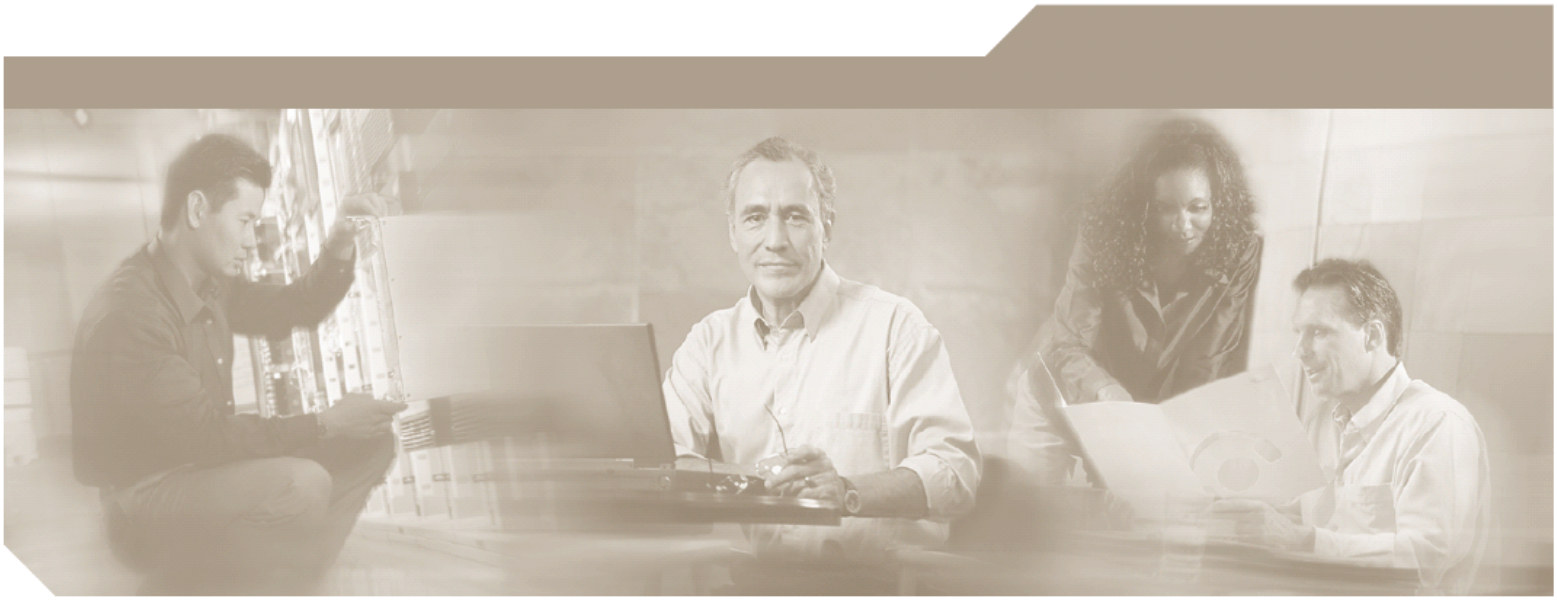


Cisco Unified PhoneProxy CLI Reference Guide

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-11919-01

Cisco Unified PhoneProxy Administration Guide

CONTENTS

Preface 1
Overview 1
Audience 1
Related Documentation 1
Reporting Security Problems in Cisco Products 3
Obtaining Technical Assistance 3
Obtaining Additional Publications and Information 5
Notational Conventions 7
CLI PURPOSE AND USAGE 8
PURPOSE 8
USAGE 8
CLI ACTIONS 13
DELETE 14
GET 15
HELP 16
LIST 17
PING 18
REBOOT 19
RUN 21
SAVE 22
SET 23
SHOW 25
SHUTDOWN 27
TRACEROUTE 29
UNSET 30
CLI OBJECTS 31
BOOTIMAGE 32
CERTIFICATE 33
CLUSTER 36
CONFIG 39

DEFAULTGATEWAY 41
DNS 42
HEARTBEAT 43
INTERFACE 46
LOG 48
NODENAME 50
NTP 51
PACKETTRACE 52
PASSWORD 55
PHONEPROXY 57
ROUTE 62
SNMP 63
SYSTEM 64
TIME 65
UPDATE 66
USER 68
VERSION 69
APPENDIX A 70
SERIAL CONNECTION 70
APPENDIX B 72
SFTP 72

Preface

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

Overview

This reference document describes all of the commands for the Cisco Unified PhoneProxy, provides the correct syntax for usage, and provides examples of proper usage.

Audience

The *Cisco Unified PhoneProxy CLI Reference* 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 Administration 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:

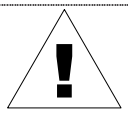
http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

• 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.

CLI PURPOSE AND USAGE

PURPOSE

The Cisco Unified PhoneProxy Command-Line Interface (CLI) is used to manage the operational parameters of the PhoneProxy platform. The administrator uses the CLI configure and control the behavior of the PhoneProxy. The settings that are managed by the CLI 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 means to setup certificates for secure sessions. Finally, the CLI can be used to view logs and status information for the PhoneProxy.

The CLI is not used for day-to-day management of the PhoneProxy users. For example, when creating and deleting user accounts, the Administrator should use the User Management Console application for management of PhoneProxy users. The User Management Console application is discussed with more detail in the *Cisco Unified PhoneProxy Quick Start Guide* and the *Cisco Unified PhoneProxy Administrator Guide.*

USAGE

Accessing the CLI

The CLI can be accessed in more than one way. One method is via a serial terminal connecting through the serial port marked “Console” on the front panel of PhoneProxy. Refer to the figure below for the serial connection settings. Once the interfaces are configured properly, the CLI can be reached by initiating a Secure Shell (SSH) connection over the network.

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

Figure 1 - 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 structured as an action and an object. The action is a verb, like 'delete'; while the object is what is acted upon, like 'certificate'. In some commands, there are additional parameters that can appear after the object. The syntax and usage of each command is defined in this 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 as shown below.

```
phoneproxy> help
Commands:
  delete     - Delete operations
  get        - Get operations
  help       - Display help on commands
  list       - List operations
  ping       - Ping another node
  reboot     - Reboot this node
  run        - Execute operations
  save       - Save operations
  set        - Set attributes
  show       - Show attributes and configuration settings
  shutdown   - Shutdown this node
  traceroute - Traceroute network to another node
  unset      - Remove attribute setting
```

For more 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 as shown in the example below.

```
phoneproxy> help delete
Command help for: delete
  delete certificate - Delete a certificate from the available pool
  delete log         - Delete node log files
  delete packettrace - Delete a packet trace
  delete update      - Delete an update package
```

For more specific help, such as command syntax information, type '?' 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. An example of this is shown below.

```
phoneproxy> delete certificate ?
Syntax:
  delete certificate <file-pattern>
```

System Management

There are several commands that enable basic system management. These commands are: `reboot`, `shutdown`, `ping`, `traceroute`, and `run`. The `reboot` command will restart the system while the `shutdown` command will halt all the processes so the power can be turned off safely. The `ping` command can be used to see if a host is available on a network while the `traceroute` command can be used to show the details of each hop along a route to a destination host. The `run` command will execute a pre-defined script.

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 PhoneProxy. The `delete` command will remove a file from the PhoneProxy. Once a file has been deleted it can not 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.

Boot Image Management

There are three boot images on the PhoneProxy—`maint`, `image0` and `image1`. All three images are visible with the `show bootimage` command, but only two of the boot images are for production use—`image0` and `image1`. The `maint` boot image is used for system recovery tasks 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. Refer to the *Cisco Unified PhoneProxy Administration Guide* for more information on boot images.

When updating the software of the PhoneProxy, updates will be applied to either `image0` or image1, whichever boot image is not currently in use. Once the update has been applied, the Administrator uses the `set bootimage` command to set which boot image will load upon restart. Once 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 image that has not had the update applied.

NOTE: *Once 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.*

The Maintenance Boot Image

The maintenance boot image is for system recovery purposes such as restoring the appliance to factory settings and resetting the administrator password. The maintenance boot image is only accessible through the serial console interface. The maintenance boot image has a very limited and unique set of allowed commands and does not any network communication.

To boot into the maintenance boot image, press the space 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. Use the '^' (**SHIFT-6**) and the 'V' to highlight option `0` to load the maintenance boot image.

Once the maintenance boot image loads, you will be prompted to enter a login name. Enter '`admin`'. By default, the password for the administration account on the maintenance boot image is empty, so you will not be prompted for a password.

Log File Management

The PhoneProxy records several log files, the most frequently used log files are — **shell.log**, **update.log**, **phoneproxy.log**.

It is the responsibility of the PhoneProxy administrator to prune log files from time-to-time. The PhoneProxy will not prune log automatically. The logs may be deleted at any time; however, deleting a log is a permanent operation. There is no way of retrieving a deleted log file.

shell.log

This log file records configuration changes issues through the CLI interface. This includes the use of the '`set`' and '`unset`' commands as well as requests to reboot the appliance. This log will not record all commands issues, only commands that have an effect on configuration. When the system is rebooted, the shell log file will record all the configurations it set while executing the startup configuration. See page 39 for more information about the startup configuration.

update.log

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

phoneproxy.log

This log file 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. These log files are named **log-<timestamp>.txt** and will accumulate in number over time. When the size limit for the log file is reached, PhoneProxy will create a new **.txt** log file and phoneproxy.log will link to the new log.

Each **.txt** log file has an associated **.xml** log file. The XML logs are used by the User Management Console or for reporting capabilities. The XML logs may also be used by the PhoneProxy administrator to generate site-specific reports.

CLI ACTIONS

Commands issued to the CLI are structured as an action and an object. The action is a verb, like '`delete`'; while the object is what is acted upon, like '`certificate`'.

This section of the guide will list the actions and each object that it can act upon. Also, it provides a description of what the action and object do, as well as what partition the command will be available in, and a reference to the pages that the actions and objects are discussed in more detail.

In the following tables, a checkmark in the "I" column means that the command is available in the `image0` or `image1` partition; a checkmark in the "M" column means that the command is available in the maintenance partition.

DELETE

The 'delete' action is a file management operation that deletes different types of files.

AVAILABLE OBJECTS:

Object	Description	I	M	More Info
certificate	Delete a certificate file from the available pool	✓		*See page 33*
log	Delete node log files	✓		*See page 48*
packettrace	Delete a packet trace file	✓		*See page 52*
update	Delete an update package file	✓		*See page 66*

SYNTAX:

```
delete <object> <file-pattern>
```

EXAMPLE:

```
phoneproxy> delete log httpproxy.log
Are you certain you want to delete these log files (httpproxy.log)
[y/N]?y
Deleting httpproxy.log
```

```
phoneproxy> delete log log-*
Are you certain you want to delete these log files (log-*) [y/N]?y
Deleting log-20060606104244366.txt
Deleting log-20060606104244403.xml
Deleting log-20060606105156100.txt
Deleting log-20060606105156139.xml
Deleting log-20060606105624632.txt
Deleting log-20060606105624647.xml
Deleting log-20060606140554734.txt
```

SEE ALSO:

get, list, show

GET

The 'get' action is a file management operation that provides the ability to pull files from a URL on to the PhoneProxy.

AVAILABLE OBJECTS:

Object	Description	I	M	More Info
certificate	Retrieve a certificate file from a URL	✓		*See page 33*
update	Retrieve an update file from a URL	✓		*See page 66*

SYNTAX:

```
get <object> <URL>
```

EXAMPLE:

```
phoneproxy> get update http://updateserver/update-1.0.3.0001.bin
```

SEE ALSO:

delete, list, show

HELP

The 'help' action and '?' character can be used interchangeably to provide brief descriptions and syntax for commands.

AVAILABLE OBJECTS:

All actions and objects.

SYNTAX:

```
help
help <action>
<action> ?
<action> <object> ?
```

EXAMPLE:

```
prompt> help delete
Command help for: delete
  delete certificate - Delete a certificate from the available pool
  delete log         - Delete node log files
  delete packettrace - Delete a packet trace
  delete update      - Delete an update package
```

```
prompt> delete certificate ?
Syntax:
  delete certificate <file-pattern>
```

LIST

The 'list' action is a file management operation that lists the available collection of an object.

AVAILABLE OBJECTS:

Object	Description	I	M	More Info
certificate	List certificates available or installed	✓		*See page 33*
log	List all log files	✓		*See page 48*
packettrace	List all packet traces	✓		*See page 52*
update	List available updates	✓		*See page 66*

SYNTAX:

```
list <object> [parameter]
```

EXAMPLE:

```
phoneproxy> list certificate
Available Certificates:
  No certificates available to install.
Installed Certificates:
File Size  Name                      MD5 Checksum
---------  ------------------------  --------------------------------
     2197  https-north.pem           5ca510c175e5cc0022636f4bec050208
```

SEE ALSO:

delete, get, show

PING

The 'ping' action is a system management operation that is used to see if a host is available on a network.

AVAILABLE OBJECTS:

n/a

SYNTAX:

```
ping <hostname or ipaddress>
```

EXAMPLE:

```
prompt> ping lisa
PING lisa (10.1.10.13) 56(84) bytes of data.
64 bytes from lisa (10.1.10.13): icmp_seq=0 ttl=63 time=0.400 ms
64 bytes from lisa (10.1.10.13): icmp_seq=1 ttl=63 time=1.95 ms
64 bytes from lisa (10.1.10.13): icmp_seq=2 ttl=63 time=0.378 ms
64 bytes from lisa (10.1.10.13): icmp_seq=3 ttl=63 time=0.345 ms
64 bytes from lisa (10.1.10.13): icmp_seq=4 ttl=63 time=0.430 ms
--- lisa ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.345/0.701/1.955/0.627 ms, pipe 2
```

SEE ALSO:

traceroute

REBOOT

The 'reboot' action is a system management operation that reboots the PhoneProxy.

AVAILABLE OBJECTS:

This action is special in that it does not need an object to act upon.

SYNTAX:

```
reboot [force] [save]
```

OPTIONS:

[force] – Restart the PhoneProxy without prompting to confirm the reboot or saving a modified running configuration

[save] – Save the running configuration to the startup configuration, regardless of if there were modifications, without prompting to confirm.

DESCRIPTION:

reboot [force] [save]

It is possible to suppress the confirmation prompts by using the force option. For example, typing the command '`reboot force`' will restart the PhoneProxy without prompting to confirm the reboot or saving a modified running configuration. 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`'.

EXAMPLE:

```
phoneproxy> reboot
Running-Config is different from Startup-Config
Save and Continue, Skip and Continue, or Abort [save/skip/abort]?
save
Saving configuration..
Are you certain you wish to reboot [y/N]? y
Broadcast message from root (pts/0) (Mon Jun 12 04:41:48 2006):
The system is going down for reboot NOW!
```

```
phoneproxy> reboot force save
Saving configuration
Broadcast message from root (pts/0) (Mon Jun 12 04:51:46 2006):
The system is going down for reboot NOW!
```

SEE ALSO:

shutdown

RUN

The 'run' action is a system management operation that is used to execute a pre-defined script such as running a packet trace or an update script.

AVAILABLE OBJECTS:

Object	Description	I	M	More Info
packettrace	Run a packet trace interactively.	✓		*See page 52*
update	Execute a system update on the inactive image.	✓		*See page 66*
factoryreset	Resets an appliance to the factory default state.		✓	

NOTE: *Factory reset overwrites both image0 and image1 with the version of the software that was originally installed. It also restores all configurations to their original default values. This is a permanent operation and cannot be undone*

SYNTAX:

```
run <object> <file-pattern>
run factoryreset
```

EXAMPLE:

```
phoneproxy> run update phoneproxy-1.0.3.0001-K9.bin
Executing update phoneproxy-1.0.3.0001-K9.bin against image1
Extracting update...
Updating.....................................................
.............................................................
.............................................................
Update complete.
```

SAVE

The 'save' action is a configuration management operation that saves the currently running configurations so they can be loaded the next time the system is restarted.

AVAILABLE OBJECTS:

Object	Description	I	M	More Info
Config	Save running configuration as startup configuration	✓		*See page 39*

SYNTAX:

```
save config
```

EXAMPLE:

```
phoneproxy> save config
```

SEE ALSO:

set, unset

SET

The 'set' action is a configuration management operation that changes the operating parameters of the running configuration.

AVAILABLE OBJECTS:

Object	Description	I	M	More Info
Bootimage	Set the node's default bootimage	✓	✓	*See page 32*
Certificate	Install a certificate	✓		*See page 33*
Cluster	Set the cluster configuration	✓		*See page 36*
defaultgateway	Set the default gateway	✓		*See page 41*
Dns	Set the primary or secondary DNS servers	✓		*See page 42*
Heartheat	Set the heartbeat configuration	✓		*See page 43*
Interface	Set interface configuration	✓		*See page 46*
Nodename	Set the name for this node	✓		*See page 50*
Ntp	Set NTP client configurations	✓		*See page 51*
Packettrace	Set the packet trace options	✓		*See page 52*
Password	Sets the password for the admin account		✓	*See page 57*
Phoneproxy	Configure PhoneProxy service parameters	✓		*See page 57*
Route	Define a static route	✓		*See page 62*
Snmp	Configure SNMP service parameters	✓		*See page 63*
Time	Set date, time, and timezones	✓		*See page 65*
User	Activate a PhoneProxy user	✓		*See page 68*

SYNTAX:

```
set <object> [parameter]
```

EXAMPLE:

```
phoneproxy> set nodename alpha
alpha> set nodename phoneproxy
phoneproxy>
```

```
phoneproxy> set bootimage image0
Setting boot image to image0
```

SEE ALSO:

unset, save

SHOW

The 'show' action is a file management operation that can be used to display runtime configurations, appliance status, or the contents of a file.

AVAILABLE OBJECTS:

Object	Description	I	M	More Info
Bootimage	Show this node's default bootimage	✓	✓	See *page 32*
Certificate	Show certificate information	✓		*See page 33*
Cluster	Show cluster configuration	✓		*See page 36*
Config	Show the running, startup configurations	✓		*See page 39*
defaultgateway	Show the default gateway	✓		*See page 41*
Dns	Show the DNS configuration	✓		*See page 42*
Heartbeat	Show heartbeat configuration	✓		*See page 43*
Interface	Show interface parameters/state	✓		*See page 46*
Log	Show node log files	✓		*See page 48*
Nodename	Show the name for this node	✓		*See page 50*
Ntp	Show NTP client configuration	✓		*See page 51*
Packettrace	Show packettraces, configuration and status	✓		*See page 52*
Phoneproxy	Show PhoneProxy configuration	✓		*See page 57*
Route	Show static routes	✓		*See page 62*
Snmp	Show SNMP configuration	✓		*See page 63*
System	Show system status information	✓		*See page 64*
Time	Show the current time/timezone	✓		*See page 65*
Update	List available updates	✓		*See page 66*
User	Show Proxy User configuration	✓		*See page 68*
Version	Show current software version	✓	✓	*See page 69*

SYNTAX:

```
show <object> [parameter]
```

EXAMPLE:

```
phoneproxy> show log
File Name                  Size     Timestamp
-------------------------- -------- ------------
http.access.log                  0 Jun  6 10:26
http.activation.log              0 Jun  6 10:26
http.error.log               21305 Jun  9 04:21
httpproxy.log                 3254 Jun  9 04:21
log-20060611120037603.xml  1205303 Jun 12 00:00
log-20060611120037615.txt   559440 Jun 11 23:59
log-20060612000037603.xml   468731 Jun 12 04:39
log-20060612000037607.txt   217560 Jun 12 04:39
phoneproxy.log                 25 Jun  7 11:26
phoneproxystdout.txt         2006 Jun  7 11:26
shell.log                   19777 Jun  9 04:29
shell.log.1                 49975 Jun  7 05:39
update.log                   4175 Jun  6 10:40
```

```
phoneproxy> show bootimage
Image  Version    Default? Current?
------ ---------- -------- --------
maint  1.0.1.0001
image0 1.0.3.0001    *        *
image1 1.0.2.0010
```

SEE ALSO:

delete, get, list

SHUTDOWN

The 'shutdown' action is a system management operation that halts all processes and shuts down the PhoneProxy.

AVAILABLE OBJECTS:

This action is special in that it does not need an object to specify what to do.

SYNTAX:

```
shutdown [force] [save]
```

OPTIONS:

[force] – Shutdown the phone proxy without prompting to confirm the shutdown or saving a modified running configuration

[save] – Save the running configuration to the startup configuration without prompting to confirm, regardless of if there were modifications.

DESCRIPTION:

shutdown [force] [save]

It is possible to suppress the confirmation prompts by using the force option. For example, typing the command '`shutdown force`' will shutdown the PhoneProxy without prompting to confirm the shutdown or saving a modified running configuration. If you would like to shutdown the system while still saving the configuration and suppressing the confirmations,
type '`shutdown force save`'.

EXAMPLE:

```
phoneproxy> shutdown
Running-Config is different from Startup-Config
Save and Continue, Skip and Continue, or Abort [save/skip/abort]?save
Saving configuration..
Are you certain you wish to shutdown [y/N]?y
Broadcast message from root (pts/0):
The system is going down for system halt NOW!
```

```
phoneproxy> shutdown force save
Saving configuration
Broadcast message from root (pts/0):
The system is going down for system halt NOW!
```

SEE ALSO:

reboot

TRACEROUTE

The 'traceroute' action is a system management operation that is used to trace the route a packet takes from origin to destination.

NOTE: Pressing CTRL+C while the traceroute command is running will interrupt the process and return the command prompt. This is useful to avoid waiting until 30 hops if there is a series of timeouts.

AVAILABLE OBJECTS:

n/a

SYNTAX:

```
traceroute <hostname or ipaddress>
```

EXAMPLE:

```
phoneproxy> traceroute lisa
traceroute to lisa (10.1.10.13), 30 hops max, 38 byte packets
 1  10.1.14.1 (10.1.14.1)  0.556 ms  0.550 ms  1.078 ms
 2  lisa (10.1.10.13)  0.290 ms  0.273 ms  0.205 ms
```

SEE ALSO:

ping

UNSET

The 'unset' action is a configuration management operation that removes a configuration that was previously set, returning it to the default value.

AVAILABLE OBJECTS:

Object	Description	I	M	More Info
certificate	Uninstall a certificate file	✓		*See page 33*
cluster	Remove cluster configuration options	✓		*See page 36*
config	Resets the configuration to the factory defaults	✓		*See page 39*
defaultgateway	Unset the default gateway	✓		*See page 41*
dns	Unset the primary or secondary DNS servers	✓		*See page 42*
heartbeat	Unset heartbeat service configuration	✓		*See page 43*
interface	Disable network interface	✓		*See page 46*
ntp	Remove NTP server from server list	✓		*See page 51*
packettrace	Unset packet trace options	✓		*See page 52*
phoneproxy	Remove PhoneProxy service parameters	✓		*See page 57*
route	Remove a static route	✓		*See page 62*
snmp	Unset SNMP service parameters	✓		*See page 63*

SYNTAX:

```
unset <object> [parameter]
```

EXAMPLE:

```
phoneproxy> unset cluster name
```

```
phoneproxy> unset cluster member 10.1.1.10
```

SEE ALSO:

set, save

CLI OBJECTS

Commands issued to the CLI are structured as an action and an object. The action is the actual command, like '`delete`'; while the object is what is acted upon, like '`certificate`'.

This section of the guide will discuss the objects that can be acted upon by actions. Furthermore, any additional parameters, whether optional or required, will be enumerated and explained. The syntax and usage of each command is defined in this guide as well as through the CLI built-in help.

BOOTIMAGE

There are three bootable partitions on the PhoneProxy – `maint`, the maintenance partition, and `image0`/`image1`, the production partitions. See page 11 for more information on boot images.

SYNTAX:

```
set bootimage image0|image1
show bootimage
```

OPTIONS:

n/a

DESCRIPTION:

set bootimage

Sets the node's default boot image. This is the boot image that will be loaded the next time the PhoneProxy is rebooted.

show bootimage

Shows a table with information about the three boot images, `maint`, `image0`, and `image1`. The table includes information about which version of the software is currently installed on each of the boot images. In addition, it shows which boot image is set as default and which boot image is currently running. The default boot image is the boot image that will load next time the PhoneProxy is rebooted. The current boot image is the boot image that is currently loaded and running.

EXAMPLE:

```
phoneproxy> show bootimage
Image  Version    Default? Current?
------ ---------- -------- --------
maint  1.0.1.0001
image0 1.0.3.0001    *        *
image1 1.0.2.0010
```

CERTIFICATE

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.

SYNTAX:

```
set certificate <certificate-file>|selfsigned [tag https-north|https-south]
unset certificate <certificate-file>
get certificate <url>
show certificate
show certificate status
show certificate <cert-file> [-page]
list certificate
delete certificate <file-pattern>
```

OPTIONS:

`tag https-north` – Installs the certificate only on the North interface.

`tag https-south` – Installs the certificate only on the South interface.

`-page` – Displays the results one page at a time.

DESCRIPTION:

set certificate and unset certificate

Install or uninstall a certificate. 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 the 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.

get certificate

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. See page 72 for more information about SFTP.

show certificate

The show certificate command shows the certificates that are available to be installed and those that are already installed.

If the filename is included at the end of the command, then the contents of the license 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.

list certificate

This command lists the certificates that are available to be installed and those that are already installed.

delete certificate

This command deletes a certificate from the pool of available certificates.

EXAMPLE:

```
phoneproxy> set certificate selfsigned
Generating a 1024 bit RSA private key
..........................++++++++++++
writing new private key to '/tmp/cert-https-north.pem.3448'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields, but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:Texas
Locality Name (eg, city) [Newbury]:Austin
Organization Name (eg, company) [My Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:Bluestreak
Common Name (eg, your name or your server's hostname) []:PhoneProxy1
Email Address []:support@metreos.com
```

```
phoneproxy> show certificate
Available Certificates:
  No certificates available to install.
Installed Certificates:
File Size  Name                      MD5 Checksum
---------  ------------------------  --------------------------------
     2197  https-north.pem           5ca510c175e5cc0022636f4bec050208
```

CLUSTER

A cluster is collection of PhoneProxy nodes grouped together in order to distribute the load of many PhoneProxy users and to provide failover capability to isolate users from the failure of any single PhoneProxy.

SYNTAX:

```
set cluster mode standalone|publisher|subscriber
set cluster name <cluster-name>
unset cluster name
set cluster publisherip A.B.C.D
unset cluster publisherip
set cluster member A.B.C.D
unset cluster member A.B.C.D
show cluster [status]
```

OPTIONS:

[status] – Displays the cluster's current status. This shows the operational status of the cluster. In particular, it shows which cluster members have connected and how recently.

DESCRIPTION:

set cluster mode

The clustering feature may be entirely disabled by setting the cluster mode to standalone. A standalone PhoneProxy will not interact with any other PhoneProxy nodes.

One PhoneProxy node in a cluster is designated the publisher. This node will collect and disseminate cluster information to the specified members of the cluster. The publisher also holds the license for the cluster.

Zero or more PhoneProxy nodes in a cluster may be subscribers. The subscribers specify the address of the publisher in the cluster. They will attempt to connect to the publisher and obtain the license, user list, and details on other members of the cluster.

A standalone PhoneProxy does not need the cluster network interface to be configured or enabled, while both publisher and subscriber nodes require the Cluster interface to be configured and enabled.

set cluster name and unset cluster name

Cluster name specifies the name of the cluster. Only PhoneProxy nodes with the same cluster name may be joined together into a cluster. Use the set command to set the cluster name and use the unset command to remove the cluster name.

set cluster publisherip and unset cluster publisherip

You must use the set cluster publisherip A.B.C.D command to set the publisherip to fully enable clustering on a subscriber. The address specified should be the address of the Cluster interface of the publisher. To participate in the cluster the subscriber must be able to connect to the publisher, authenticate, and obtain information about other members of the cluster, the licensing, and the configured users. To temporarily disable clustering in a subscriber, you may unset the publisherip. Changing the cluster mode to something besides subscriber will also clear the publisherip.

set cluster member and unset cluster member

A publisher must define the members (subscribers) of the cluster. Only the defined members will be allowed to connect and obtain cluster information from the publisher. Use set cluster member A.B.C.D to define A.B.C.D as a cluster member. The address specified should be the address of the Cluster interface of the member.

show cluster [status]

Shows the cluster configuration, or if the optional keyword status is present, the current status. The configuration includes the cluster state, mode, name, this node's unique id, name, and cluster ip, the publisher ip (if a subscriber), and the members (if a publisher). The current status shows connection state of all the known members (if publisher or subscriber).

EXAMPLE:

```
phoneproxy> show cluster
Cluster State        : enabled
Cluster Mode         : publisher
Cluster Name         : PProxyCluster
Cluster Node Name    : blue03
Cluster Node IP      : 192.168.2.13
Cluster Publisher IP : 192.168.2.13
Cluster Members::::
 192.168.2.12
 192.168.2.14
```

```
blue03> show cluster status
  name         addr           me publisher age     status
  ----         ----           -- --------- ---     ------
  blue04       192.168.2.14               3s      connected: 22h 18m
  blue03       192.168.2.13   *  *         4m 46s  (connected)
  blue02       192.168.2.12               2s      connected: 22h 18m
```

CONFIG

The config is the set of all configurations for the PhoneProxy.

SYNTAX:

```
save config
unset config all
show config running [-page]
show config startup [-page]
```

OPTIONS:

[-page] – Displays the results one page at a time.

DESCRIPTION:

save config

Saves the running configuration as the startup configuration to be applied on the next reboot. If the PhoneProxy is rebooted without saving any changes from running configuration to startup configuration, the changes will be lost.

unset config

Resets the configuration to the factory defaults.

show config startup

Shows the startup configuration which is the set of configurations that will be applied at the next PhoneProxy restart.

show config running

Shows the startup configuration which is the set of configurations that are currently running on the PhoneProxy.

EXAMPLE:

```
phoneproxy> show config running
set interface cluster netmask 255.255.255.0 address 192.168.2.13
set interface north netmask 255.255.255.0 address 192.168.1.13
set interface south netmask 255.255.255.0 address 10.1.14.97
set interface mgmt netmask 255.255.255.0 address 10.1.14.92
set interface mgmt disable
set interface south enable
set interface north enable
set interface cluster enable
set nodename blue03
set defaultgateway 10.1.14.1
set dns domain metreos.com
set dns primary 10.1.10.12
set dns secondary 10.1.10.13
set snmp disable
set ntp server pool.ntp.org
set ntp enable
set time timezone US/Central
set cluster mode publisher
set cluster name alice
set cluster member 192.168.2.12
set cluster member 192.168.2.14
set heartbeat disable
set phoneproxy loglevel brief
set phoneproxy activation mode required
set phoneproxy httpproxy mode internal
set phoneproxy httpproxy enable
set phoneproxy rtp enable
set phoneproxy http enable
set phoneproxy enable
```

DEFAULTGATEWAY

The default gateway is a node on a network that directs traffic to destination(s) outside of the local network(s) and which is not otherwise covered by a statically assigned route.

SYNTAX:

```
set defaultgateway A.B.C.D [interface north|south]
unset defaultgateway address
show defaultgateway
```

OPTIONS:

[interface north | south] – In addition to providing an IP address for the default gateway, one can explicitly set an interface to use. A default gateway must always be configured if the interface is set to DHCP.

DESCRIPTION:

set defaultgateway and unset defaultgateway

Set the default gateway.

Unset the default gateway.

show defaultgateway

Show the default gateway.

EXAMPLE:

```
phoneproxy> show defaultgateway
Default Gateway : 10.1.14.1
```

DNS

The DNS server is the computer that translates domain names, or computer hostnames, to IP addresses.

SYNTAX:

```
set dns primary A.B.C.D [secondary A.B.C.D]
unset dns primary
unset dns secondary
set dns domain <domain.com>
unset dns domain
show dns
```

OPTIONS:

[secondary A.B.C.D] – Sets the secondary DNS server.

DESCRIPTION:

set dns primary [secondary] and unset dns primary [secondary]

Set the primary or secondary DNS server.

Unset the primary or secondary DNS servers.

set dns domain and unset dns domain

sets the default domain name applied to unqualified names.

unset the DNS domain name.

show dns

Show the DNS configuration.

EXAMPLE:

```
prompt> show dns
DNS Domain    : metreos.com
DNS Primary   : 10.1.10.12
DNS Secondary : 10.1.10.13
```

HEARTBEAT

A pair of nodes in a PhoneProxy cluster can be configured as a heartbeat group. Heartbeat groups are useful in the following scenarios:

Provide a single high-availability TFTP address that phone devices can be provisioned to use.

Provide a single high-availability HTTP proxy address that phone devices can use to access HTTP-based IP Phone Services

Provide a single high-availability HTTP address that end users can use for Activation.

NOTE: *If you want to have more than one pair of PhoneProxies providing high-availability services for HTTP or have more complex load balancing of HTTP-based activation, you should consider using a Content-Services-Switch in front of HTTP traffic to PhoneProxy.*

SYNTAX:

```
set heartbeat enable|disable
set heartbeat group <group-name>
set heartbeat preferrednode <node-name>
set heartbeat peer A.B.C.D
set heartbeat manage tftp|http enable|disable
unset heartbeat group
unset heartbeat preferrednode
unset heartbeat peer
show heartbeat [status]
```

OPTIONS:

[status] – Show heartbeat current status.

DESCRIPTION:

The heartbeat allows a pair of PhoneProxy nodes to function as a heartbeat group for the various services running on the North interface (TFTP, web activation, and web proxy) and the South interface (activation).

This heartbeat will be configured with an additional virtual IP address on both their North and South interfaces. The addresses are specified by configuring the 'virtnorth' and 'virtsouth' interfaces. The 'enabled/disabled' status of these interfaces is controlled by heartbeat, and for example, doing a 'set interface virtnorth enable' is not an allowed operation.

NOTE: *Neither interfaces virtnorth nor virtsouth should be configured unless the appliance will be a member of a heartbeat group. Doing so will result in undesired behavior.*

When heartbeat is enabled, and detects that the other node failed, it will assign the IP address defined on the virtnorth interface as a second IP address on the North interface, and the IP address defined on the virtsouth interface as a second IP address on the South interface.

NOTE: *Heartbeat is currently configured to wait a few seconds between heartbeats, so it may take a few seconds before the failure of the other node is detected.*

The virtual IP is active on only one node in the heartbeat group. When one member of the pair becomes unavailable, the other member will assume control of the virtual IP and all of the services associated with that IP.

In a cluster composed of nodes A and B, node A currently holds the resources. If node A fails, then node B will take over the resources. If node A later regains connectivity and rejoins the heartbeat group, the resources will stay on node B, even if node A is configured as the preferred node. PhoneProxy is configured in this way to eliminate unnecessary downtime that would be caused by the swap back to node A.

set heartbeat and unset heartbeat

The set heartbeat command enables the heartbeat service so a pair of PhoneProxy nodes can function as back-ups for each other.

The heartbeat group is a security token used to sign and decrypt messages sent between nodes in a heartbeat group. It is a string that behaves like a password and it can be set to an arbitrary value. This is a required parameter, and it needs to be set to the same value on both nodes in the heartbeat group.

NOTE: *Heartbeat should be disabled prior to changing the groupname; otherwise, each node may determine the other node went down, since it will not be able to authenticate the messages.*

The heartbeat preferred node defines which of the heartbeat nodes is the preferred owner of the heartbeat resources (the virtual IPs). This is a required parameter, and both nodes need to be the same value. This value will be the node-name that was configured on the appliance that will be the preferred node. This setting is used to resolve potential conflicts in situations where it may not be immediately clear who should own the resources. For example, if heartbeat was enabled on both nodes at exactly the same time, the node marked as preferred grabs the resources.

The heartbeat peer setting is used to specify the IP address of the other heartbeat node in the group. This is a required setting, and it will be the IP address defined on the Cluster interface. For example, if the Cluster interface address on node A is 192.168.100.1, and the Cluster interface address on node B is 192.168.100.2, then '`set heartbeat peer 192.168.100.2`' should be run on node A and '`set heartbeat peer 192.168.100.1`' on node B.

The 'heartbeat manage' setting allows the admin to control which services (activation web server, web proxy, and TFTP) are managed by the system. For example, if the administrator does not want the TFTP service to be managed by heartbeat, in other words, the admin does not want TFTP to bind to the virtnorth IP address, they should run the '`set heartbeat manage tftp disable`' command.

Whenever the TFTP service is restarted, it will see the virtual IP is there, but it will also see that a flag is set that tells it to not listen on that virtual IP. This same concept applies to the http services.

These settings apply to both the virtnorth and virtsouth interfaces. As such, the command '`set heartbeat manage http disable`' was run, the appliance will not listen for any web activity on either one of the virtual IP addresses.

The unset command removes the heartbeat service configuration component specified. For example, the unset heartbeat group command would clear the configured value of the heartbeat group parameter back to the default blank state. The **unset heartbeat preferrednode** and **unset heartbeat peer** commands would clear the values of their respective fields.

show heartbeat

The show heartbeat command displays the heartbeat configuration settings. If the optional status parameter is included, as in show heartbeat status, the results will display the heartbeat status.

EXAMPLE:

```
phoneproxy> show heartbeat
Heartbeat State            : enabled
Heartbeat Group            : METREOS
Heartbeat Preferred Node   : blue03
Heartbeat Peer             : 192.168.2.13
Heartbeat Managed Services : tftp http

phoneproxy> show heartbeat status
Heartbeat Status: Running
```

INTERFACE

The PhoneProxy has four network interface connections that each have a specific dedicated purpose. Generally, the North interface is used to connect to phones, the South interface is used to connect to Cisco Unified CallManagers and manage the cluster, the Cluster interface is used to connect to other PhoneProxy nodes in a cluster, and the Mgmt interface may also be used to manage the cluster. Two other interfaces, virtnorth and virtsouth, do not have physical connectors but share the North and South connector, respectively.

SYNTAX:

```
set interface <iface> address A.B.C.D netmask W.X.Y.Z
set interface <iface> dhcp
set interface <iface> enable|disable
unset interface <iface> address|dhcp
show interface <iface>
show interface
```

NOTE: <iface> is north | south | mgmt | cluster | virtnorth | virtsouth

OPTIONS:

n/a

DESCRIPTION:

set interface and unset interface

Configure network interfaces. The North and South interfaces must always be configured. The Mgmt interface may be configured if the South interface is not accessible to the management staff. The Cluster interface must be configured to enable the clustering feature. The virtnorth and virtsouth interfaces are covered elsewhere in this document. See page 43 for more information on virtual interfaces.

Interfaces are normally configured statically; however, DHCP may be used if the DHCP server supports permanent reservations. Changing the North and South addresses while phones are connected will certainly disrupt services and interrupt calls in progress.

The **unset interface** command reverts an interface to the default disabled state.

show interface

Show the interface parameters and state.

EXAMPLE:

```
blue03> show interface
```

```
Name       Active? Mode    Address         Netmask
---------- ------- ------- --------------- ---------------
mgmt               static  10.1.14.95      255.255.255.0
north         *    static  192.168.1.13    255.255.255.0
south         *    static  10.1.14.97      255.255.255.0
cluster       *    static  192.168.2.13    255.255.255.0
virtnorth          static
virtsouth          static

Default Gateway : 10.1.14.1
```

LOG

The logs are a set of files in which system events are recorded.

SYNTAX:

```
list log [<file-pattern>] [-page] [-nodetail]
show log <logfile> [-tail|-page] [-filter <regexp>]
delete log <file-pattern>
```

OPTIONS:

[<file-pattern>] – Pattern to match file names against.

[-page] – Displays results one page at a time.

[-nodetail] – Suppresses detailed properties like file size and timestamp.

[-tail] – Displays appended output as file grows.

[-filter <regexp>] – Display results that contain the filtered regular expression.

DESCRIPTION:

list log

Display a list all log files on the PhoneProxy. There are three main types of logs saved—shell.log, update.log, phoneproxy.log. Shell.log records configuration changes. Update.log records events during the update process. Phoneproxy.log is the main log for general system messages, events, and statistics. See page 12 for more information about logs.

show log

Show the contents of node log file. This will allow you to see the actual recorded entries in the particular log file.

delete log

Delete a log file from a PhoneProxy. Once the log is deleted, it can not be retrieved. Multiple logs can be deleted at one time by specifying a file-pattern to match. For example, the command `delete log log-2006*` will delete all logs with the filename that starts with "log-2006"

EXAMPLE:

```
phoneproxy> show log
File Name                  Size     Timestamp
-------------------------- -------- ------------
http.access.log                  0 Jun  6 10:26
http.activation.log              0 Jun  6 10:26
http.error.log               21305 Jun  9 04:21
httpproxy.log                 3254 Jun  9 04:21
log-20060611120037603.xml  1205303 Jun 12 00:00
log-20060611120037615.txt   559440 Jun 11 23:59
log-20060612000037603.xml   468731 Jun 12 04:39
log-20060612000037607.txt   217560 Jun 12 04:39
phoneproxy.log                 25 Jun  7 11:26
phoneproxystdout.txt         2006 Jun  7 11:26
shell.log                   19777 Jun  9 04:29
shell.log.1                 49975 Jun  7 05:39
update.log                   4175 Jun  6 10:40
```

NODENAME

The nodename is the name of the PhoneProxy.

SYNTAX:

```
set nodename <nodename>
show nodename
```

OPTIONS:

n/a

DESCRIPTION:

set nodename

Set the name for this node.

show nodename

Show the name for this node.

EXAMPLE:

```
prompt> show nodename
Nodename : blue03
```

NTP

The NTP server is the computer that will be used to synchronize time between computers on the network.

SYNTAX:

```
set ntp enable|disable
set ntp server <servername>
set ntp resync
unset ntp server
show ntp
```

OPTIONS:

n/a

DESCRIPTION:

set ntp and unset ntp

Enable and configure NTP client. The set ntp resync command will force NTP synchronization with the NTP server as long as the NTP server name is set and the NTP service is enabled.

The unset ntp command will remove the NTP server from server list.

show ntp

Show NTP server configuration and state.

EXAMPLE:

```
phoneproxy> show ntp
NTP State  : enabled
NTP Server : ntp.pool.org
```

```
phoneproxy> set ntp resync
20 Jun 10:21:46 ntpdate[8921]: adjust time server 60.56.119.79 offset
0.075393 sec
```

PACKETTRACE

A packet trace is a diagnostic tool that will record all incoming and outgoing packets to a file for analysis. A packet trace can be run in two modes, either interactively or in the background.

SYNTAX:

```
set packettrace name <name>
set packettrave size <packetcount>
set packettrace filter <filter-expression>
set packettrace interface north|south
set packettrace enable|disable
unset packettrace name|size|fileter|interface
show packettrace
show packettrace status
show packettrace <filename> [-tail|-page] [-nodetail]
list packettrace [<file-pattern>] [-page] [-nodetail]
run packettrace [name <name>] [filter <filter-expression>]
delete packettrace <file-pattern> [-noprompt]
```

OPTIONS:

[-tail] – Displays appended output as file grows.

[-page] – Displays results one page at a time.

[-nodetail] – Suppresses detailed properties like file size and timestamp.

[<file-pattern>] – Pattern to match file names against.

[name <name>] – The name of the packet trace file.

[filter <filter-expression>] – Filters

[-noprompt] – Suppresses the confirmation prompt.

DESCRIPTION:

set packettrace and unset packettrace

`name` – set the name of the background packet trace file to record

`size <packetcount>` – limit the background packet trace to `<packetcount>` packets

filter – limit the background packet trace to packets that match `<filter-expression>` . Filters are valid `tcpdump` filter expressions.

`interface north|south` – limit the background packet trace to either the North or South interface

`enable|disable` – start and stop a background packet trace

show packettrace

Show packet traces, configuration, and status.

list packettrace

List all packet traces.

run packettrace

Run a packet trace interactively. Options:

`name <name>` - specify the name of the interactive packet trace

`filter <filter-expression>` - limit the packet trace to the packets that match `<filter-expression>`. Filters are valid `tcpdump` filter expressions.

delete packettrace

Delete a packet trace.

EXAMPLE:

```
phoneproxy> show packettrace trace.out

reading from file /data/public/logs/tcpdump/trace.out, link-type EN10MB
(Ethernet)

20:51:52.325082 802.1d config 8000.00:50:50:b7:81:80.8005 root
8000.00:50:50:b7:81:80 pathcost 0 age 0 max 20 hello 2 fdelay 15

   0x0000:  0180 c200 0000 0050 50b7 8185 0026 4242  .......PP....&BB

   0x0010:  0300 0000 0000 8000 0050 50b7 8180 0000  .........PP.....

   0x0020:  0000 8000 0050 50b7 8180 8005 0000 1400  .....PP.........

   0x0030:  0200 0f00 0000 0000 0000 0000 7800 0c00  ............x...

20:51:54.327898 802.1d config 8000.00:50:50:b7:81:80.8005 root
8000.00:50:50:b7:81:80 pathcost 0 age 0 max 20 hello 2 fdelay 15

   0x0000:  0180 c200 0000 0050 50b7 8185 0026 4242  .......PP....&BB

   0x0010:  0300 0000 0000 8000 0050 50b7 8180 0000  .........PP.....

   0x0020:  0000 8000 0050 50b7 8180 8005 0000 1400  .....PP.........

   0x0030:  0200 0f00 0000 0000 0000 0000 7800 0c00  ............x...

20:51:55.293584 IP (tos 0x0, ttl  50, id 45863, offset 0, flags [none],
proto 6, length: 52) cpe-66-69-217-49.austin.res.rr.com.50419 >
209.253.50.191.sieve: P [tcp sum ok] 553629040:553629052(12) ack 3022321403
win 1400

   0x0000:  0010 f309 02d1 0012 7f1f 2480 0800 4500  ..........$...E.

   0x0010:  0034 b327 0000 3206 b569 4245 d931 d1fd  .4.'..2..iBE.1..

   0x0020:  32bf c4f3 07d0 20ff b570 b424 f6fb 5018  2........p.$..P.

   0x0030:  0578 37c1 0000 0400 0000 0000 0000 0000  .x7.............

   0x0040:  0000                                     ..
```

PASSWORD

There are two passwords protecting the boot images. One password for the `image0` and `image1` boot images, and a separate password for the maintenance partition.

SYNTAX:

```
set password [<password>] [-old <old password>]
```

Maintenance Bootimage Only:

```
set password maint|image [<password>]
```

OPTIONS:

[<password>] – The new password, if omitted the administrator will be prompted

[-old <old password>] – The old password, if omitted the administrator will be prompted

DESCRIPTION:

set password

This command sets the password for the administrator's account, 'admin', on either the maintenance boot image or both the production boot images. The command is context-sensitive in that it behaves slightly different depending on the boot image that is running while it is executed.

If the command is executed in one of the image partitions, the password will be reset for the administrator's account on both image0 and image1. The maintenance partition password cannot be set from either of the image partitions. Furthermore, the password must be a strong password. For a password to be considered strong, it must be eight or more characters in length without repeating the same character three times in a row. Also, the password should contain characters from three of the four following categories:

Uppercase letters

Lowercase letters

Numerical digits

Punctuation characters (all the other printable ASCII characters)

If the command is executed in the maintenance partition, an extra parameter must be included to indicate which boot image password to reset, the maintenance boot image or one of the production boot images. The password for the image partitions cannot be blank, but the password for the maintenance partition can be. Since the maintenance boot image password is empty by default, specifying a new password for this boot image will require the password to be entered when logging into the maintenance boot image.

EXAMPLE:

NOTE: The example shown below is on an image partition.

```
phonephoxy> set password metreos
Password changed on 'image0' partition
Password changed on 'image1' partition
```

NOTE: The examples shown below are on the maint partition.

```
phoneproxy> set password image metreos
Password changed on 'image0' partition
Password changed on 'image1' partition
```

```
phoneproxy> set password maint metreos
Password changed on 'maint' partition
```

```
phoneproxy> set password maint
Enter new Password:
   Repeat Password:
Password cleared on the ‘maint’ partition
```

PHONEPROXY

The phoneproxy object controls the operating parameters of the remote phones.

SYNTAX:

```
set phoneproxy activation mode required|open
unset phoneproxy activation mode
set phoneproxy activation idletimeout N
unset phoneproxy activation idletimeout
set phoneproxy activation authtimeout N
unset phoneproxy activation authtimeout
set phoneproxy http enable|disable
set phoneproxy http publish webpage|webservice
unset phoneproxy http publish webpage|webservice
set phoneproxy httpproxy enable|disable
set phoneproxy httpproxy mode internal|external
unset phoneproxy httpproxy mode
set phoneproxy httpproxy externaladdress A.B.C.D
unset phoneproxy httpproxy externaladdress
set phoneproxy httpproxy allow URL
unset phoneproxy httpproxy allow URL
set phoneproxy loglevel brief|full
unset phoneproxy loglevel
set phoneproxy phone http disable|enable
unset phoneproxy phone http
set phoneproxy rtp enable|disable
set phoneproxy rtp maxchannels N
unset phoneproxy rtp maxchannels
set phoneproxy rtp portstart N
unset phoneproxy rtp portstart
set phoneproxy rtp portlimit N
unset phoneproxy rtp portlimit
set phoneproxy sccp maxconnects N
unset phoneproxy sccp maxconnects
set phoneproxy sccp security off|on
unset phoneproxy sccp security
```

```
set phoneproxy tcp ratelimit N
unset phoneproxy tcp ratelimit
set phoneproxy udp ratelimit N
unset phoneproxy udp ratelimit
show phoneproxy [status|httpproxy]
```

OPTIONS:

[status] – Displays the PhoneProxy's current status

[httpproxy] – Displays allow list of http proxy

DESCRIPTION:

set phoneproxy activation and unset phoneproxy activation

The activation service of PhoneProxy controls how and when phones can connect.

The activation mode is used to control whether phone IP addresses must be specifically authorized to connect or not. If the phone's IP address must be authorized (activation mode 'required'), then before the phone can connect the user must login and specify the exact IP address of the phone as the PhoneProxy will see it. This means, in some deployments, that the IP address will be the WAN IP address rather than an internal NAT address like 192.168.1.0. If the phone's IP address need not be authorized (activation mode 'open'), then the phone is allowed to connect using any IP address. If the activation mode configuration is unset, then the PhoneProxy will return to the default value 'required'.

When activation mode is 'required', the idletimeout setting will allow the authorization of unconnected IP addresses to timeout and be removed after a specified number of seconds. Once a phone registers with a PhoneProxy, the connection will not go idle because traffic is sent back and forth between the IP phone and the PhoneProxy. The default idletimeout setting is 300 seconds (five minutes). This means the user must connect their phone within five minutes of activation or they will have to reactivate. There is no idle timeout when the activation mode is 'open'. If idletimeout configuration is unset then the PhoneProxy will return to the default value of 300 seconds.

When the activation mode is 'required', the authtimeout setting will require the user to re-authenticate connected accounts after a specified number of seconds. The default setting is 0 which means that authorizations do not time out. There is no auth timeout when the activation mode is 'open'. If authtimeout configuration is unset then the PhoneProxy will return to the default value of 0 for no auth timeout.

Refer to the Cisco *Unified PhoneProxy Administration Guide* for more information about activation modes.

set phoneproxy http or unset phoneproxy http

The http service of PhoneProxy is used to handle activation requests. This command enables or disables the http service that is used for activation. This PhoneProxy HTTP service must be enabled, if webpage activation is to be used.

The http publish service of the PhoneProxy will allow the administrator to specify what methods are available for activation, webpage and/or web service. Of course these activation methods are only applicable when the activation mode is 'required'. The administrator can set activation to be available from a webpage on the North interface IP address, or activation can be available through a web service available on the South and Mgmt interfaces. Either method can be individually enabled, or both can be enabled by using the command twice—once to set the webpage and one to set the web service. For the webpage activation method to function properly, the PhoneProxy HTTP service must also be enabled. The unset phoneproxy http publish command disables that particular activation method. Again, if both activation methods are to be disabled, the command should be used for each method.

set phoneproxy httpproxy and unset phoneproxy httpproxy

The HTTPProxy service of PhoneProxy can be enabled or disabled. It is used to handle HTTP-based service requests from the phone (softkeys, etc.). If enabled, an HTTP proxy address will be inserted into the ProxyServerURL of phone records. If disabled, the phone records' ProxyServerURL will not be changed.

If the HTTPProxy service is enabled, it can either be hosted internally or externally. If the mode is internal, then HTTP requests are proxied by the built-in HTTP proxy. If the mode is external then an external HTTP proxy must be specified. If the HTTPProxy mode configuration is unset then the PhoneProxy will return 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. If the httpproxy externaladdress configuration is unset then the PhoneProxy will return to the default unconfigured state.

NOTE: The 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.

The `set phoneproxy httpproxy allow` sub-command adds URLs to the httpproxy whitelist. The unset command will remove URLs from the whitelist.

By default no URLs will be proxied even if the httpproxy is enabled. URLs must be explicitly added to the whitelist to be proxied.

set phoneproxy loglevel and unset phoneproxy loglevel

The loglevel of the phone proxy service determines how much logging information will be recorded and made available for later analysis. The loglevel can be set to full or brief.

set phoneproxy phone http and unset phoneproxy phone http

The `set phoneproxy phone http enable/disable` command will enable or disable the remote IP Phones embedded HTTP server.

set phoneproxy rtp and unset phoneproxy rtp

The RTP service of PhoneProxy is used to route audio channels from the phones.

If enabled, the rtp service will rewrite the phone records to redirect audio channels to the PhoneProxy device where they are forwarded to the appropriate destination. If disabled, the audio channels are not redirected.

The rtp maxchannels setting specifies the maximum number of channels that will be allowed. Each call requires one channel. Each channel is composed of two audio streams, one from the phone and one to the phone.

The rtp portstart setting specifies the starting port number of redirected audio channels. Some phones have a constraint upon which port numbers they will tolerate. Generally the range from 20480 to 32768 is safe.

The rtp portlimit setting specifies the ending port number of redirected audio channels. Portlimit must be greater than portstart, and only even numbered ports in the range of portstart up to but not including portlimit are used. For example, if portstart is 20480 and portlimit is 20580, only even numbered ports from 20480 thru 20578 will be used. Only 50 ports are available within that port range.

set phoneproxy sccp and unset phoneproxy sccp

The sccp maxconnects setting specifies the maximum number of SCCP connections (port 2000) that will be allowed to connect to the SCCP service of PhoneProxy.

The sccp security setting specifies whether or not remote IP Phones should use SecureSCCP/SRTP protocols. The default is operate with security off.

set phoneproxy tcp ratelimit and unset phoneproxy tcp ratelimit

set phoneproxy udp ratelimit and unset phoneproxy udp ratelimit

The ratelimit settings control the rate at which new tcp/udp connection will be allowed to be made.

show phoneproxy

Show the active PhoneProxy service configuration.

EXAMPLE:

```
phoneproxy> show phoneproxy
PhoneProxy Loglevel                  : full
PhoneProxy Activation Mode           : required
```

```
PhoneProxy Activation Idle Timeout    : 300 (seconds)
PhoneProxy Activation Auth Timeout    : 86400 (seconds)
PhoneProxy Http State                 : enabled
PhoneProxy Http Publish               :
PhoneProxy HttpProxy State            : enabled
PhoneProxy HttpProxy Mode             : internal
PhoneProxy HttpProxy External Address :
PhoneProxy HttpProxy Allow            :
PhoneProxy Phone Http                 : disable
PhoneProxy RTP State                  : enabled
PhoneProxy RTP Max Channels           : 300
PhoneProxy RTP Port Start             : 20480
PhoneProxy RTP Port End               : 32768
PhoneProxy SCCP Max Connects          : 3000
PhoneProxy SCCP Max User Connects     : 1
PhoneProxy SCCP Security              : off
PhoneProxy TCP Ratelimit              : 0 (connections/minute)
PhoneProxy UDP Ratelimit              : 0 (connections/minute)
```

ROUTE

A route is the path network traffic will take on its way to the destination host.

SYNTAX:

```
set route addressmask A.B.C.D/W.X.Y.Z gateway A.B.C.D [interface ethN]
unset route addressmask A.B.C.D/W.X.Y.Z gateway A.B.C.D [interface ethN]
show route
```

OPTIONS:

[interface ethN] – Sets the route specifically for this interface.

DESCRIPTION:

Define a static route.

Remove a static route.

Show static routes.

EXAMPLE:

```
phoneproxy> show route
Kernel IP routing table
Destination   Gateway     Genmask         Flags Metric Ref   Use Iface
10.1.12.0     *           255.255.255.0   U     0      0     0  eth0
10.1.12.0     *           255.255.255.0   U     0      0     0  eth2
192.168.1.0   *           255.255.255.0   U     0      0     0  eth1
169.254.0.0   *           255.255.0.0     U     0      0     0  eth2
default       10.1.12.1   0.0.0.0         UG    0      0     0  eth0
```

SNMP

SNMP is used by a network management system for monitoring PhoneProxy for events and conditions that need attention.

SYNTAX:

```
set snmp enable|disable
set snmp community <community-string>
set snmp location <location-string>
set snmp contactname <contactname-string>
set snmp contactemail <contactemail-string>
unset snmp community
unset snmp location
unset snmp contactname
unset snmp contactemail
show snmp
```

OPTIONS:

n/a

DESCRIPTION:

set snmp and unset snmp

`community` – set the SNMP community string (default is 'public')

`enable|disable` – enable or disable the SNMP service

show snmp

The show snmp command displays the SNMP service parameter configurations

EXAMPLE:

```
phoneproxy> show snmp
Snmp State         : enabled
Snmp Community     : public
Snmp Location      : Unknown
Snmp Contact Name  : PhoneProxy Administrator
Snmp Contact Email : admin@unknown
```

SYSTEM

The system is set of resources used in the PhoneProxy. Two of these main resources are the memory and processor.

SYNTAX:

```
show system memory
show system processor
show system uptime
```

OPTIONS:

n/a

DESCRIPTION:

show system memory

Show total real memory and swap usage at the current instant in time

show system processor

Show total CPU usage for system and user processes at the current instant in time.

show system uptime

Show the total time the PhoneProxy has been running since last boot.

EXAMPLE:

```
phoneproxy> show system memory
         total       used       free     shared    buffers     cached
Mem:    255920     247344       8576          0      21704     174248
-/+ buffers/cache:  51392     204528
Swap:  1052216          0    1052216
```

```
phoneproxy> show system processor
Total: 1%  User: 0%  System: 1%
```

TIME

The time is the local time and time zone.

SYNTAX:

```
set time time HH:MM:SS
set time date YYYY-MM-DD
set time timezone <tzname>
show time
```

OPTIONS:

n/a

DESCRIPTION:

set time

Set date, time, and time zone. The time should be entered in 24hr format, however, specifying an NTP server is the easiest method to keep time correct on the PhoneProxy.

The time zone should be entered in the Zoneinfo database format. Type the command '`help 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

show time

Show current time/time zone.

EXAMPLE:

```
phoneproxy> show time
Local Time : 2006-06-17 11:26:40
Timezone   : US/Central
```

UPDATE

Update is the process for downloading and installing newer version of the PhoneProxy software.

SYNTAX:

```
get update <url>
show update
list update
run update <update-name>
delete update <file-pattern>
```

OPTIONS:

n/a

DESCRIPTION:

get update

Retrieve an update from a URL.

show update

Show available updates.

list update

List available updates.

run update

Execute a system update on the inactive image.

delete update

Remove and update package.

EXAMPLE:

```
phoneproxy> delete update phoneproxy-1.0.0.0911.bin
Deleting update phoneproxy-1.0.0.0911.bin ...

prompt> get update http://updateserver/phonephoxy-1.0.0.0911.bin

prompt> show update
Available Updates:
File Size  Name                      MD5 Checksum
---------  ------------------------  ------------------------------
 11262099  update-1.0.0.0911.bin     551f0d5dc4d19f9135f22c5aab22cf30
 11272571  update-1.0.0.0910.bin     946db8fb688d91f0c9d85ce8cfb49548

prompt> run update update-1.0.0.0911.bin
Executing update update-1.0.0.0911.bin against image0
Extracting update...
Updating.....................................................
.............................................................
.............................................................
Update complete.

phoneproxy> set bootimage image0
Setting boot image to image0

phoneproxy> reboot force save
Saving configuration
Broadcast message from root (pts/0) (Mon Jun 12 04:51:46 2006):
The system is going down for reboot NOW!
```

USER

A user is the person or account that is authorized to use the PhoneProxy to make phone calls via their IP phone.

SYNTAX:

```
set user active name <username> address <ip-address>
set user inactive name <username>
show user
```

OPTIONS:

n/a

DESCRIPTION:

set user

Activate a PhoneProxy user.

show user

Show Proxy User configuration.

EXAMPLE:

```
phoneproxy> show user
  name             sid             addr            duration connected
  ----             ---             ----            -------- ---------
  homer            SEP000000112233 [inactive]
  marge            SEP000000445566 [inactive]
  bart             SEP000000778899 72.176.42.51    5d 10h   *
  lisa             SEP112233000000 [inactive]
  maggie           SEP445566000000 66.69.215.43    5d 10h   *
```

VERSION

The version is the numerical representation of the current PhoneProxy software revision.

SYNTAX:

```
show version
```

OPTIONS:

n/a

DESCRIPTION:

show version

Show current software version.

EXAMPLE:

```
prompt> show version
Product Name     : PhoneProxy 500
Software Version : 1.0.1.0001
Signature        : …
Serial Number    : DEV00000000
Hardware Level   : 74-XXXX-XX –XX
Software Level   : 800-XXXXX-XX -XX
Manufacture Date : 2006-06-14
```

APPENDIX A

SERIAL CONNECTION

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

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

Figure 2 - Serial Connection Settings

RJ45-to-DB9 Serial Port Adapter Cable

The console port on the front of the PhoneProxy chassis uses an RJ45 connector. The system ships with an RJ45-to-DB9 adapter cable that can be used to connect the system to standard serial ports with the addition of a null modem.

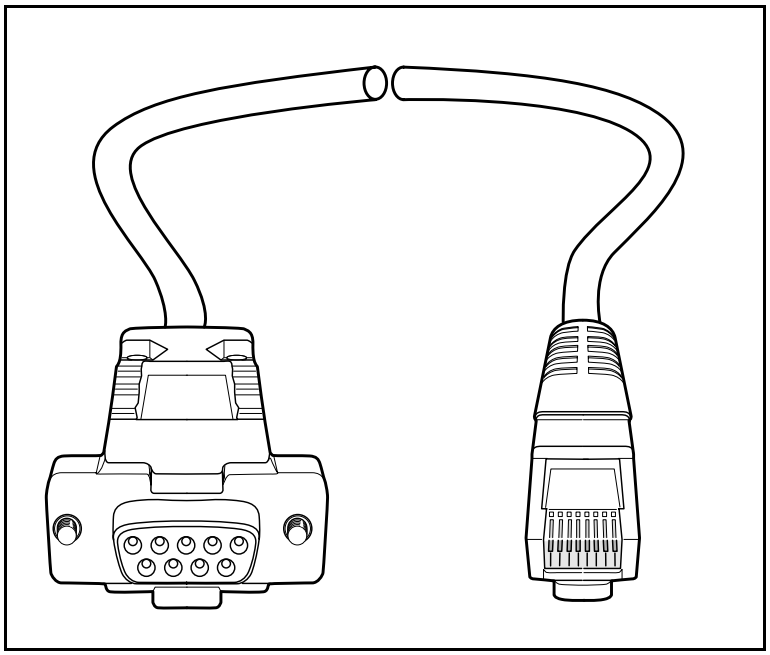


Figure 3 - RJ45 to DB9 Serial Adapter Cable.

RJ45-to-DB9 Serial Port Adapter Pin Assignments

If the included cable is not useful for your environment, the following table of pin assignments can be used to create a compatible cable.

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

Figure 4. RJ45-to-DB9 Serial Port Adapter Pin Assignments

APPENDIX B

SFTP

PhoneProxy supports SFTP (and only SFTP, not SCP) for secure file transfer. The admin user will be able to login via SFTP to a single secure location. The admin-user will be able to upload updates and raw configuration files or download log files from this location.

When and admin user SFTPs to the PhoneProxy, the following directory structure present:

incoming/ – Location to place configuration files that need to be installed.

update/ – Location to place system-updates that need to be installed.

logs/ – Location from which to pull log files.

outgoing/ – Read-only location from which to pull cluster.xml, user.xml etc.

NOTE: *The 'incoming', 'update', and 'logs' directories are writeable. The 'outgoing' directory is not.*