CHAPTER 7

Viewing Operational Information for Cisco IP Communicator

Some tasks in this chapter required configuration in Cisco Unified Communications Manager, formerly known as Cisco Unified CallManager.

Overview of Operational Information

Table 7-1 describes how to access different types of operational information (status messages, network statistics, and other types of operational information). You can access this information through these methods:

- Locally (on the Cisco IP Communicator interface)
- Remotely (from a web site)

For details on accessing the device web page, see the "Accessing the Web Page for a Device" section on page 7-15.

Table 7-1 Overview of Operational Information

If you want to view...	Look here...	For details, see...
Model Information	• Cisco IP Communicator: **Settings** button > **Model Information**	• Model Information, page 7-7
Device Information	• Cisco IP Communicator: **Settings** button > **Device Configuration** • Service web page: **Device Information**	• Device Configuration Information, page 7-2 • Device Information, page 7-15
Security Configuration	Cisco IP Communicator: **Settings** button > **Security Configuration**	Security Configuration Information, page 7-7
Software Version	Cisco IP Communicator: **right-click** > **About Cisco IP Communicator**	Build Versions in the About Window Vary, page 8-15

Table 7-1 Overview of Operational Information (continued)

If you want to view...	Look here...	For details, see...
Status Messages	• Cisco IP Communicator: **Settings** button > **Status > Status Messages** • Device web page: **Device Logs > Status Messages**	• Status Messages Displayed, page 7-9 • Status Messages, Device Logs, and Alarm Information, page 7-17
Statistics	• Cisco IP Communicator: click the **?** button twice quickly during a call • Device web page: **Streaming Statistics > Stream 1**, **Stream 2**, or **Stream 3**	• Call Statistic Information, page 7-13 • Streaming Statistic Information, page 7-18
Alarm Messages	Device web page: **Device Logs > Debug Display**	Status Messages, Device Logs, and Alarm Information, page 7-17

About Operational Information Displayed Locally on Cisco IP Communicator

Device Configuration Information

To view the Device Configuration screen, click **Settings > Device Configuration**. Table 7-2 describes the non-networking settings in the display.

To modify configurable items that appear in this menu, use Cisco Unified Communications Manager Administration.

Table 7-2 Device Configuration Information Displayed in Cisco IP Communicator

Option	Description
CallManager Configuration	List of servers in prioritized order (CallManager 1 through CallManager 5) that are available for processing calls from this application. For an available server, an option shows server IP address and one of these states: • Active—Server from which the application is currently receiving call-processing services. • Standby—Server to which the application switches if the current server becomes unavailable. • Blank—No current connection to this server. An option might also include the SRST[1] designation, which indicates an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. You configure the SRST router address in Cisco Unified Communications Manager Administration (**System > Device Pool**).
HTTP Configuration	This menu has these options: • Directories URL—URL of the server from which the application obtains directory information. • Services URL—URL of the server from which the application obtains Cisco Unified IP Phone services. • Messages URL—URL of the server from which the application obtains message services. • Information URL—URL of the help text that appears in the application. • Authentication URL—URL that the application uses to validate requests made to the application web server. • Proxy Server URL—URL used to proxy HTTP requests for access to non-local host addresses from the application HTTP client. • Idle URL—URL that the application displays when the application has not been used for the time specified in the Idle URL Time option. For example, you can use the Idle URL option and the Idle URL Timer option to display a log on the phone screen when the application is not used for five minutes. • Idle URL Time—Amount of time in seconds that elapses before the URL specified in the Idle URL option appears.
Locale Configuration	This menu has these options: • User Locale—User locale associated with the application user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information. • Network Locale—Network locale associated with the application user. The network locale identifies a set of detailed information to support the application in a specific location, including definitions of the tones and cadences used by the application. • User Locale Version—Version of the user locale loaded on the application. • Network Locale Version—Version of the network locale loaded on the application. • User Locale Char Set—Character set that the application uses for the user locale.

Table 7-2 Device Configuration Information Displayed in Cisco IP Communicator (continued)

Option	Description
UI Configuration	• Auto Line Select Enabled—When enabled, the phone shifts the call focus to incoming calls on all lines. When disabled, the phone shifts the focus to incoming calls only on the currently used line. • BLF for Call Lists—When enabled, the phone displays phone status (presence information such as off-hook and on-hook) in the call lists.
SIP Configuration	Provides access to the SIP General Configuration menu and the Line Settings menu. See the "Related Topics."

1. SRST = Survivable Remote Site Telephony

Related Topics

- SIP General Configuration Information, page 7-4
- Line Settings Information, page 7-5
- Call Preferences Information, page 7-6

SIP General Configuration Information

To view the SIP General Configuration screen, click **Settings > Device Configuration > SIP Configuration > SIP General Configuration**. Table 7-3 describes the SIP parameters on Cisco IP Communicator.

You can modify configurable items that appear in this screen through Cisco Unified Communications Manager Administration Release 5.x and later by choosing **Device > Device Settings > SIP Profile**.

Table 7-3 SIP General Configuration Information Displayed in Cisco IP Communicator

Option	Description
Preferred CODEC	Displays the CODEC to use when a call is initiated. This value is always set to none and is not configurable.
Out of Band DTMF	Displays the configuration of the out-of-band signaling (for tone detection on the IP side of a gateway). The SIP Phone supports out-of-band signaling through the AVT tone method. This value is always set to avt and is not configurable.
Register with Proxy	Displays if the phone must register with a proxy server during initialization. This value is always set to true and is not configurable.
Register Expires	Displays the amount of time, in seconds, after which a registration request expires.
Phone Label	Displays the text that is on the top right status line of the Cisco IP Communicator phone screen. This text is for end-user display only and has no effect on caller identification or messaging. This value is always set to null and is not configurable.
Enable VAD	Displays if VAD[1] is enabled.
Start Media Port	Displays the start RTP[2] range for media.
End Media Port	Displays the end RTP range for media.
Backup Proxy	Displays the IP address of the backup proxy server or gateway. This value is always set to USECALLMANAGER and is not configurable.

Table 7-3 SIP General Configuration Information Displayed in Cisco IP Communicator (continued)

Option	Description
Backup Proxy Port	Displays the port number of the backup proxy server or gateway. This value is always be set to 5060 and is not configurable.
Emergency Proxy	Displays the IP address of the emergency proxy server or gateway. This value is always set to USECALLMANAGER and is not configurable.
Emergency Proxy Port	Displays the port number of the emergency proxy server or gateway. This value is always set to 5060.
Outbound Proxy	Displays the IP address of the outbound proxy server. This value is always set to USECALLMANAGER and is not configurable.
Outbound Proxy Port	Displays the port number of the outbound proxy server. This value is always set to 5060 and is not configurable.
NAT Enabled	Displays if NAT is enabled. This value is always set to false and is not configurable.
NAT Address	Displays the WAN IP address of the NAT[3] or firewall server. This value is always set to null and is not configurable.
Call Statistics	Displays if call statistics are enabled on the phone.

1. VAD = voice activation detection
2. RTP = Real-Time Transport Protocol
3. NAT = Network Address Translation

Related Topics

- Line Settings Information, page 7-5
- Call Preferences Information, page 7-6

Line Settings Information

To view the Line Settings screen, click **Settings > Device Configuration > SIP Configuration > Line Settings**. The Line Settings screen displays information about the configurable parameters for each of the lines on your SIP phone. Table 7-4 describes the options in the display. These options are SIP specific.

To modify configurable items that appear in this screen, use Cisco Unified Communications Manager Administration.

Table 7-4 Line Settings Information Displayed in Cisco IP Communicator

Option	Description
Name	Displays the number the line uses when registering.
Short Name	Displays the short name configured for the line.
Authentication Name	Displays the name used by the phone for authentication if a registration is challenged by the call control server during initialization.
Display Name	Displays the identification the phone uses for display for caller identification purposes.
Proxy Address	Displays the IP address of the proxy server that will be used by the phone. This value is always set to USECALLMANAGER and is not configurable.

Table 7-4 Line Settings Information Displayed in Cisco IP Communicator (continued)

Option	Description
Proxy Port	Displays the port number of the proxy server that will be used by the phone. This value is always set to 5060 and is not configurable.
Shared Line	Displays if the line is part of a shared line (Yes) or not (No) and is not configurable.

Related Topics

- SIP General Configuration Information, page 7-4
- Call Preferences Information, page 7-6

Call Preferences Information

To view the Call Preferences screen, click **Settings > Device Configuration > Call Preferences**. Table 7-5 describes the options in the display. These options are SIP specific.

Table 7-5 Call Preferences Information Displayed in Cisco IP Communicator

Option	Description
Do Not Disturb	Indicates whether do not disturb is enabled (Yes) or disabled (No) for the phone. To change this setting in Cisco Unified Communications Manager Administration Release 5.x and later, choose **Device > Device Settings > SIP Profile**. You can also modify this setting from the phone if enabled in Cisco Unified Communications Manager.
Caller ID Blocking	Indicates whether caller ID blocking is enabled (Yes) or disabled (No) for the phone. To change this setting in Cisco Unified Communications Manager Administration Release 5.x and later, choose **Device > Device Settings > SIP Profile**.
Anonymous Call Block	Indicates whether anonymous call block is enabled (Yes) or disabled (No) for the phone. To change this setting in Cisco Unified Communications Manager Administration Release 5.x and later, choose **Device > Device Settings > SIP Profile**.
Call Waiting Preferences	Displays a sub-menu that indicates whether call waiting is enabled (Yes) or disabled (No) for each line. To change this setting, use Cisco Unified Communications Manager Administration.
Call Hold Ringback	Indicates whether the call hold ringback feature is enabled (Yes) or disabled (No) for the phone. To change this setting in Cisco Unified Communications Manager Administration Release 5.x and later, choose **Device > Device Settings > SIP Profile**.
Stutter Msg Waiting	Indicates whether stutter message waiting is enabled (Yes) or disabled (No) for the phone. To change this setting in Cisco Unified Communications Manager Administration Release 5.x and later, choose **Device > Device Settings > SIP Profile**.
Call Logs BLF Enabled	Indicates whether BLF for call logs is enabled (Yes) or disabled (No) for the phone. To change this setting, use Cisco Unified Communications Manager Administration.
Auto Answer Preferences	Displays a sub-menu that indicates whether auto answer is enabled (Yes) or disabled (No) for the each line. To change this setting in Cisco Unified Communications Manager Administration Release 5.x and later, choose **Call Routing > Directory Number**.
Speed Dials	Displays a sub-menu that displays the lines available on the phone. Select a line to see the speed dial label and number assigned to that line. To change this setting, go to the Phone Configuration page > **Add/Update Speed Dials**.

Related Topics

- SIP General Configuration Information, page 7-4
- Line Settings Information, page 7-5

Model Information

To view the Model Information screen, click **Settings > Model Information**. This screen provides the phone model number of the phone, the factory-installed load running on the phone, and shows whether the phone is running SCCP or SIP.

Security Configuration Information

To view the Security Configuration screen, click **Settings > Security Configuration**. Table 7-6 describes the options in the display.

Table 7-6 Security Configuration Information Displayed in Cisco IP Communicator

Option	Description
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for Cisco IP Communicator. For details about disabling access, see the "Disabling the Internal Web Server" section on page 4-14.
Security Mode	Displays the security mode that is set for Cisco IP Communicator. You configure the device security mode in Cisco Unified Communications Manager Administration. For details, see the "How to Configure Security Features for Cisco IP Communicator" section on page 2-12. For details, see the *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
LSC[1]	Indicates whether an LSC, which is used for the security features, is installed on the phone (Yes) or is not installed (No) on Cisco IP Communicator. For details about managing the LSC for your phone, see the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
CTL[2] File	Displays the MD5 hash of the CTL file that is installed for Cisco IP Communicator. If no CTL file is installed, this field displays *No*. If security is configured for Cisco IP Communicator, the CTL file automatically installs when Cisco IP Communicator reboots or resets. For details, see the "Configuring the Cisco CTL Client" chapter in *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html If a CTL file is installed, this option also provides access to the CTL File screen.
Trust List	Displays information about all of the servers that the phone trusts. If a CTL file is installed, this option provides access to the Trust List menu.
CAPF[3] Server	Displays the IP address and the port of the CAPF that Cisco IP Communicator uses.

1. LSC = Locally Significant Certificate
2. CTL = certificate trust list
3. CAPF = Certificate Authority Proxy Function

Related Topics

- CTL File Information, page 7-8
- Trust List Information, page 7-8

CTL File Information

If a CTL file is installed on Cisco IP Communicator, you can access the CTL File screen by clicking **Settings > Security Configuration > CTL File**.

Table 7-7 describes the options in the display.

Table 7-7 CTL File Information Displayed in Cisco IP Communicator

Option	Description
CTL File	Displays the MD5 hash of the CTL file that is installed for Cisco IP Communicator. If no CTL file is installed, this field displays *No*. If security is configured for Cisco IP Communicator, the CTL file automatically installs when Cisco IP Communicator reboots or resets. For details, see the "Configuring the Cisco CTL Client" chapter in *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html A locked padlock icon means that the CTL file is locked. An unlocked padlock icon means that the CTL file is unlocked.
CAPF Server	Displays the IP address of the CAPF server used by the phone. Also displays a certificate icon if a certificate is installed for this server.
CallManager/TFTP Server	Displays the IP address of the Cisco Unified Communications Manager and the TFTP server used by the phone. Also displays a certificate icon if a certificate is installed for this server.

Related Topics

- Security Configuration Information, page 7-7
- Trust List Information, page 7-8

Trust List Information

The Trust List screen displays information about all of the servers on the trusted list.

If a CTL file is installed on Cisco IP Communicator, you can access the Trust List screen by choosing **Settings > Security Configuration > Trust List**.

Table 7-8 describes the options in the display.

Table 7-8 Trust List Information Displayed in Cisco IP Communicator

Option	Description
CAPF Server	Displays the IP address of the CAPF that is used by Cisco IP Communicator. Also displays a certificate icon if a certificate is installed for this server.
CallManager/TFTP Server	Displays the IP address of a Cisco Unified Communications Manager server and a TFTP server that is used by Cisco IP Communicator. Also displays a certificate icon if a certificate is installed for this server.
SRST Router	Displays the IP address of the trusted SRST router that is available to Cisco IP Communicator, if such a device has been configured in Cisco Unified Communications Manager Administration. Also displays a certificate icon if a certificate is installed for this server.

Related Topics

- Security Configuration Information, page 7-7
- CTL File Information, page 7-8

Status Messages Displayed

The Status menu displays the Status Messages screen, which shows a log of important system messages. To display the Status menu, click **Settings > Status > Status Messages**. Table 7-9 describes the possible messages.

Table 7-9 Status Messages Displayed in Cisco IP Communicator

Message	Description	Possible Explanation and Action
BootP server used	Cisco IP Communicator obtained its IP address from a BootP server rather than from 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 is created when Cisco IP Communicator is added to the Cisco Unified Communications Manager database. If it has not been added to the database, the TFTP server generates a `CFG File Not Found` response. • Cisco IP Communicator is not registered with Cisco Unified Communications Manager. You must manually add Cisco IP Communicator to the database if you are not allowing these devices to auto-register. • 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 the TFTP server configuration.

Table 7-9 Status Messages Displayed in Cisco IP Communicator (continued)

Message	Description	Possible Explanation and Action
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 might be corrupted.
CTL Installed	A CTL file is installed on Cisco IP Communicator.	None. This message is informational only. See the *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
CTL update failed	Cisco IP Communicator could not update its CTL file.	A problem occurred with the CTL file on the TFTP server. See the *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
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 Cisco IP Communicator —Verify the network connections. • DHCP server is down—Check the DHCP server configuration. • Errors persist—Consider 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 Cisco IP Communicator—Verify the network connections. • DNS server is down—Check the DNS server configuration.
DNS unknown host	DNS could not resolve the TFTP server name or Cisco Unified Communications Manager.	• Verify that the TFTP server host names of Cisco Unified Communications Manager are properly configured in DNS. • Consider using IP addresses rather than host names.
Duplicate IP	Another device is using the IP address assigned to Cisco IP Communicator.	• If Cisco IP Communicator has a static IP address, verify that you have not assigned a duplicate IP address. If you are using DHCP, check the DHCP server configuration.

Table 7-9 Status Messages Displayed in Cisco IP Communicator (continued)

Message	Description	Possible Explanation and Action
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 these files are located within subdirectories in the TFTPPath directory: • Located in subdirectory with same name as network locale: – g3-tones.xml • Located in subdirectory with same name as user locale: – ipc-sccp.jar – ipc-sip.jar
File auth error	An error occurred when Cisco IP Communicator 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 Cisco IP Communicator from the database. Then add it to the database by using Cisco Unified Communications Manager 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.
File not found	Cisco IP Communicator cannot locate the phone load file that is specified in the phone configuration file on the TFTP server.	Make sure that the phone load file is on the TFTP server and that the entry in the configuration file is correct.
IP address released	Cisco IP Communicator has been configured to release its IP address.	Cisco IP Communicator remains idle until you reset the DHCP address.
Load Auth Failed	Cisco IP Communicator could not load a configuration file.	The configuration file that Cisco IP Communicator received from the server identified in this message is corrupt. Make sure that a good version of the configuration file exists on that server.
Load Auth Failed	A signed phone load file has been modified or renamed.	Make sure that the phone load file that Cisco IP Communicator is downloading has not been altered or renamed.
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to Cisco IP Communicator in Cisco Unified Communications Manager Administration (**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 Cisco IP Communicator that did not support hardware changes on this newer phone. Check the load ID assigned to the phone in Cisco Unified Communications Manager Administration (**Device > Phone**). Re-enter the load displayed on the phone.

Table 7-9 Status Messages Displayed in Cisco IP Communicator (continued)

Message	Description	Possible Explanation and Action
No CTL installed	A CTL file is not installed in Cisco IP Communicator.	Occurs if security is not configured or, if security is configured, because the CTL file does not exist on the TFTP server. See the *Cisco Unified Communications Manager Security Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
No default router	DHCP or static configuration did not specify a default router.	• If Cisco IP Communicator has a static IP address, verify that the default router has been configured. • 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 Cisco IP Communicator has a static IP address, verify that the DNS server has been configured. If you are using a DHCP server, it did not provide a DNS server address. Check the DHCP server configuration.
Programming Error	Cisco IP Communicator failed during programming.	Attempt to resolve this error by exiting (or closing) the application and then relaunching it. If the problem persists, contact Cisco technical support for 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 the TFTP server configuration.
TFTP Error	Cisco IP Communicator 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 TFTPPath directory.	Check the load ID assigned to Cisco IP Communicator in Cisco Unified Communications Manager Administration (**Device > Phone**). Verify that the TFTPPath directory contains a .bin file with this load ID as the name.
TFTP server not authorized	The specified TFTP server could not be found in CTL for Cisco IP Communicator.	• The DHCP server is not configured properly, and the TFTP server address is not correct. In this case, update the TFTP server configuration to specify the correct TFTP server. • If Cisco IP Communicator is using a static IP address, the phone might 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 might 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.

Table 7-9 Status Messages Displayed in Cisco IP Communicator (continued)

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 Cisco IP Communicator—Verify the network connections. • TFTP server is down—Check TFTP server configuration.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.
XmlDefault.cnf.xml, or .cnf.xml corresponding to Cisco IP Communicator device name	Name of the configuration file.	None. This is an informational message indicating the name of the configuration file for the phone.

Related Topics

- Device Configuration Information, page 7-2
- Security Configuration Information, page 7-7
- Call Statistic Information, page 7-13

Call Statistic Information

The Call Statistics screen shows counters and statistics for the current call. To display the Call Statistics screen, click the **?** button twice rapidly during a call. Table 7-10 describes the options in the display.

Table 7-10 Call Statistics Displayed in Cisco IP Communicator

Item	Description
Rcvr Codec	Type of voice stream received (RTP[1] streaming audio). For a list of supported codecs, see the data sheet at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_data_sheet09186a00801f8e48.html
Sender Codec	Type of voice stream transmitted (RTP streaming audio). For a list of supported codecs, see the data sheet at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_data_sheet09186a00801f8e48.html
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 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.

Table 7-10 Call Statistics Displayed in Cisco IP Communicator (continued)

Item	Description
Sender Packets	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 Jitter	The 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 Jitter	Maximum jitter observed since the receiving voice stream was opened.
RxDisc	Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on). **Note** The application discards payload type 19 comfort noise packets that are generated by Cisco Gateways, which increments this counter.
Recvr Lost Packets	Missing RTP packets (lost in transit).

1. RTP = Real-Time Transport Protocol

About Operational Information Displayed Remotely from a Web Page

Each Cisco IP Communicator device has a web page from which you can view operational information. You can use this information to remotely monitor the device and to assist with troubleshooting.

Note Remote access is not possible if you disabled the internal web server as described in the "Disabling the Internal Web Server" section on page 4-14.

You can also obtain much of this information directly from Cisco IP Communicator. For details, see the "About Operational Information Displayed Locally on Cisco IP Communicator" section on page 7-2. For troubleshooting information, see Chapter 8, "Troubleshooting Cisco IP Communicator."

Accessing the Web Page for a Device

Procedure

Step 1 Search for the device in Cisco Unified Communications Manager Administration (**Device > Phone**). Devices registered with Cisco Unified Communications Manager display the IP address at the top of the Phone Configuration web page.

Step 2 Open a web browser, and enter the following URL, where *IP_address* is the IP address of Cisco IP Communicator:

http://*IP_address*

Tip If you are performing this on the PC on which Cisco IP Communicator is installed, you can use *localhost* for the IP address if Cisco IP Communicator is running.

Related Topics

- Device Information, page 7-15
- Network Configuration Information, page 7-16
- Status Messages, Device Logs, and Alarm Information, page 7-17
- Streaming Statistic Information, page 7-18

Device Information

To display device information, access the web page as described in the "Accessing the Web Page for a Device" section on page 7-15, and click **Device Information**. The web page displays device settings and related information. Table 7-11 describes the information.

Table 7-11 Device Information Items Displayed on the Web Page

Item	Description
Host Name	Host name that the DHCP server assigned to the device.
Phone DN	Directory number assigned to the device.
Version	Version of the boot load running on the device.
Model Number	Model number of the device.
Message Waiting	Indicates if there is a voice message waiting on any line for the device.

Related Topics

- Network Configuration Information, page 7-16
- Status Messages, Device Logs, and Alarm Information, page 7-17
- Streaming Statistic Information, page 7-18

Network Configuration Information

To display network configuration information, access the web page as described in the "Accessing the Web Page for a Device" section on page 7-15, and click **Network Configuration**.

The web page displays network configuration information and information about other settings. You can view some of these items in Cisco IP Communicator (**Settings > Device Configuration**). For details, see the "Device Configuration Information" section on page 7-2.

Table 7-12 describes the information.

Table 7-12 Network Configuration Items Displayed on the Web Page

Item	Description
DHCP Server	IP address of the DHCP server from which the device obtains its TFTP server address.
Host Name	Host name that the DHCP server assigned to the device.
IP Address	IP address of the device.
TFTP Server 1	Primary TFTP server used by the device.
CallManager 1–5	Servers, in prioritized order, that are available for processing calls from the device. For an available server, an option shows the server IP address and one of these states: • Active—Server from which the device is currently receiving call-processing services. • Standby—Server to which the device switches if the current server becomes unavailable. • Blank—No current connection to this server. An option might also include the SRST designation, which indicates an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers even if it is active. You configure the SRST router address in Cisco Unified Communications Manager Administration (**System > Device Pool**).
Information URL	URL of the help text that appears on the device.
Directories URL	URL of the server from which the device obtains directory information.
Messages URL	URL of the server from which the device obtains message services.
Services URL	URL of the server from which the device obtains Cisco Unified IP Phone services.
Alternate TFTP	Indicates whether the device is using an alternative TFTP server.
Idle URL	URL that the phone displays when the device has not been used for the time specified by Idle URL Time.
Idle URL Time	Time in seconds that elapses before the URL shown in Idle URL appears.
Proxy Server URL	URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the device HTTP client and provides responses from the non-local host to the device HTTP client.
Authentication URL	URL that the device uses to validate requests made to the web server.
TFTP Server 2	Backup TFTP server that the device uses if the primary TFTP server is unavailable.
User Locale	User locale associated with the Cisco IP Communicator user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale associated with the Cisco IP Communicator user. Identifies a set of detailed information to support the device in a specific location, including definitions of tones and cadences.

Table 7-12 Network Configuration Items Displayed on the Web Page (continued)

Item	Description
Headset Enabled	Current state of the Cisco IP Communicator headset (enabled or disabled).
User Locale Version	Version of the user locale loaded on the device.
Network Locale Version	Version of the network locale loaded on the phone.
Auto Line Select Enabled	When enabled, the phone shifts the call focus to incoming calls on all lines. When disabled, the phone shifts the focus to incoming calls only on the currently used line.

Related Topics

- Device Information, page 7-15
- Status Messages, Device Logs, and Alarm Information, page 7-17
- Streaming Statistic Information, page 7-18

Status Messages, Device Logs, and Alarm Information

To display status messages or debug display information, access the web page as described in the "Accessing the Web Page for a Device" section on page 7-15, and click **Status Messages** or **Debug Display**. The web page displays device logs, which provides information you can use to help monitor and troubleshoot the application.

The Status Messages area displays up to the 10 most recent status messages that Cisco IP Communicator generated since it was last powered up. These are the same status messages that you can see on the interface (**Settings > Status > Status Message**). Table 7-9 on page 7-9 describes the status messages that can appear.

The Debug Display area displays a log of up to the 50 most recent alarms for the phone. Alarms indicate a variety of errors or conditions. Table 7-13 describes the alarm messages.

Table 7-13 Alarms Displayed on the Web Page

Alarm Number	Explanation
1	Configuration file that the device tried to obtain from the TFTP server was too large (greater than 2 MB)
3	Firmware image that the device tried to obtain has an incorrect name
4	The PC on which Cisco IP Communicator is installed has run out of disk space
6	Configuration file that the device requested does not exist on the TFTP server
7	A request to the TFTP server timed out
8	The device could not log in to the TFTP server
9	General TFTP error
14	Cisco Unified Communications Manager closed socket
15	The device lost its connection to the remote host
16	Cisco Unified Communications Manager indicates that the device could not unregister for some reason
17	Cisco Unified Communications Manager stopped responding to KeepAlive requests

Table 7-13 Alarms Displayed on the Web Page (continued)

Alarm Number	Explanation
18	The device failed back to a higher priority Cisco Unified Communications Manager
20	User clicked **#** on the phone
21	The device obtained a new IP address
22	Cisco Unified Communications Manager sent a reset instruction to the device
23	Cisco Unified Communications Manager sent a restart instruction to the device
24	Cisco Unified Communications Manager rejected a registration attempt from the device
25	No prior reset cause (default condition)
32	General alarm
33	Could not write to the hard drive

Related Topics

- Device Information, page 7-15
- Network Configuration Information, page 7-16
- Streaming Statistic Information, page 7-18

Streaming Statistic Information

To display streaming statistics, access the web page as described in the "Accessing the Web Page for a Device" section on page 7-15, and click **Stream 1**, **Stream 2**, or **Stream 3**. The web pages provides streaming statistics information.

Cisco IP Communicator can simultaneously stream information to and from up to three devices. It streams information when it is on a a call or running a service that sends or receives audio or data. Most calls use only one stream (Stream 1), but some calls use two or three streams. For example, a barged call uses Stream 1 and Stream 2. Table 7-14 describes the streaming statistics information.

Table 7-14 Streaming Statistics Displayed on the Web Page

Item	Description
Domain	Domain of the device
Remote Address	IP address of the destination of the stream
Local Address	IP address of the device
Sender Joins	Number of times the device has started transmitting a stream
Receiver Joins	Number of times the device has started receiving a stream
Byes	Number of times the device has stopped transmitting a stream
Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requested that the device start transmitting packets
Row Status	Whether the device is streaming
Host Name	Host name of the device
Sender Packets	Total number of packets sent by the device

Table 7-14 Streaming Statistics Displayed on the Web Page (continued)

Item	Description
Sender Octets	Total number of octets sent by the device
Sender Tool	Type of audio encoding used for the stream
Sender Reports	Number of times this streaming statistics report has been accessed from the web page (resets when the device resets)
Sender Report Time	Internal time stamp indicating when this streaming statistics report was generated
Sender Start Time	Time that the stream started
Rcvr Lost Packets	Total number of packets lost
Rcvr Jitter	Maximum jitter of stream
Receiver Tool	Type of audio encoding used for the stream
Rcvr Reports	Number of times this streaming statistics report has been accessed from the web page (resets when the device resets)
Rcvr Report Time	Internal time stamp indicating when this streaming statistics report was generated
Rcvr Packets	Total number of packets received by the device
Rcvr Octets	Total number of octets received by the device
Rcvr Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requested that the device start receiving packets

Related Topics

- Device Information, page 7-15
- Network Configuration Information, page 7-16
- Status Messages, Device Logs, and Alarm Information, page 7-17

How to Set Up and Run the Windows Performance Tool

- Setting Up and Running the Windows 2000 and XP Performance Tool, page 7-19
- Setting Up and Running the Windows Vista Performance Tool, page 7-21

Setting Up and Running the Windows 2000 and XP Performance Tool

You can monitor application performance by using the Windows Performance tool to gauge the impact that other applications might have on Cisco IP Communicator (for example, in preparation for an internal pilot). You might also want to monitor performance if users complain of degraded Cisco IP Communicator performance when other applications are running.

Before You Begin

Before starting this test, ensure that only the operating system and applications that run all the time (anti-virus, security, instant message applications, and so forth) are running along with Cisco IP Communicator.

Procedure

Step 1 Start the Windows Performance Tool by choosing **Start > Control Panel > Administrative Tools > Performance**.

Step 2 In the left pane of the Performance window:

a. For Windows 2000, make sure the Tree Tab is selected.

b. Click **Performance Logs and Alerts** to expand it.

Step 3 Name the log file:

a. In the left pane, select **Counter Logs**, right-click, and choose **New Log Settings**.

b. In the New Log Settings pop-up, enter the log file name, and click **OK**.

Step 4 Choose Cisco IP Communicator-specific performance counters when the next pop-up window appears:

a. Make sure the General Tab is selected, and click **Add Counters** (or **Add** for Windows 2000) to add counters to monitor.

b. In the next window, perform these steps:

- Choose **Select Counters From Computer** (the name of the computer should appear in the list).
- Set Performance Object to **Process**.
- In Select Counters From List, choose process-related counters (**% Processor Time**, **IO Other Bytes**, I**O Read Bytes/sec**, **IO Write Bytes/sec**, **Private Bytes, Working Set**) recommended) from the list. While selecting these counters, press the **Ctrl** key to add more than one at a time.
- In Select Instances From List, choose **Communicator** from the list, and click **Add**.

c. When you are finished adding counters, click **Close**.

d. In the window that appears, review the list of counters that you added. Make adjustments, if necessary.

Step 5 Define the time interval for monitoring. Enter values for Interval and Units (for example Interval = 1 and Units = seconds). This setting applies to all counters in the list.

Step 6 Select the Log Files Tab, and define the format in which performance data is saved:

a. For Log File Type, select **Text File (Comma Delimited)** (or **Text File - CSV** for Windows 2000) to create a comma-delimited file.

b. Note the location where the file is saved.

c. Click **Apply**.

Step 7 Select the Schedule Tab, and enter information to start and stop the log. Click **Apply** and **OK**.

You can also manually start and stop the log by clicking the buttons on the toolbar.

Run the test for the duration that seems appropriate for the type of problem that you are trying to resolve. For example, if Cisco IP Communicator fails right after it is launched, you might want to run the performance test for only 5 to 10 minutes. However, if there are problems that occur after a long period of usage, you might need to run the test for 8 hours.

Step 8 Run the test again when other CPU intensive applications (Microsoft Excel, Outlook, Word) are running in the background.

Compare the results from the tests. Cisco IP Communicator CPU usage should stay near the baseline while other applications are running in the background.

Step 9 Import the file from its saved location into a spreadsheet.

Setting Up and Running the Windows Vista Performance Tool

You can monitor application performance by using the Windows Performance tool to gauge the impact that other applications might have on Cisco IP Communicator (for example, in preparation for an internal pilot). You might also want to monitor performance if users complain of degraded Cisco IP Communicator performance when other applications are running.

Before You Begin

Before starting this test, ensure that only the operating system and applications that run all the time (anti-virus, security, instant message applications, and so forth) are running along with Cisco IP Communicator.

Procedure

Step 1 From the Control Panel, choose **Performance Information and Tools**.

Step 2 From the Tasks pane on the left, choose **Advanced Tools**.

Step 3 From the list of tools, click **Open Reliability and Performance Monitor**.

Step 4 In the Reliability and Performance Monitor window, in the left pane, click **Data Collector Sets** to expand it.

Step 5 Right-click **User Defined**, and choose **New > Data Collector Set**.

Step 6 In the Create New Data Collector Set window:

a. Enter a name for the collector set, click **Create Manually (Advanced)**, and click **Next**.

b. For what type of data do you want to include, click **Performance Counter**, and click **Next**.

c. Define the sample interval for the performance counters you want to log, and click **Add**.

d. Under the Available Counters section in the left panel, click **Process** to expand it:

- Select **% Processor Time**, **IO Other Bytes**, I**O Read Bytes/sec**, **IO Write Bytes/sec**, **Private Bytes, Working Set** (recommended) from the list. While selecting these counters, press the **Ctrl** key to add more than one at a time.
- From the Instance of Selected Object list, select **Communicator**, click **Add**, and then **OK**.

e. Verify the list of performance counters, and click **Next**.

f. Define the folder for the log file by clicking **Browse**.

g. Click **Finish**.

Step 7 In the Reliability and Performance Monitor window, in the left pane, select the name of the collector set that you specified in Step 6a under **Data Collector Sets > User Defined**, and double-click the corresponding **DataCollector01** in the right pane.

Step 8 In the DataCollector01 Properties window, Performance Counters tab, select the log format as **Comma Separated**, click **Apply**, and **OK** to dismiss the window.

Step 9 In the Reliability and Performance Monitor window, in the left pane, right-click the name of the collector set, and select **Start**.

Run the test for the duration that seems appropriate for the type of problem that you are trying to resolve. For example, if Cisco IP Communicator fails right after it is launched, you might want to run the performance test for only 5 to 10 minutes. However, if there are problems that occur after a long period of usage, you might need to run the test for 8 hours.

Step 10 Run the test again when other CPU intensive applications (Microsoft Excel, Outlook, Word) are running in the background.

Compare the results from the tests. Cisco IP Communicator CPU usage should stay near the baseline while other applications are running in the background.

Step 11 Import the file from its saved location into a spreadsheet.