CHAPTER 1

Overview of Cisco IP Communicator

Revised: 1/24/12

Overview of Cisco IP Communicator Features

Cisco IP Communicator is a software-based application that allows users to place and receive phone calls by using their personal computers. Cisco IP Communicator depends upon the Cisco Unified Communications Manager call-processing system (formerly known as Cisco Unified CallManager) to provide telephony features and voice-over-IP capabilities through eight telephone lines (or a combination of lines, softkeys, and direct access to telephony features).

Note Depending on context, this guide refers to Cisco IP Communicator as a *phone*, *device*, *application*, or an *interface*.

When registered to Cisco Unified Communications Manager, Cisco IP Communicator has the capabilities of a full-featured Cisco Unified IP Phone, including the ability to transfer calls, forward calls, and conference additional participants to an existing call. This means that you can provision and upgrade Cisco IP Communicator as any other Cisco Unified IP Phone, greatly simplifying IP phone management. Through automatic software updates, Cisco IP Communicator keeps pace with new software features and changes.

Cisco IP Communicator enables you to deliver Extensible Markup Language (XML)-based applications to the display and provide quick access to diverse information such as weather, stocks, quote of the day, or any other web-based information.

Cisco IP Communicator offers high-quality audio features such as the Audio Tuning Wizard, an advanced (adaptive) jitter buffer and packet loss (error) concealment, acoustic echo cancellation, noise suppression, voice activity detection, and silence suppression.

Cisco IP Communicator offers other advanced features that accommodate ever-mobile users and changing network conditions. These features include auto-detection of Cisco VPN clients, automated support for most VPN clients (including Microsoft PPTP client), interoperability with Cisco Unified Video Advantage for desktop video calls, and non-MAC-based device name for easy PC refreshes (requires a Cisco Unified Communications Manager version 4.1.3 or later).

For details about configuring Cisco IP Communicator for different protocols, for security features, and for details about supported call features, see the Related Topics section.

For details about the all Cisco IP Communicator features, see the data sheet at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_data_sheet09186a00801f8e48.html

For details about using the application, see the user guide at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html

Related Topics

- How to Configure Cisco IP Communicator the SCCP or SIP Protocol, page 2-9
- How to Configure Security Features for Cisco IP Communicator, page 2-12
- Telephony Features Available for Cisco IP Communicator, page 5-2

Supported Networking Protocols

Table 1-1 lists the industry-standard and Cisco networking protocols required for voice communication Use this information to help you design your network.

Table 1-1 Supported Networking Protocols

Networking Protocol	Purpose	Usage Notes
BootP (Bootstrap Protocol)	Enables a network device such as Cisco IP Communicator to discover certain startup information, such as its IP address.	If you are using BootP to assign IP addresses to Cisco IP Communicator, the BOOTP Server option shows “Yes” in the network configuration settings on the phone.
CDP(Cisco Discovery Protocol)	Device-discovery protocol that runs on all Cisco-manufactured equipment. By using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	Cisco IP Communicator uses CDP to communicate information such as auxiliary VLAN ID, per-port power management details, and QoS (quality of service) configuration information with the Cisco Catalyst switch.
DHCP (Dynamic Host Configuration Protocol)	Dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect Cisco IP Communicator into the network and have it become operational without you manually assigning an IP address or configuring additional network parameters.	We recommend that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DCHP configurations, see the *Cisco Unified Communications Manager System Guide* at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
HTTP (HyperText Transfer Protocol)	Uses TCP to transfer web content over the Internet.	Cisco IP Communicator uses HTTP to obtain the configuration file, LDAP directories configuration, dialing rules, XML services, and locale strings.

Table 1-1 Supported Networking Protocols (continued)

Networking Protocol	Purpose	Usage Notes
IP (Internet Protocol)	Messaging protocol that addresses and sends packets across the network.	To communicate by using IP, network devices must have an assigned IP address, subnet, and gateway. Cisco IP Communicator obtains its IP information from the system network configuration.
LDAP (Lightweight Directory Access Protocol)	Protocol for accessing directories.	Cisco IP Communicator can use LDAP to search for names and phone numbers.
RTP (Real-Time Transport Protocol)	Standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco IP Communicator uses the RTP to receive from and send real-time voice traffic to other Cisco IP Communicators and gateways.
RTCP (Real-Time Control Protocol)	RTCP works with Real-Time Transport Protocol (RTP) to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams.	RTCP is disabled by default, but you can enable it on a per-phone basis using Cisco Unified Communications Manager.
SDP (Session Description Protocol)	Portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that are supported by all endpoints in the conference.	SDP capabilities (such as codec types, DTMF detection, and comfort noise) are normally configured on a global basis by Cisco Unified Communications Manager or the Media Gateway in operation. Some SIP endpoints might allow these parameters to be configured on the endpoint. This might vary from vendor to vendor.
SCCP (Skinny Client Control Protocol)	Includes a messaging set that allows communications between call control servers and endpoint clients such as IP Phones. SCCP is proprietary to Cisco Systems.	Cisco IP Communicator to can use either SCCP or SIP.
SIP (Session Initiation Protocol)	Standard for setting up telephone calls, multimedia conferencing, and other types of communications on the Internet. SIP can be used to establish, maintain, and terminate calls between two or more endpoints. SIP provides signaling, which allows call information to be carried across network boundaries. SIP provides session management, which controls the attributes of an end-to-end call.	Cisco IP Communicator to can use either SCCP or SIP.
TCP (Transmission Control Protocol)	Connection-oriented transport protocol.	Cisco IP Communicator uses TCP to connect to Cisco Unified Communications Manager and to access XML services.

Table 1-1 Supported Networking Protocols (continued)

Networking Protocol	Purpose	Usage Notes
TFTP (Trivial File Transfer Protocol)	Allows you to transfer files over the network. On Cisco IP Communicator, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want Cisco IP Communicator to use a TFTP server other than the one specified by the DHCP server, you must manually assign the TFTP server in Cisco IP Communicator.
TLS (Transport Layer Security)	Standard protocol for securing and authenticating communications.	When security is implemented, Cisco IP Communicator uses the TLS protocol when securely registering with Cisco Unified Communications Manager.
UDP (User Datagram Protocol)	Connectionless messaging protocol for delivery of data packets.	Cisco IP Communicator transmits and receives RTP streams, which uses UDP.

Related Topics

- How Cisco IP Communicator Interacts with Cisco Unified Communications Manager, page 1-4
- How Cisco IP Communicator Interacts With the Network at Startup, page 1-5

How Cisco IP Communicator Interacts with Cisco Unified Communications Manager

Cisco IP Communicator is a software application that enables you to communicate by using voice over a data network. To provide this capability, Cisco IP Communicator depends upon Cisco Unified Communications Manager to set up and tear down calls between phone devices, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages all components of the IP telephony system—the phone devices, access gateways, and the resources necessary for such features as conference calls and route plans. Cisco Unified Communications Manager also provides:

- Firmware for phones
- Authentication (if configured for the telephony system)
- Device configuration file and certificate trust list (CTL) file through the TFTP service
- Cisco IP Communicator registration
- Call preservation so that a media session continues if signaling is lost between the primary Cisco Unified Communications Manager and Cisco IP Communicator

As you would do with other Cisco Unified IP Phones that rely on Cisco Unified Communications Manager, you must configure and manage Cisco IP Communicator as a network device through Cisco Unified Communications Manager Administration. For details, see *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

For details about supported Cisco Unified Communications Manager releases, see the Cisco IP Communicator release notes at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/prod_release_notes_list.html

Related Topics

- How Cisco IP Communicator Interacts With the Network at Startup, page 1-5
- About Configuration Files, page 1-6
- QoS Modifications to Prioritize Voice Traffic, page 1-8
- Network, Server, and Client PC Requirements, page 2-1
- Telephony Features Available for Cisco IP Communicator, page 5-2

How Cisco IP Communicator Interacts With the Network at Startup

At startup, Cisco IP Communicator interacts with the network as follows:

1. Locates the configuration server.

   Upon startup, Cisco IP Communicator always attempts to use DHCP to locate its TFTP server. Cisco IP Communicator first tries to use HTTP (by default) to retrieve files from the server, and if it is not able, Cisco IP Communicator uses TFTP.

   If you used the Cisco IP Communicator Administration Tool, Cisco IP Communicator can also use HTTP to retrieve software updates, thereby accelerating file transfer for remote users. This tool is for Windows-based Cisco Unified Communications Managers only.

   If you do not use DHCP in your network to identify TFTP servers, or if you want the device to use an alternate TFTP server, you must manually configure your TFTP server from Cisco IP Communicator or instruct users to do this task.

2. Requests the CTL file (if security is configured).

   The TFTP server stores the CTL file, which contains a list of Cisco Unified Communications Managers and TFTP servers that Cisco IP Communicator is authorized to connect to. It also contains the certificates necessary for establishing a secure connection between Cisco IP Communicator and Cisco Unified Communications Manager.

   The security CTLFile.tlv file is downloaded to the [*ApplicationData*]\Cisco\Communicator\sec folder.

3. Requests configuration files.

   Configuration files (.cnf.xml) reside on the TFTP server and define parameters for connecting to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified Communications Manager that requires a device to be reset, a change is made to the configuration file for that device.

   - If you have enabled auto-registration in Cisco Unified Communications Manager, Cisco IP Communicator accesses a default configuration file (xmldefault.cnf.xml) from the TFTP server.
   - Otherwise, Cisco IP Communicator accesses a .cnf.xml file corresponding to its device name.

4. Downloads locale strings.

   The.cnf.xml file configuration file tells Cisco IP Communicator which user locale strings to use. To make this request, Cisco IP Communicator first tries to use HTTP. If you have not enabled HTTP access, Cisco IP Communicator uses TFTP.

5. Contacts Cisco Unified Communications Manager.

   After obtaining the configuration file from the TFTP server, Cisco IP Communicator attempts to make a connection to the highest priority Cisco Unified Communications Manager on the list. If security is implemented, Cisco IP Communicator makes a TLS connection; otherwise, it makes a nonsecure TCP connection.

   - If the device was added to the database individually (through Cisco Unified Communications Manager Administration or in bulk through the Bulk Administration Tool (BAT), Cisco Unified Communications Manager identifies the device. This is only true if you are not using BAT with the Tool for Auto-Registered Phones Support (TAPS).
   - Otherwise, the device attempts to register itself in the Cisco Unified Communications Manager database (when auto-registration is enabled in Cisco Unified Communications Manager).

Note Auto-registration is disabled when security is enabled on Cisco Unified Communications Manager. In this case, you must manually add Cisco IP Communicator to the Cisco Unified Communications Manager database.

Related Topics

- About Configuration Files, page 1-6
- About Methods for Adding Devices to the Cisco Unified Communications Manager Database, page 2-6
- How to Configure Cisco IP Communicator the SCCP or SIP Protocol, page 2-9
- How to Configure Security Features for Cisco IP Communicator, page 2-12
- Specifying a TFTP Server, page 4-6
- About Updating the Application, page 3-6
- How to Resolve Startup Problems, page 8-5

About Configuration Files

Configuration files for Cisco IP Communicator are stored on the TFTP server and define parameters for connecting to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified Communications Manager that requires Cisco IP Communicator to be reset, a change is automatically made to the configuration file on Cisco IP Communicator.

In addition, if the device security mode in the configuration file is set to Authenticated and the CTL file on Cisco IP Communicator has a valid certificate for Cisco Unified Communications Manager, Cisco IP Communicator establishes a TLS connection to Cisco Unified Communications Manager. Otherwise, Cisco IP Communicator establishes a TCP connection. The transport protocol in the configuration file must also be set to TLS (corresponding to the transport type in the SIP Security Profile on Cisco Unified Communications Manager).

Note If the device security mode in the configuration file is set to Authenticated or Encrypted, but Cisco IP Communicator has not received a CTL file, Cisco IP Communicator continuously tries to obtain a CTL file so that it can register securely.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, refer to the "Configuring Encrypted Phone Configuration Files" chapter in *Cisco Unified Communications Manager Security Guide*.

Related Topics

- Cisco IP Communicator Requests for Configuration Files, page 1-7
- Configuration Files Stored on the TFTP Server, page 1-7

Cisco IP Communicator Requests for Configuration Files

Cisco IP Communicator requests a configuration file whenever it resets and registers with Cisco Unified Communications Manager.

If auto-registration is not enabled and Cisco IP Communicator has not been added to the Cisco Unified Communications Manager database, the registration request is rejected. In this case, Cisco IP Communicator resets and repeatedly attempts to register.

If this installation of Cisco IP Communicator has registered before, Cisco IP Communicator accesses the configuration file named *device_name*.cnf.xml, where *device_name* is the user-defined device name for this instance of Cisco IP Communicator.

Related Topics

- About Configuration Files, page 1-6
- Configuration Files Stored on the TFTP Server, page 1-7

Configuration Files Stored on the TFTP Server

The TFTP server provides these configuration files for SIP and SCCP devices:

- IP Phones:
  - For unsigned and unencrypted files—*device_name*.cnf.xml
  - For signed files—*device_name*.cnf.xml.sgn
  - For signed and encrypted files—*device_name*.cnf.xml.enc.sgn
- Dial Plan—*dialplan*.xml

  You must configure and associate dial plans with a phone device to enable dial plans to be sent to the configuration file. If you do not configure a phone dial plan, Cisco IP Communicator does not display any indication of a dial plan.

  If you are using a version of Cisco Unified Communications Manager other than 4.x, you can configure SIP dial rules. You configure these dial rules from the SIP Dial Rule Configuration window (**Call Routing > Dial Rules > SIP Dial Rules**) in Cisco Unified Communications Manager Administration.

You configure SCCP dial rules from the Application Dial Rules Configuration window (**Call Routing > Dial Rules > Application Dial Rules**) in Cisco Unified Communications Manager Administration.

For details about configuring dial rules, see the *Cisco Unified Communications Manager Administration Guide* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

- Softkey Template—*softkey_template*.xml

The filenames are derived from the devicename field in the Cisco Unified Communications Manager database. The devicename uniquely identifies a particular Cisco IP Communicator installation.

Related Topics

- How Cisco IP Communicator Interacts With the Network at Startup, page 1-5

QoS Modifications to Prioritize Voice Traffic

Voice quality can be compromised on an IP device by data traffic. Because Cisco IP Communicator is a software-based phone instead of a hardware phone, you cannot solve this problem by isolating voice-over-IP traffic to an auxiliary VLAN. We recommend that the prioritization of voice traffic is done on the network level rather than on an individual user system. This allows voice data traffic to be prioritized over generic data traffic.

For details about configuring QoS in your network, see:

Cisco Unified Communications SRND based on Cisco Unified Communications Manager

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html

Related Topics

- How Cisco IP Communicator Interacts with Cisco Unified Communications Manager, page 1-4
- Selections for Audio Port Range, page 4-11
- How to Resolve Voice-Quality Issues, page 8-9