Model Information, Status, and Statistics

Model Information, Status, and Statistics Overview

This chapter describes how to use the following menus and screens on the Cisco Unified IP Phone to view model information, status messages, network statistics, and firmware information for the phone:

- Model Information screen: Displays hardware and software information about the phone.
- Status menu: Provides access to screens that display the status messages, network statistics, and firmware versions.
- Call Statistics screen: Displays counters and statistics for the current call.

You can use the information on these screens to monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information, and obtain other related information, remotely through the phone web page. For more information, see Remote Monitoring.

For more information about troubleshooting the Cisco Unified IP Phone, see Troubleshooting and Maintenance.

Display Model Information Screen

Procedure

Step 1 To display the Model Information screen, press the **Settings** button and then select **Model Information**.

Step 2 To exit the Model Information screen, press **Exit**.

Model Information Settings

Table 1: Model Information Settings

Option	Description	To Change
Model Number	Model number of the phone.	Display only. Cannot configure.
MAC Address	MAC address of the phone.	Display only. Cannot configure.
Load File	Identifier of the factory-installed load running on the phone.	Display only. Cannot configure.
Boot Load ID	Identifier of the factory-installed load running on the phone.	Display only. Cannot configure.
Serial Number	Serial number of the phone.	Display only. Cannot configure.
MIC	Indicates whether a manufacturing installed certificate is present on the phone.	For more information about how to manage the MIC for your phone, see the “Using the Certificate Authority Proxy Function” chapter in *Cisco Unified Communications Manager Security Guide*.
LSC	Indicates whether a locally significant certificate is present on the phone.	For more information about how to manage the LSC for your phone, see the “Using the Certificate Authority Proxy Function” chapter in *Cisco Unified Communications Manager Security Guide*.
Call Control Protocol	Indicates the call processing protocol used by the phone.	For more information, see Cisco Unified IP Phones and Different Protocols.

Status Menu

The Status menu includes these options, which provide information about the phone and its operation:

- Status Messages: Displays the Status Messages screen, which shows a log of important system messages.
- Network Statistics: Displays the Network Statistics screen, which shows Ethernet traffic statistics.
- Firmware Versions: Displays the Firmware Versions screen, which shows information about the firmware that is running on the phone.
- Expansion Modules: Displays the Expansion Modules screen, which shows information about the Cisco Unified IP Phone Expansion Modules, if connected to the phone.

Related Topics

Status Messages Screen, on page 3

Display Status Menu

Procedure

Step 1 Press **Apps**.

Step 2 Select **Admin Settings** > **Status Menu**.

Status Messages Screen

The Status Messages screen displays the 10 most recent status messages that the phone has generated. You can access this screen at any time, even if the phone has not finished starting up. See Status Messages, on page 3, which describes the status messages that might display. This table also includes actions that you can take to address errors.

Display Status Messages Screen

To display the Status Messages screen, follow these steps:

Procedure

Step 1 Press **Settings**.

Step 2 Select **Status**.

Step 3 Select **Status Messages**.

Step 4 To remove current status messages, press **Clear**.

Step 5 To exit the Status Messages screen, press **Exit**.

Status Messages

Table 2: Status Messages on the Cisco Unified IP Phone

Message	Description	Possible explanation and action
BootP server used	The phone obtained its IP address from a BootP server rather than a DHCP server.	None. This message is informational only.

Message	Description	Possible explanation and action
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	Cisco Unified Communications Manager creates a configuration file for the phone with the phone is added to the database. If the phone has not been added to the Cisco Unified Communications Manager database, the TFTP server generates a **`CFG File Not Found`** response. • Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to autoregister. See Cisco Unified Communications Manager Administration Phone Addition for details. • If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check configuration of the TFTP server. See Network Configuration Menu for details on assigning a TFTP server.
CFG TFTP Size Error	The configuration file is too large for the file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTP directory. You should only copy files into this directory when the TFTP server software is shut down, otherwise the files may be corrupted.

Message	Description	Possible explanation and action
CTL and ITL installed	CTL and ITL files are installed on the phone.	None. This message is informational only. Neither the CTL file nor the ITL file was installed on the phone previously. For more information about the Trust List, see the *Cisco Unified Communications Manager Security Guide*.
CTL installed	The CTL file is installed on the phone.	None. This message is informational only. The CTL file was not installed previously. For more information about the CTL file, see the *Cisco Unified Communications Manager Security Guide*.
DHCP timeout	DHCP server did not respond.	• Network is busy: The errors should resolve themselves when the network load reduces. • No network connectivity between the DHCP server and the phone: Verify the network connections. • DHCP server is down: Check configuration of DHCP server. • Errors persist: Consider assigning a static IP address. See Network Configuration Menu for details on assigning a static IP address.
Disabled	802.1X Authentication is disabled on the phone.	You can enable 802.1X authentication by using the **Settings** > **Security Configuration** > **802.1X Authentication** option on the phone. For more information, see 802.1X Authentication and Status Menus.

Message	Description	Possible explanation and action
DNS timeout	DNS server did not respond.	Network is busy: The errors should resolve themselves when the network load reduces. No network connectivity between the DNS server and the phone: Verify the network connections. DNS server is down: Check configuration of DNS server.
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS. Consider using IP addresses rather than host names.
Duplicate IP	Another device is using the IP address assigned to the phone.	If the phone has a static IP address, verify that you have not assigned a duplicate IP address. See Network Configuration Menu for details. If you are using DHCP, check the DHCP server configuration.
Erasing CTL and ITL files	Erasing CTL or ITL file.	None. This message is informational only. For more information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*.
Error update locale	One or more localization files could not be found in the TFTP directory or were not valid. The locale was not changed.	From Cisco Unified Operating System Administration, check that the following files are located within the subdirectories in TFTP File Management: • Located in subdirectory with same name as network locale: • tones.xml • Located in subdirectory with same name as user locale: • glyphs.xml • dictionary.xml • kate.xml

Message	Description	Possible explanation and action
Failed	The phone attempted an 802.1X transaction but authentication failed.	Authentication typically fails for one of the following reasons: • No shared secret is configured in the phone or authentication server. • The shared secret configured in the phone and the authentication server do not match. • Phone has not been configured in the authentication server.
File auth error	An error occurred when the phone tried to validate the signature of a signed file. This message includes the name of the file that failed.	The file is corrupted. If the file is a phone configuration file, delete the phone from the Cisco Unified Communications Manager database by using Cisco Unified Communications Manager Administration. Then add the phone back to the Cisco Unified Communications Manager database by using Cisco Unified Communications Manager Administration. The CTL file has a problem and the key for the server from which files are obtained is bad. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.
File not found	The phone cannot locate, on the TFTP server, the phone load file that in the phone configuration file specifies.	From Cisco Unified Operating System Administration, ensure that the TFTP File Management lists the phone load file.
IP address released	The phone has been configured to release its IP address.	The phone remains idle until it is power cycled or you reset the DHCP address. See Network Configuration Menu for details.

Message	Description	Possible explanation and action
ITL installed	The ITL file is installed in the phone. The ITL file was not installed.	None. This message is informational only. Phone does not have prior installation of the ITL file. For more information about the ITL file, see the *Cisco Unified Communications Manager Security Guide*.
ITL update failed	Updating ITL file failed.	Phone has CTL or ITL file installed and it failed to update new ITL file. Possible reasons for failure: • Network failure • TFTP server was down • Trust Verification Service (TVS) server was down Possible solutions: • Check the network connectivity. • Check whether the TFTP server is active and functioning normally. • Check whether the Trust Verification Service (TVS) server is active and functioning normally. • Manually delete CTL and ITL files if all the above solutions fail.
Load Auth Failed	The phone could not load a configuration file.	Check that: • A good version of the configuration file exists on the applicable server. • The phone load being downloaded has not been altered or renamed. • Phone load type is compatible; for example, you cannot place a DEV load configuration file on a REL-signed phone.

Message	Description	Possible explanation and action
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose **Device** > **Phone**). Verify that the load ID is entered correctly.
Load rejected HC	The application that was downloaded is not compatible with the phone hardware.	Occurs if you were attempting to install a version of software on this phone that did not support hardware changes on this newer phone. Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose **Device** > **Phone**). Re-enter the load displayed on the phone. See Firmware Version Screen, on page 15 to verify the phone setting.
Load Server is invalid	Indicates an invalid TFTP server IP address or name in the Load Server option.	The Load Server setting is not valid. The Load Server specifies a TFTP server IP address or name from which the phone firmware can be retrieved for upgrades on the phones. Check the Load Server entry (from Cisco Unified Communications Manager Administration choose **Device** > **Phone**).
No default router	DHCP or static configuration did not specify a default router.	If the phone has a static IP address, verify that the default router has been configured. See Network Configuration Menu for details. If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	If the phone has a static IP address, verify that the DNS server has been configured. See Network Configuration Menu for details. If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.

Message	Description	Possible explanation and action
No Trust List installed	The Trust List is not configured on Cisco Unified Communications Manager, which does not support security by default.	Occurs if the Trust List is not configured on Cisco Unified Communications Manager and Cisco Unified Communications Manager does not support security by default. For more information about CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*.
Programming Error	The phone failed during programming.	Attempt to resolve this error by power cycling the phone. If the problem persists, contact Cisco technical support for additional assistance.
Successful – MD5	The phone attempted an 802.1X transaction and authentication achieved.	The phone achieved 802.1X authentication.
TFTP access error	TFTP server is pointing to a directory that does not exist.	If you are using DHCP, verify that the DHCP server points to the correct TFTP server. If you are using static IP addresses, check configuration of TFTP server. See Network Configuration Menu for details on assigning a TFTP server.
TFTP Error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.
TFTP file not found	The requested load file (.bin) was not found in the TFTP directory.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose **Device** > **Phone**). Verify that the TFTP directory contains a .bin file with this load ID as the name.

Message	Description	Possible explanation and action
TFTP timeout	TFTP server did not respond.	Network is busy: The errors should resolve themselves when the network load reduces. No network connectivity between the TFTP server and the phone: Verify the network connections. TFTP server is down: Check configuration of TFTP server.
Timed Out	Supplicant attempted 802.1X transaction but timed out due the absence of an authenticator.	Authentication typically times out if 802.1X authentication is not configured on the switch.
Trust List update failed	The CTL and ITL files are installed on the phone, and it failed to update the new files.	Phone has CTL and ITL files installed and it failed to update the new CTL and ITL files. **Possible reasons for failure**: • Network failure. • TFTP server was down. • The new security token used to sign CTL file and the TFTP certificate used to sign ITL file are introduced, but are not available in the current CTL and ITL files in the phone. • Internal phone failure. **Possible solutions**: • Check the network connectivity. • Check if the TFTP server is active and functioning normally. • If the Trust Verification Service (TVS) server is supported on Cisco Unified Communications Manager, check if the TVS server is active and functioning normally. • Verify if the security token and the TFTP server are valid. • Manually delete the CTL and ITL files if all the above solutions fail, and reset the phone.

Message	Description	Possible explanation and action
Trust List updated	The CTL file, the ITL file, or both files are updated.	None. This message is informational only. For more information about the Trust List, see the *Cisco Unified Communications Manager Security Guide*.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.
XmlDefault corresponding to the phone device name	Name of the configuration file.	None. This is an informational message indicating the name of the configuration file for the phone.

Network Statistics Screen

The Network Statistics screen displays information about the phone and network performance. Network Statistics Items, on page 12 describes the information that displays in this screen.

Display Network Statistics Screen

To display the Network Statistics screen, perform these steps:

Procedure

Step 1 Press **Applications**.

Step 2 Select **Settings**.

Step 3 Select **Status**.

Step 4 Select **Network Statistics**.

Step 5 To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press **Clear**.

Network Statistics Items

The following table describes the Network Statistics items.

Table 3: Network Statistics Information

Item	Description
Rx Frames	Number of packets that the phone receives
Tx Frames	Number of packets that the phone sends
Rx Broadcasts	Number of broadcast packets that the phone receives

Item	Description
One of the following values: • Initialized • TCP-timeout • CM-closed-TCP • TCP-Bad-ACK • CM-reset-TCP • CM-aborted-TCP • CM-NAKed • KeepaliveTO • Failback • Phone-Keypad • Phone-Re-IP • Reset-Reset • Reset-Restart • Phone-Reg-Rej • Load Rejected HC • CM-ICMP-Unreach • Phone-Abort	Cause of the last phone reset
Elapsed Time	Amount of time that has elapsed since the phone connected to Cisco Unified Communications Manager
Port 1	Link state and connection of the Network port
Port 2 (applies to 7911G only)	Link state and connection of the PC port. For example, **`Auto 100 Mb Full-Duplex`** means that the PC port is in a link up state and has autonegotiated a full-duplex, 100-Mbps connection.

Item	Description
IPv4	Information on the DHCP status. This includes the following states: • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • SET DHCP COLDBOOT • SET DHCP DISABLED • DISABLED DUPLICATE IP • SET DHCP FAST

Item	Description
IPv6	Information on the DHCPv6 status. This includes the following states: • DHCP6 BOUND; • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6 INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DHCP6 DECLINED DUPLICATE IP • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT. CANNOT RESTORE • STACK TURNED OFF

Firmware Version Screen

The Firmware Version screen displays information about the firmware version that is running on the phone. Firmware Version Items, on page 16 describes the information that displays on this screen.

Display Firmware Version Screen

To display the Firmware Version screen, follow these steps:

Procedure

Step 1 Press **Settings**.

Step 2 Select **Status**.

Step 3 Select **Firmware Version**.

Step 4 To exit the Firmware Version screen, press **Exit**.

Firmware Version Items

Table 4: Firmware Version Information

Item	Description
Load File	Load file running on the phone
App Load ID	JAR file running on the phone
JVM Load ID	Java Virtual Machine (JVM) running on the phone
OS Load ID	Operating system running on the phone
Boot Load ID	Ffactory-installed load running on the phone
Expansion Module 1 Expansion Module 2	Load running on the Expansion Modules, if connected to a SIP or SCCP phone
DSP Load ID	Digital signal processor (DSP) software version used

Expansion Modules Screen

The Expansion Modules screen displays information about each Cisco Unified IP Phone Expansion Module that is connected to the phone.

Expansion Module Items, on page 17 explains the information displays on this screen for each connected expansion module. You can use this information to troubleshoot the expansion module, if necessary. In the Expansion Modules screen, a statistic preceded by "A" applies to the first expansion module. A statistic preceded by "B" applies to the second expansion module.

Display Expansion Modules Screen

To display the Expansion Modules screen, follow these steps:

Procedure

Step 1 Press **Settings**.

Step 2 Select **Status**.

Step 3 Select **Expansion Modules**.

Step 4 To exit the Expansion Modules screen, press **Exit**.

Expansion Module Items

Table 5: Expansion Module Information

Item	Description
Link State	Overall expansion module status
RX Discarded Bytes	Number of bytes that are discarded due to errors
RX Length Err	Number of packets that are discarded due to improper length
RX Checksum Err	Number of packets that are discarded due to invalid checksum information
RX Invalid Message	Number of packets that are discarded because a message was invalid or unsupported
TX Retransmit	Number of packets that are retransmitted to the expansion module
TX Buffer Full	Number of packets that are discarded because the expansion module was not able to accept new messages

Call Statistics Screen

The Call Statistics screen displays counters statistics and voice-quality metrics in these ways:

- During call: You can view the call information by rapidly pressing the **?** button twice.
- After the call: You can view the call information captured during the last call by displaying the Call Statistics screen.

Note You can also remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics not available on the phone. For more information about remote monitoring, see Remote Monitoring.

A single call can have multiple voice streams, but data is captured for only the last voice stream. A voice stream is a packet stream between two endpoints. If one endpoint is put on hold, the voice stream stops even though the call is still connected. When the call resumes, a new voice packet stream begins, and the new call data overwrites the former call data.

Display Call Statistics Screen

To display the Call Statistics screen for information about the last voice stream, follow these steps:

Procedure

Step 1 Press **Settings**.

Step 2 Select **Status**.

Step 3 Select **Call Statistics**.

Call Statistics Items

The following table explains the items displayed in the Call Statistics screen:

Table 6: Call Statistics Items

Item	Description
Rcvr Codec	Type of voice stream received (RTP streaming audio from codec): G.729, G.711 Mu-law, G.711 A-law, or Lin16k.
Sender Codec	Type of voice stream transmitted (RTP streaming audio from codec): G.729, G.728/iLBC, G.711 Mu-law, G.711 A-law, or Lin16k.
Rcvr Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Rcvr Packets	Number of RTP voice packets received since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets received since the call began because the call might have been placed on hold.
Sender Packets	Number of RTP voice packets transmitted since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets transmitted since the call began because the call might have been placed on hold.

Item	Description
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream opened.
Max Jitter	Maximum jitter observed since the receiving voice stream opened.
Rcvr Discarded	Number of RTP packets in the receiving voice stream that have been discarded (such as bad packets or packets received too late). **Note** The phone discards payload type 19 comfort noise packets that by Cisco Gateways generate, which increment this counter.
Rcvr Lost Packets	Missing RTP packets (lost in transit).
Voice Quality Metrics	
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see Voice Quality Monitoring. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5. • G.722 gives 4.5. • G.728/iLBC gives 3.9. • G.729 A/AB gives 3.8.
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.

Item	Description
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency (see note)	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Network Protocol	Identifies the current Network Protocol—IPv4.

Note When the RTP Control Protocol is disabled, no data generates for this field and thus displays as 0.

Test Tone

The Cisco Unified IP Phone supports a test tone, which allows you to troubleshoot echo on a call as well as to test low volume levels.

To use a test tone, you must:

- Enable the tone generator
- Create a test tone

Enable Tone Generator

To enable the tone generator, follow these steps:

Procedure

Step 1 Verify that the phone is unlocked.

When options are inaccessible for modification, a locked padlock icon 🔒 appears on the configuration menus. When options are unlocked and accessible for modification, an unlocked padlock 🔓 icon appears on these menus.

To unlock or lock options on the Settings menu, press ****#** on the phone keypad. This action either locks or unlocks the options, depending on the previous state.

Note If a Settings Menu password has been provisioned, SIP phones present an "Enter password" prompt after you enter **#.

Make sure to lock options after you have made your changes.

Caution Do not press ****#**** to unlock options and then immediately press ****#**** again to lock options. The phone will interpret this sequence as ****#****, which will reset the phone. To lock options after unlocking them, wait at least 10 seconds before you press ****#** again.

Step 2 While offhook, press **Help** twice to invoke the Call Statistics screen, or press **Settings** > **Status** > **Call Statistics** to invoke the Call Statistics screen.

Step 3 Look for the Tone softkey.

When the Tone softkey is visible, the softkey remains enabled for as long as this Cisco Unified IP phone is registered with Cisco Unified Communications Manager.

Step 4 If the Tone softkey is present, proceed to Create Test Tone, on page 21.

Step 5 If the Tone softkey is not present, exit the Call Statistics screen and enter the Setting Menu.

Step 6 Press ****3** on the phone keypad to enable (toggle) the Tone softkey.

Note If you press ****# **3** consecutively, with no pause, you will inadvertently reset the phone because of the ****#**** sequence.

Step 7 While offhook, press the Help button twice to invoke the Call Statistics screen, or press **Settings** > **Status** > **Call Statistics** to invoke the Call Statistics screen.

Step 8 Verify that the Tone softkey is present.

When the Tone softkey is visible, the softkey remains enabled for as long as this Cisco Unified IP Phone is registered with Cisco Unified Communications Manager.

Create Test Tone

Note When measuring echo, make sure you first set the input and output levels to 0 dB gain/attenuation on the trunk. This is set for the gateway (in Cisco Unified Communications Manager for MGCP) or under IOS CLI for H.323 or SIP.

To create a test tone, follow these steps:

Procedure

Step 1 Place a call.

Step 2 After the call is established, press **Help** twice, or press **Settings** > **Status** > **Call Statistics**.

The Call Statistics screen and Tone softkey should appear.

Step 3 Press **Tone**.

The phone generates a 1004 Hz tone at -15 dBm.

- For a good network connection, the tone sounds at the call destination only.
- For a bad network connection, the phone generating the tone may receive echo from the destination phone.

Step 4 To stop the tone, end the call.

For information on interpreting the results of test tone for volume and echo, see *Echo Analysis for Voice over IP*.