



CHAPTER 2

Preparing to Install the Cisco Unified IP Phone on Your Network

Cisco Unified IP Phones enable you to communicate using voice over a data network. To provide this capability, the phones depend upon and interact with several other key Cisco IP Telephony and network components, including Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, media resources, Cisco prestandard PoE, and so on.

This chapter focuses on the interactions between the Cisco Unified IP Phone 7931G and Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, and switches. It also describes options for powering phones.

For related information about voice and IP communications, refer to this URL (you must be a registered Cisco.com user):

<http://www.cisco.com/en/US/partner/products/sw/voicesw/index.html>

This chapter includes these topics:

- [Understanding Interactions with Other Cisco Unified IP Communications Products, page 2-2](#)
- [Providing Power to the Phone, page 2-4](#)
- [Understanding Phone Configuration Files, page 2-6](#)
- [Understanding the Phone Startup Process, page 2-8](#)
- [Adding Phones to the Cisco Unified Communications Manager Database, page 2-11](#)
- [Determining the MAC Address of a Cisco Unified IP Phone, page 2-15](#)

Understanding Interactions with Other Cisco Unified IP Communications Products

To function in the IP telephony network, the Cisco Unified IP Phone must be connected to a networking device, such as a Cisco Catalyst switch. You must also register the Cisco Unified IP Phone with a Cisco Unified Communications Manager system before sending and receiving calls.

This section includes these topics:

- [Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager, page 2-2](#)
- [Understanding How the Cisco Unified IP Phone Interacts with the VLAN, page 2-3](#)

Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager

Cisco Unified Communications Manager is an open and industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between phones, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the IP telephony system—the phones, the access gateways, and the resources necessary for features such as call conferencing and route planning. Cisco Unified Communications Manager also provides:

- Firmware for phones
- Authentication and encryption (if configured for the telephony system)
- Configuration file and CTL file, via TFTP service
- Phone registration
- Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

For information about configuring Cisco Unified Communications Manager to work with the IP devices that described in this chapter, refer to *Cisco Unified Communications Manager Administration Guide*, *Cisco Unified Communications Manager System Guide*, and to *Cisco Unified Communications Manager Security Guide*.

For an overview of security functionality for the Cisco Unified IP Phone, see the “Understanding Security Features for Cisco Unified IP Phones” section on page 1-14.

**Note**

If the Cisco Unified IP Phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified Communications Manager Administration, go to the following URL and install the latest support patch for your version of Cisco Unified Communications Manager:
<http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>

Related Topic

- [Telephony Features Available for the Phone, page 5-2](#)

Understanding How the Cisco Unified IP Phone Interacts with the VLAN

The Cisco Unified IP Phone 7931G has an internal Ethernet switch, enabling forwarding of packets to the phone, and to the access port and the network port on the back of the phone.

If a computer is connected to the access port, the computer and the phone share the same physical link to the switch and share the same port on the switch. This shared physical link has the following implications for the VLAN configuration on the network:

- The current VLANs might be configured on an IP subnet basis. However, additional IP address might not be available to assign the phone to the same subnet as other devices connect to the same port.
- Data traffic present on the data/native VLAN may reduce the quality of Voice-over-IP traffic.
- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN. The switch port that the phone is connected to would be configured to have separate VLANs for carrying:

- Voice traffic to and from the IP phone (auxiliary VLAN, on the Cisco Catalyst 6000 series, for example)
- Data traffic to and from the PC connected to the switch through the access port of the IP phone (native VLAN)

Isolating the phones on a separate, auxiliary VLAN improves the quality of the voice traffic and allows a large number of phones to be added to an existing network where there are not enough IP addresses for each phone.

For more information, refer to the documentation included with a Cisco switch. You can also access related documentation at this URL:

http://www.cisco.com/en/US/products/hw/switches/tsd_products_support_category_home.html

Related Topics

- [Understanding the Phone Startup Process, page 2-8](#)
- [Network Configuration Menu, page 4-7](#)

Providing Power to the Phone

The Cisco Unified IP Phones 7931G can be powered with external power or with Power over Ethernet (PoE). External power is provided through a separate power supply. PoE is provided by a switch through the Ethernet cable attached to a phone.

- [Power Outage, page 2-5](#)
- [Power Guidelines, page 2-5](#)
- [Obtaining Additional Information about Power, page 2-6](#)

Power Outage

Your accessibility to emergency service through the phone is dependent on the phone being powered. If there is an interruption in the power supply, Service and Emergency Calling Service dialing will not function until power is restored. In the case of a power failure or disruption, you may need to reset or reconfigure equipment before using the Service or Emergency Calling Service dialing.

Power Guidelines

[Table 2-1](#) provides guidelines that apply to external power and to PoE power for the Cisco Unified IP Phones 7931G.

Table 2-1 Guidelines for Powering the Cisco Unified IP Phones 7931G

Power Type	Guidelines
External power— Provided through a Cisco external power supply.	The CP-PWR-CUBE-3 external power supply may be used with the Cisco Unified IP Phones 7931G.
External power— Provided through the Cisco Unified IP Phone Power Injector.	The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector is connected between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the phone.
PoE power—Provided by a switch through the Ethernet cable attached to the phone.	<ul style="list-style-type: none"> The Cisco Unified IP Phones 7931G supports IEEE 802.3af Power over Ethernet. To ensure uninterrupted operation of the phone, make sure that the switch has a backup power supply. Make sure that the CatOS or IOS version running on your switch supports your intended phone deployment. Refer to the documentation for your switch for operating system version information.

Obtaining Additional Information about Power

For related information about power, refer to the documents shown in [Table 2-2](#). These documents provide information about these topics:

- Cisco switches that work with the Cisco Unified IP Phones
- The Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions regarding power

Table 2-2 *Related Documentation for Power*

Document Topics	URL
Cisco Unified IP Phone Power Injector	http://www.cisco.com/en/US/products/hw/phones/ps379/prod_installation_guides_list.html
PoE Solutions	http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns412/networking_solutions_package.html
Cisco Catalyst Switches	http://www.cisco.com/en/US/products/hw/switches/tsd_products_support_category_home.html
Integrated Service Routers	http://www.cisco.com/en/US/products/hw/routers/index.html
Cisco IOS Software	http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html

Understanding Phone Configuration Files

Configuration files for a phone 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 the phone to be reset, a change is made automatically to the phone configuration file.

Configuration files also contain information about which image load the phone should be running. If this image load differs from the one currently that is loaded on a phone currently, the phone contacts the TFTP server to request the required load files. (These files are digitally signed to ensure the authenticity of the file source.)

In addition, if the device security mode in the configuration file is set to Authenticated and the CTL file on the phone has a valid certificate for Cisco Unified Communications Manager, the phone establishes a TLS connection to Cisco Unified Communications Manager. Otherwise, the phone establishes a TCP connection.

**Note**

If the device security mode in the configuration file is set to Authenticated or Encrypted, but the phone has not received a CTL file, the phone will continuously try 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*.

A phone accesses a default configuration file named `XmlDefault.cnf.xml` from the TFTP server when these conditions exist:

- You have enabled auto-registration in Cisco Unified Communications Manager
- The phone has not been added to the Cisco Unified Communications Manager database
- The phone is registering for the first time

If auto registration is not enabled and the phone has not been added to the Cisco Unified Communications Manager Database, the phone registration request will be rejected. In this case, the phone resets and attempts to register repeatedly.

If the phone has registered before, the phone accesses the configuration file named `SEPmac_address.cnf.xml`, where `mac_address` is the MAC address of the phone.

For more information about how the phone interacts with the TFTP server, refer to the *Cisco Unified Communications Manager System Guide*, “Cisco TFTP” chapter.

Understanding the Phone Startup Process

When connecting to the VoIP network, the Cisco Unified IP Phone goes through a standard startup process, as described in [Table 2-3](#). Depending on your network configuration, not all of these process steps may occur on your Cisco Unified IP Phone.

Table 2-3 Cisco Unified IP Phone Startup Process

Process Step and Purpose	Related Topics
<p>Step 1 Obtaining Power from the Switch</p> <p>If a phone is not using external power, the switch provides in-line power through the Ethernet cable attached to the phone.</p>	<p>See the “Providing Power to the Phone” section on page 2-4.</p> <p>See the “Resolving Startup Problems” section on page 9-2.</p>
<p>Step 2 Loading the Stored Phone Image</p> <p>The Cisco Unified IP Phone has non-volatile Flash memory in which it stores firmware images and user-defined preferences. At startup, the phone runs a bootstrap loader that loads a phone image stored in Flash memory. Using this image, the phone initializes its software and hardware.</p>	<p>See the “Resolving Startup Problems” section on page 9-2.</p>
<p>Step 3 Configuring VLAN</p> <p>If the Cisco Unified IP Phone is connected to a Cisco switch, the switch next informs the phone of the voice VLAN defined on the switch port. The phone needs to know its VLAN membership before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address.</p>	<p>See the “Network Configuration Menu” section on page 4-7.</p> <p>See the “Resolving Startup Problems” section on page 9-2.</p>

Table 2-3 Cisco Unified IP Phone Startup Process (continued)

Process Step and Purpose	Related Topics
<p>Step 4 Obtaining an IP Address</p> <p>If the Cisco Unified IP Phone is using DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each phone locally.</p>	<p>See the “Network Configuration Menu” section on page 4-7.</p> <p>See the “Resolving Startup Problems” section on page 9-2.</p>
<p>Step 5 Accessing a TFTP Server</p> <p>In addition to assigning an IP address, the DHCP server directs the Cisco Unified IP Phone to a TFTP Server. If the phone has a statically defined IP address, you must configure the TFTP server locally on the phone; the phone then contacts the TFTP server directly.</p> <p>Note You can also assign an alternative TFTP server to use instead of the one assigned by DHCP.</p>	<p>See the “Network Configuration Menu” section on page 4-7.</p> <p>See the “Resolving Startup Problems” section on page 9-2.</p>
<p>Step 6 Requesting the CTL file</p> <p>The TFTP server stores the certificate trust list (CTL) file. This file contains a list of Cisco Unified Communications Managers and TFTP servers that the phone is authorized to connect to. It also contains the certificates necessary for establishing a secure connection between the phone and Cisco Unified Communications Manager.</p>	<p>Refer to the <i>Cisco Unified Communications Manager Security Guide</i>, “Configuring the Cisco CTL Client” chapter.</p>

Table 2-3 Cisco Unified IP Phone Startup Process (continued)

Process Step and Purpose	Related Topics
<p>Step 7 Requesting the Configuration File</p> <p>The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the phone.</p>	<p>See the “Understanding Phone Configuration Files” section on page 2-6.</p> <p>See the “Resolving Startup Problems” section on page 9-2.</p>
<p>Step 8 The configuration file defines how the Cisco Unified IP Phone communicates with Cisco Unified Communications Manager and provides a phone with its load ID. After obtaining the file from the TFTP server, the phone attempts to make a connection to the highest priority Cisco Unified Communications Manager on the list. If security is implemented, the phone makes a TLS connection. Otherwise, it makes a non-secure TCP connection.</p> <p>If the phone was manually added to the database, Cisco Unified Communications Manager identifies the phone. If the phone was not manually added to the database and auto-registration is enabled in Cisco Unified Communications Manager, the phone attempts to auto-register itself in the Cisco Unified Communications Manager database.</p> <p>Note Auto-registration is disabled when security is enabled on Cisco Unified Communications Manager. In this case, the phone must be manually added to the Cisco Unified Communications Manager database.</p>	<p>See the “Resolving Startup Problems” section on page 9-2.</p>

Adding Phones to the Cisco Unified Communications Manager Database

Before installing the Cisco Unified IP Phone, you must choose a method for adding phones to the Cisco Unified Communications Manager database. These sections describe the methods:

- [Adding Phones with Auto-Registration, page 2-12](#)
- [Adding Phones with Auto-Registration and TAPS, page 2-13](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 2-14](#)
- [Adding Phones with BAT, page 2-14](#)

[Table 2-4](#) provides an overview of these methods for adding phones to the Cisco Unified Communications Manager database.

Table 2-4 *Methods for Adding Phones to the Cisco Unified Communications Manager Database*

Method	Requires MAC Address?	Notes
Auto-registration	No	Results in automatic assignment of directory numbers. Not available when security or encryption is enabled.
Auto-registration with TAPS	No	Requires auto-registration and the Bulk Administration Tool (BAT); updates the Cisco Unified Communications Manager database with the MAC address and DN for the device when user calls TAPS from the phone.
Using Cisco Unified Communications Manager Administration	Yes	Requires phones to be added individually.
Using BAT	Yes	Can add groups of same model of phone. Can schedule when phones are added to the Cisco Unified Communications Manager database.

Adding Phones with Auto-Registration

By enabling auto-registration before you begin installing phones, you can:

- Add phones without first gathering MAC addresses from the phones.
- Automatically add a Cisco Unified IP Phone to the Cisco Unified Communications Manager database when you physically connect the phone to your IP telephony network. During auto-registration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone.
- Quickly enter phones into the Cisco Unified Communications Manager database and modify any settings, such as the directory numbers, from Cisco Unified Communications Manager.
- Move auto-registered phones to new locations and assign them to different device pools without affecting their directory numbers.



Note

Cisco recommends that you use auto-registration to add fewer than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). See the [“Adding Phones with BAT”](#) section on page 2-14.

Auto-registration is disabled by default. In some cases, you might not want to use auto-registration: for example, if you want to assign a specific directory number to the phone, or if you plan to implement authentication or encryption, as described in *Cisco Unified Communications Manager Security Guide*. For information about enabling auto-registration, refer to “Enabling Auto-Registration” in *Cisco Unified Communications Manager Administration Guide*.



Note

When you configure the cluster for mixed mode through the Cisco CTL client, auto-registration is automatically disabled. When you configure the cluster for non-secure mode through the Cisco CTL client, auto-registration is automatically enabled.

Related Topics

- [Adding Phones with Auto-Registration and TAPS, page 2-13](#)

- [Adding Phones with Cisco Unified Communications Manager Administration, page 2-14](#)
- [Adding Phones with BAT, page 2-14](#)

Adding Phones with Auto-Registration and TAPS

You can add phones with auto-registration and TAPS, the Tool for Auto-Registered Phones Support, without first gathering MAC addresses from phones.

TAPS works with the Bulk Administration Tool (BAT) to update a batch of phones that were already added to the Cisco Unified Communications Manager database with dummy MAC addresses. Use TAPS to update MAC addresses and download pre-defined configurations for phones.



Note

Cisco recommends that you use auto-registration and TAPS to add fewer than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). See the [“Adding Phones with BAT” section on page 2-14](#).

To implement TAPS, you or the end-user dial a TAPS directory number and follow voice prompts. When the process is complete, the phone will have downloaded its directory number and other settings, and the phone will be updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Auto-registration must be enabled in Cisco Unified Communications Manager Administration (**System > Cisco Communications Manager**) for TAPS to function.



Note

When you configure the cluster for mixed mode through the Cisco CTL client, auto-registration is automatically disabled. When you configure the cluster for non-secure mode through the Cisco CTL client, auto-registration is automatically enabled.

Refer to *Cisco Unified Communications Manager Bulk Administration Guide* for detailed instructions about BAT and about TAPS.

Related Topics

- [Adding Phones with Auto-Registration, page 2-12](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 2-14](#)
- [Adding Phones with BAT, page 2-14](#)

Adding Phones with Cisco Unified Communications Manager Administration

You can add phones individually to the Cisco Unified Communications Manager database using Cisco Unified Communications Manager Administration. To do so, you first need to obtain the MAC address for each phone.

For information about determining a MAC address, see the “[Determining the MAC Address of a Cisco Unified IP Phone](#)” section on page 2-15.

After you have collected MAC addresses, in Cisco Unified Communications Manager Administration, choose **Device > Phone** and click **Add New** to begin.

For complete instructions and conceptual information about Cisco Unified Communications Manager, refer to *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide*.

Related Topics

- [Adding Phones with Auto-Registration, page 2-12](#)
- [Adding Phones with Auto-Registration and TAPS, page 2-13](#)
- [Adding Phones with BAT, page 2-14](#)

Adding Phones with BAT

Cisco Unified Communications Manager Bulk Administration Tool (BAT), a standard Cisco Unified Communications Manager application, enables you to perform batch operations, which includes registration, on multiple phones.

Before you can add phones using BAT only (not in conjunction with TAPS), you must obtain the MAC address for each phone.

For information about determining a MAC address, see the “[Determining the MAC Address of a Cisco Unified IP Phone](#)” section on page 2-15.

For detailed instructions about using BAT, refer to *Cisco Unified Communications Manager Bulk Administration Guide*.

Related Topics

- [Adding Phones with Auto-Registration](#), page 2-12
- [Adding Phones with Auto-Registration and TAPS](#), page 2-13
- [Adding Phones with Cisco Unified Communications Manager Administration](#), page 2-14

Determining the MAC Address of a Cisco Unified IP Phone

Several of the procedures that are described in this manual require you to determine the MAC address of a Cisco Unified IP Phone. You can determine the MAC address for a phone in any of these ways:

- If the phone is registered with Cisco Unified Communications Manager, press the Application Menu button, then choose **Settings > Model Information** and look at the MAC Address field.

By default, the Application Menu button is line button 24 (the top left line button).

- If the phone is not registered with Cisco Unified Communications Manager, press the **Settings** softkey, then choose **Model Information** and look at the MAC Address field.

This softkey appears only when the phone is not registered.

- Look at the MAC label on the back of the phone.
- Display the web page for the phone and click the **Device Information** hyperlink.

For information about accessing the web page, see the “[Accessing the Web Page for a Phone](#)” section on page 8-2.

