneProxy supports clustering to ease user administration and also to prevent service disruption due to the failure of a single node.

Cisco Unified PhoneProxy Management

There are two distinct management interfaces:

Command-line interface (CLI) accessible via the built-in serial line or though secure shell (SSH) and used to configure the operating properties and environment of the appliance.

The User Management Console, which is used to provision users and IP telephony endpoints.

Anatomy of a Cisco Unified PhoneProxy

The Cisco Unified PhoneProxy has four Gigabit Ethernet ports. Each port has a fixed role in the PhoneProxy:

MGMT -- Management Ethernet Port. Used to maintain a dedicated management network.

NORTH -- North Ethernet Port, this interface should be configured with an address on the public or unsecured data network.

SOUTH -- South Ethernet Port, this interface should be configured with an address on the internal or secured voice network.

CLUSTER -- Cluster Ethernet Port, this interface should be configured on a private network, shared only with other Cisco Unified PhoneProxy nodes (cluster deployments only).

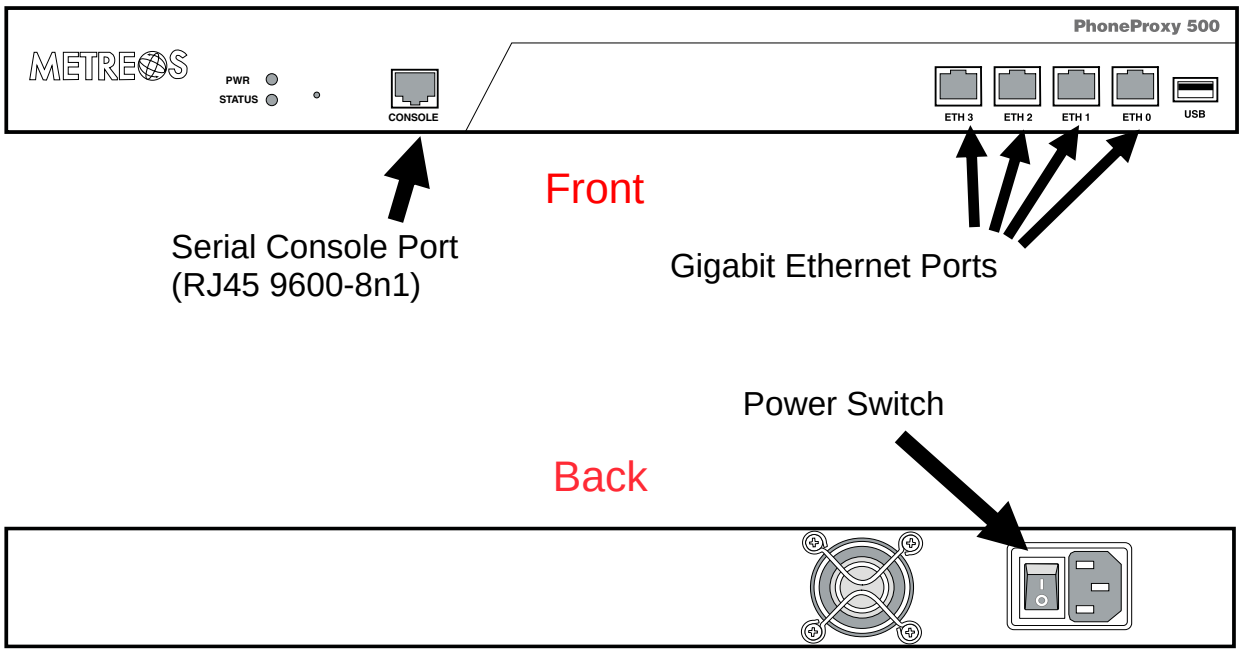

Figure 3 – Front and back of PhoneProxy

All ports are located on the front of the unit:

1x RJ45 – Serial Console Port

4x Gigabit Ethernet Ports

The serial console port is configured at 9600 Baud, 8-databits, no parity, and 1-stop bit. These settings are fixed and cannot be changed. Use a Cisco rolled cable to connect a Cisco Unified PhoneProxy to a PC or Terminal Server.

The four Gigabit Ethernet ports are labeled **LEFT to RIGHT**:

CLUSTER, SOUTH, NORTH, MGMT

Cisco Unified PhoneProxy CLI and Management Console

This section describes the CLI and management console

Command Line Interface

The Cisco Unified PhoneProxy CLI is used to manage the operational configuration of the PhoneProxy platform. It is used to configure and control the behavior of the PhoneProxy in your production network. These settings include network and cluster information that determine how the PhoneProxy will interact with the network as well as other PhoneProxy nodes. The CLI also provides a means to install user licensing and manage certificates for secure sessions. Additionally, the CLI can be used to view logs and status information for the PhoneProxy, plus other related functions.

The CLI is not used for the provisioning of Cisco Unified PhoneProxy end-users. Creating, deleting and related end-user configuration is managed by the User Management Console.

Accessing the CLI

The CLI can be accessed in multiple ways. One method is via a serial terminal connecting through the serial port marked “Console” on the front panel of the Cisco Unified PhoneProxy. Refer to the figure below for the serial connection settings. After the Ethernet interfaces are configured properly, the CLI can be reached by SSH over the network.

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

Figure 4 - Serial port settings

Case Sensitivity

The CLI is case sensitive and all commands are all lower case. Commands that are entered with incorrect capitalization will not be recognized by the command shell. If you attempt to enter a command and receive an error that states the command is unrecognized, check the spelling and capitalization of the command.

Command Structure

Commands issued to the CLI are predominately structured as an action and an object. The action is a verb, such as 'delete'; while the object is what is acted upon, like 'certificate'. Some commands do not have an object, such as ping, reboot, etc. In many commands, there are additional parameters that can appear after the object. The syntax and usage of each command is defined in the *Cisco Unified PhoneProxy Command Line Interface Guide*.

CLI Help System

The CLI has a built-in help system. The CLI help provides context-sensitive information about the available commands or detailed information about how to use a specific one. For a list of general actions and what they do, type `help` at the shell prompt.

To get help about a specific action, type `help` before the action in question. When help is used before the action in question, it will provide a brief description of what the action does. The '?' can also be used in the place of the word help. For example, typing the command `help delete` or `? delete` will provide a list of objects that can be acted upon and a brief description of what that combination does.

For more specific help, such as command syntax information, enter `?` after the action and object in question and hit return. When help is used after an action and an object, it will display the syntax for the combination of the action and object. For example, typing the command `delete certificate help` or `delete certificate ?` will display the syntax for using the combination of delete and certificate.

Logging into the CLI

Account Names

There is only one single administrator account—admin. Furthermore, no additional administrator accounts can be created. The administrator account can be used to log into the production boot images—image0 or image1— and it can also log into the maintenance boot image.

Password Management

The account can and should have different passwords for the maintenance and production boot images. After you have successfully signed in the first time, you will be prompted to change the admin password for the production boot images.

Strong Passwords

There are certain rules for acceptable passwords. Because the Cisco Unified PhoneProxy is often located in a network's DMZ, it must be protected by a strong password.

For a password to be considered strong, it must be eight or more characters in length without repeating the same character more than three times in a row. Also, the password should contain characters from three of the four following categories:

Uppercase letters

Lowercase letters

Numbers

Punctuation Characters (all the other printable ASCII characters)

Resetting the Production Boot Image Password

The first time you login to one of the production boot images you will be prompted to reset the password. While in one of the production boot images, the only password that can be changed is the admin password for the production boot images, and the password for both images will be changed at the same time. It is not possible to set a different password for image0 and image1.

NOTE: In case the password for the production images is forgotten, it can be reset by booting into the maintenance boot image.

Resetting the Maintenance Boot image Password

The first time you login to the maintenance boot image, you should use the account name 'admin' but there will be no password by default. After you have successfully logged in to the maintenance boot image, the `set password` command provides the ability to reset the maintenance partition password as well as the password for both production boot images.

If you set a password on the maintenance boot image and then forget it, there is no way for you to reset it. If you forget both the production and maintenance boot image passwords, you will have to return the box to have the passwords reset.

Authentication Failure Lockout on SSH Connections

If a password is entered incorrectly three times while trying to authenticate via SSH, the account will be locked out. As an additional security measure, there is no indication given that the lockout has occurred. The account can still be logged into via the serial connection. This will allow an administrator access to the Cisco Unified PhoneProxy even though the system has closed off the point of attack. Logging into the serial will reset the lockout. The lockout will also be reset 20 minutes after the last login attempt.

NOTE: You cannot log in by using SSH during such a denial of service attack. You must first neutralize the attack or isolate the box. Also remember that the user management application uses SSH to perform many of its tasks and will also be disabled by such an attack.

Authorization to Change Passwords

When changing passwords in either the maintenance or production boot images, you will be prompted to enter the current password.

Remote Access via SSH

After you have set the network configurations, primarily the South interface, the gateway, the routes, and the primary DNS server, the appliance can be remotely accessed via SSH. For example, if the South address is 10.1.14.99, at a command prompt, enter: `ssh admin@10.1.14.99` and then, when prompted, enter the password that was set earlier. You may also use PuTTY or SecureCRT, other any other SSH client.

Configuration Management

The current configuration will stay in effect until the system is rebooted, which is when the startup configuration will be loaded. To retain the current configuration across power fails and reboot, you should save the configuration.

The configuration for the production images is shared between them.

save config

To save the configuration settings beyond the system restart, the running configuration must be copied to the startup configuration by using the `save config` command.

show config startup or show config running

To show the configuration settings.

User Activation

After an account has been provisioned, it can be activated to allow the phone to register and make and receive calls. The activation can be done by the administrator via the CLI, or the end user via a User Activation web page. A third option is to use the user activation web service available on the South interface.

When a user activates, the supplied IP address is associated with the account. If another user activates with the same IP address, the first user account will be deactivated and the new user account will be associated with the IP address. If the same user activates with a new IP address, the account is re-associated with the new IP address. There is no way to connect to the Cisco Unified PhoneProxy from the same account with more than one IP address, or to connect two accounts to the same IP address.

CLI

A previously provisioned account can be activated by the administrator using the Cisco Unified PhoneProxy command shell. The administrator will need to know the account username and the IP address of the phone trying to connect. In the case that the user will be connecting from behind a NAT router, the WAN IP address should be the IP address supplied.

At the command shell prompt, enter:

```
>  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.

At this point, the phone is authorized to connect. The administrator can use the show user command to verify the activation status as well as the duration of time the account has been activated.

At the command shell prompt, enter:

```
>  show user
  name         sid             addr            duration connected
  ----         ---             ----            -------- ---------
  marge        SEP0003E348E321 [inactive]
  homer        SEP001647051B3A 192.168.1.100   2m 40s   c 1:1
```

Webpage

A previously provisioned account can also be activated by the end user using the Cisco Unified PhoneProxy User Activation Page. The user will need to know the account username and password as well as the IP address of the phone trying to connect. In the case that the user will be connecting from behind a NAT router, the WAN IP address should be the IP address supplied.

The Cisco Unified PhoneProxy User Activation page can be accessed at the IP address of the PhoneProxy's North interface. To do this, open a web browser and go to *https://<north>*. (If the web server certificate has not been installed yet, go to *http://<north>*.)

For convenience, the User Activation Page displays the IP address of the browser accessing the webpage. In most cases, this is the appropriate IP address that should be supplied; however, if a different IP address is needed, it can be specified explicitly.

For the webpage activation method to function properly, the Cisco Unified PhoneProxy HTTP service must be enabled. Also, the PhoneProxy must be set to publish the webpage.

At the command shell prompt, enter:

```
>  set phoneproxy http enable
>  set phoneproxy http publish webpage
```

Certificate Management

A certificate is used to authenticate and establish a secure session with a server. To enable secure web communications for user activation, a certificate must be created and installed on the appropriate interface.

Cisco Unified PhoneProxy supports 1024- and 2048-bit key encryption.

You may use an official certificate signed by a well-known certificate authority, or you may use a self-signed certificate. Standard browsers will recognize and automatically accept an official certificate, while a browser will prompt your users to verify the authenticity of a server presenting a self-signed certificate. Furthermore, you can specify which interface to install the certificate on. If a certificate is not given an interface qualifier, it will be used for both. The only way to explicitly set a certificate for a single particular interface is to specify that interface.

You may also retrieve a certificate from a URL. This will download the certificate file and place it in the appropriate incoming directory to install. Another option is to use SFTP to put the file into the incoming directory and then install it from there.

The Cisco Unified PhoneProxy command shell also allows you to show the certificates that are available to be installed and those that are already installed. This is done with the `show certificate` command. If the filename is included at the end of the command, then the contents of the certificate file will be displayed. For example, `show certificate` <certificate-file>. The `show certificate status` command is similar to the show certificate command; however, it only displays certificates that have been installed.

Certificates can be deleted from the pool of available certificated by using the `delete certificate` <file-pattern> command.

Web Services

The Cisco Unified PhoneProxy User Activation Web Service is available on the South interface (if enabled). It is described in Appendix A.

Licensed Users

Initially, the Cisco Unified PhoneProxy comes with a 25-user license. If you need more licenses please contact your reseller.

Setting the "activation authtimeout"

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

At the command shell prompt, enter:

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

The default value is 0, which means that phones that have been activated and connected will not time out.

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. After a phone registers with a Cisco Unified PhoneProxy, the connection will not go idle because traffic is sent back and forth between the IP phone and the PhoneProxy.

Idle connections often occur when an IP phone is physically disconnected or when DHCP assigns the phone a new IP address. Since the Cisco Unified PhoneProxy does not get a response from a phone at the expected IP address, the PhoneProxy considers the connection idle. The administrator can configure the number of seconds before an idle account times out.

At the command shell prompt, enter:

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

The default value is 300 seconds (5 minutes). This means the user must connect their phone within five minutes of activation or they will have to reactivate.

Administrator Inactivating a User via CLI

There are cases where a user should be manually inactivated. 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 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>
```

IP Phones

Configuration

See the Cisco *Unified PhoneProxy Installation and Quick Start Guide* for information on how to prepare a phone for connection via PhoneProxy.

Security

Security must be either enabled or disabled for all nodes in a cluster. If security is enabled on any one node in a cluster and not the others, then the cluster will not function.

When security is enabled, all phones on the North side of Cisco Unified PhoneProxy are required to use security. This means that the North side phones must all be supported by PhoneProxy for secure communication, namely 7941,7961,7970,7971.

Httpproxy

Cisco Unified PhoneProxy can be configured to also be an http-proxy for the remote IP phones. This will allow SoftKeys on the IP phone, for example, the Directory button, to operate normally for the remote IP phone user.

If the North network is not secure, then corporate security could be compromised, because requests and responses using httpproxy are not encrypted.

If the HTTPProxy service is enabled, Cisco Unified PhoneProxy will insert an HTTP proxy address into the ProxyServerURL of phone records. If HTTPProxy service is disabled, the phone records' ProxyServerURL will not be changed.

The Http proxy can either be hosted internally or externally. If the mode is internal, then HTTP requests are proxied by the HTTP proxy built-into the Cisco Unified PhoneProxy. If the mode is external then an external HTTP proxy must be specified. Unsetting the HTTPProxy mode configuration will return PhoneProxy to the default internal HTTPProxy mode.

The HTTPProxy externaladdress is the IP address of an external HTTP proxy that will be used to service HTTP requests from the phones. This is only used if mode is external. Requests will be directed to port 8088 at the specified address.

By default, no URLs will be proxied even if the httpproxy is enabled. URLs must be explicitly added to the whitelist to be proxied. The `set phoneproxy httpproxy allow` sub-command adds URLs to the httpproxy whitelist. The unset command will remove URLs from the whitelist. The asterisk character (*) can be used as a wildcard. A summary URL can be used to allow requests to many files from the same server. For example, entering the following into the whitelist, `set phoneproxy httpproxy allow http://10.1.1.10/*`, will allow all http requests to that server.

An important behavior to note is that Cisco Unified PhoneProxy will not proxy DNS requests between a phone on the North side and a DNS server on the South side. Therefore, all URLs that the IP phone will access from the North side should contain IP addresses rather than hostnames. Moreover, an IP phone's behavior is to resolve hostnames to IP addresses before sending the request. If the phone is trying to request, for example, the Cisco Unified CallManager Directory at *http://example.cisco.com/path/to/xmldirectory.asp* it will attempt to resolve the hostname example.cisco.com to an IP address before trying to send the request. Since the IP phone on the North side cannot query the corporate DNS server on the South side directly, the phone will return a "Host Not Found" error. If the CallManager Directory URL was instead configured as *http://10.1.1.10/path/to/xmldirectory.asp* then the phone will fire off the request as-is to the PhoneProxy which is also serving as the httpproxy. Provided that the URL is in the httpproxy allow list, the PhoneProxy will fetch the file and deliver it to the IP phone.

NOTE: The Cisco Unified PhoneProxy does not support importing HTTP proxy settings specified by the Cisco Unified CallManager. To use the same HTTP proxy settings, they must be configured manually through the CLI.

Be aware that if the North network is not secure (i.e., the Internet) then there is the possibility of compromising corporate security, as requests and responses using httpproxy are not encrypted.

http

Incoming HTTP from Cisco Unified CallManager administration page to the IP phone is not supported by Cisco Unified PhoneProxy. Normally this phone feature is disabled as an additional security measure. Where is it needed for debugging purposes, it must be enabled in PhoneProxy and then the phones must be reset to get the newly updated configuration XML file.

Using the Management Console

For IP phones to make and receive calls, they must have a user account created for them so they can login. This will require the Cisco Unified PhoneProxy Management Console to be installed on the administrator's computer.

NOTE: The Cisco Unified PhoneProxy Management 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).

When you first open the Management Console you will be presented the new configuration wizard. For step-by-step directions to walk through the configuration wizard, please refer to the *Cisco Unified PhoneProxy Installation and Quick Start Guide.*

To create and configure accounts that can be activated so an IP phone can register and make and receive calls on the Cisco Unified PhoneProxy cluster, you must install and use the PhoneProxy Management Console on the administrator's computer. The Management Console will create and publish a file (users.xml) that specifies all the user accounts allowed to activate on the cluster. Please see page 75 for an example of a users.xml file.

Installing Cisco Unified PhoneProxy Management Console

The Cisco Unified PhoneProxy Management Console software requires that J2SE v1.5 is installed on the computer that will run the console. The installer will install java for you if it is not present.

The software is not included in the box; however, it can be downloaded from the Cisco website. Please visit

http://www.cisco.com/en/US/partner/products/ps7057/index.html

to download the file (something like CUPPMgmtConsole-1.0.3.0001.exe). After the file is downloaded, you can use the following steps to install the Management Console.

Procedure

1. Double-click the executable file after the software has been downloaded to the administrator's desktop.
2. Follow on-screen instructions.

Configurations

The Cisco Unified Management Console allows you to manage the configuration of several Cisco Unified PhoneProxy clusters. Each configuration is given a name which is used to identify the configuration to the administrator.

Certain information stored in the configuration of the cluster is encrypted to prevent accidental disclosure. The protected information is the passwords used to access the admin accounts for each machine in the cluster. You must choose a strong password for encrypting this information, and the password must be supplied when you attempt to access the configuration.

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. There is nothing of particular lasting value in a configuration. You can ways rebuild the information in a configuration by importing cluster info and user lists from the publisher; however, you will lose any changes you made since you last published.*

Cluster Info

The cluster info describes the members of the cluster, the security status, whether you want to assign users to a given member, and whether you want logs downloaded automatically from a given member. The Certificate Trust List (needed by the phones when security is enabled) is also kept here.

CCMs

This is the list of Cisco Unified CallManagers available for assignment to users. A PhoneProxy cluster can manage users from many different CallManagers. Each CallManager in the list is identified by a unique name and the TFTP address used to access the CallManager cluster.

Users

This list specifies the users allowed to activate a phone using the Cisco Unified PhoneProxy. Each user must have a unique username, and a password, a CCM (from the list above), and the SID of their phone (e.g., SEP001122334455). An enable flag allows the administrator to exclude the user from the configuration temporarily if needed. Other fields are present for the convenience of the administrator.

Add

The add button creates a new empty row in the list of users. You must fill in all the required fields of the row before you can publish. The user name must be unique.

Edit

The user list operates somewhat like a spreadsheet. All the fields are live; you can edit them by clicking on them. You may use the Tab and Return keys to navigate around.

Delete

This Delete capability permanently removes the user from the configuration.

Publish

Click Publish to push the Certificate Trust List and users file to the Cisco Unified PhoneProxy cluster and install them. After the files have been installed, you can use the PhoneProxy command line interface to verify the users were provisioned successfully.

At the command shell prompt, enter:

```
>show user

  name       sid              addr        duration connected
  ----       ---              ----        -------- ---------
  marge      SEP0003E348E321 [inactive]
  homer      SEP001647051B3A [inactive]
```

Import/Export

The user list can be exported in a comma-separated value (CSV) format or its native XML format. To export users, click *Configuration* in the tool bar, and then choose *Export Users…* You will be asked to pick the fields you want to export, or mark the *Select All Fields* checkbox to export everything.

NOTE: *If exporting user data to be modified and re-imported later, be sure and export the Id. Otherwise you won't preserve the identity of the users.*

On the next screen, you will be asked to select which file format you would like to save the exported users as. The choices are comma-separated values file (CSV) or the native xml format. Both of these formats can be re-imported at a later point in time.

You can also request a CSV template, with field labels but no data if you wanted to create a template to populate with users from another source and then import.

You can import users from a Cisco Unified PhoneProxy, from a local xml file, or from a CSV file. To import users, click Configuration in the tool bar, and then choose *Import Users...* The next screen will ask you how you would like to populate your configuration with users.

If you choose to use a CSV file, the file must have proper field labels in the first row. The easiest way to insure this is to use the user export feature to create a CSV template file for you. Then just add the users' information... one user per row.

Things to be aware of with CSV imports:

In the template, only include the columns that will be imported. Import function does not import records (users) that contain a null value in one of the fields, even if the field is not a required field. At minimum, have the four required columns in the CSV (Username, Password, Sid, and CCM Name) because all accounts will need that information.

If you have exported a user list before, you will notice that the password field is hashed for security. When importing users, the password fields do not need to be pre-hashed. Specify the password in the CSV template and Cisco Unified PhoneProxy will hash the passwords itself.

Reports and Stats

For future use only.

System Maintenance

Network Configuration

Interfaces

The Cisco Unified PhoneProxy has four special-purpose Ethernet interfaces that can connect to various networks. By default, all of the interfaces are disabled. This means that the administrator must enable the ports that will need to be used for their deployment.

Interface Schematic

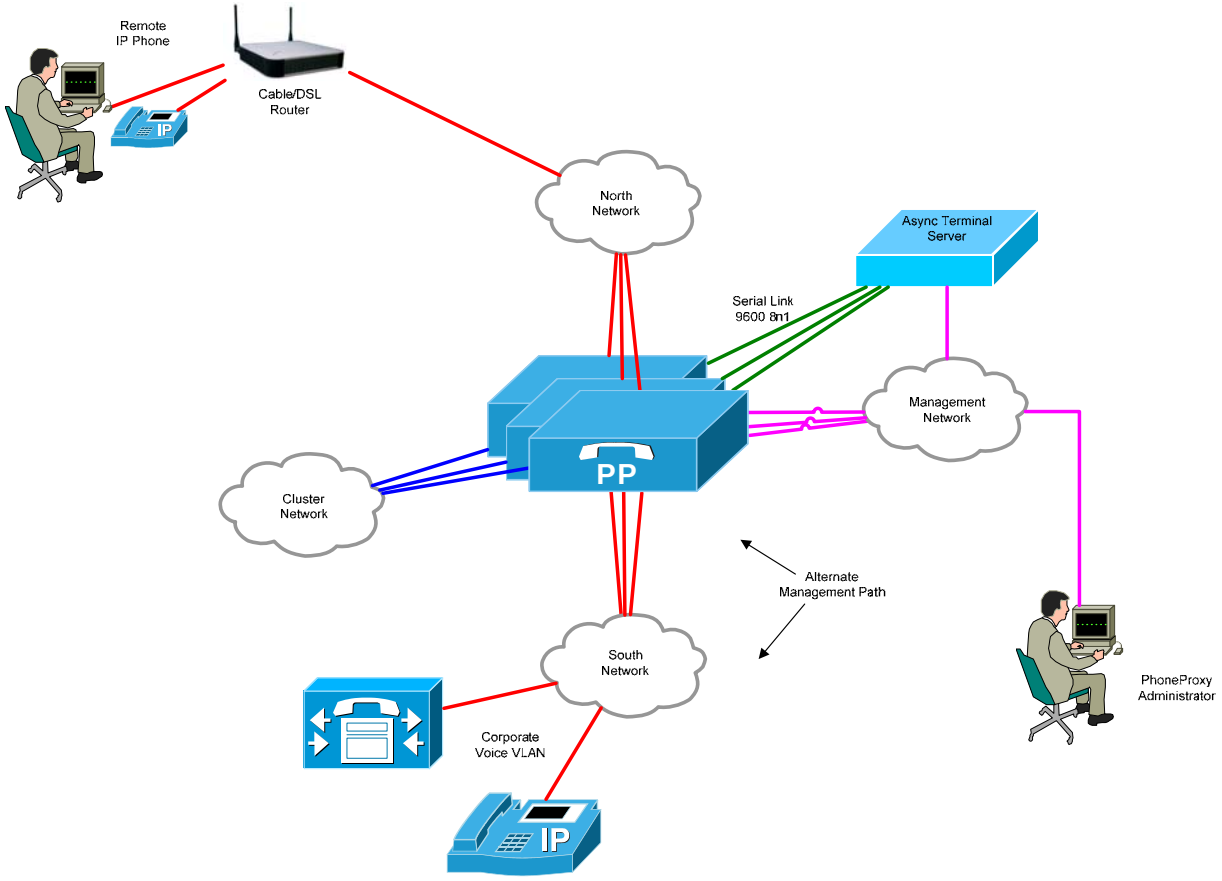

Figure 5 - Cisco Unified PhoneProxy network interfaces in action

North

The North interface connects to the network that the IP phones are on. In most deployments, this will mean exposing this interface to the public data network that end users connect.

South

The South interface is on the VLAN network used to connect to Cisco Unified CallManager. This interface is not exposed to the public network which means that the proxied IP phones will not connect to this network directly.

The South interface is also used to manage the Cisco Unified PhoneProxy if the Mgmt interface is not enabled.

Care should be taken to ensure this interface is reasonably secure. Certain Denial-of-Service (DoS) attacks may be directed at the active management ports (if enabled on the South interface). While every effort has been to ensure that the security of the device itself cannot be compromised on the South interface, South is a reasonable place to attempt to hijack signaling or voice traffic (since those appear unencrypted on this interface). Security may be enhanced by enabling the Mgmt interface, as this removes the need for data VLAN access to South.

Mgmt

The Mgmt interface may be used to manage the Cisco Unified PhoneProxy. It should not be exposed to the public data network.

Care should be taken to ensure this interface is reasonably secure. While the SSH protocol is secured from attacks, two other protocols available here are not: there is a proprietary protocol available on port 3140 used to deliver real time stats to the management console application, and SNMP ports 161/162 are also open here.

Cluster

This interface is used for clustered Cisco Unified PhoneProxy nodes to communicate. The clustered nodes exchange user activation information and configuration files. They do this with an unencrypted proprietary protocol.

Care should be taken to ensure this interface is very secure. Nothing significant could be gained by monitoring (user names and their IP addresses), but cluster performance could be seriously hampered or even disrupted by packet injection attacks and other types of DoS.

Dynamic Addresses (DHCP)

Cisco Unified PhoneProxy interfaces can be configured to use DHCP. However PhoneProxy will only honor the IP Address and netmask fields of the DHCP server response. DNS, NTP, default gateway, etc that the DHCP server may provide will be ignored by PhoneProxy.

The Cisco Unified PhoneProxy supports obtaining IP address and netmask information from a DCHP server. If, for example, the South network has a DHCP server running, the administrator can let that DHCP server assign an IP

address and netmask automatically by typing the following at the command shell prompt:

```
>  set interface south dhcp enable
```

Static Addresses

The IP addresses can also be statically assigned to the Cisco Unified PhoneProxy. For example, if the North network does not have DHCP enabled, the administrator can specify a static IP address for the PhoneProxy to use for the North interface. If the administrator is manually specifying the IP address, the netmask will need to be set also. At the command shell prompt, enter:

```
>  set interface north address 192.168.1.12 netmask 255.255.255.0
>  set interface north enable
```

Show Interface

This example shows the settings and status of the interfaces.

```
>  show interface
Name       Active? Mode    Address         Netmask
---------- ------- ------- --------------- ---------------
mgmt               static
north         *    static  192.168.1.12    255.255.255.0
south         *    dhcp    10.1.14.25      255.255.255.0
cluster            static
virtnorth          static
virtsouth          static

Default Gateway : 10.89.31.1
```

Default Gateway

The default gateway must be explicitly configured on the Cisco Unified PhoneProxy. In almost all circumstances, the default gateway should route out the PhoneProxy North interface. Routes to subnets accessible on the South, Management and Cluster interface must be explicitly configured.

```
>  set defaultgateway 192.168.1.1
```

Routes

Routes must be set to override the default gateway previously specified, if needed South, Mgmt, or Cluster resources are not on networks directly connected to the respective interfaces. For instance, if the Cisco Unified CallManagers, Cisco Unity servers, or DNS servers are located on the 10.1.12.0 network and the PhoneProxy South network is 10.1.14.0, we'd need this route to reach the CallManagers:

```
> set route addressmask 10.1.12.0/255.255.255.0 gateway 10.1.14.1 interface south
```

Use the "show route" command to show active routes:

```
> show route

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.28.0    *               255.255.255.0   U     0      0        0 eth0
169.254.0.0     *               255.255.0.0     U     0      0        0 eth0
default         192.168.28.2    0.0.0.0         UG    0      0        0 eth0
```

Ping

The ping command can be used to test connectivity to a host on the network. Note that some routers / firewalls block ping and so it is not a definitive test. For example, ping cannot be used to test connectivity to another Cisco Unified PhoneProxy, because PhoneProxy does not respond to ping.

Example:

```
> ping 10.89.31.1
PING 10.89.31.1 (10.89.31.1) 56(84) bytes of data.
64 bytes from 10.89.31.1: icmp_seq=0 ttl=128 time=3.31 ms
64 bytes from 10.89.31.1: icmp_seq=1 ttl=128 time=1.49 ms
64 bytes from 10.89.31.1: icmp_seq=2 ttl=128 time=1.70 ms
64 bytes from 10.89.31.1: icmp_seq=3 ttl=128 time=0.212 ms
64 bytes from 10.89.31.1: icmp_seq=4 ttl=128 time=1.42 ms

--- 10.89.31.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.212/1.627/3.310/0.990 ms, pipe 2
```

Nodename, DNS, and NTP

The nodename is used when requesting a DHCP address and also in various reports which show the status of nodes in the cluster. Often the DHCP server might associate the nodename and the assigned address in the external DNS records made available to others. Problems might arise when the same name resolves to more than one address (say, a North address and a South address).

Nodename

Typically, this would be the DNS name of your Cisco Unified PhoneProxy node; however, this is not the fully qualified name. If the PhoneProxy is to be fred.cisco.com, this command would set the nodename:

```
> set nodename fred
```

Safety of NTP and DNS

When NTP and DNS are configured they should almost always point to servers on the South interface (certainly when North is the internet). NTP servers on South are presumed safer, although the only real dependence upon time of day is log entries. A DNS server on South will ensure that HTTP requests from remote IP Phones will resolve to the correct addresses (particularly in networks with split DNS deployments). There are other places where a compromised DNS server could affect the system, such as when the Cisco Unified CallManager of a user is specified by name instead of by address.

Remember that you may have to set explicit routes to these services if they are not directly connected to one of the four interfaces.

DNS

Use `set dns` to configure the DNS domain name and primary and secondary DNS servers:

```
> set dns primary 10.1.1.2
> set dns secondary 10.1.1.3
> set dns domain example.com
> show dns
DNS Domain    : example.com
DNS Primary   : 10.1.1.2
DNS Secondary : 10.1.1.3
```

The domain name is not necessarily the domain qualifier to be applied to the nodename, but rather the domain qualifier to attach to non-qualified names presented for lookup.

NTP

Use `set ntp` to configure an ntp server and enable it:

```
> set ntp server 10.1.1.99 enable
> show ntp
NTP State  : enabled
NTP Server : 10.1.1.99
```

Advanced Configuration

Time

The time shown is the local time in the configured time zone. The time is shown and entered in ISO format. Always ensure the time zone is properly set before manually setting the time.

> ***NOTE:*** *Specifying an NTP server is the best method to keep time correct on the Cisco Unified PhoneProxy.*

```
> show time
Local Time : 2006-10-30 15:35:29
Timezone   : US/Central
```

The time zone should be entered in the Zoneinfo database format. Type the command `set time timezone ?` to see the complete list of acceptable time zones. Some example US time zones and GMT offsets are listed below:

US/Eastern	Etc/GMT	Etc/GMT-1
US/Central	Etc/GMT+1	Etc/GMT-2
US/Mountain	Etc/GMT+2	Etc/GMT-3
US/Pacific	Etc/GMT+3	Etc/GMT-4
US/Alaska	Etc/GMT+4	Etc/GMT-5
US/Hawaii	Etc/GMT+5	Etc/GMT-6

```
> set time timezone US/Central
> set time date 2006-10-29 time 15:35:39
```

SNMP

SNMP is disabled by default. You must enable SNMP before you can use it, and set the community string, location, contact name and email.

Cisco Unified PhoneProxy supports the Basic Linux Library (UCP-SNMP-MIB) as well as the generic IF-MIB.

SNMP is present on the South interface unless the Mgmt interface is enabled, in which case it is only available on the Mgmt interface.

Cluster

A number of Cisco Unified PhoneProxy nodes may be tied together into a cluster for ease of management and fail-over. There is a large section later in this document about clusters.

TFTP and HTTP Failover

A Cisco Unified PhoneProxy cluster may also support fail-over of TFTP and HTTP. This is documented in a later section, Heartbeat.

Advanced Networking

Some more complex tools are described for network debugging.

Packet Traces

You can capture a limited amount of packet data to attempt to diagnose certain problems. You might do better with span ports on your switch.

Traceroute

The traceroute command can be used to show the details of each hop along a route to a destination host by sending an ICMP ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE datagram from a host or a gateway.

System Management

There are several commands that enable basic system management like rebooting or shutting down the Cisco Unified PhoneProxy and switching between boot images.

Reboot and Shutdown

The `reboot` command will restart the system while the `shutdown` command will halt all the processes so the power can be turned off safely. If modifications to the running configuration have been made but not yet saved, the system will prompt the user to save them before rebooting or shutting down.

It is possible to suppress the confirmation prompts by using the force option. For example, typing the command '`reboot force`' will restart the Cisco Unified PhoneProxy without prompting to confirm the reboot or saving a modified running configuration. This would work similarly for the shutdown command. The command '`reboot save`' will save the running configuration, and then prompt to confirm rebooting the system. If you would like to reboot the system while still saving the configuration and suppressing the confirmations, type '`reboot force save`'.

***NOTE**: The force and save options work the same for both the shutdown command and the reboot command.*

Boot image Management

The boot images are the three bootable partitions that contain the Cisco Unified PhoneProxy operating system – maint, the maintenance boot image, and image0/image1, the production boot images. All three images are visible with the show command, but only two of the boot images are for production use—image0 and image1. Maint is the maintenance boot image and is only accessible at boot time through the serial connection. Under most situations, you will not use the maint boot image. During normal usage, either image0 or image1 will be active.

In order to update the software of the Cisco Unified PhoneProxy, the update will be applied to either image0 or image1, whichever boot image is not currently in use. Then, the **`set bootimage`** command can modify which boot image will load upon restart. After the system is restarted, it will load the configured boot image. If you need to revert to the previous version for some reason, you can set the boot image back to the other image that has not had the update applied.

***NOTE:** After a particular boot image has been updated to a newer version, it cannot be reverted to an older version of the software. The only exception to this is performing a factory reset which returns all boot images to the factory installed version.*

To see which version of the software is currently on each of the boot images, which boot image is set as default, and which boot image is currently running, use the **`show bootimage`** command. The default boot image is the boot image that will load next time the Cisco Unified PhoneProxy is rebooted. The current boot image is the boot image that is currently loaded and running.

Maintenance Boot Image

See Maintenance Partition section.

File Management

There are several commands that enable basic file management. These commands are `get`, `delete`, `list`, and `show`. The `get` command will retrieve a file from a URL and place it in the 'Incoming' directory of the Cisco Unified PhoneProxy. The `delete` command will remove a file from the PhoneProxy. After a file has been deleted it cannot be retrieved. The `list` command will display a table containing the entire collection of an object, so, for example, you can display a list of all the log files. The `show` command will display the contents of a file, so, for example, you can display the contents of a particular log file.

Configuration Management

There are several commands that enable system configuration management. These commands are `set`, `unset`, and `save`. The `set` command changes the operating parameters of the running configuration, while the `unset` command removes the configuration and returns the value to the factory default. The `save` command will copy the running configuration to the startup configuration, so the settings will be loaded the next time the system is restarted. If the settings are not saved any modifications to the running configuration will not appear after the system is restarted.

Updating Cisco Unified PhoneProxy

Cisco Unified PhoneProxy has been designed with ease of update in mind. Cisco may from time to time publish bug fixes and maintenance releases as update files that you download and install. The update files are encrypted and signed for your protection. It is also easy to return the Cisco Unified PhoneProxy to the software revision that was running prior to the update.

Getting updates

The `get update` command will download new software updates and save them on the Cisco Unified PhoneProxy so they can be applied at a later time. At the command shell prompt, enter:

```
>  get update <url>
```

Applying System Updates

After the software updates have been downloaded they can be applied to the Cisco Unified PhoneProxy. The update will be applied to either image0 or image1, whichever bootimage is not currently in use. At the command shell prompt, enter:

```
>  run update <updatename>
```

Because the update will automatically be applied to the boot image that is not in use, you will need to change the default boot image so that the updated image will load. The `set bootimage` command can modify which boot image will load upon restart. At the command shell prompt, enter:

```
>  set bootimage <image0|image1>
```

After the boot image has been changed, the Cisco Unified PhoneProxy will need to be restarted for the new image to load. At the command shell prompt, enter:

```
>  reboot
```

After the system is restarted, it will load the updated boot image. If you need to revert to the previous version for some reason, you can set the boot image back to the other image that has not had the update applied.

NOTE: *After a particular boot image has been updated to a newer version, it cannot be reverted to an older version of the software. The only exception to this is performing a factory reset which returns all boot images to the factory installed version.*

If the new boot image will not load or cannot be used, use the serial console to select the previous boot image after rebooting (or power-cycling if you must).

System Logs

The logs are a set of files in which system events are recorded. The Cisco Unified PhoneProxy saves three main types of logs—shell.log, update.log, phoneproxy.log. There are other logs for the activation service (activation*.log, http*.log), SNMP (snmpd.log), and the phoneproxy log archives (log-*.{txt,xml}).

To display a list all log files on the Cisco Unified PhoneProxy, type the following at the command shell prompt:

```
>  list log [<file-pattern>] [-page] [-nodetail]
```

To view a log, type the following at the command shell prompt:

```
>  show log <logfile> [-tail|-page] [-filter <regexp>]
```

The logs are safe to be deleted at any time if you would like a fresh record of events; however, deleting a log is a permanent operation. There is no way of retrieving a deleted log file. To delete a log, type the following at the command shell prompt:

```
>  delete log <file-pattern>
```

shell.log

Shell.log records configuration changes. This includes the use of the `set` and `unset` commands as well as requests to reboot the Cisco Unified PhoneProxy. When the system is rebooted, the shell.log file will record all the configurations it set while executing the startup configuration.

update.log

Update.log records events during the update process. This file will not appear the first time you run the Cisco Unified PhoneProxy, but it will appear after an update is attempted.

phoneproxy.log

The phoneproxy.log is the main log for general system messages, events, and statistics. The phoneproxy.log is not actually a log file but a link to the most recent general PhoneProxy log (log-<timestamp>.txt). When the size limit for the log file is reached, PhoneProxy will create a new log file and phoneproxy.log will be moved to link to the new log. This means if you would like to see the most recent log, just use this command:

```
>  show log phoneproxy.log
```

The Cisco Unified PhoneProxy can be configured to provide different levels of logging detail—min, brief, or full. To adjust this setting, at the command shell prompt, enter:

```
>  set phoneproxy loglevel <min|brief|full>
```

For almost all situations, the loglevel should be set to min or brief. Setting the loglevel to full will create a lot of log entries and will decrease the system's performance.

NOTE: *In the current version of the system, it is the administrator's responsibility to clean up the log files. Failure to clean-up the log files could result in filling up the log partition and unpredictable system behavior.*

NOTE: *Do not delete phoneproxy.log. If you do, it may not be correctly recreated.*

NOTE: If you delete the active log-<ts>.{txt,xml} files, Cisco Unified PhoneProxy will not create new ones until the normal time to rotate the files. It will continue to log to the files that you can no longer see. If this occurs and is a problem, rebooting the Cisco Unified PhoneProxy will restore visibility to all log files. The files are rotated after 5000 messages or at midnight.

Maintenance Partition

The maintenance boot image is for special circumstances such as restoring the system to factory settings and resetting the administrator password. The maintenance boot image is only accessible through the serial console interface. Also, it does not load network interfaces.

To boot into the maintenance boot image, press the up arrow key as soon as "GRUB Loading stage2" appears on the screen. There is only a small window of time to press the key so if you do not press the key in time, it will continue to load the configured boot image—either image0 or image1.

When the boot menu appears, you will be provided three choices. Your highlighted entry is shown at the bottom. Press the up arrow key to highlight option 0 to load the maintenance boot image.

Factoryreset

The `factoryreset` command restores the production partitions (image0 and image1) to their condition at manufacture, wiping out all settings, data, and updates. If some mishap renders the production partitions unusable, or if you just need to repurpose the machine and want to start with a clean slate, factory reset will do the job.

```
>  run factoryreset
```

Password

The `set password` allows you to change the password of the admin account on the maint boot image and also the production boot images. If you set a maint boot image password, be very careful to remember it. If you lose it, it cannot be recovered or reset. Write it down and put it in a safe place.

```
>  set password image
Enter old Password:
Enter new Password:
Repeat new Password:
Password changed on 'image0' partition
Password changed on 'image1' partition
```

You must enter the maint boot image's admin password (the 'old' password) in order to be allowed to change the password for any boot image.

Use the `unset password` command to remove the admin password from the maint boot image.

Miscellaneous

The maint boot image supports the usual system commands, `set bootimage`, `show bootimage`, `reboot`, `shutdown`, and `show version`.

Cisco Unified PhoneProxy Network Configuration and Firewalls

In this section we will introduce some common deployments and discuss their design.

No Firewalls Configuration

By far the preferred configuration is to simply not bracket the Cisco Unified PhoneProxy with firewalls. The PhoneProxy is at its core a firewall (based on Linux 2.6 netfilter/iptables). It is a smart, special purpose firewall for Voice traffic.

So if the network topology is:

Figure 6 - Example Corporate firewall scheme

The preferred Cisco Unified PhoneProxy configuration is:

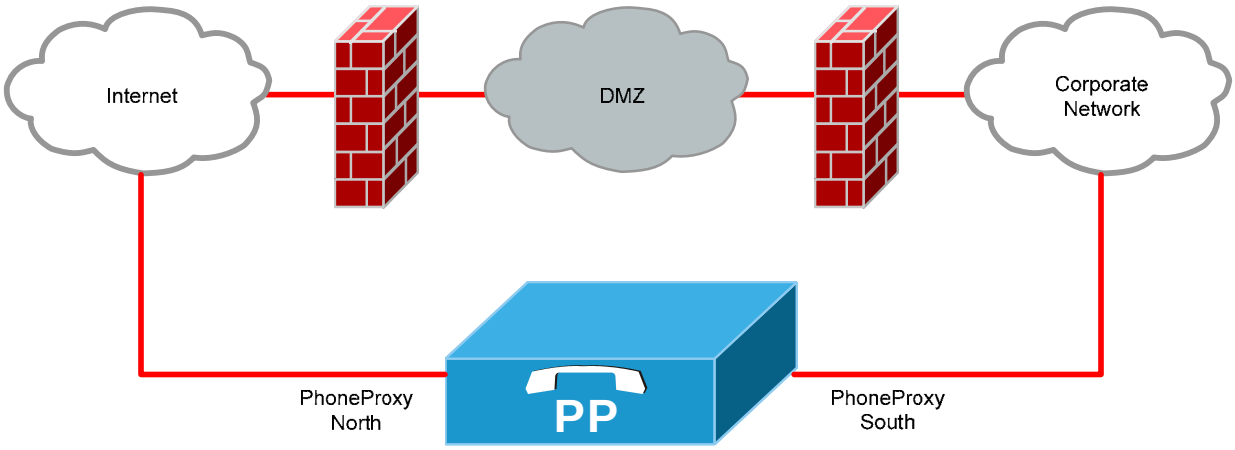

Figure 7 - Cisco Unified PhoneProxy bypasses data firewalls

Bracketed by Firewalls Configuration

If you simply must bracket the Cisco Unified PhoneProxy cluster by firewalls, is possible but the firewalls on each end must comply with these rules; otherwise, it will simply not work.

Reference this schematic:

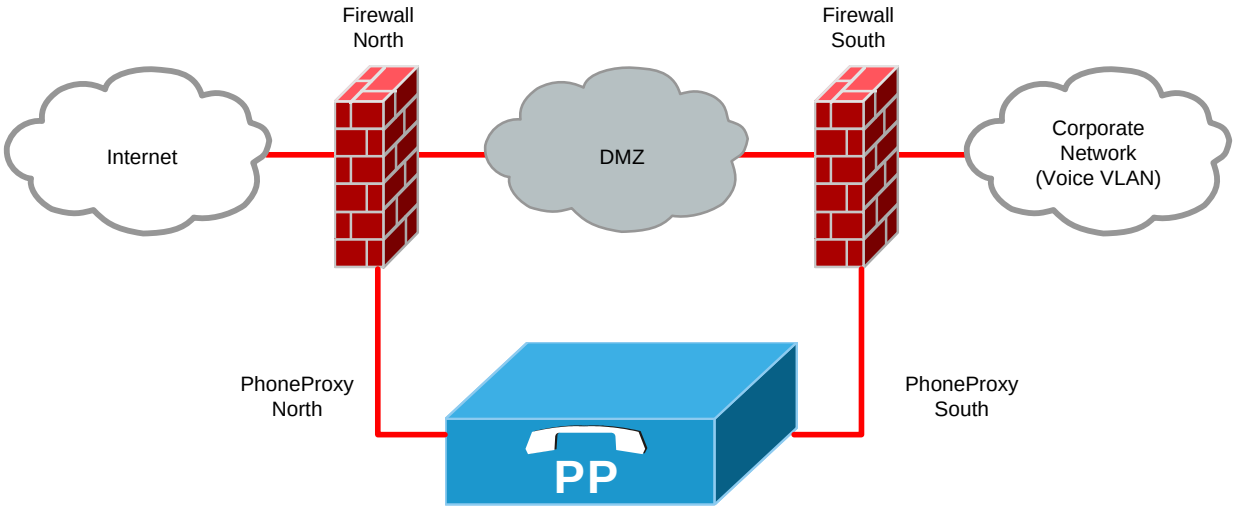

Figure 8 - Cisco Unified PhoneProxy bracketed by data firewalls

North-side Firewall configuration

1. No incoming address translation or port translation, the remote address from the internet must be visible to the Cisco Unified PhoneProxy's North interface as-is.
2. No outgoing address translation or port translation (NAT or PAT). The remote address on the Internet must see the Cisco Unified PhoneProxy's North interface address exactly as it is. The FW[North] cannot remap or obscure the real IP address of the PhoneProxy North interface to the Internet.
3. Enable stateful connection tracking.
4. The following port connections must be supported on the FW[North] to Cisco Unified PhoneProxy's North interface:

Port	Protocol	Description
Dst TCP 80	HTTP	User Activation Web Page (if HTTP is enabled and webpage is published; redirected to port TCP-443 when certificates are installed)

Dst TCP 443	HTTPS	User Activation Web Page (if HTTP is enabled and webpage is published and certificates are installed)
Dst TCP 2000 or 2443	SCCP, SecureSCCP	SCCP; only one is used TCP-2000 when secure SCCP is disabled, TCP-2443 when secure SCCP is enabled.
Dst TCP 8088	HTTP	HTTP proxy service for incoming HTTP request from remote IP phone (if enabled)
Dst UDP 69	TFTP	Used by remote IP phone to download its configuration
Dst UDP 20480-21680	RTP, SRTP	RTP media from remote IP phone; this range can be moved by the Cisco Unified PhoneProxy administrator.

Table 1 - North-side firewall incoming port connection requirements

Port	Protocol	Description
Src UDP 20480-21680	RTP, SRTP	RTP media to remote IP phone; this range can be moved by the Cisco Unified PhoneProxy administrator.
Dst UDP 53	DNS	Only if DNS is located to the North.
Dst UDP 123	NTP	Only if NTP is located to the North.
Src UDP 1024-65535	TFTP	TFTP data connections; not needed if FW[North] is TFTP aware.

Table 2 - North-side firewall outgoing port connection requirements

Special note on TFTP connections

The remote IP phone will send a TFTP request from phone UDP port N to PhoneProxy UDP port 69. That incoming connection must be allowed by the FW[North]. If there is an error in the request, PhoneProxy will respond to that request with a TFTP error response from PhoneProxy UDP port 69 to phone UDP port N.

This response is not a new connection, but rather a response on the existing connection.

If there is no error in the TFTP request, Cisco Unified PhoneProxy opens a new connection by allocating a new UDP port K, and sending a data packet from PhoneProxy UDP port K to phone UDP port N. The FW[North] must allow this new connection. The phone responds with an ACK from UDP port N to PhoneProxy UDP port K. The firewall must allow this response on the existing connection, and so on.

The phones will make TFTP request to Cisco Unified PhoneProxy; PhoneProxy in turn makes TFTP requests to Cisco Unified CallManager. The same rules apply then on the FW[South].

There is no way to limit which ports the phone will use for this process, nor can we limit (today) which ports Cisco Unified PhoneProxy will use. This is why such a large UDP incoming/outgoing range must be supported. If the firewall supports connection tracking and allows for incoming UDP connections and outgoing UDP connections to port 69, then things should just work. It is also possible to configure port triggering on the firewall to allow a new outgoing connection to UDP port N when a new incoming UDP connection to port 69 from port N is detected.

South-side Firewall Configuration

1. No incoming address translation, no port translation, the devices on the Voice VLAN (desktop phone, Cisco Unified CallManagers, voice gateways, and so on) must be visible to the Cisco Unified PhoneProxy's South interface as-is. To these devices Cisco Unified PhoneProxy will appears as just another end-point.
2. No outgoing address translation, i.e. NAT, no port translation. The devices on the Voice VLAN must see the Cisco Unified PhoneProxy's South interface exactly as it is configured on PhoneProxy. The FW[South] cannot remap or obscure the real IP address of the PhoneProxy South interface from the Voice VLAN.
3. Enable stateful connection tracking.
4. The following port connections must be supported by the FW[South]:

Port	Protocol	Description
Dst TCP 80	HTTP	User Activation Web Service (if http is enabled and webservice is published; redirected to port TCP-443 when certificates are installed)
Dst TCP 443	HTTPS	User Activation Web Service (if http is

		enabled and webservice is published and certificates are installed)
Dst TCP 22*	SSH/SFTP	Cisco Unified PhoneProxy CLI management
Dst TCP 3140*	PhoneProxy IPC	Proprietary management protocol for stats reporting through the User Management Console (if ipclog is enabled)
Dst UDP 161-162*	SNMP	SNMP based monitoring (if enabled)
Dst UDP 20480-21680	RTP	RTP media from IP telephony endpoints to PhoneProxy; this range can be moved by the PhoneProxy administrator.
Dst UDP 1024-65535	TFTP	TFTP data transfer (see explanation above)

Table 3 - South-side firewall incoming port connection requirements

* These ports only need to be enabled on FW[South] if the Cisco Unified PhoneProxy management port is not enabled. Management ports must be enabled on one or both of the PhoneProxy Management or PhoneProxy South interfaces. If the Management interface is not enabled, then the South interface becomes the default home of the management ports. If the Management interface is enabled, management on South interface is disabled.

Port	Protocol	Description
Dst UDP 69	TFTP	TFTP to configured CallManager(s)
Dst TCP 2000	SCCP	SCCP to configured CallManager(s)
Dst TCP xxx	HTTP, etc.	TCP connections required by HTTP-based phone services, e.g. if the CallManager cluster defines a service URL like http://myservicehost:8000/service.xml then the TCP connection to myservicehost through port 8000 must be allowed. Only needed if httpproxy is enabled and the service is listed in the allow list.

Dst UDP 53	DNS	Only if DNS is located to the South.
Dst UDP 123	NTP	Only if NTP is located to the South.
Src UDP 20480-21680	RTP	RTP media from PhoneProxy to IP telephony endpoints; this range can be moved by the PhoneProxy administrator.

Table 4 - South-side firewall outgoing port connection requirements

Management Network Configuration

Cisco Unified PhoneProxy provides a dedicated interface for management traffic, eth0 or MGMT. If this interface is not configured, then the PhoneProxy[South] port takes on double duty as the designated Management port. This means that if a Management port is not configured on a management network, then a PhoneProxy administrator must be able to traverse any FW[South] to reach the PhoneProxy[South] interface on ports TCP 22, TCP 3140, and UDP 161/162.

The management ports are required (at least TCP 22, the others are optional). You must deploy Cisco Unified PhoneProxy with either an enabled Management interface or with a South interface with the appropriate network access topology.

If there is to be a firewall between the Cisco Unified PhoneProxy management port and the management network, then the following ports must be supported in the firewall. The firewall must support stateful connection tracking:

Port	Protocol	Description
TCP 22	SSH/SFTP	Cisco Unified PhoneProxy CLI management
TCP 3140	PhoneProxy IPC	Proprietary management protocol for stats reporting through the User Management Console (if ipclog is enabled)
UDP 161-162	SNMP	SNMP based monitoring (if enabled)

Table 5 - Management network incoming port connections

Cluster Network Configuration

If the Cisco Unified PhoneProxy is to be deployed in a cluster, the Cluster interface on all the PhoneProxies to be clustered must be configured. The Cluster interface should only be connected to a private VLAN shared only with other PhoneProxies.

Cisco Unified PhoneProxy Actions

Cisco Unified PhoneProxy incorporates firewall functionality and understands how to manage IP telephony connections. It will only allow connections through its firewall as required for activated devices that remain registered and furthermore only open UDP ports on a per call basis.

For example, if you configure Cisco Unified PhoneProxy with HTTPS-based User Activation and then perform a port-scan on PhoneProxy's North interface from some arbitrary IP address. The port-scan would detect the following ports:

PORT TCP-80 - (HTTP)

PORT TCP-443 - (HTTPS)

Opening a web browser to PORT 80, you are redirected to HTTPS on port 443 and presented with the Cisco Unified PhoneProxy User Activation login page.

At the login page, the remote IP phone user activates their device by entering their user ID, password, and the IP address of the remote IP phone. In most cases this remote IP address will be pre-filled by the web-page to the correct value. When the user submits the form with the correct credentials, Cisco Unified PhoneProxy will open its firewall for the following ports for incoming traffic restricted to the remote phone IP address specified in the form:

PORT UDP-69 - TFTP

PORT TCP-2000 - SCCP (will be TCP-2443 if SecureSCCP is enabled)

PORT TCP-8088 - HTTP (if the http-proxy is enabled)

The remote IP phone will then proceed to TFTP configuration files from Cisco Unified PhoneProxy, which will in turn TFTP them from Cisco Unified CallManager. The files retrieved from CallManager are returned to the phone. PhoneProxy will monitor the configuration files and, in some cases, edit them to reflect the proxy environment configuration. In some cases PhoneProxy will generate a configuration file of its own to return to the remote IP phone without consulting a CallManager, again to keep the remote IP phone consistent with the proxy environment.

After all of the necessary configuration files have been received by the remote IP phone, the phone will open a SCCP (or SecureSCCP) connection to its configured primary Cisco Unified PhoneProxy which will in turn open a SCCP (always

SCCP, never SecureSCCP) connection to the configured primary Cisco Unified CallManager for that remote device, "proxying" whatever traffic the remote IP phone and CallManager send to each other.

When a connection is made, either for TFTP or SCCP (or SecureSCCP), the remote phone IP address is used to find the user record in the Cisco Unified PhoneProxy user database and lookup the information about the user's phone (the primary Cisco Unified CallManager). Two users cannot share a single remote IP address, and a single user cannot be associated with two different IP addresses at the same time. The rule is one user, one active IP address. From activation to activation a user may activate with any North-side IP address that is not currently associated with another user.

Furthermore, the ports opened for a given remote IP Address are not held open forever. Depending upon the Cisco Unified PhoneProxy configuration, the ports will be closed within a few minutes if the remote IP phone is not able to connect via SCCP (or SecureSCCP) and stay connected. The PhoneProxy administrator can also force the user to re-activate periodically even when connected. Failure to properly re-activate will close the opened ports for that remote IP address and disconnect the remote IP phone.

Because the user is configured in Cisco Unified PhoneProxy with a specific phone SID, then only a remote IP phone presenting that SID from that user will be allowed to register. Also access to configuration files will be restricted to only those allowed for that SID from the remote IP phone's IP address.

When calls are made and received across Cisco Unified PhoneProxy, the PhoneProxy firewall only opens the ports necessary to connect the specific endpoints with RTP streams.

The net effect is that a port-scan from an arbitrary IP address on the North-side of Cisco Unified PhoneProxy will never show any ports other than TCP80/TCP443 as being available. A port-scan from an 'activated' IP will only show TCP-2000 (or TCP-2443) and TCP-8088 (if enabled) open.

Activation

Activation is the process of associating a user with the IP address of a phone. This association is necessary because it ties together information from SCCP and TFTP with the SID of the phone and the assigned Cisco Unified CallManager for the user. This information is used for the following purposes:

Determining which Cisco Unified CallManager should handle phone configuration (TFTP) requests

Distributing load over the Cisco Unified PhoneProxy cluster

Securing the Cisco Unified PhoneProxy from unauthorized access

Audit records

The user provisioning process (using the Cisco Unified PhoneProxy Management Console) takes care of the first two items. The first is handled when the administrator picks the Cisco Unified CallManager for the user, the second when the user record is created. Users are each statically assigned up to three Cisco Unified PhoneProxy nodes to use as their primary, secondary, and tertiary CallManagers.

When the user is activated (by the user activation web page, the user activation web service, the CLI command line, or by open activation mode), the firewall built into the Cisco Unified PhoneProxy opens the three ports needed for proper phone operation to the user's address: TFTP, SCCP, and HTTP Proxy. If the ports are not opened, the user's phone will not be able to connect. The user activation step takes care of items 3 and 4 above.

When the phone uses TFTP to request its configuration file, TFTP is used to contact the assigned Cisco Unified CallManager (pulled from the user record) and obtain the file. Cisco Unified PhoneProxy then rewrites the file, substituting the user's assigned PhoneProxies for the assigned CallManagers and remembering the mapping (PhoneProxy to CallManager) for that phone.

When the phone connects with SCCP to a particular Cisco Unified PhoneProxy, the mapping of PhoneProxy to Cisco Unified CallManager for that phone is consulted, and the assigned CallManager is contacted. This process is central and critical to the proper operation of the PhoneProxy and the phones, ensuring that the load is distributed across the PhoneProxy cluster as well as the CallManager cluster.

A special operating mode, called open activation mode, opens all the ports, and handles requests for service by automatically activating the user when it knows enough to do so. Currently it only knows enough to automatically activate the user when the phone requests its configuration file (because the SID of the phone is embedded in the file name, and we can associate the user who owns the SID with the address of the TFTP request). This is why it is important for phones to start the connection process with a TFTP of their configuration file when using open activation mode.

NOTE: *open activation mode exposes your Cisco Unified PhoneProxy cluster and Cisco Unified CallManagers to DoS attacks. It should probably not be used when the North interface is connected to the Internet.*

Setting Up Required Activation Mode with the User Activation Web Page

1. Define users in the Management Console and publish them.
2. Pick a Cisco Unified PhoneProxy to be the official user activation host.
3. On Cisco Unified PhoneProxy, run these commands:

```
set phoneproxy http enable
set phoneproxy http publish webpage
set certificate selfsigned tag https-North
```

4. On all the PhoneProxies in your cluster, run this command:

```
set phoneproxy activation mode required
```

5. Tell the users to activate with their web browser at *https://<northip>*, where <northip> is the North address of the official user activation host. You can also give them the dns name of it, if that name is officially listed in the public DNS maps.

You might want to get an official certificate for the site so your users will not get a message from their browser about the self-signed certificate.

You should configure a second Cisco Unified PhoneProxy as a user activation host in case the first one goes down. You can provide access to it in various ways:

1. Tell your users both names or addresses and let them pick which one they want to use.
2. Change the public DNS maps to define a name which maps to both addresses, tell the name to your users, and let DNS take care of it.
3. Define the same virtnorth address on the two PhoneProxies, tell the address (or DNS name mapping to the address) to your users, and enable heartbeat.
4. Router or CSS games.

Setting Up Open Activation Mode

1. Define your users in the Cisco Unified PhoneProxy Management Console. Users must be assigned the (unique) SID of their phones. Cisco Unified PhoneProxy will use the SID to lookup the user.
2. Define a special user named AdHoCuSeR (spelled exactly like that).

3. Give the AdHoCuSeR the SID SEP000000000000, a nonsense password, and a Cisco Unified CallManager. When inactivated users connect with SCCP or request non-configuration files, this CallManager will field the requests.
4. Publish the users.
5. Execute this command on all the PhoneProxies in your cluster:

```
set phoneproxy activation mode open
```

You're done. Ready to go.

Some phones are better than others about TFTPing their configuration files when they've been disconnected. You may need to force the phones to reset by pressing the Settings button on the phone and then using the keypad to enter "**#**". Some versions of Cisco IP Communicator must be restarted to force a TFTP request of its configuration file.

Security Caveats

Be aware of the following caveats regarding the user activation service:

The service can be enabled without a certificate.

The service can have a self-signed certificate.

A man-in-the-middle attack which would cause a certificate warning pop-up in the user's browser, which they ignore.

Other Considerations

After users activate there are several ways their activation could be removed:

Idle timeout – If their phone does not connect or does not stay connected, the activation will be removed a few minutes after the last connection was closed (or when they were activated, which ever is later). This is meant to clean up idle activations, such as might happen if the phone (or the phone's router) gets a new IP address. The default delay is 5 minutes, and can be adjusted (command: `set phoneproxy activation idletimeout` N).

Auth timeout – Even if their phone is connected, they might still be periodically inactivated and forced to re-activate. By default this feature is turned off, but may be enabled by the administrator (command: `set phoneproxy activation authtimeout` N).

Explicit inactivation at the web page, web service, or CLI.

Activating a user with a new address will cause a phone connected on the old address to be disconnected.

A second user activating with the first user's address. The first user's phone will disconnect, try to reconnect, but likely the SID will not match and the first user's phone will not be allowed to stay connected.

Cisco Unified PhoneProxy cluster has only a single node and it is shutdown or rebooted.

Encrypted Communications

When Secure SCCP is enabled, the signaling traffic and any audio stream between Cisco Unified PhoneProxy and the remote IP phone will always be encrypted (encryption cannot be negotiated away). Encryption is only supported on compatible phones.

Encrypted Communications Schematic

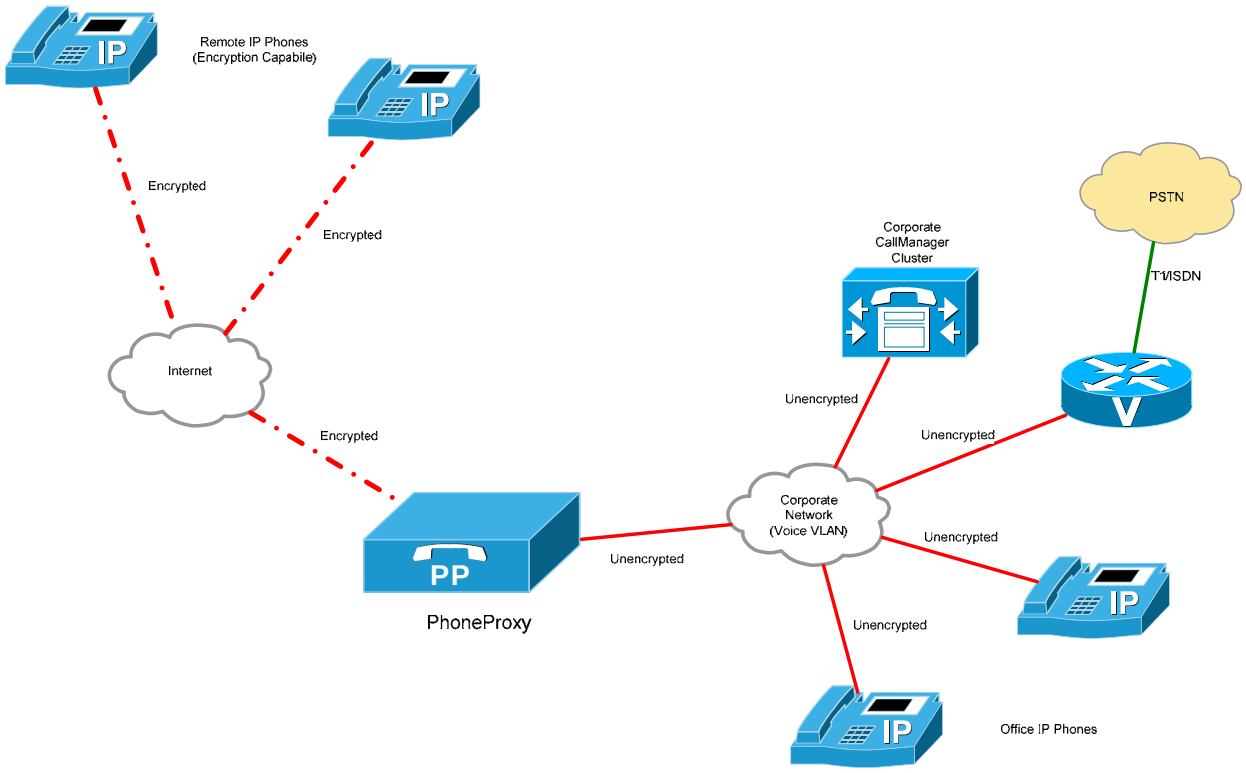

Figure 9 - Encrypted communications for remote IP Phones

Enabling Secure Communications

Prerequisites

Start with a system that is otherwise configured and online, users defined, phones connected, and so on.

The phones must be Cisco Unified PhoneProxy security compatible, i.e., they must be one of the following models: 7941, 7961, 7970, 7971

Two Cisco security eTokens (Cisco Part Number: *KEY-CCM-ADMIN-K9=*)

Enabling security on the Cisco Unified PhoneProxy

At the PhoneProxy CLI, enable SCCP security:

```
> set phoneproxy sccp security on
7155 semi-random bytes loaded
Generating RSA private key, 2048 bit long modulus
.....+++
.......................................+++
e is 65537 (0x10001)
Alias name: tftpkey
Creation date: Sep 21, 2006
Entry enter: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=tftpbd4140b3409f6f9996cd5054909b16155f1c6a15
Issuer: CN=tftpbd4140b3409f6f9996cd5054909b16155f1c6a15
Serial number: afb2fb5abecfcca3
Valid from: Thu Sep 21 14:04:53 GMT 2006 until: Sun Sep 20 14:04:53 GMT 2009
Certificate fingerprints:
         MD5:  58:C8:AB:C9:32:A6:FD:5E:EA:4E:11:9A:E3:90:4B:A6
         SHA1: 53:FB:5B:C5:D8:01:E6:D8:B5:D4:BA:D8:2A:B7:B3:CB:A2:A3:DE:36
7155 semi-random bytes loaded
Generating RSA private key, 2048 bit long modulus
..........................+++
................+++
e is 65537 (0x10001)
Alias name: capfkey
Creation date: Sep 21, 2006
Entry enter: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=capfbd4140b3409f6f9996cd5054909b16155f1c6a15
Issuer: CN=capfbd4140b3409f6f9996cd5054909b16155f1c6a15
Serial number: 8e47160473a5d901
Valid from: Thu Sep 21 14:04:54 GMT 2006 until: Sun Sep 20 14:04:54 GMT 2009
Certificate fingerprints:
```

```
        MD5:  1C:E6:8A:92:6C:FA:A9:DA:B6:D0:27:B3:73:58:77:42
        SHA1: 93:52:28:6C:13:36:4E:42:14:4C:77:83:0D:EE:DB:E2:2F:CF:FB:F3
```

Activating SCCP security will generate and save two self-signed certificates. Existing connected phones will stay connected, but new connections will be refused because Cisco Unified PhoneProxy will no long accept new insecure SCCP connections after SCCP security is enabled.

Open the Cisco Unified PhoneProxy User Management Console and open the configuration for the SCCP security enabled PhoneProxy cluster.

Select the menu item **Configuration -> Update Cluster**. This will cause the User Management Console to download the two new self-signed certificates from the Cisco Unified PhoneProxy cluster and combine them into a *certificate trust list (CTL)*.

When prompted insert one of the security tokens into the computer running the Management Console. When prompted for the second key, remove the first key and replace it with the second security token in the same USB port of the computer. The certificate from each token will be copied into the CTL. One of the tokens is used to sign the CTL. After the CTL has been signed the User Management Console will automatically publish the CTL to the Cisco Unified PhoneProxy cluster.

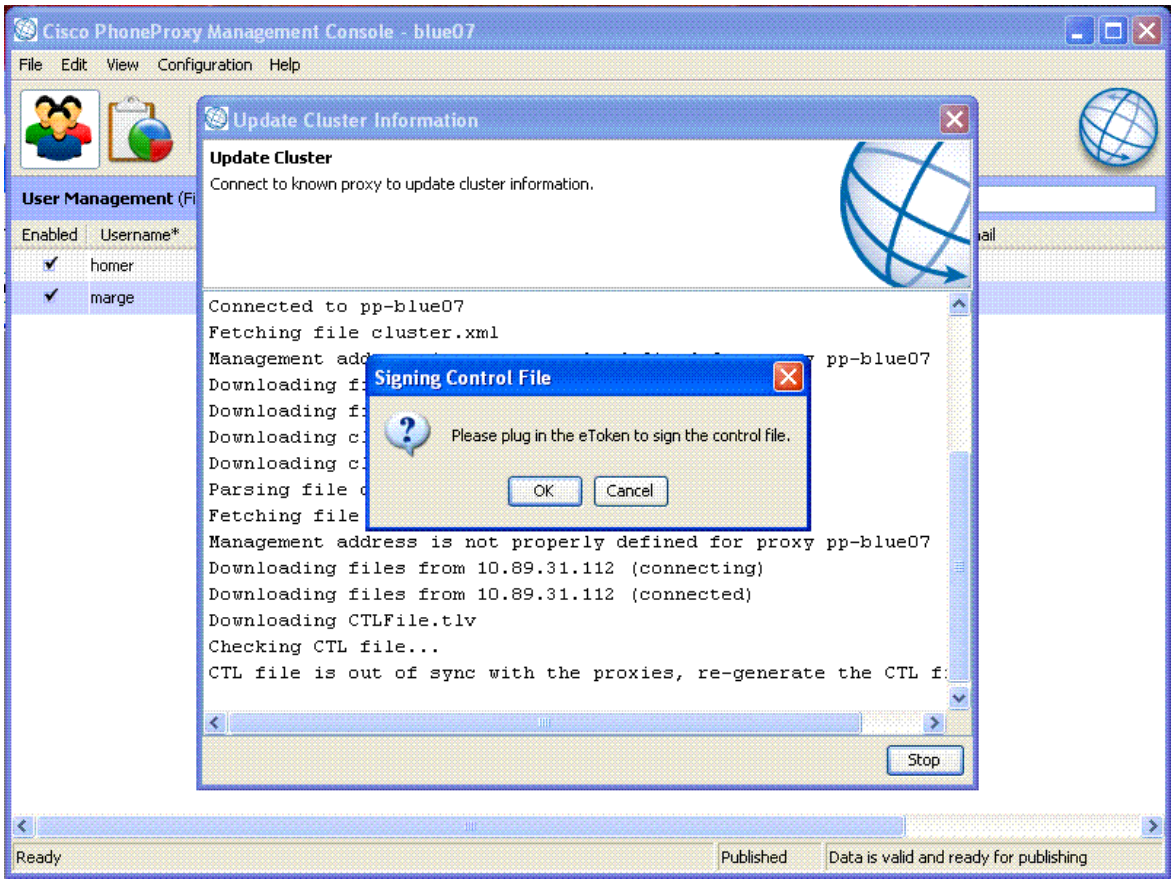

Figure 10 - User Management Console prompting for secure token

Reset all remote IP Phones (by pressing the settings button on the phone and then using the keypad to enter **#**). This will cause the remote IP Phones to disconnect and fetch new configuration files from Cisco Unified PhoneProxy, including the newly minted CTL. The presence of the CTL will forces the phones to use Secure SCCP and signed configuration files. The process of resetting the phones and activating security can take several minutes and the users may need to re-activate the remote IP phone during the process.

Because enabling security can be complicated for users, it is best if the administrator secures the phone at the office before sending the user home with it.

NOTE: *a phone will only accept a new CTL if it does not have one loaded now or if there is a certificate in common between the old one and the new one. Any phone used with another secure system will have to have its CTL removed first before it can be activated.*

NOTE: *whenever the cluster info changes, such as a cluster member added or removed, or an IP address or name changed, you must update the cluster info in the User Management Console and republish the user list. When you do this, you will be prompted to insert the tokens and regenerate the CTL, too.*

Taking Care of the Tokens

Keep them safe, under lock and key, and keep them each in separate places. If you put both of the security tokens in the same place, someone can steal them both, or you can lose them both.

If you lose one of the tokens, you should obtain a replacement as soon as possible, regenerate the CTL, and reset all the phones. Remember, the phones will accept a new CTL as long as one of the certificates in the old CTL is also in the new CTL.

If you lose both tokens, you will have to obtain replacements, regenerate the CTL, clear the old CTL from the phones, and reset them.

To clear the CTL from the phone:

1. press Settings.
2. select Security Configuration.
3. select CTL File.
4. press **# on the keypad to unlock.
5. press the More button, then the Erase button.

Some phones have a slightly different way of doing this. And you may need to clear Network Settings, too. See the *Cisco Unified PhoneProxy Quick Start Guide* for how to reconfigure the phone if you clear the Network Settings.

Clustering

Multiple Cisco Unified PhoneProxy nodes may be tied together into a cluster using the PhoneProxy Cluster interface.

Members of a Cisco Unified PhoneProxy cluster all share the same User Authentication, Device Activation, and Licensing domain. This means that when a user is activated on one node of the PhoneProxy, all the other nodes of the cluster are made aware of the activation. Also, when a device successfully registered to the Cisco Unified CallManager, all PhoneProxy nodes in the cluster are made aware. Finally, all nodes in the PhoneProxy cluster share the same set of user licenses so you do not need to purchase licenses for each individual node of the cluster.

Phones provisioned with a Cisco Unified PhoneProxy cluster will use the PhoneProxy cluster members for SCCP fault-tolerance after registered.

A pair of PhoneProxies in a cluster can be configured in a "heartbeat" pair to provide High-Availability for TFTP and HTTP-based user activation services.

NOTE: *Clusters are currently limited to a maximum of 3000 activated users. Therefore, the maximum practical size of a cluster is three or four nodes, but there is no actual limit on the number of nodes in a cluster.*

Clusters provide approximately linear scaling of registration. Users are statically balanced across the cluster members. That's the extent of the load sharing, though. A single Cisco Unified PhoneProxy can handle 1000 registered phones with up to 100 concurrent calls. Three nodes in a cluster can handle 3000 registered phones, and up to 300 concurrent calls as long as the calls are evenly spread across the cluster. A single node is still limited to 100 concurrent calls. If the users are very active phone callers, you may have to limit the number of users in the cluster in order to not exceed the recommended call volume.

Phones connected to a Cisco Unified PhoneProxy cluster will behave in a similar manner to phones connected to a Cisco Unified CallManager cluster. Each phone will maintain an Active (primary) connection and a Standby (secondary) connection, each to their configured PhoneProxy. The PhoneProxies in turn each maintain a single connection per phone to the configured CallManager.

Failover

Consider a Cisco Unified PhoneProxy cluster with two nodes (pp1 and pp2) and 2000 active and registered phones. Also consider that the PhoneProxy cluster is proxying to a Cisco Unified CallManager cluster that has at least as many nodes running the CallManager service as there are PhoneProxy nodes.

The Cisco Unified PhoneProxy users are assigned to PhoneProxy nodes such that each user has a primary (1000 users to pp1 and 1000 users to pp2) and a secondary node. Thus each node will have 1000 primary connections and 1000 secondary connections.

Now, suppose pp1 goes down. The phones using pp1 as their primary will switch their registration to their secondary (pp2) - after a brief blip they will be perfectly operational. The phones using pp1 as their secondary will not be affected at all. But, pp2 will now be handling 2000 active phones and all the call traffic for them. Our performance specifications have taken this scenario into consideration.

Cluster Schematic

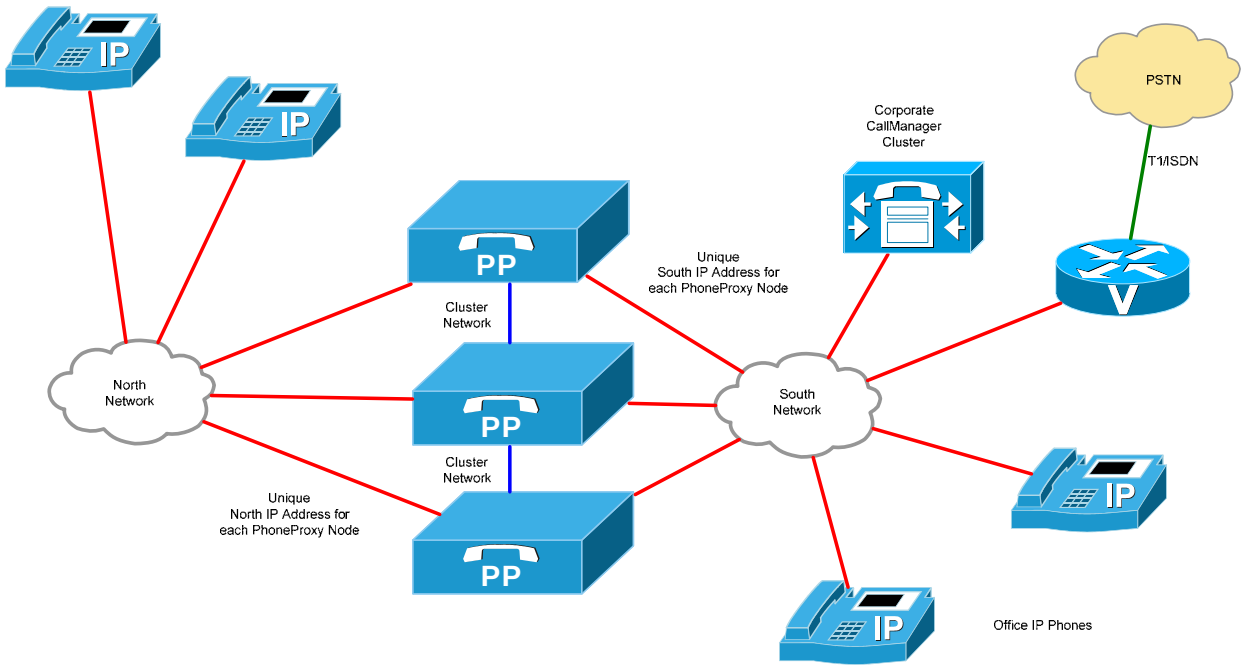

Figure 11 - Example Cisco Unified PhoneProxy cluster

Heartbeat

The IP phones are robust in regard to SCCP connections. To enhance availability two other important services need to be covered: TFTP (for configuration files) and HTTP (for user activation).

A cluster may be configured with one (or more) heartbeat pairs. Each member of heartbeat pair has two virtual interfaces—virtnorth and virtsouth. The virtnorth interface on both members of the pair are configured to share a North-side IP address but only one or the other member has the virtual interface enabled, never both at the same time. The same is true for the heartbeat pair's virtsouth interfaces and shared South-side IP address.

A software process running on each node in the pair negotiates with its peer to make sure that the IP address(es) are enabled on an interface somewhere. If one of the machines in the pair fails, the other will enable the address(es) on an interface and take over operations associated with it.

Here are the interfaces and services which may be bound to the virtual North or South address as needed:

virtnorth: tftp, http

virtsouth: http

The following steps to setup high availability assume that you are using the user activation web page available on the North IP address.

1. Allocate a third IP address on the North network to be the 'virtnorth' address. Pick your heartbeat pair, and assign that same virtnorth address to the virtnorth interface on both of the nodes in the pair, but do not try to enable the interface.
2. Dream up a name for the pair (this is a password of sorts). This will be the group name. Set this on both the nodes in the pair.
3. Set the heartbeat peer on each member of the pair to be the cluster IP address of the other member of the pair.
4. Enable heartbeat management of both TFTP and http. Do this on both the nodes in the pair.
5. Pick one of the heartbeat pair members to be the preferred node. Set the preferred node name on both to be the hostname of the node you chose.
6. Enable heartbeat on each member of the pair.
7. Tell your users to activate using the virtnorth IP address from now on, and also program that address as the TFTP server on the IP phones.

Use the `show interface` command to verify that the virtnorth interface is enabled on only one node of the pair. Shutdown that node, and the other should enable the interface.

Heartbeat Schematic

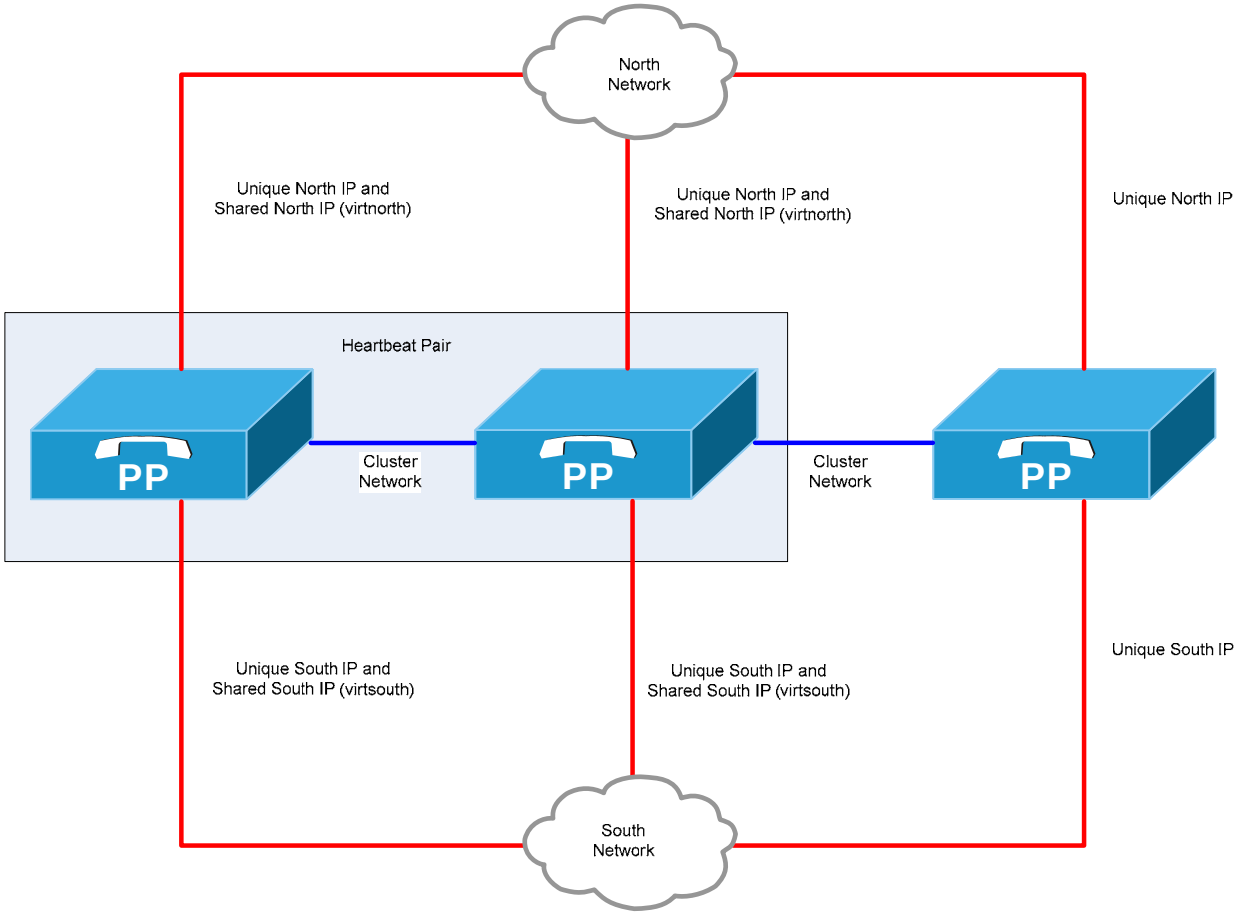

Figure 12 - Cisco Unified PhoneProxy cluster with a heartbeat pair enabled

Troubleshooting

This section includes some tips and tricks for diagnosing common problems.

Cisco Unified PhoneProxy network connectivity

Cannot 'ping' the Cisco Unified PhoneProxy

ICMP is disabled, you cannot ping Cisco Unified PhoneProxy. To test network connectivity use the `ping` and `traceroute` network commands in the PhoneProxy CLI. Ping other hosts on the network in question (e.g., router or gateway), and then ping hosts on networks that should be reachable from that network (tests routing).

Cannot SSH to Cisco Unified PhoneProxy or Connect via User Management Console

Ensure that networking is enabled on the IP address you are trying to connect to. Interfaces can be configured, but are not active until they are enabled.

Ensure that any firewall that is between you and the interface you are trying to connect to will allow you to connect via SSH (port 22) and IPC (port 3180)

Ensure you are using the correct password. If you issue an incorrect password 3-times, Cisco Unified PhoneProxy will lock you out of SSH-based logins for 20minutes. Serial Console logins are never locked out.

Device Activation and Registration

Cannot access User Activation Web Page

The web page is not published (set phoneproxy http publish webpage).

The http service is not enabled (set phoneproxy http enable).

The North interface is not configured or not enabled (set interface north …), or the virtnorth interface is not configured or enabled if you are using heartbeat.

The defaultgateway is not set to a North router, or other routes are not correct. Test connectivity and routing with ping and traceroute. Start with other machines on the North network and then try machines further away.

A firewall between the Cisco Unified Cisco Unified PhoneProxy and the user is blocking the traffic.

Remote IP Phone Will Not Register

Can the user reach the user activation web page? (if not, see preceding tips)

The phone TFTP address is set wrong.

The user is not activated with the right address. The address must be the address of the phone, not the user's computer. If at home behind a home router / firewall, the two will be the same. If at work using IP Communicator, the two will be the same. If at work with an IP phone, the two will not be the same.

The user is configured with the wrong SID. Check the SID of the phone vs. the user's configured SID.

The assigned Cisco Unified CallManager is down or not reachable or does not support TFTP. Use the ping command to test connectivity to the CallManager.

The phone is not provisioned at the Cisco Unified CallManager or provisioned incorrectly. The CallManager does not have auto-registration enabled or is out of phone numbers. The CallManager is oversubscribed.

The user's assigned Cisco Unified CallManager has security enabled. We do not support proxying to a secure CallManager.

Security was previously enabled on the phone? Perhaps you need to clear the phone settings and try again. Clear them all (network and security). Do it with the phone unplugged from the network.

Security is enabled? Perhaps the phone is not supported? Only 7941, 7961, 7970, and 7971 are supported for secure operation.

Phone is a 7985? Not yet supported.

Check the logs for messages related to the SID of the phone (you may need to increase the loglevel first before you'll see the good stuff – be sure to turn it down again when you are done):

```
>  show log phoneproxy.log –filter SEP001122334455
```

Remote IP Phone Reboots Repeatedly

See above.

If open activation mode is enabled, then the phone needs to get its configuration files before it can connect. This needs to be done each time the user activates: reset the phone.

Remote IP Phone registers for a while, but becomes in-activated

Has the administrator enabled authentication timeout? If so, the users will have to periodically re-authenticate to activate their phone or keep it activated.

General Registration Problems

The general debugging strategy will need some info from logs:

```
set phoneproxy loglevel full
show log phoneproxy.log -tail -filter Tftp
```

(using another ssh session...)
(activate the user)
(reset the phone)

You should see some messages about TFTP, including file requests and errors. If you do, we'll want your log files. You might just start with sending us the TFTP error messages. If you don't see any TFTP file requests, then you may have other problems. See paragraph below about phoneproxy log files.

It is totally normal for the phone to request CTLSEPblah.tlv and get an error. An error such as file not found is generally ok. A crash with a java exception is not. Now, if the phone requests SEPblah.cnf.xml (or SEPblah.cnf.xml.sgn) and gets a file not found error, it means the phone is not already provisioned with Cisco Unified CallManager.

(A note about log files: phoneproxy.log is a symbolic link to the most recent text log file (log-blah.txt). Blah is the date of the first entry, using ISO date format, e.g., 20061017134538907 would be 10/17/2006 at 1:45:38.907 pm. After 5000 lines, or at midnight, phoneproxy closes the current log file and starts a new one. So when using tail as above, you may stop seeing output. Hit ctrl-c, and then just run the command again. The symbolic link will be moved to the new log file.)

No-audio issues

Remote IP Phone can be heard but cannot hear audio (1-way remote audio)

There is a firewall (either the user's or the company's) which is not performing connection tracking right. The audio stream from the Cisco Unified PhoneProxy is being blocked. Try putting the phone in the DMZ of the home router. Trying disabling the firewall altogether (not advised for the company firewall).

If the situation is a remote phone calling another remote phone, try each calling a non-proxied phone. Then work from there with each phone separately.

Remote IP Phone can hear but cannot be heard (1-way local audio)

There is a firewall which is blocking the audio stream to the Cisco Unified PhoneProxy. This is likely the company firewall.

Remote IP Phone cannot hear audio, nor can it be heard (no-way audio)

Try the above remedies for one-way audio.

Is security enabled? Is the phone supported? Determine what the audio stream characteristics are. G.711 with 20 ms packets should work. There is a known issue when security is enabled and larger packet sizes are used. Turn the packet sizes down and try again.

Poor-audio issues

Remote IP Phone hears poor audio

Connection too slow?

Routing problems?

Firewall not good enough?

Heavy load on the Cisco Unified PhoneProxy?

Remote IP Phone user's audio is poor to local users

See above.

Appendix A

Activation Web-Service SOAP API

The activation web service may be used when corporate back-end systems are being used to authenticate users for Cisco Unified PhoneProxy use, and now need to actually activate the user on the PhoneProxy cluster.

There are two main styles: activation and login. The activation style is uses the credentials of the admin. You authenticate the admin first, get a token, then activate a user users with the token. The token will expire after a period of inactivity.

The login style you provide the user credentials including name, password, and ipaddr.

WSDL URL

The WSDL for the SOAP methods supported by the Activation Web-Service SOAP API can be retrieved from the Cisco Unified PhoneProxy at the following URL:

http://<phoneproxy-south-address/activation_service/service.wsdl

SOAP Methods

login

ARGUMENTS		
	Adminname	*Name of the administrator account (always 'admin' in release 1.0)*
	Password	*Password for administrator account*
RETURNS		
	Token	*Security token for subsequent request.*

phoneproxy_activate

ARGUMENTS		
	Token	*Security token (returned by 'login' method)*
	Username	*User to activate*
	Ipaddr	*IP address to activate user at*
RETURNS		
	"NOT-AUTHORIZED"	*String returned if security token is invalid or expired*
	"Activate Failed"	*If activation of username fails*
	"Activate Successful"	*If activation of username succeeds*

phoneproxy_inactivate

ARGUMENTS		
	Token	*Security token (returned by 'login' method)*
	Username	*User to inactivate*
RETURNS		
	"NOT-AUTHORIZED"	*String returned if security token is invalid or expired*
	"Inactivate Failed"	*If inactivation of username fails*
	"Inactivate Successful"	*If inactivation of username succeeds*

phoneproxy_login

ARGUMENTS		
	Username	*User to activate*
	Password	*Password for user*

	Ipaddr	*IP Address to activation user at*
RETURNS		
	"Login Failed"	*String returned if user activation fails*
	"Login Successful"	*String returned if user activation succeeds*

phoneproxy_logout

ARGUMENTS		
	Username	*User to inactivate*
	Password	*Password for user*
RETURNS		
	"Logout Failed"	*String returned if user inactivation fails*
	"Logout Successful"	*String returned if user inactivation succeeds*

Appendix B

Management Console XML Files

Cluster.xml

This file contains the configuration settings for a Cisco Unified PhoneProxy cluster. Specifically, it defines the name and interface IP addresses of the member nodes in the PhoneProxy cluster.

This file is created and managed by the Cisco Unified PhoneProxy in conjunction with the PhoneProxy's Management Console. It cannot be changed by the user.

An example cluster.xml file is shown below.

```
<cluster>
   <proxy
      uuid="17a98efd474962b0247eb2325d0d85b91a5ded15"
      name="pp-blue03"
      cluster_ip="192.168.2.13"
      mgmt_ip=""
      south_ip="10.89.31.108"
      north_ip="192.168.1.13"
      timestamp="1162484179070"
      />
   <master
      uuid="17a98efd474962b0247eb2325d0d85b91a5ded15"
      licensedUsers="3000"
      />
</cluster>
```

Users.xml

This XML file contains the user and IP phone information for all users authorized to activate on the Cisco Unified PhoneProxy. Each user entry in the file defines the user's name, username, password, IP phone SID, and the Cisco Unified CallManager they should connect to.

This file is created and published to the Cisco Unified PhoneProxy by the Management Console and should not be edited manually unless directed by the Cisco support staff.

An example users.xml file is shown below.

```
<users name="pp-blue03">
   <ccm name="ccm" default="true">
      <address>192.168.5.109</address>
   </ccm>
   <proxy uuid="17a98efd474962b0247eb2325d0d85b91a5ded15"
      assign_users="true" />
   <user id="568e3845-ecc3-4408-8cee-6ed731f35675" name="homer">
      <first>homer</first>
      <last>simpson</last>
      <ccmName>ccm</ccmName>
      <sccpProxy>17a98efd474962b0247eb2325d0d85b91a5ded15</sccpProxy>
      <sid>SEP001122334455</sid>
      <enabled>true</enabled>
      <seed>BpWSOSJv9pH_bbAnCd7j9UAQvm7F8v5U</seed>
      <hashPw>eGy7g1orzdhyffgrptVQv2dmDZg=</hashPw>
      <pwDate>2006-10-19-11-59-15-562</pwDate>
   </user>
</users>
```

Appendix C

3rd Party Cable/DSL Router Configuration

Remote IP Phones are often situated behind a 3rd party Cable/DSL router. These routers are usually configured to perform a type of Network Address Translation (aka NAT Overload). This allows the router to have a single public IP address on the 'outside' and a private IP network on the 'inside'. For media to reach an IP phone situated on the inside of a NATing router, the router must forward the UDP packets containing the RTP stream to the IP phone without changing the port number. Most newer Cable/DSL routers will do this automatically. If the router does modify the port number, you will have audio issues. Also, if the router supports Stateful Packet Inspection (SPI), you will not likely need to configure UDP port forwarding. However, if you experience audio issues, or if you have an older router without this capability, you may need to explicitly configure UDP port forwarding.

The NATing router should be configured to forward the UDP ports 20480-30000 to the IP address of the IP phone.

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

Configure your router

Some firewall/routers need to be configured to forward a range of UDP ports to the IP phone. This will allow the IP phone to receive audio when calls are made/received.

The configuration of each brand/model of firewall/router is different, but the basic task is the same.

Linksys routers

Procedure

1. From your web browser, connect to your router's administrative webpage. For Linksys this is typically *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

IP phone	20480	32768	UDP	*phone IP address*	**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.

Appendix D

Example Router ACLs for Bracketed Cisco Unified PhoneProxy Deployment

Router ACL Configurations for Cisco Unified PhoneProxy

Here are example ACL configurations for the routers that would exist
on either side of Cisco Unified PhoneProxy.

North-side router -- router between PhoneProxy and public network
South-side router -- router between PhoneProxy and corporate network

There are four (4) ACLs defined:
North-side Inbound -- inbound traffic ACL... public to PhoneProxy
North-side OutBound -- outbound traffic ACL... PhoneProxy to public
South-side Inbound -- inbound traffic ACL... corporate to PhoneProxy
South-side OutBound -- outbound traffic ACL... PhoneProxy to corporate

== North-side router configuration

```
NorthsideRouter#
interface GigabitEthernet0/1
description Northside int
ip address 10.10.10.1 255.255.255.0
ip access-group 111 in
ip access-group 112 out

;; Allow Incoming TFTP requests
;; TFTP is required
access-list 111 permit udp any host 10.10.10.2 eq tftp

;; Allow Incoming RTP streams (can be narrowed in PhoneProxy configuration)
;; RTP is required
access-list 111 permit udp any host 10.10.10.2 range 20480 32763

;; Allow Incoming HTTP/HTTPS user activation requests
;; HTTP/HTTPS based user activation is optional
;; HTTP is only used if a certficate for HTTPS is not installed
access-list 111 permit tcp any host 10.10.10.2 eq www
access-list 111 permit tcp any host 10.10.10.2 eq 443

;; Allow Incoming SCCP/SecureSCCP connections
```

```
;; Either SCCP (2000) or SecureSCCP (2443)
;; SCCP is the default unless sccp security is enabled on PhoneProxy
access-list 111 permit tcp any host 10.10.10.2 eq 2000
access-list 111 permit tcp any host 10.10.10.2 eq 2443

;; Allow HTTP service requests from remote IP Phones
;; HTTP-Proxy is optional
;; This port has an Http-Proxy listener that will forward
;; Http requests from remote-ip-phones to URLs in the corporate
;; network
access-list 111 permit tcp any host 10.10.10.2 eq 8088

;; Allow outbound TFTP messages
;; TFTP is required
access-list 112 permit udp host 10.10.10.2 any eq tftp
access-list 112 permit udp host 10.10.10.2 any gt 1024


== South-side router configuration

SouthisideRouter#
interface GigabitEthernet0/1
description SouthSide int
ip address 192.168.2.1 255.255.255.0
ip access-group 113 in
ip access-group 114 out

;; Allow inbound HTTP/HTTPS activation web-service requests
;; HTTP/HTTPS web-service based activation is optional
;; HTTP is only used if a certficate for HTTPS is not installed
access-list 113 permit tcp any host 192.168.2.2 eq www
access-list 113 permit tcp any host 192.168.2.2 eq 443

;; Allow inbound SSH management connections
;; One interface, either South or Mgmt must allow incoming SSH
access-list 113 permit tcp any host 192.168.2.2 eq 22

;; Allow inbound IPCLOG connections
;; This port is optional
;; IPCLOG is used to stream performance statistics from the
;; PhoneProxy to the User Management Console
;; These connection can be made on either South or Mgmt, but
;; SSH must be allowed to the same interface as IPCLOG
access-list 113 permit tcp any host 192.168.2.2 eq 3140

;; Allow inbound SNMP connections
```

```
;; SNMP is optional
access-list 113 permit udp any host 192.168.2.2 range snmp snmptrap

;; Allow inbound TFTP/RTP connections
;; TFTP/RTP are required
access-list 113 permit udp any host 192.168.2.2 range 1024 65535

;; Allow outbound SCCP connections
;; SCCP is required
access-list 114 permit tcp host 192.168.2.2 any eq 2000

;; Allow outbound DNS requests
;; DNS is strongly recommended; alternatively DNS
;; could be allowed outbound from north instead
access-list 114 permit udp host 192.168.2.2 any eq domain

;; Allow outbound NTP requests
;; NTP is strongly recommended; alternatively NTP
;; could be allowed outbound from south instead
access-list 114 permit udp host 192.168.2.2 any eq ntp

;; Allow outbound SNMP
;; SNMP is optional
access-list 114 permit udp host 192.168.2.2 any range snmp snmptrap

;; Allow outbound TFTP/RTP
;; TFTP/RTP is required
access-list 114 permit udp host 192.168.2.2 any eq tftp
access-list 114 permit udp host 192.168.2.2 any range 1024 65535
```