CHAPTER 1

An Overview of the Cisco Unified IP Phone

The Cisco Unified IP Phone 7962G and 7942G are full-feature telephones that provide voice communication over an Internet Protocol (IP) network. The Cisco Unified IP Phone functions much like a digital business phone, allowing you to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because the phone is connected to your data network, it offers enhanced IP telephony features, including access to network information and services, and customizeable features and services. The phone also supports security features that include file authentication, device authentication, signaling encryption, and media encryption.

A Cisco Unified IP Phone, like other network devices, must be configured and managed. These phones encode G.711a, G.711µ, G.722, G.729a, G.729ab, iLBC, and decode G.711a, G.711u, G.722, iLBC, G.729, G729a, G729b, and G729ab. These phones also support uncompressed wideband (16bits, 16kHz) audio.

This chapter includes the following topics:

- Understanding the Cisco Unified IP Phone 7962G and 7942G, page 1-2
- What Networking Protocols are Used?, page 1-4
- What Features are Supported on the Cisco Unified IP Phone 7962G and 7942G?, page 1-7
- Understanding Security Features for Cisco Unified IP Phones, page 1-8
- Overview of Configuring and Installing Cisco Unified IP Phones, page 1-17

Caution Using a cell, mobile, or GSM phone, or two-way radio in close proximity to a Cisco Unified IP Phone might cause interference. For more information, refer to the manufacturer's documentation of the interfering device.

Understanding the Cisco Unified IP Phone 7962G and 7942G

Figure 1-1 shows the main components of the Cisco Unified IP Phone 7962G.

Figure 1-2 shows the main components of the Cisco Unified IP Phone 7942G.

Figure 1-1 Cisco Unified IP Phone 7962G

Figure 1-2 Cisco Unified IP Phone 7942G

The following table describes the buttons on the Cisco Unified IP Phone 7962G and 7942G:

1	Programmable buttons 	Depending on configuration, programmable buttons provide access to: • Phone lines (line buttons) • Speed-dial numbers (speed-dial buttons, including the BLF speed-dial feature) • Web-based services (for example, a Personal Address Book (PAB) button) • Phone features (for example, a Privacy button) The buttons illuminate to indicate status:  Green, steady—Active call  Green, flashing—Held call  Amber, steady—Privacy in use  Amber, flashing—Incoming call  Red steady—Remote line in use (shared line, BLF status, or active Mobile Connect call)
2	Phone screen	Shows phone features.
3	Footstand button	Allows you to adjust the angle of the phone base.
4	Messages button 	Auto-dials your voice message service (varies by service).
5	Directories button 	Opens/closes the Directories menu. Use it to access call logs and directories.
6	Help button 	Activates the Help menu.
7	Settings button 	Opens/closes the Settings menu. Use it to control phone screen contrast and ring sounds.
8	Services button 	Opens/closes the Services menu.
9	Volume button 	Controls the handset, headset, and speakerphone volume (off-hook) and the ringer volume (on-hook).
10	Speaker button 	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.
11	Mute button 	Toggles the Mute feature on or off. When Mute is on, the button is lit.
12	Headset button 	Toggles the headset on or off. When the headset is on, the button is lit.
13	Navigation button 	Allows you to scroll through menus and highlight items. When the phone is on-hook, displays phone numbers from your Placed Calls log.

14	Keypad	Allows you to dial phone numbers, enter letters, and choose menu items.
15	Softkey buttons 	Each activates a softkey option (displayed on your phone screen).
16	Handset light strip	Indicates an incoming call or new voice message.

What Networking Protocols are Used?

Cisco Unified IP Phones support several industry-standard and Cisco networking protocols required for voice communication. Table 1-1 provides an overview of the networking protocols that the Cisco Unified IP Phone 7962G and 7942G support.

Table 1-1 Supported Networking Protocols on the Cisco Unified IP Phone

Networking Protocol	Purpose	Usage Notes
Bootstrap Protocol (BootP)	BootP enables a network device such as the Cisco Unified IP Phone to discover certain startup information, such as its IP address.	If you are using BootP to assign IP addresses to the Cisco Unified IP Phone, the BOOTP Server option shows "Yes" in the network configuration settings on the phone.
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and have the phone become operational without your needing to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, refer to *Cisco Unified Communications Manager System Guide*.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for the XML services and for troubleshooting purposes.

Table 1-1 Supported Networking Protocols on the Cisco Unified IP Phone (continued)

Networking Protocol	Purpose	Usage Notes
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.	The Cisco Unified IP Phone implements the IEEE 802.1X standard by providing support for the EAP-MD5 option for 802.1X authentication. When 802.1X authentication is enabled on the phone, you should disable the PC port and voice VLAN. Refer to the "Supporting 802.1X Authentication on Cisco Unified IP Phones" section on page 1-15 for additional information.
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.
Link Layer Discovery Protocol (LLDP)	LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.	The Cisco Unified IP Phone supports LLDP on the PC port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voice products.	The Cisco Unified IP Phone supports LLDP-MED on the SW port to communicate information such as: • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED support, see the *LLDP-MED and Cisco Discovery Protocol* white paper: http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
Cisco Peer to Peer Distribution Protocol (CPPDP)	CPPDP is a Cisco proprietary protocol used to form a peer to peer hierarchy of devices. CPPDP is also used to copy firmware or other files from peer devices to neighboring devices.	CPPDP is used by the Peer Firmware Sharing feature.
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.

Table 1-1 Supported Networking Protocols on the Cisco Unified IP Phone (continued)

Networking Protocol	Purpose	Usage Notes
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with 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 by using Cisco Unified Communications Manager. For more information, see the "Network Configuration Menu" section on page 4-23.
Session Description Protocol (SDP)	SDP is the 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 Media Gateway in operation. Some SIP endpoints may allow these parameters to be configured on the endpoint itself.
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.
Skinny Client Control Protocol (SCCP)	SCCP 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 Unified IP Phones use SCCP for call control. You can configure the Cisco Unified IP Phone to use either SCCP or Session Initiation Protocol (SIP).
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, Cisco Unified IP Phones use the TLS protocol when securely registering with Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco Unified IP Phone, 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 a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign the IP address of the TFTP server by using the Network Configuration menu on the phone.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones transmit and receive RTP streams, which utilize UDP.

Related Topics

- Understanding Interactions with Other Cisco Unified IP Telephony Products, page 2-1
- Understanding the Phone Startup Process, page 2-7

- Network Configuration Menu, page 4-5

What Features are Supported on the Cisco Unified IP Phone 7962G and 7942G?

The Cisco Unified IP Phone functions much like a digital business phone, allowing you to place and receive telephone calls. In addition to traditional telephony features, the Cisco Unified IP Phone includes features that enable you to administer and monitor the phone as a network device.

This section includes the following topics:

- Feature Overview, page 1-7
- Configuring Telephony Features, page 1-8
- Configuring Network Parameters Using the Cisco Unified IP Phone, page 1-8
- Providing Users with Feature Information, page 1-8

Feature Overview

Cisco Unified IP Phones provide traditional telephony functionality, such as call forwarding and transferring, redialing, speed dialing, conference calling, and voice messaging system access. Cisco Unified IP phones also provide a variety of other features. For an overview of the telephony features that the Cisco Unified IP Phone supports and for tips on configuring them, see the "Telephony Features Available for the Cisco Unified IP Phone" section on page 5-1.

As with other network devices, you must configure Cisco Unified IP Phones to prepare them to access Cisco Unified Communications Manager and the rest of the IP network. By using DHCP, you have fewer settings to configure on a phone, but if your network requires it, you can manually configure an IP address, TFTP server, and subnet mask. For instructions on configuring the network settings on the Cisco Unified IP Phones, see Chapter 4, "Configuring Settings on the Cisco Unified IP Phone."

The Cisco Unified IP Phone can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate the Cisco Unified IP Phones with the corporate Lightweight Directory Access Protocol 3 (LDAP3) standard directory to enable users to search for co-worker contact information directly from their IP phones. You can also use XML to enable users to access information such as weather, stocks, quote of the day, and other web-based information. For information about configuring such services, see the "Configuring Corporate Directories" section on page 5-13 and the "Setting Up Services" section on page 5-14.

Finally, because the Cisco Unified IP Phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their IP phones. See Chapter 7, "Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone," for more information.

Related Topics

- Configuring Settings on the Cisco Unified IP Phone, page 4-1
- Configuring Features, Templates, Services, and Users, page 5-1
- Troubleshooting and Maintenance, page 9-1

Configuring Telephony Features

You can modify additional settings for the Cisco Unified IP Phone from Cisco Unified Communications Manager Administration. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks. See the "Telephony Features Available for the Cisco Unified IP Phone" section on page 5-1 and the Cisco Unified Communications Manager documentation for additional information.

For more information about Cisco Unified Communications Manager Administration, refer to Cisco Unified Communications Manager documentation, including *Cisco Unified Communications Manager Administration Guide*. You can also use the context-sensitive help available within the application for guidance.

You can access the complete Cisco Unified Communications Manager documentation suite at this location:

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

Related Topic

- Telephony Features Available for the Cisco Unified IP Phone, page 5-1

Configuring Network Parameters Using the Cisco Unified IP Phone

You can configure parameters such as DHCP, TFTP, and IP settings on the phone itself. You can also obtain statistics about a current call or firmware versions on the phone.

For more information about configuring features and viewing statistics from the phone, see Chapter 4, "Configuring Settings on the Cisco Unified IP Phone" and see Chapter 7, "Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone."

Providing Users with Feature Information

If you are a system administrator, you are likely the primary source of information for Cisco Unified IP Phone users in your network or company. To ensure that you distribute the most current feature and procedural information, familiarize yourself with Cisco Unified IP Phone documentation. Make sure to visit the Cisco Unified IP Phone web site:

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

From this site, you can view various user guides.

In addition to providing documentation, it is important to inform users of available Cisco Unified IP Phone features—including those specific to your company or network—and of how to access and customize those features, if appropriate.

For a summary of some of the key information that phone users need their system administrators to provide, see Appendix A, "Providing Information to Users Via a Website."

Understanding Security Features for Cisco Unified IP Phones

Implementing security in the Cisco Unified Communications Manager system prevents identity theft of the phone and Cisco Unified Communications Manager server, prevents data tampering, and prevents call signaling and media stream tampering.

To alleviate these threats, the Cisco IP telephony network establishes and maintains authenticated and encrypted communication streams between a phone and the server, digitally signs files before they are transferred to a phone, and encrypts media streams and call signaling between Cisco Unified IP phones.

The Cisco Unified IP Phone 7962G and 7942G use the Phone security profile, which defines whether the device is nonsecure, authenticated, or encrypted. For information on applying the security profile to the phone, refer to the *Cisco Unified Communications Manager Security Guide*.

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.*

Table 1-2 shows where you can find additional information about security in this and other documents.

Table 1-2 Cisco Unified IP Phone and Cisco Unified Communications Manager Security Topics

Topic	Reference
Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones	Refer to *Cisco Unified Communications Manager Security Guide*
Security features supported on the Cisco Unified IP Phone	See the "Overview of Supported Security Features" section on page 1-10
Restrictions regarding security features	See the "Security Restrictions" section on page 1-16
Viewing a security profile name	See the "Understanding Security Profiles" section on page 1-12
Identifying phone calls for which security is implemented	See the "Identifying Encrypted and Authenticated Phone Calls" section on page 1-13
TLS connection	• See the "What Networking Protocols are Used?" section on page 1-4 • See the "Adding Phones to the Cisco Unified Communications Manager Database" section on page 2-8
Security and the phone startup process	See the "Understanding the Phone Startup Process" section on page 2-7
Security and phone configuration files	See the "Adding Phones to the Cisco Unified Communications Manager Database" section on page 2-8
Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented	See Table 4-2, in the "Network Configuration Menu" section on page 4-5
Understanding security icons in the Communications Manager 1 through Communications Manager 5 options in the Device Configuration Menu on the phone	See the "CallManager Configuration Menu" section on page 4-10
Items on the Security Configuration menu that you access from the Device Configuration menu on the phone	See the "Security Configuration Menu" section on page 4-21

Table 1-2 Cisco Unified IP Phone and Cisco Unified Communications Manager Security Topics (continued)

Topic	Reference
Items on the Security Configuration menu that you access from the Settings menu on the phone	See the "Security Configuration Menu" section on page 4-26
Unlocking the CTL file	See the "CTL File Screen" section on page 4-27
Disabling access to a phone's web pages	See the "Disabling and Enabling Web Page Access" section on page 8-3
Troubleshooting	• See the "Troubleshooting Cisco Unified IP Phone Security" section on page 9-9 • Refer to the *Cisco Unified Communications Manager Security Guide*
Deleting the CTL file from the phone	See the "Resetting or Restoring the Cisco Unified IP Phone" section on page 9-13
Resetting or restoring the phone	See the "Resetting or Restoring the Cisco Unified IP Phone" section on page 9-13
802.1X Authentication for Cisco Unified IP Phones	See these sections: • "Supporting 802.1X Authentication on Cisco Unified IP Phones" section on page 1-15 • "Security Configuration Menu" section on page 4-21 • "Status Menu" section on page 7-2 • "Troubleshooting Cisco Unified IP Phone Security" section on page 9-9

Overview of Supported Security Features

Table 1-3 provides an overview of the security features that the Cisco Unified IP Phone 7962G and 7942G support. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, refer to *Cisco Unified Communications Manager Security Guide*.

For information about current security settings on a phone, choose **Settings > Security Configuration** and choose **Settings > Device Configuration > Security Configuration**. For more information, see the "Security Configuration Menu" section on page 4-21.

Note Most security features are available only if a certificate trust list (CTL) is installed on the phone. For more information about the CTL, refer to "Configuring the Cisco CTL Client" chapter in *Cisco Unified Communications Manager Security Guide*.

Table 1-3 Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sgn) prevent tampering with the firmware image before it is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer-site certificate installation	Each Cisco Unified IP Phone requires a unique certificate for device authentication. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a Locally Significant Certificate (LSC) from the Security Configuration menu on the phone. See the "Configuring Security on the Cisco Unified IP Phone" section on page 3-14 for more information.
Device authentication	Occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the phone and a Cisco Unified Communications Manager should occur; and, if necessary, creates a secure signaling path between the entities by using TLS protocol. Cisco Unified Communications Manager will not register phones unless they can be authenticated by the Cisco Unified Communications Manager.
File authentication	Validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.
Signaling Authentication	Uses the TLS protocol to validate that no tampering has occurred to signaling packets during transmission.
Manufacturing installed certificate	Each Cisco Unified IP Phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC is a permanent unique proof of identity for the phone, and allows Cisco Unified Communications Manager to authenticate the phone.
Secure SRST reference (SCCP phones only)	After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Media encryption	Uses SRTP to ensure that the media streams between supported devices proves secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.
Signaling encryption	Ensures that all SCCP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and it interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally.

Table 1-3 Overview of Security Features (continued)

Feature	Description
Security profiles	Defines whether the phone is nonsecure, authenticated, or encrypted. See the "Understanding Security Profiles" section on page 1-12 for more information.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional disabling of the web server functionality for a phone	You can prevent access to a phone's web page, which displays a variety of operational statistics for the phone.
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: • Disabling PC port • Disabling Gratuitous ARP (GARP) • Disabling PC Voice VLAN access • Disabling access to the Setting menus, or providing restricted access that allows access to the User Preferences menu and saving volume changes only • Disabling access to web pages for a phone. **Note** You can view current settings for the PC Port Disabled, GARP Enabled, and Voice VLAN enabled options by looking at the phone's Security Configuration menu. For more information, see the "Device Configuration Menu" section on page 4-10.
802.1X Authentication	The Cisco Unified IP Phone can use 802.1X authentication to request and gain access to the network. See the "Supporting 802.1X Authentication on Cisco Unified IP Phones" section on page 1-15 for more information.

Related Topics

- Understanding Security Profiles, page 1-12
- Identifying Encrypted and Authenticated Phone Calls, page 1-13
- Security Restrictions, page 1-16
- Device Configuration Menu, page 4-10

Understanding Security Profiles

All Cisco Unified IP Phones that support Cisco Unified Communications Manager 6.0 use a security profile, which defines whether the phone is nonsecure, authenticated, or encrypted. For information about configuring the security profile and applying the profile to the phone, refer to *Cisco Unified Communications Manager Security Guide*.

To view the security mode that is set for the phone, look at the Security Mode setting in the Security Configuration menu. For more information, see the "Security Configuration Menu" section on page 4-21.

Related Topics

- Identifying Encrypted and Authenticated Phone Calls, page 1-13
- Security Restrictions, page 1-16
- Device Configuration Menu, page 4-10

Identifying Encrypted and Authenticated Phone Calls

When security is implemented for a phone, you can identify authenticated or encrypted phone calls by icons on the screen on the phone.

In an authenticated call, all devices participating in the establishment of the call are authenticated by Cisco Unified Communications Manager. When a call in progress is authenticated, the call progress icon to the right of the call duration timer in the phone LCD screen changes to this icon .

In an encrypted call, all devices participating in the establishment of the call are authenticated by Cisco Unified Communications Manager. In addition, call signaling and media streams are encrypted. An encrypted call offers the highest level of security, providing integrity and privacy to the call. When a call in progress is being encrypted, the call progress icon to the right of the call duration timer in the phone LCD screen changes to the following icon: .

Note If the call is routed through non-IP call legs, for example, PSTN, the call may be nonsecure even though it is encrypted within the IP network and has a lock icon associated with it.

Related Topic

- Understanding Security Profiles, page 1-12
- Understanding Security Features for Cisco Unified IP Phones, page 1-8
- Security Restrictions, page 1-16

Establishing and Identifying Secure Conference Calls

You can initiate a secure conference call and monitor the security level of participants. A secure conference call is established using this process:

1. A user initiates the conference from a secure phone (encrypted or authenticated security mode).
2. Cisco Unified Communications Manager assigns a secure conference bridge to the call.
3. As participants are added, Cisco Unified Communications Manager verifies the security mode of each phone (encrypted or authenticated) and maintains the secure level for the conference.
4. The phone displays the security level of the conference call. A secure conference displays (encrypted) or (authenticated) icon to the right of "Conference" on the phone screen. If icon displays, the conference is not secure.

Note There are interactions, restrictions, and limitations that affect the security level of the conference call depending on the security mode of the participant's phones and the availability of secure conference bridges. See Table 1-4 and Table 1-5 for information about these interactions.

Call Security Interactions and Restrictions

Cisco Unified Communications Manager checks the phone security status when conferences are established and changes the security indication for the conference or blocks the completion of the call to maintain integrity and also security in the system. Table 1-4 provides information about changes to call security levels when using Barge.

Table 1-4 Call Security Interactions When Using Barge

Initiator's Phone Security Level	Feature Used	Call Security Level	Results of Action
Non-secure	Barge	Encrypted call	Call barged and identified as non-secure call
Secure (encrypted)	Barge	Authenticated call	Call barged and identified as authenticated call
Secure (authenticated)	Barge	Encrypted call	Call barged and identified as authenticated call
Non-secure	Barge	Authenticated call	Call barged and identified as non-secure call

Table 1-5 provides information about changes to conference security levels depending on the initiator's phone security level, the security levels of participants, and the availability of secure conference bridges.

Table 1-5 Security Restrictions with Conference Calls

Initiator's Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Non-secure	Conference	Encrypted or authenticated	Non-secure conference bridge Non-secure conference
Secure (encrypted or authenticated)	Conference	At least one member is non-secure	Secure conference bridge Non-secure conference
Secure (encrypted)	Conference	All participants are encrypted	Secure conference bridge Secure encrypted level conference
Secure (authenticated)	Conference	All participants are encrypted or authenticated	Secure conference bridge Secure authenticated level conference
Non-secure	Conference	Encrypted or authenticated	Only secure conference bridge is available and used Non-secure conference
Secure (encrypted or authenticated)	Conference	Encrypted or authenticated	Only non-secure conference bridge is available and used Non-secure conference
Secure (encrypted or authenticated)	Conference	Encrypted or secure	Conference remains secure. When one participant tries to hold the call with MOH, the MOH does not play.
Secure (encrypted)	Join	Encrypted or authenticated	Secure conference bridge Conference remains secure (encrypted or authenticated)

Table 1-5 Security Restrictions with Conference Calls (continued)

Initiator's Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Non-secure	cBarge	All participants are encrypted	Secure conference bridge Conference changes to non-secure
Non-secure	MeetMe	Minimum security level is encrypted	Initiator receives message "Does not meet Security Level", call rejected.
Secure (encrypted)	MeetMe	Minimum security level is authenticated	Secure conference bridge Conference accepts encrypted and authenticated calls
Secure (encrypted)	MeetMe	Minimum security level is non-secure	Only secure conference bridge available and used Conference accepts all calls

Supporting 802.1X Authentication on Cisco Unified IP Phones

These sections provide information about 802.1X support on the Cisco Unified IP Phones:

- Overview, page 1-15
- Required Network Components, page 1-15
- Best Practices—Requirements and Recommendations, page 1-16

Overview

Cisco Unified IP phones and Cisco Catalyst switches have traditionally used Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements. However, CDP is not used to identify any locally attached PCs; therefore, Cisco Unified IP Phones provide an EAPOL pass-through mechanism, whereby a PC locally attached to the IP phone, may pass through EAPOL messages to the 802.1X authenticator in the LAN switch. This prevents the IP phone from having to act as the authenticator, yet allows the LAN switch to authenticate a data end point prior to accessing the network.

In conjunction with the EAPOL pass-through mechanism, Cisco Unified IP Phones provide a proxy EAPOL-Logoff mechanism. In the event that the locally attached PC is disconnected from the IP phone, the LAN switch would not see the physical link fail, because the link between the LAN switch and the IP phone is maintained. To avoid compromising network integrity, the IP phone sends an EAPOL-Logoff message to the switch, on behalf of the downstream PC, which triggers the LAN switch to clear the authentication entry for the downstream PC.

The Cisco Unified IP phones also contain an 802.1X supplicant, in addition to the EAPOL pass-through mechanism. This supplicant allows network administrators to control the connectivity of IP phones to the LAN switch ports. The 802.1X supplicant implements the EAP-MD5 option for 802.1X authentication.

Required Network Components

Support for 802.1X authentication on Cisco Unified IP Phones requires several components, including:

- Cisco Unified IP Phone—The phone acts as the 802.1X *supplicant*, which initiates the request to access the network.

- Cisco Secure Access Control Server (ACS) (or other third-party authentication server)—The authentication server and the phone must both be configured with a shared secret that is used to authenticate the phone.
- Cisco Catalyst Switch (or other third-party switch)—The switch must support 802.1X, so it can act as the *authenticator* and pass the messages between the phone and the authentication server. When the exchange is completed, the switch then grants or denies the phone access to the network.

Best Practices—Requirements and Recommendations

- Enable 802.1X Authentication—If you want to use the 802.1X standard to authenticate Cisco Unified IP Phones, be sure that you have properly configured the other components before enabling it on the phone. See the "802.1X Authentication and Status" section on page 4-29 for more information.
- Configure PC Port—The 802.1X standard does not take into account the use of VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multi-domain authentication. The switch configuration determines whether you can connect a PC to the phone's PC port.
  - Enabled—If you are using a switch that supports multi-domain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco Unified IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, refer to the Cisco Catalyst switch configuration guides at:

    http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
  - Disabled—If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. See the "Security Configuration Menu" section on page 4-21 for more information. If you do not disable this port and subsequently attempt to attach a PC to it, the switch will deny network access to both the phone and the PC.
- Configure Voice VLAN—Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
  - Enabled—If you are using a switch that supports multi-domain authentication, you can continue to use the voice VLAN.
  - Disabled—If the switch does not support multi-domain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN. See the "Security Configuration Menu" section on page 4-21 for more information.
- Enter MD5 Shared Secret—If you disable 802.1X authentication or perform a factory reset on the phone, the previously configured MD5 shared secret is deleted. See the "802.1X Authentication and Status" section on page 4-29 for more information.

Security Restrictions

A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. When barge fails in this case, a reorder tone (fast busy tone) plays on the phone on which the user initiated the barge.

If the initiator phone is configured for encryption, the barge initiator can barge into an authenticated or nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified Communications Manager classifies the call as nonsecure.

If the initiator phone is configured for encryption, the barge initiator can barge into an encrypted call, and the phone indicates that the call is encrypted.

A user can barge into an authenticated call, even if the phone that is used to barge is nonsecure. The authentication icon continues to appear on the authenticated devices in the call, even if the initiator phone does not support security.

Overview of Configuring and Installing Cisco Unified IP Phones

When deploying a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setting up and configuring a complete Cisco IP telephony network, refer to the "System Configuration Overview" chapter in *Cisco Unified Communications Manager System Guide*.

After you have set up the IP telephony system and configured system-wide features in Cisco Unified Communications Manager, you can add IP phones to the system.

The following topics provide an overview of procedures for adding Cisco Unified IP Phones to your network:

- Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager, page 1-17
- Installing Cisco Unified IP Phones, page 1-20

Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager

To add phones to the Cisco Unified Communications Manager database, you can use:

- Auto-registration
- Cisco Unified Communications Manager Administration
- Bulk Administration Tool (BAT)
- BAT and the Tool for Auto-Registered Phones Support (TAPS)

For more information about these choices, see the "Adding Phones to the Cisco Unified Communications Manager Database" section on page 2-8.

For general information about configuring phones in Cisco Unified Communications Manager, refer to the "Cisco Unified IP Phone" chapter in *Cisco Unified Communications Manager System Guide*.

Checklist for Configuring the Cisco Unified IP Phone 7962G and 7942G in Cisco Unified Communications Manager

Table 1-6 provides an overview and checklist of configuration tasks for the Cisco Unified IP Phone 7962G and 7942G in Cisco Unified Communications Manager Administration. The list presents a suggested order to guide you through the phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table 1-6 Checklist for Configuring the Cisco Unified IP Phone 7962G and 7942G in Cisco Unified Communications Manager

Configuration Step and Purpose		For More Information
Step 1	Gather the following information about the phone: • Phone Model • MAC address • Physical location of the phone • Name or user ID of phone user • Device pool • Partition, calling search space, and location information • Number of lines and associated directory numbers (DNs) to assign to the phone • Cisco Unified Communications Manager user to associate with the phone • Phone usage information that affects phone button template, softkey template, phone features, IP Phone services, or phone applications Provides list of configuration requirements for setting up phones. Identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates or softkey templates.	Refer to *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter. See the "Telephony Features Available for the Cisco Unified IP Phone" section on page 5-1.
Step 2	Customize phone button templates (if required). Changes the number of line buttons, speed-dial buttons, Service URL buttons or adds a Privacy button to meet user needs.	Refer to *Cisco Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter. See the "Modifying Phone Button Templates" section on page 5-13.
Step 3	Add and configure the phone by completing the required fields in the Phone Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, MAC address and device pool. Adds the device with its default settings to the Cisco Unified Communications Manager database.	Refer to *Cisco Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter. For information about Product Specific Configuration fields, refer to "?" Button Help in the Phone Configuration window.
Step 4	Add and configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, directory number and presence group. Adds primary and secondary directory numbers and features associated with directory numbers to the phone.	Refer to the *Cisco Unified Communications Manager Administration Guide*, Directory Number Configuration chapter, "Creating a Cisco Unity Voice Mailbox" section See the "Telephony Features Available for the Cisco Unified IP Phone" section on page 5-1.

Table 1-6 Checklist for Configuring the Cisco Unified IP Phone 7962G and 7942G in Cisco Unified Communications Manager (continued)

Configuration Step and Purpose		For More Information
Step 5	Customize softkey templates. Adds, deletes, or changes order of softkey features that display on the user's phone to meet feature usage needs.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Softkey Template Configuration" chapter. See the "Configuring Softkey Templates" section on page 5-14.
Step 6	Configure speed-dial buttons and assign speed-dial numbers (optional). Adds speed-dial buttons and numbers. Users can change speed-dial settings on their phones by using Cisco Unified CM User Options.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter, "Configuring Speed-Dial Buttons" section.
Step 7	Configure Cisco Unified IP Phone services and assign services (optional). Provides IP Phone services. Users can add or change services on their phones by using the Cisco Unified CM User Options.	Refer to *Cisco Communications Manager Administration Guide*, "Cisco Unified IP Phone Services Configuration" chapter. See the "Setting Up Services" section on page 5-14.
Step 8	Assign services to phone buttons (optional). Provides single button access to an IP phone service or URL.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter, "Adding a Cisco Unified IP Phone Service to a Phone Button" section.
Step 9	Add user information by configuring required fields. Required fields are indicated by an asterisk (*); for example, User ID and last name. **Note** Assign a password (for User Options web pages) and PIN (for Extension Mobility and Personal Directory) Adds user information to the global directory for Cisco Unified Communications Manager.	Refer to *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" chapter. See the "Adding Users to Cisco Unified Communications Manager" section on page 5-15
Step 10	Associate a user to a user group. Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manager user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users.	Refer to *Cisco Unified Communications Manager Administration Guide*: • "End User Configuration" chapter, "End User Configuration Settings" section • "User Group Configuration" chapter, "Adding Users to a User Group" section.
Step 11	Associate a user with a phone (optional). Provides users with control over their phone such a forwarding calls or adding speed-dial numbers or services. **Note** Some phones, such as those in conference rooms, do not have an associated user.	Refer to *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" chapter, "Associating Devices to a User" section.

Installing Cisco Unified IP Phones

After you have added the phones to the Cisco Unified Communications Manager database, you can complete the phone installation. You (or the phone users) can install the phone at the users's location. The Cisco Unified IP Phone Installation Guide, which is provided on the cisco.com web site, provides directions for connecting the phone handset, cables, and other accessories.

Note Before you install a phone, even if it is new, upgrade the phone to the current firmware image. For information about upgrading, refer to the Readme file for your phone, which is located at:

http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser

After the phone is connected to the network, the phone startup process begins, and the phone registers with Cisco Unified Communications Manager. To finish installing the phone, configure the network settings on the phone depending on whether you enable or disable DHCP service.

If you used auto-registration, you need to update the specific configuration information for the phone such as associating the phone with a user, changing the button table, or directory number.

Checklist for Installing the Cisco Unified IP Phone 7962G and 7942G

Table 1-7 provides an overview and checklist of installation tasks for the Cisco Unified IP Phone 7962G and 7942G. The list presents a suggested order to guide you through the phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table 1-7 Checklist for Installing the Cisco Unified IP Phone 7962G and 7942G

Configuration Step and Purpose		For More Information
Step 1	Choose the power source for the phone: • Power over Ethernet (PoE) • External power supply Determines how the phone receives power.	See the "Providing Power to the Cisco Unified IP Phone" section on page 2-3.
Step 2	Assemble the phone, adjust phone placement, and connect the network cable. Locates and installs the phone in the network.	See the "Installing the Cisco Unified IP Phone" section on page 3-6. See the "Adjusting the Placement of the Cisco Unified IP Phone" section on page 3-10.
Step 3	Add a Cisco Unified IP Phone Expansion Module 7914 to the Cisco Unified IP Phone 7962G (optional). Adds the device with its default settings to the Cisco Unified Communications Manager database. Extends functionality of a Cisco Unified IP Phone 7962G by adding 14 line appearances or speed dial numbers.	See the "Attaching the Cisco Unified IP Phone Expansion Module 7914 (SCCP Phones Only)" section on page 3-9.

Table 1-7 Checklist for Installing the Cisco Unified IP Phone 7962G and 7942G (continued)

Configuration Step and Purpose		For More Information
Step 4	Monitor the phone startup process. Adds primary and secondary directory numbers and features associated with directory numbers to the phone. Verifies that phone is configured properly.	See the "Verifying the Phone Startup Process" section on page 3-12.
Step 5	Configure these network settings on the phone by choosing **Settings > Network Configuration**. To enable DHCP: • Set DHCP Enabled to **Yes** • To use an alternate TFTP server, set Alternate TFTP Server to **Yes** Enter **IP address** for TFTP Server 1 To disable DHCP: • Set DHCP Enabled to **No** • Enter static **IP address** for phone • Enter subnet mask • Enter default router IP addresses • Enter domain name where phone resides Set Alternate TFTP Server to **Yes** Enter **IP address** for TFTP Server 1. Using DHCP—The IP address is automatically assigned, and the Cisco Unified IP Phone is directed to a TFTP Server. **Note** Consult with the network administrator if you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP. Without DHCP—You must configure the IP address, TFTP server, subnet mask, domain name, and default router locally on the phone.	See the "Configuring Startup Network Settings" section on page 3-13. See the "Network Configuration Menu" section on page 4-5.
Step 6	Set up security on the phone. Provides protection against data tampering threats and identity theft of phones.	See the "Configuring Security on the Cisco Unified IP Phone" section on page 3-14.
Step 7	Make calls with the Cisco Unified IP Phone. Verifies that the phone and features work correctly.	Refer to *Cisco Unified IP Phone 7962G and 7942G Guide for Cisco Unified Communications Manager 6.0 (SCCP and SIP)*
Step 8	Provide information to end users about how to use their phones and how to configure their phone options. Ensures that users have adequate information to successfully use their Cisco Unified IP Phones.	See Appendix A, "Providing Information to Users Via a Website."