CHAPTER 2

Preparing to Install the ATA 187 on Your Network

The ATA 187 enables you to communicate using voice over a data network. To provide this capability, the ATA 187 depends upon and interacts with several other key Cisco Unified IP Telephony and network components, including Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, media resources, and so on.

This chapter focuses on the interactions between the ATA 187, Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, and switches. It also describes options for powering the ATA 187.

For related information about voice and IP communications, see this URL:

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

This chapter provides an overview of the interaction between the ATA 187 and other key components of the Voice over IP (VoIP) network. It includes these topics:

- Understanding Interactions with Other Cisco Unified IP Communications Products, page 2-1
- Providing Power to the ATA 187, page 2-2
- Understanding Phone Configuration Files, page 2-3
- Understanding the ATA 187 Startup Process, page 2-4
- Adding the ATA 187 to the Cisco Unified Communications Manager Database, page 2-5
- Determining the MAC Address of an ATA 187, page 2-7

Understanding Interactions with Other Cisco Unified IP Communications Products

To function in the IP telephony network, the ATA 187 must be connected to a networking device, such as a Cisco Catalyst switch. You must also register the ATA 187 with a Cisco Unified Communications Manager system before sending and receiving calls.

This section includes information on Understanding How the ATA 187 Interacts with Cisco Unified Communications Manager, page 2-2.

Understanding How the ATA 187 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 connected to the ATA 187, 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 devices
- Authentication and encryption (if configured for the telephony system)
- Configuration and CTL files via the 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 described in this chapter, see *Cisco Unified Communications Manager Administration Guide*, *Cisco Unified Communications Manager System Guide*, and *Cisco Unified Communications Manager Security Guide*.

Providing Power to the ATA 187

The ATA 187 is powered with external power. External power is provided through a separate power supply.

The following sections provide more information about powering a ATA 187:

- Power Guidelines, page 2-2
- Power Outage, page 2-2
- Understanding Phone Configuration Files, page 2-3

Power Guidelines

The following power type and guideline applies to external power for the ATA 187:

- Power Type—External power (Provided through the Universal AC external power supply)
- Guidelines—The ATA 187 uses the Universal AC power supply 110/240V

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.

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 automatically made to the phone's configuration file. If the system needs to reset or restart, both ports must reset or restart at the same time.

Configuration files also contain information about which image load the phone should be running. If this image load differs from the one that is currently loaded on a phone, 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. For SIP phones, a TLS connection requires that the transport protocol in the phone configuration file be set to TLS, which corresponds to the transport type in the SIP Security Profile in Cisco Unified Communications Manager.

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 tries four times to obtain it so it can register securely.

Note Cisco Extension Mobility Cross Cluster is an exception, in that the phone permits a TLS connection to Cisco Unified Communications Manager for secure signaling even without the CTL file.

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, see Configuring Encrypted Phone Configuration Files in *Cisco Unified Communications Manager Security Guide*.

A phone accesses a default configuration file named XmlDefault.cnf.xml only when the phone has not received a valid Trust List file containing a certificate assigned to the Cisco Unified Communications Manager and TFTP.

If auto registration is not enabled and you did not add the phone to the Cisco Unified Communications Manager database, the phone does not attempt to register with Cisco Unified Communications Manager. The phone continually displays the "Configuring IP" message until you either enable auto-registration or add the phone to the Cisco Unified Communications Manager database.

If the phone has registered before, the phone accesses the configuration file named ATA<*mac_address*>.cnf.xml, where *mac_address* is the MAC address of the phone.

For SIP phones, the TFTP server generates these SIP configuration files:

- SIP IP Phone:
  - For unsigned and unencrypted files—ATA<*mac*>.cnf.xml
  - For signed files—ATA<*mac*>.cnf.xml.sgn
  - For signed and encrypted files—ATA<*mac*>.cnf.xml.enc.sgn
- Dial Plan—<*dialplan*>.xml
  - No support "**,**" for second dial tone; "**,**" will be ignored

- No support > for configuring termination key
- No support + dial pattern which contains + will be ignored
- Maximum length of match string is **196**
- Maximum length of a dial pattern is **4095**
- Maximum rule set in one dial pattern is **100**

The filenames are derived from the MAC Address and Description fields in the Phone Configuration window of Cisco Unified Communications Manager Administration. The MAC address uniquely identifies the phone. For more information see the *Cisco Unified Communications Manager Administration Guide*.

For more information about how the phone interacts with the TFTP server, see the *Cisco Unified Communications Manager System Guide*, Cisco TFTP section.

Understanding the ATA 187 Startup Process

When connecting to the VoIP network, the ATA 187 goes through a standard startup process, as described in Table 2-1. Depending on your specific network configuration, not all of these process steps may occur on your ATA 187.

Table 2-1 ATA 187 Startup Process

Task	Purpose	Related Topics
1.	Obtaining Power. The ATA 187 uses external power.	See Providing Power to the ATA 187, page 2-2.
2.	Loading the Stored Image. The ATA 187 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.	
3.	Obtaining an IP Address. If the ATA 187 is using DHCP to obtain an IP address, the device queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each device locally.	
4.	Requesting the CTL file. The TFTP server stores the CTL file. This file contains the certificates necessary for establishing a secure connection between the device and Cisco Unified Communications Manager.	See the *Cisco Unified Communications Manager Security Guide,* Configuring the Cisco CTL Client.

Table 2-1 ATA 187 Startup Process (continued)

Task	Purpose	Related Topics
5.	Requesting the Configuration File. The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the ATA 187.	See Understanding Phone Configuration Files, page 2-3.
6.	Contacting Cisco Unified Communications Manager. The configuration file defines how the ATA 187 communicates with Cisco Unified Communications Manager and provides a device with its load ID. After obtaining the file from the TFTP server, the device attempts to make a connection to the highest priority Cisco Unified Communications Manager on the list. If the security profile of the device is configured for secure signaling (encrypted or authenticated), and the Cisco Unified Communications Manager is set to secure mode, the device makes a TLS connection. Otherwise, it makes a nonsecure TCP connection.	See Understanding Phone Configuration Files, page 2-3.

Adding the ATA 187 to the Cisco Unified Communications Manager Database

Before installing the ATA 187, you must choose a method for adding the devices to the Cisco Unified Communications Manager database. These sections describe the methods:

- Adding the ATA 187 with Auto-Registration, page 2-6
- Adding the ATA 187 with Cisco Unified Communications Manager Administration, page 2-6

Table 2-2 provides an overview of these methods for adding the ATA 187 to the Cisco Unified Communications Manager database.

Table 2-2 Methods for Adding the ATA 187 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.
Using the Cisco Unified Communications Manager Administration	Yes	Requires phones to be added individually.

Adding the ATA 187 with Auto-Registration

By enabling auto-registration before you begin installing the ATA 187, you can:

- Add devices without first gathering MAC addresses from the ATA 187.
- Automatically add a ATA 187 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 devices into the Cisco Unified Communications Manager database and modify any settings, such as the directory numbers, from Cisco Unified Communications Manager.
- Move auto-registered devices to new locations and assign them to different device pools without affecting their directory numbers.

Note The ATA 187 will auto-register two devices in the Unified CM.

Auto-registration is disabled by default. In some cases, you may 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 use secure connection with Cisco Unified Communications Manager as described in *Cisco Unified Communications Manager Security Guide*. For information about enabling auto-registration, see the Enabling Auto-Registration in the *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 nonsecure mode through the Cisco CTL client, auto-registration is not automatically enabled.

Related Topics

Adding the ATA 187 with Cisco Unified Communications Manager Administration, page 2-6

Adding the ATA 187 with Cisco Unified Communications Manager Administration

You can add the ATA 187 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 device.

For information about determining a MAC address, see Determining the MAC Address of an ATA 187, page 2-7.

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

Note The first device used the MAC address and the second device uses the shifted MAC address (example, AABBCCDDEEFF to BBCCDDEEFF01). You can add two devices from the Unified CM administration page.

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

Related Topics

Adding the ATA 187 with Auto-Registration, page 2-6

Determining the MAC Address of an ATA 187

Several of the procedures that are described in this manual require you to determine the MAC address of an ATA 187. You can determine the MAC address for a device in any of these ways:

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