Viewing Security Information, Model Information, Status, and Statistics on the Cisco IP Phone

This chapter describes how to use the following menus on the Cisco IP Phone 7970 Series to view model information, status messages, network statistics, and firmware information for the phone:

- Security Configuration screen—Displays information about security on 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's web page. For more information, see Chapter 8, "Monitoring the Cisco IP Phone Remotely."

For more information about troubleshooting the Cisco IP Phone 7970 Series, see Chapter 9, "Troubleshooting and Maintenance."

This chapter includes these topics:

Security Configuration Screen

The Security Configuration screen shows the following information:

- Web Access—Indicates whether web access is enabled (Yes) or disabled (No) for the phone. You configure web access in Cisco CallManager Administration.
- Security Mode—Displays the security mode that is set for the phone. You configure the security mode in Cisco CallManager Administration.
- MIC—Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).
- LSC—Indicates whether a locally significant certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).
- CTL—Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone. If no CTL file is installed on the phone, this field displays No. (If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets. For more information about this file, refer to *Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)*.)

To display the Security Configuration screen, press the **Settings** button and then select **Security Configuration**.

To exit the Security Configuration screen, press the **Exit** softkey.

If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file, you must unlock the CTL file before you can save changes that you make on the Network Configuration menu to the TFTP Server 1 option or the

TFTP Server 2 option. (For information about changing these options, see the "Network Configuration Menu" section on page 4-6.) To unlock the CTL file from the Security Configuration screen, follow these steps:

Procedure

Step 1 Press ****#** to unlock options on the Security Configuration menu.

If you decide not to continue, press ****#** again to lock options on this menu.

Step 2 Highlight the CTL option.

Step 3 Press the **Unlock** softkey to unlock the CTL file.

After you change and save the TFTP Server 1 or the TFTP Server 2 option, the CTL file will be locked automatically.

Note When you press the **Unlock** softkey, it changes to **Lock**. If you decide not to change the TFTP Server 1 or TFTP Server 2 option, press the **Lock** softkey to lock the CTL file.

Model Information Screen

The Model Information screen shows the following information:

- Model Number—Model number of the phone.
- MAC Address—MAC address of the phone.
- Load File—Identifier of the factory-installed load running on the phone.
- Boot Load ID—Identifier of the factory-installed load running on the phone.
- Serial Number—Serial number of the phone.

- CTL—Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone. If no CTL file is installed on the phone, this field displays No. (If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets. For more information about this file, refer to *Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)*.)
- MIC—Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).
- LSC—Indicates whether a locally significant certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).

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

To exit the Model Information screen, press the **Exit** softkey.

Status Menu

The Status menu contains the following 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. For more information, see the "Status Messages Screen" section on page 7-5.
- Network Statistics—Displays the Network Statistics screen, which shows Ethernet traffic statistics. For more information, see the "Network Statistics Screen" section on page 7-12.
- Firmware Versions—Displays the Firmware Versions screen, which shows information about the firmware running on the phone. For more information, see the "Firmware Versions Screen" section on page 7-14.

To display the Status menu, press the **Settings** button and then select **Status**.

To exit the Status menu, press the **Exit** softkey.

Status Messages Screen

The Status Messages screen displays up to 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. Table 7-1 describes the status messages that might appear. This table also includes actions you can take to address errors that are indicated.

To display the Status Messages screen, follow these steps:

Procedure

Step 1 Press the **Settings** button.

Step 2 Select **Status**.

Step 3 Select **Status Messages**.

To remove current status messages, press the **Clear** softkey.

To exit the Status Messages screen, press the **Exit** softkey.

Table 7-1 Status Messages on the Cisco IP Phone 7970 Series

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.
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	The configuration file for a phone is created when the phone is added to the Cisco CallManager database. If the phone has not been added to the Cisco CallManager database, the TFTP server generates a `CFG File Not Found` response. • Phone is not registered with Cisco CallManager. You must manually add the phone to Cisco CallManager if you are not allowing phones to auto-register. See the "Adding Phones with Cisco CallManager Administration" section on page 2-18 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 the "Network Configuration Menu" section on page 4-6 for details on assigning a TFTP server.
CFG TFTP Size Error	The configuration file is too large for 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 TFTPPath directory. You should only copy files into this directory when the TFTP server software is shut down, otherwise the files may be corrupted.

Table 7-1 Status Messages on the Cisco IP Phone 7970 Series (continued)

Message	Description	Possible Explanation and Action
CTL Installed	A certificate trust list (CTL) file is installed in the phone.	None. This message is informational only. For more information about the CTL file, refer to *Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)*.
CTL update failed	The phone could not update its certificate trust list (CTL) file.	Problem with the CTL file on the TFTP server. For more information, refer to *Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)*.
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 the "Network Configuration Menu" section on page 4-6 for details on assigning a static IP address.
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.

Table 7-1 Status Messages on the Cisco IP Phone 7970 Series (continued)

Message	Description	Possible Explanation and Action
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco CallManager.	• Verify that the host names of the TFTP server or Cisco CallManager 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 the "Network Configuration Menu" section on page 4-6 section for details • If you are using DHCP, check the DHCP server configuration.
Error update locale	One or more localization files could not be found in the TFTPPath directory or were not valid. The locale was not changed.	Check that the following files are located within subdirectories in the TFTPPath directory: • 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 – dictionary.xml

Table 7-1 Status Messages on the Cisco IP Phone 7970 Series (continued)

Message	Description	Possible Explanation and Action
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 CallManager database using Cisco CallManager Administration. Then add the phone back to the Cisco CallManager database using Cisco CallManager Administration. • There is a problem with the CTL file 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.
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 the "Network Configuration Menu" section on page 4-6 section for details.
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (from Cisco CallManager, 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's 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 CallManager, choose **Device > Phone**). Re-enter the load displayed on the phone. See the "Firmware Versions Screen" section on page 7-14 to verify the phone setting.

Table 7-1 Status Messages on the Cisco IP Phone 7970 Series (continued)

Message	Description	Possible Explanation and Action
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 the "Network Configuration Menu" section on page 4-6 section 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 the "Network Configuration Menu" section on page 4-6 section for details. • If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.
No CTL installed	A certificate trust list (CTL) file is not installed in the phone.	Occurs if security is not configured or, if security is configured, because the CTL file does not exist on the TFTP server. For more information, refer to *Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)*.
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.
TFTP access error	TFTP server is pointing to a directory that does not exist.	• 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 TFTP server. See the "Network Configuration Menu" section on page 4-6 for details on assigning a TFTP server.

Table 7-1 Status Messages on the Cisco IP Phone 7970 Series (continued)

Message	Description	Possible Explanation and Action
TFTP file not found	The requested load file (.bin) was not found in the TFTPPath directory.	Check the load ID assigned to the phone (from Cisco CallManager, choose **Device > Phone**). Verify that the TFTPPath directory contains a .bin file with this load ID as the name.
XmlDefault.cnf.xml, or .cnf.xml 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.
TFTP server not authorized	The specified TFTP server could not be found in the phone's CTL.	• The DHCP server is not configured properly and is not server the correct TFTP server address. In this case, update the TFTP server configuration to specify the correct TFTP server. • If the phone is using a static IP address, the phone may be configured with the wrong TFTP server address. In this case, enter the correct TFTP server address in the Network Configuration menu on the phone. • If the TFTP server address is correct, there may be a problem with the CTL file. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.
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.

Network Statistics Screen

The Network Statistics screen provides information about the phone and network performance. Table 7-2 describes the information that appears in this screen.

To display the Network Statistics screen, follow these steps:

Procedure

Step 1 Press the **Settings** button.

Step 2 Select **Status**.

Step 3 Select **Network Statistics**.

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

To exit the Network Statistics screen, press the **Exit** softkey.

Table 7-2 Network Statistics Message Components

Item	Description
Rx Frames	Number of packets received by the phone
Tx Frames	Number of packets sent by the phone
Rx Broadcasts	Number of broadcast packets received by the phone

Table 7-2 Network Statistics Message Components (continued)

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 reset of the phone
Elapsed Time	Amount of time that has elapsed since the phone connected to Cisco CallManager
Port 1	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 auto-negotiated a full-duplex, 100-Mbps connection)
Port 2	Link state and connection of the Network port

Firmware Versions Screen

The Firmware Versions screen displays information about the firmware running on the phone.Table 7-3 explains the information that appears in this screen.

To display the Firmware Version screen, follow these steps:

Procedure

Step 1 Press the **Settings** button.

Step 2 Select **Status**.

Step 3 Select **Firmware Versions**.

To exit the Firmware Version screen, press the **Exit** softkey.

Table 7-3 Firmware Version Information

Item	Description
Load File	Load file running on the phone
App Load ID	Identifies the JAR file running on the phone
JVM Load ID	Identifies the Java Virtual Machine (JVM) running on the phone
OS Load ID	Identifies the operating system running on the phone
Boot Load ID	Identifies the factory-installed load running on the phone

Call Statistics Screen

Use the Call Statistics screen to view counters and statistics for the current call. Table 7-4 explains the information that appears in this screen.

To display the Call Statistics screen, press the **?** button twice rapidly during a call.

To exit the Call Statistics screen, press the **Exit** softkey.

Table 7-4 Call Statistics

Item	Description
RxType	Type of voice stream received (RTP streaming audio): G.729, G.711 u-law, G.711 A-law, or Lin16k.
RxSize	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
RxCnt	Number of RTP voice packets received since voice stream was 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.
TxType	Type of voice stream transmitted (RTP streaming audio): G.729, G.711 u-law, G.711 A-law, or Lin16k.
TxSize	Size of voice packets, in milliseconds, in the transmitting voice stream.
TxCnt	Number of RTP voice packets transmitted since voice stream was 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.
Avg Jtr	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened.
Max Jtr	Maximum jitter observed since the receiving voice stream was opened.

Table 7-4 Call Statistics (continued)

Item	Description
RxDisc	Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on). **Note** The phone will discard payload type 19 comfort noise packets that are generated by Cisco Gateways, which will increment this counter.
RxLost	Missing RTP packets (lost in transit).